H3C MSR 系列路由器

三层技术-IP 业务配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

Copyright © 2013-2014 杭州华三通信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。

H3C、  、H3CS、H3CIE、H3CNE、Aolynk、  、H^{3}Care、  、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于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。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《三层技术-IP 业务配置指导》主要介绍了基本的三层 IPv4 及 IPv6 技术的原理及配置。包括 IP 地址的配置、ARP、域名解析、DHCP、NAT、隧道配置等。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

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
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*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 | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、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. 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。

3. 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。

4. 端口编号示例约定

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。

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

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

感谢您的反馈，让我们做得更好！

目 录

1 ARP

1.1 ARP简介

1.1.1 ARP作用

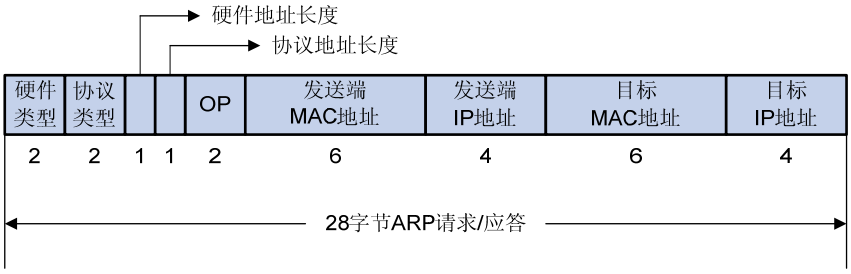
ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

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）。但是仅仅有 IP 地址是不够的，因为 IP 数据报必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

1.1.2 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。

1.1.3 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：

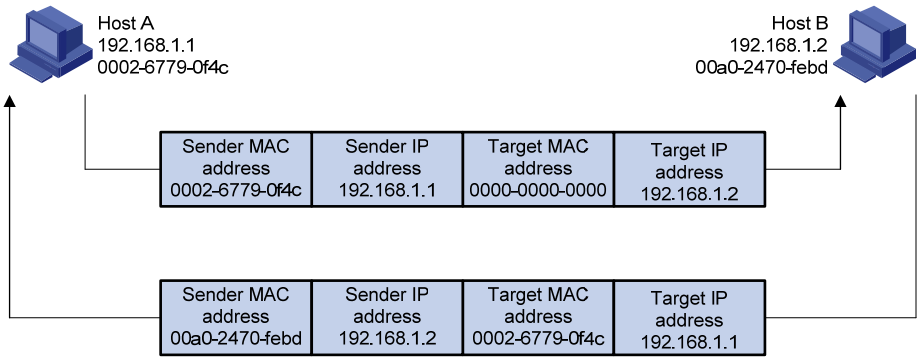
(1) 主机 A 首先查看自己的 ARP 表，确定其中是否包含有主机 B 对应的 ARP 表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 表中的 MAC 地址，对 IP 数据报进行帧封装，并将 IP 数据报发送给主机 B。

(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。

1.1.4 ARP表

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 表项和静态 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 表项和长静态 ARP 表项。

- 在配置长静态 ARP 表项时，除了配置 IP 地址和 MAC 地址项外，还必须配置该 ARP 表项所在 VLAN 和出接口。长静态 ARP 表项可以直接用于报文转发。
- 在配置短静态 ARP 表项时，只需要配置 IP 地址和 MAC 地址项。如果出接口是三层以太网接口，短静态 ARP 表项可以直接用于报文转发；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。

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。

1.2 配置ARP

1.2.1 手工添加静态ARP表项

静态 ARP 表项在设备正常工作时间一直有效，当设备的 ARP 表项所对应的 VLAN 或 VLAN 接口被删除时，如果是长静态 ARP 表项则被删除，如果是已经解析的短静态 ARP 表项则重新变为未解析状态。

对于已经解析的短静态 ARP 表项，也会由于外部事件，比如解析到的出接口状态 down 等原因，恢复到未解析状态。

对于长静态 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 表项中的 IP 地址与本地 IP 地址冲突，或者设备上没有与该 ARP 表项中的 IP 地址在同一网段的接口地址。处于无效状态的长静态 ARP 表项不能指导报文转发。

表1-1 手工添加静态 ARP 表项

操作		命令	说明
进入系统视图		**system-view**	-
手工添加静态ARP表项	手工添加长静态ARP表项	**arp static** *ip-address mac-address vlan-id interface-type interface-number* [**vpn-instance** *vpn-instance-name*]	二者选其一 缺省情况下，没有配置任何静态ARP表项
	手工添加短静态ARP表项	**arp static** *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]	

说明

- 参数 *vlan-id* 用于指定 ARP 表项所对应的 VLAN，*vlan-id* 必须是用户已经创建好的 VLAN 的 ID，且 *vlan-id* 参数后面指定的以太网接口必须属于这个 VLAN。VLAN 对应的 VLAN 接口必须已经创建。
- 指定参数 *vlan-id* 和 *ip-address* 的情况下，参数 *vlan-id* 对应的 VLAN 接口的 IP 地址必须和参数 *ip-address* 指定的 IP 地址属于同一网段。

1.2.2 配置设备学习动态ARP表项的最大个数

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 表项的最大个数来进行限制。当设备学习动态 ARP 表项的个数达到所设置的值时，该设备上将不再学习动态 ARP 表项。

表1-2 配置设备学习动态 ARP 表项的最大个数

操作	命令	说明
进入系统视图	**system-view**	-
配置设备允许学习动态ARP表项的最大个数	**arp max-learning-number** *number*	缺省情况下，MSR 2600/MSR 3600设备允许学习动态ARP表项的最大个数为4096，MSR 5600设备允许学习动态ARP表项的最大个数为16384 当配置设备允许学习动态ARP表项的最大个数为0时，表示禁止本设备学习动态ARP表项

说明

当本命令配置的动态 ARP 表项的最大个数小于设备当前已经学到的动态 ARP 表项个数，那么已学到的动态 ARP 表项个数不会被删除。

1.2.3 配置接口学习动态ARP表项的最大个数

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 表项的最大个数来进行限制。当接口学习动态 ARP 表项的个数达到所设置的值时，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 表项的最大个数，则只有二层接口及 VLAN 接口上的动态 ARP 表项个数都没有超过各自配置的最大值时，才会学习 ARP 表项。

表1-3 配置接口学习动态 ARP 表项的最大数目

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置接口允许学习动态ARP表项的最大个数	**arp max-learning-num** *number*	缺省情况下，MSR 2600/MSR 3600设备接口允许学习动态ARP表项的最大个数为4096，MSR 5600设备接口允许学习动态ARP表项的最大个数为16384 当配置接口允许学习动态ARP表项的最大个数为0时，表示禁止接口学习动态ARP表项

1.2.4 配置动态ARP表项的老化时间

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纪录被刷新，则重新计算老化时间。

表1-4 配置动态 ARP 表项的老化时间

操作	命令	说明
进入系统视图	**system-view**	-
配置动态ARP表项的老化时间	**arp timer aging** *aging-time*	缺省情况下，动态ARP表项的老化时间为20分钟

1.2.5 启用动态ARP表项的检查功能

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。

- 启用 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。

表1-5 启用动态 ARP 表项的检查功能

操作	命令	说明
进入系统视图	**system-view**	-
启用动态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

1.2.6 开启ARP日志信息功能

ARP 日志是为了满足网络管理员审计的需要，对处理 ARP 报文的信息进行的记录，包括设备未使能 ARP 代理功能时收到目的 IP 不是设备接口 IP 地址、VRRP 备份组中的虚拟 IP 地址或 NAT 转换

的外部网络地址；收到的 ARP 报文中源地址和接收接口 IP 地址、VRRP 备份组中的虚拟 IP 地址或 NAT 转换的外部网络地址冲突，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”。

表1-6 开启 ARP 日志信息功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.3 ARP显示和维护

提示

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1-7 ARP 显示和维护

操作	命令
显示ARP表项（MSR 2600/MSR 3600）	**display arp** [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
显示ARP表项（MSR 5600）	**display arp** [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
显示指定IP地址的ARP表项（MSR 2600/MSR 3600）	**display arp** *ip-address* [**verbose**]
显示指定IP地址的ARP表项（MSR 5600）	**display arp** *ip-address* [**slot** *slot-number*] [**verbose**]
显示指定VPN实例的ARP表项	**display arp vpn-instance** *vpn-instance-name* [**count**]
显示动态ARP表项的老化时间	**display arp timer aging**
清除ARP表项（MSR 2600/MSR 3600）	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }
清除ARP表项（MSR 5600）	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

1.4 ARP典型配置举例

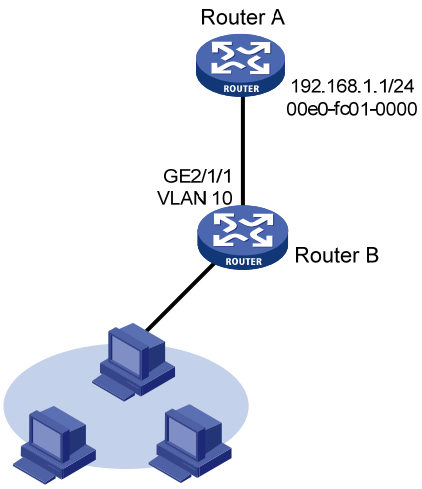
1. 组网需求

- Router B 连接主机，通过接口 GigabitEthernet2/1/1 连接 Router A。接口 GigabitEthernet2/1/1 属于 VLAN 10。
- Router A 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-0000。

为了增加 Router B 和 Router A 通信的安全性，可以在 Router B 上为 Router 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 配置静态 ARP 表项组网图



3. 配置步骤

在 Router B 上进行下列配置。

创建 VLAN 10。

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

将接口 GigabitEthernet2/1/1 加入到 VLAN 10 中。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] port access vlan 10
[RouterB-GigabitEthernet2/1/1] quit
```

创建接口 Vlan-interface10，并配置 IP 地址。

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

配置一条静态 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 GigabitEthernet2/1/1。

```
[RouterB] arp static 192.168.1.1 00e0-fc01-0000 10 gigabitethernet 2/1/1
```

查看静态 ARP 表项信息。

```
[RouterB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP address       MAC address     VLAN     Interface              Aging Type
192.168.1.1      00e0-fc01-0000  10       GE2/1/1                N/A   S
```

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 IP 地址。

设备通过对外发送免费 ARP 报文来实现以下功能：

- 确定其它设备的 IP 地址是否与本机的 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。
- 设备改变了硬件地址，通过发送免费 ARP 报文通知其它设备更新 ARP 表项。

1. 免费ARP报文学习功能的作用

启用了免费 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. 定时发送免费ARP功能的作用

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：

(1) 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启用定时发送免费 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，每台主机都可以学习到正确的网关，从而正常访问网络。

(2) 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启用定时发送免费 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。

(3) 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 配置免费ARP

配置免费 ARP 时，需要注意：

- 设备最多允许同时在 1024 个接口上启用定时发送免费 ARP 功能。
- 配置定时发送免费 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 报文的发送周期，则在下一个发送周期才能生效。
- 如果同时在很多接口下启用定时发送免费 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 报文的发送频率可能会远远低于用户设定的时间间隔。

表2-1 配置免费 ARP

操作	命令	说明
进入系统视图	**system-view**	-
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
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请求时不发送免费ARP报文
进入接口视图	**interface** *interface-type interface-number*	-
启用定时发送免费ARP功能，并设置发送免费ARP报文的周期	**arp send-gratuitous-arp** [**interval** *milliseconds*]	缺省情况下，定时发送免费ARP功能处于关闭状态

2.3 启用源IP地址冲突提示功能

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，如果收到对应的 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。

表2-2 启用源 IP 地址冲突提示功能

操作	命令	说明
进入系统视图	**system-view**	-
启用源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

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。

如无特殊说明，本章后续描述中的代理 ARP 均指普通代理 ARP。

3.2 配置代理ARP功能

代理 ARP 和本地代理 ARP 功能均可在 VLAN 接口视图/三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图下进行配置。

表3-1 配置代理 ARP 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置代理ARP功能	**proxy-arp enable**	缺省情况下，代理ARP功能处于关闭状态

表3-2 配置本地代理 ARP 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地代理ARP功能	**local-proxy-arp enable** [**ip-range** *startIP* **to** *endIP*]	缺省情况下，本地代理ARP功能处于关闭状态

3.3 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3-3 代理 ARP 显示和维护

操作	命令
显示代理ARP的状态	**display proxy-arp** [**interface** *interface-type interface-number*]
显示本地代理ARP的状态	**display local-proxy-arp** [**interface** *interface-type interface-number*]

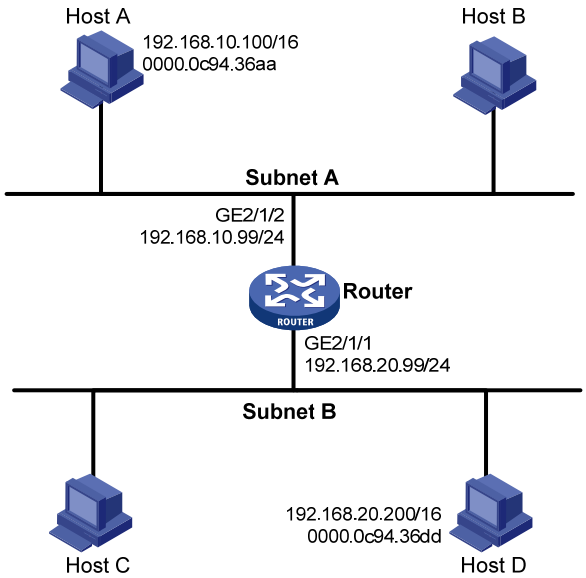
3.4 代理ARP典型配置举例

1. 组网需求

- Host A 的 IP 地址是 192.168.10.100/16，所在局域网的网络号为 192.168.0.0/16。
- Host D 的 IP 地址是 192.168.20.200/16，所在局域网的网络号为 192.168.0.0/16。
- Host A 和 Host D 互相认为处于同一子网，但实际却被设备 Router 分在两个不同的子网。
- Host A 和 Host D 没有配置缺省网关，要求在设备 Router 上启用代理 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

配置接口 GigabitEthernet2/1/2 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 192.168.10.99 255.255.255.0
```

开启接口 GigabitEthernet2/1/2 的代理 ARP 功能。

```
[Router-GigabitEthernet2/1/2] proxy-arp enable
[Router-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.20.99 255.255.255.0
```
开启接口 GigabitEthernet2/1/1 的代理 ARP 功能。
```
[Router-GigabitEthernet2/1/1] proxy-arp enable
[Router-GigabitEthernet2/1/1] quit
```
配置完成后，Host A 和 Host D 可以互相 ping 通。

目 录

1 IP地址

若非特别指明，本文所指的 IP 地址均为 IPv4 地址。

1.1 IP地址简介

1.1.1 IP地址的分类和表示

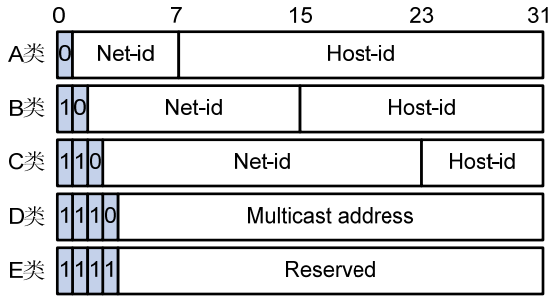
IP 地址就是给每个连接到 IPv4 网络上的设备分配的一个网络唯一的地址。IP 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.1.1.1。

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。

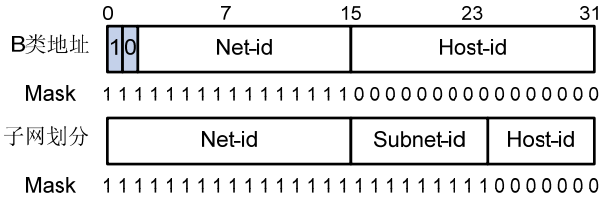
1.1.3 子网和掩码

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*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。

1.2 配置接口的IP地址

1. 功能简介

接口有了 IP 地址后就可以与其它主机进行 IP 通信。接口获取 IP 地址有以下几种方式：

- 通过手动指定 IP 地址
- 通过 BOOTP 分配得到 IP 地址
- 通过 DHCP 分配得到 IP 地址
- 通过 PPP 协商获得 IP 地址

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。

本节只介绍通过手动指定 IP 地址的方式。通过 BOOTP 和 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”，通过 PPP 协商获得 IP 地址方式的介绍请参见“二层技术-广域网接入配置指导”中的“PPP”。

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、PPP 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、主接口及其子接口之间、同一主接口下不同子接口之间的 IP 地址不可以在同一网段。

3. 配置步骤

表1-2 配置接口的 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，没有为接口配置IP地址

1.3 配置接口借用IP地址

1. 功能简介

所谓“IP 地址借用”，是指一个接口上没有配置 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

- 三层以太网接口和 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。

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 动态获取或通过 PPP 协商分配。

4. 配置步骤

此处所列的配置过程仅包含配置接口借用 IP 地址的过程。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。完整的配置过程请参考后面的配置举例。

表1-3 配置接口借用 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置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，本接口不借用其它接口的IP地址

1.4 IP地址的显示和维护

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1-4 IP 地址的显示和维护

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

1.5 地址配置和地址借用举例

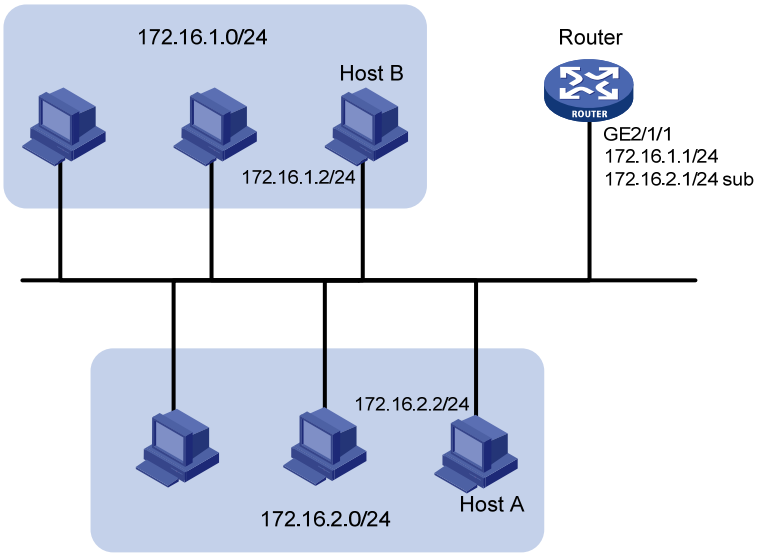
1.5.1 IP地址配置举例

1. 组网需求

Router 的以太网接口 GigabitEthernet2/1/1 连接一个局域网，该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 Router 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 Router 的接口上只配置一个 IP 地址，则只有一部分主机能够通过 Router 与外部网络通信。为了使局域网内的所有主机都能够通过 Router 访问外部网络，需要配置接口的从 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 Router 设置为网关。

配置接口 GigabitEthernet2/1/1 的主 IP 地址和从 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 172.16.1.1 255.255.255.0
[Router-GigabitEthernet2/1/1] 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 Router 与网络 172.16.1.0/24 内主机的连通性。

```
<Router> 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 Router 与网络 172.16.1.0/24 内的主机可以互通。

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

```
<Router> 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 Router 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。

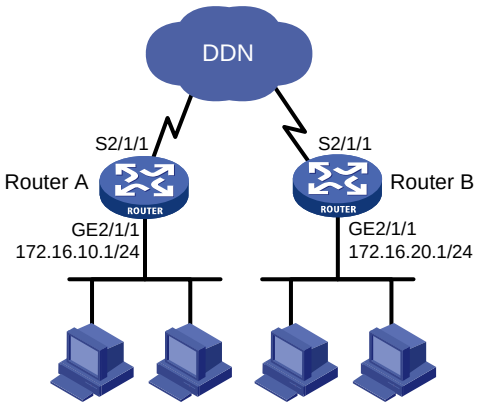
1.5.2 接口借用IP地址配置举例

1. 组网需求

某企业通过 DDN 组建内部网，节点路由器之间通过同步串口相连，并分别通过以太网接口连接本地的局域网。为了节省 IP 地址，规划串口借用以太网接口的 IP 地址。

2. 组网图

图1-4 借用 IP 地址示例的组网图



3. 配置步骤

(1) 配置 Router A

配置被借用以太网接口的主 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 172.16.10.1 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

配置串口借用以太网接口的 IP 地址。

```
[RouterA] interface serial 2/1/1
```

```
[RouterA-Serial2/1/1] ip address unnumbered interface gigabitethernet 2/1/1
[RouterA-Serial2/1/1] quit
```

配置到 Router B 所连的局域网的路由，指定出接口为串口 Serial2/1/1。

```
[RouterA] ip route-static 172.16.20.0 255.255.255.0 serial 2/1/1
```

(2)　配置 Router B

配置被借用以太网接口的主 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 172.16.20.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

配置串口借用以太网接口的 IP 地址。

```
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] ip address unnumbered interface gigabitethernet 2/1/1
[RouterB-Serial2/1/1] quit
```

配置到 Router A 所连的局域网的路由，指定出接口为串口 Serial2/1/1。

```
[RouterB] ip route-static 172.16.10.0 255.255.255.0 serial 2/1/1
```

4. 验证配置

在 Router A 上可以 Ping 通与 Router B 相连的局域网中主机。

```
[RouterA] ping 172.16.20.2
Ping 172.16.20.2 (172.16.20.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.20.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.20.2 ---
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
```

目 录

1 DHCP概述

1.1 DHCP简介

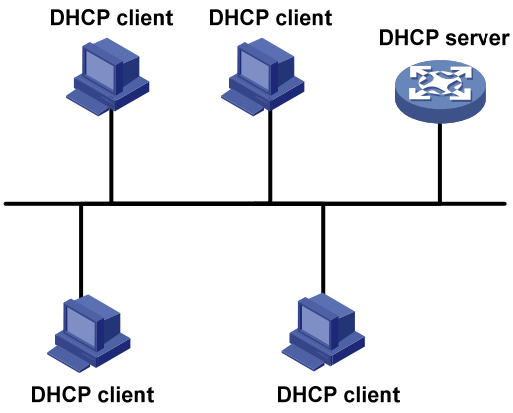
DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态地分配 IP 地址等网络配置参数。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出请求分配网络配置参数的申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现 IP 地址等信息的动态配置。

在DHCP的典型应用中，一般包含一台DHCP服务器和多台客户端（如PC和便携机），如 图 1-1 所示。

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 DHCP 典型应用



1.2 DHCP的IP地址分配

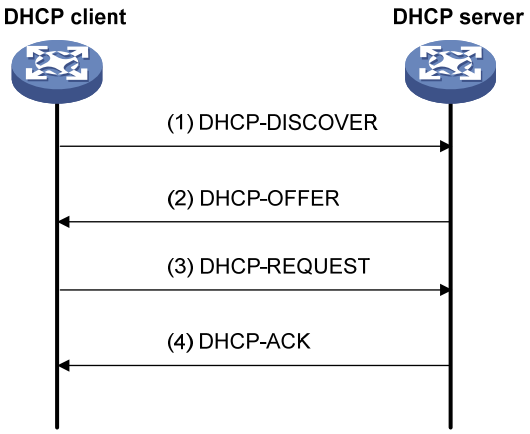
1.2.1 IP地址分配策略

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没有收到回应，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

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

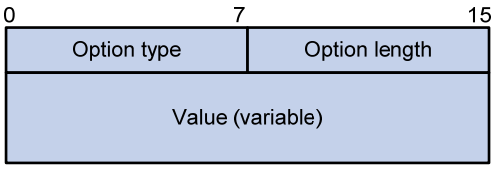
1.4.1 DHCP选项简介

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



1.4.2 DHCP常用选项介绍

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。

1.4.3 自定义的选项格式

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格式。

1. 厂商特定信息选项（Option 43）

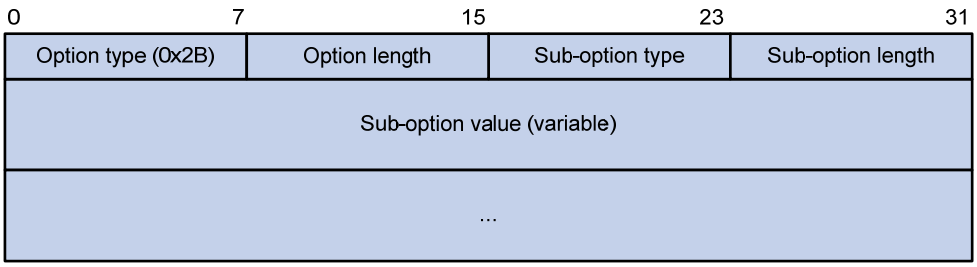
Option 43 称为厂商特定信息选项。DHCP 服务器和 DHCP 客户端通过 Option 43 交换厂商特定的信息。

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。
- 在无线网络中，AP（Access Point，接入点）作为 DHCP 客户端，可以通过 Option 43 获取 AC（Access Controller，接入控制器）地址，以便 AP 从 AC 获取启动文件或其他控制信息。

(1) Option 43 格式

图1-5 Option 43 格式



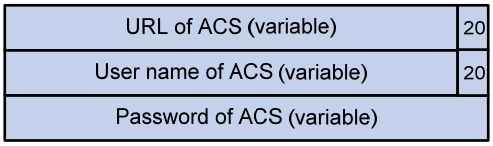
为了提供可扩展性，通过Option 43 为客户端分配更多的信息，Option 43 采用子选项的形式，通过不同的子选项为用户分配不同的网络配置参数。如 图 1-5 所示。子选项中各字段的含义为：

- 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，详细介绍请参见下文。

(2) Option 43 子选项取值字段的格式

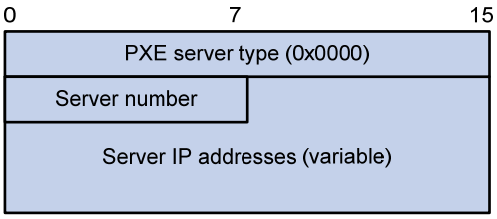
- ACS参数子选项的取值字段格式如 图 1-6 所示。ACS的URL地址、用户名和密码长度可变，每个参数之间用空格（十六进制数为 0x20）隔开。

图1-6 ACS 参数子选项取值字段的格式



- 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



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等控制。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）和 sub-option 2（Remote ID，远程 ID 子选项）。

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。

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，会话初始化协议）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。

1.5 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

2.1.1 DHCP服务器的应用环境

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。例如，Internet 接入服务提供商限制同时接入网络的用户数目，用户必须动态获得自己的 IP 地址。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

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 服务器功能，不仅可以为公网上的 DHCP 客户端分配 IP 地址，还可以实现为私网内的 DHCP 客户端分配 IP 地址，但是公网和私网之间、不同私网之间的 IP 地址空间不能重叠。MCE 的详细介绍，请参见“MPLS 配置指导”中的“MPLS L3VPN”。

2.1.2 DHCP地址池

每个 DHCP 地址池都拥有一组可供分配的地址和网络配置参数。DHCP 服务器从地址池中为客户端选择并分配 IP 地址及其他参数。

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：

- 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。
- 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。

- 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。
- 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。
- 如果动态分配的 IP 地址范围内也没有空闲地址，或者没有配置动态分配的 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. 地址池的选取原则

DHCP 服务器为客户端分配 IP 地址时，地址池的选择原则如下：

(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) 如果不存在静态绑定的地址池，且接收到 DHCP 请求报文的接口没有引用地址池，则按照以下方法选择地址池：

- 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。如果没有匹配到主网段，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。如果没有匹配到主网段，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，且没有引用地址池，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“2.1.2 DHCP地址池”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地址租约才能够被服务器分配给新的 DHCP 客户端。

2.2 DHCP服务器配置任务简介

表2-1 DHCP 服务器配置任务简介

操作	说明	详细配置
配置DHCP服务器的地址池	必选	2.3
启用DHCP服务	必选	2.4
配置接口工作在DHCP服务器模式	必选	2.5
配置接口引用地址池	可选	2.6
配置IP地址冲突检测功能	可选	2.7
配置Option 82的处理方式	可选	2.8
配置DHCP服务器协议兼容性	可选	2.9

操作	说明	详细配置
配置DHCP服务器发送DHCP报文的DSCP优先级	可选	2.10

2.3 配置DHCP服务器的地址池

2.3.1 DHCP服务器地址池配置任务简介

表2-2 DHCP 服务器地址池配置任务简介

操作	说明	详细配置
创建DHCP地址池	必选	2.3.2
配置为客户端分配的IP地址	至少选其一	2.3.3
配置DHCP客户端使用的网关地址		2.3.4
配置DHCP客户端使用的域名后缀		2.3.5
配置DHCP客户端使用的DNS服务器地址		2.3.6
配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型		2.3.7
配置DHCP客户端使用的BIMS服务器信息		2.3.8
配置DHCP客户端使用的TFTP服务器地址及启动文件名		2.3.9
配置DHCP客户端使用的下一个提供服务的服务器IP地址		2.3.10
配置DHCP客户端使用的Option 184参数		2.3.11
自定义DHCP选项		2.3.12

2.3.2 创建DHCP地址池

表2-3 创建 DHCP 地址池

操作	命令	说明
进入系统视图	**system-view**	-
创建DHCP地址池，并进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	缺省情况下，设备上不存在任何DHCP地址池

2.3.3 配置为客户端分配的IP地址

提示

对一个 DHCP 地址池可以同时配置静态地址管理方式和动态地址管理方式。动态地址管理方式分为一个主网段多个地址范围和一个主网段多个从网段两种，用户可以根据实际需要，选择不同的动态地址管理方式。同一个地址池中不能同时配置两种动态地址管理方式。

1. 配置一个主网段多个地址范围的动态地址管理方式

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。

表2-4 配置一个主网段多个地址段的动态地址管理方式

操作	命令	说明
进入系统视图	**system-view**	-
创建DHCP用户类，并进入DHCP用户类视图	**dhcp class** *class-name*	缺省情况下，不存在任何DHCP用户类 在地址池下，需要为DHCP用户类指定地址范围时，为必选
配置DHCP用户类的匹配规则	**if-match rule** *rule-number* **option** *option-code* [**hex** *hex-string* [**offset** *offset* **length** *length* | **mask** *mask*]]	缺省情况下，没有配置DHCP用户类的匹配规则 在地址池下，需要为DHCP用户类指定地址范围时，为必选
退回系统视图	**quit**	-
进入地址池视图	**dhcp server ip-pool** *pool-name*	-
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，没有配置主网段
（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，没有配置动态分配的IP地址范围
（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，没有配置为指定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

操作	命令	说明
（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
（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
退回系统视图	**quit**	-
（可选）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

说明

- 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。

2. 配置一个主网段多个从网段的动态地址管理方式

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。

表2-5 配置一个主网段多个从网段的地址管理方式

操作	命令	说明
进入系统视图	**system-view**	-
进入地址池视图	**dhcp server ip-pool** *pool-name*	-
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，没有配置主网段 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
（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，没有配置从网段
（可选）退回地址池视图	**quit**	-
（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

操作	命令	说明
（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 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
退回系统视图	**quit**	-
（可选）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

说明

- 每个 DHCP 地址池中，最多可以配置 32 个从网段。
- 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. 配置静态地址绑定

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。

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。

表2-6 配置静态地址绑定

操作	命令	说明
进入系统视图	**system-view**	-
进入地址池视图	**dhcp server ip-pool** *pool-name*	-

操作	命令	说明
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，没有配置静态地址绑定 多次执行**static-bind ip-address**命令，可以配置多个静态地址绑定 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
（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

2.3.4 配置DHCP客户端使用的网关地址

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。

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 8 个网关地址。

表2-7 配置 DHCP 客户端使用的网关地址

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
配置为DHCP客户端分配的网关地址	**gateway-list** *ip-address*&<1-8>	缺省情况下，没有配置为DHCP客户端分配的网关地址
（可选）进入从网段视图	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	-
（可选）配置为DHCP客户端分配的网关地址	**gateway-list** *ip-address*&<1-8>	缺省情况下，没有配置为DHCP客户端分配的网关地址

说明

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。

2.3.5 配置DHCP客户端使用的域名后缀

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”。

表2-8 配置 DHCP 客户端使用的域名后缀

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
配置为DHCP客户端分配的域名后缀	**domain-name** *domain-name*	缺省情况下，没有配置为DHCP客户端分配的域名后缀

2.3.6 配置DHCP客户端使用的DNS服务器地址

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。

表2-9 配置 DHCP 客户端使用的 DNS 服务器地址

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
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，没有配置为DHCP客户端分配的DNS服务器地址

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

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。目前，每个 DHCP 地址池视图下最多可以配置 8 个 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。

表2-10 配置 DHCP 客户端使用的 WINS 服务器地址和 NetBIOS 节点类型

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
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，没有配置为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
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，没有配置为DHCP客户端分配的NetBIOS节点类型

2.3.8 配置DHCP客户端使用的BIMS服务器信息

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。

表2-11 配置 DHCP 客户端使用的 BIMS 服务器信息

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
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** } *key*	缺省情况下，没有配置为DHCP客户端分配的BIMS服务器信息

2.3.9 配置DHCP客户端使用的TFTP服务器地址及启动文件名

设备在空配置启动时自动获取并执行配置文件的功能，被称为自动配置。具体过程如下：

(1) 设备在空配置启动时，系统会自动将处于 up 状态的接口（如缺省 VLAN 对应的虚接口或三层以太网接口）设置为 DHCP 客户端，并向 DHCP 服务器获取 IP 地址及后续获取配置文件所需要的信息（例如：TFTP 服务器的 IP 地址、TFTP 服务器名、启动文件名等）。

(2) 如果获取到相关信息，则 DHCP 客户端就可发起 TFTP 请求，从指定的 TFTP 服务器获取配置文件，之后设备就使用获取到的配置文件进行设备初始化工作。如果没有获取到相关信息，则设备在空配置的情况下正常启动。

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。

表2-12 配置 DHCP 客户端使用的 TFTP 服务器地址及启动文件名

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
配置为DHCP客户端分配的TFTP服务器地址	**tftp-server ip-address** *ip-address*	二者至少选其一 缺省情况下，没有配置为DHCP客户端分配的TFTP服务器地址和TFTP服务器名
配置为DHCP客户端分配的TFTP服务器名	**tftp-server domain-name** *domain-name*	
配置为DHCP客户端分配的启动文件名	**bootfile-name** *bootfile-name*	缺省情况下，没有配置为DHCP客户端分配的启动文件名

2.3.10 配置DHCP客户端使用的下一个提供服务的服务器IP地址

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。

表2-13 配置 DHCP 客户端使用的下一个提供服务的服务器 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
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，没有配置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

2.3.11 配置DHCP客户端使用的Option 184 参数

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“1.4.3 3. Option 184”。

表2-14 配置 DHCP 客户端使用的 Option 184 参数

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-
配置网络呼叫处理器的地址	**voice-config ncp-ip** *ip-address*	缺省情况下，没有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
（可选）配置备用服务器的地址	**voice-config as-ip** *ip-address*	缺省情况下，没有配置备用服务器的地址
（可选）配置语音VLAN	**voice-config voice-vlan** *vlan-id* { **disable** | **enable** }	缺省情况下，没有配置语音VLAN
（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，没有配置自动故障转移呼叫路由

2.3.12 自定义DHCP选项

提示

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 的工作工程造成影响，请谨慎使用该功能。

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。

表2-15 自定义 DHCP 选项

操作	命令	说明
进入系统视图	**system-view**	-
进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	-

操作	命令	说明
自定义DHCP选项	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	缺省情况下，没有自定义DHCP选项

表2-16 常用 Option 配置说明

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	**gateway-list**	**ip-address**
6	Domain Name Server Option	**dns-list**	**ip-address**
15	Domain Name	**domain-name**	**ascii**
44	NetBIOS over TCP/IP Name Server Option	**nbns-list**	**ip-address**
46	NetBIOS over TCP/IP Node Type Option	**netbios-type**	**hex**
66	TFTP server name	**tftp-server**	**ascii**
67	Bootfile name	**bootfile-name**	**ascii**
43	Vendor Specific Information	-	**hex**

2.4 启用DHCP服务

只有启用 DHCP 服务后，其它相关的 DHCP 服务器配置才能生效。

表2-17 启用 DHCP 服务

操作	命令	说明
进入系统视图	**system-view**	-
启用DHCP服务	**dhcp enable**	缺省情况下，DHCP服务处于禁止状态

2.5 配置接口工作在DHCP服务器模式

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。

表2-18 配置接口工作在 DHCP 服务器模式

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口工作在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

2.6 配置接口引用地址池

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。

表2-19 配置接口引用地址池

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口引用地址池	**dhcp server apply ip-pool** *pool-name*	缺省情况下，接口没有引用任何地址池。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IP地址冲突检测功能

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探测。

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。如果在指定时间内没有收到回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的回显显示报文数目达到最大值。如果仍然没有收到回显响应报文，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。

表2-20 配置 IP 地址冲突检测功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置DHCP服务器发送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
（可选）配置DHCP服务器等待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

2.8 配置Option 82的处理方式

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“3.3.6 配置DHCP中继支持Option 82 功能”。

表2-21 配置 Option 82 的处理方式

操作	命令	说明
进入系统视图	**system-view**	-
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

2.9 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。

2.9.1 配置DHCP服务器始终以广播方式回复请求报文

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，无论是否启用 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，无论是否启用 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）。

表2-22 配置 DHCP 服务器始终以广播方式回复请求报文

操作	命令	说明
进入系统视图	**system-view**	-
启用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

2.9.2 配置DHCP服务器忽略BOOTP请求报文

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。

表2-23 配置 DHCP 服务器忽略 BOOTP 请求报文

操作	命令	说明
进入系统视图	**system-view**	-
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

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

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。

启用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。

表2-24 配置 DHCP 服务器以 RFC 1048 规定的格式发送 BOOTP 应答报文

操作	命令	说明
进入系统视图	**system-view**	-
启用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 本配置只在客户端通过BOOTP报文申请静态绑定地址时有效

2.10 配置DHCP服务器发送DHCP报文的DSCP优先级

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。

表2-25 配置 DHCP 服务器发送 DHCP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
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

2.11 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服务器上不存在任何租约信息。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2-26 DHCP服务器显示和维护

操作	命令
显示DHCP的地址冲突信息	**display dhcp server conflict** [**ip** *ip-address*]
显示租约过期的地址绑定信息	**display dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
显示DHCP地址池的空闲地址信息	**display dhcp server free-ip** [**pool** *pool-name*]
显示DHCP地址绑定信息	**display dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
显示DHCP服务器的统计信息	**display dhcp server statistics** [**pool** *pool-name*]
显示DHCP地址池的信息	**display dhcp server pool** [*pool-name*]
清除DHCP的地址冲突信息	**reset dhcp server conflict** [**ip** *ip-address*]
清除租约过期的地址绑定信息	**reset dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
清除DHCP的正式绑定和临时绑定信息	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
清除DHCP服务器的统计信息	**reset dhcp server statistics**

2.12 DHCP服务器典型配置举例

常见的DHCP组网方式可以分为两类：

- DHCP服务器和客户端位于同一个网段，直接进行DHCP报文的交互；
- DHCP服务器和客户端位于不同的网段，必须通过DHCP中继实现IP地址的分配。

无论在哪种情况下，DHCP服务器的配置都是相同的。

2.12.1 静态绑定地址典型配置举例

1. 组网需求

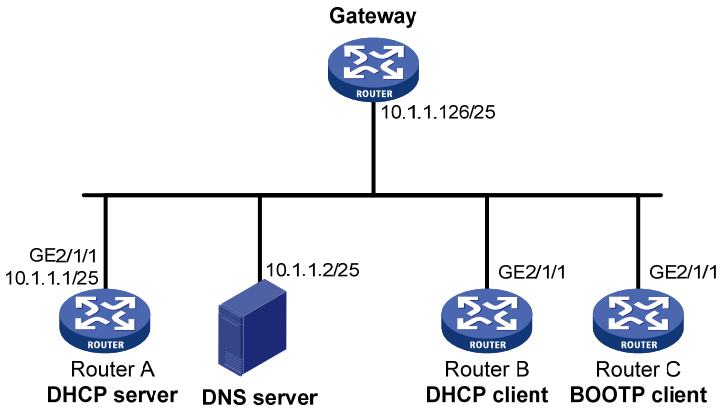
Router B和Router C分别作为DHCP客户端和BOOTP客户端，从DHCP服务器Router A获取静态绑定的IP地址、域名服务器、网关地址。

其中：

- Router B 的接口 GigabitEthernet2/1/1 的客户端 ID 为：0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574-302f-30；
- Router C 的接口 GigabitEthernet2/1/1 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

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.1.1.1 25
[RouterA-GigabitEthernet2/1/1] quit
```

(2) 配置 DHCP 服务

启用 DHCP 服务。

```
[RouterA] dhcp enable
```

配置接口 GigabitEthernet2/1/1 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] dhcp select server
[RouterA-GigabitEthernet2/1/1] quit
```

创建 DHCP 地址池 0。

```
[RouterA] dhcp server ip-pool 0
```

配置采用静态绑定方式为 Router B 分配 IP 地址。

```
[RouterA-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-6574-302f-30
```

配置采用静态绑定方式为 Router C 分配 IP 地址。

```
[RouterA-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。

```
[RouterA-dhcp-pool-0] dns-list 10.1.1.2
[RouterA-dhcp-pool-0] gateway-list 10.1.1.126
```

4. 验证配置

配置完成后，Router B 和 Router C 可以从 DHCP 服务器 Router 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。

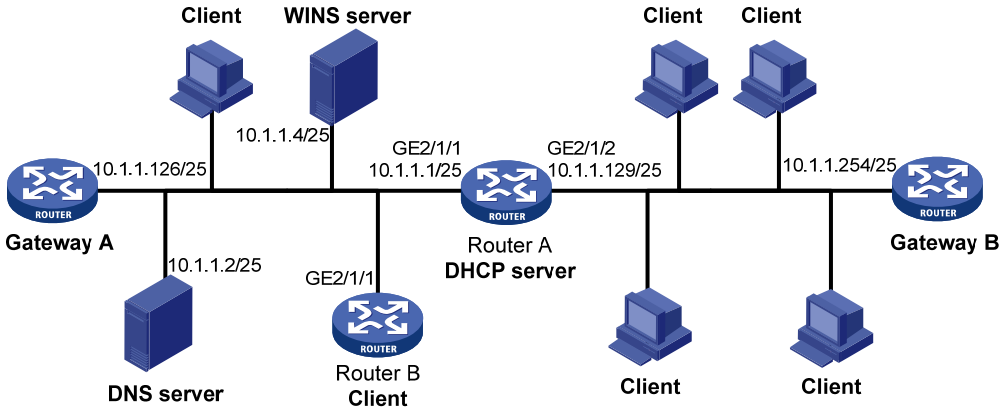
2.12.2 动态分配地址典型配置举例

1. 组网需求

- 作为 DHCP 服务器的 Router 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；
- Router A 的两个以太网接口，GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 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 DHCP server 各接口的 IP 地址（略）

(2) 配置 DHCP 服务

启用 DHCP 服务。

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

配置接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] dhcp select server
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] dhcp select server
```

```
[RouterA-GigabitEthernet2/1/2] quit
```
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）。
```
[RouterA] dhcp server forbidden-ip 10.1.1.2
[RouterA] dhcp server forbidden-ip 10.1.1.4
[RouterA] dhcp server forbidden-ip 10.1.1.126
[RouterA] 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。
```
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[RouterA-dhcp-pool-1] expired day 10 hour 12
[RouterA-dhcp-pool-1] domain-name aabbcc.com
[RouterA-dhcp-pool-1] dns-list 10.1.1.2
[RouterA-dhcp-pool-1] gateway-list 10.1.1.126
[RouterA-dhcp-pool-1] nbns-list 10.1.1.4
[RouterA-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。
```
[RouterA] dhcp server ip-pool 2
[RouterA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[RouterA-dhcp-pool-2] expired day 5
[RouterA-dhcp-pool-2] domain-name aabbcc.com
[RouterA-dhcp-pool-2] dns-list 10.1.1.2
[RouterA-dhcp-pool-2] gateway-list 10.1.1.254
```

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 Router 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。

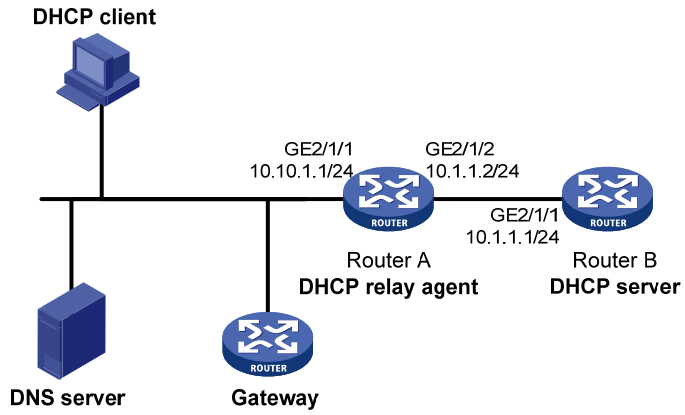
2.12.3 用户类典型配置举例

1. 组网需求

- Router A 作为 DHCP 中继转发 DHCP 报文。在 Router A 上配置 DHCP 中继支持 Option 82 功能，使得 Router A 能够为 DHCP 客户端发送的请求报文添加 Option 82。
- Router 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 Router 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。
- Router 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 DHCP 用户类组网图



3. 配置步骤

(1) 配置 DHCP server 各个接口的 IP 地址（略）

(2) 配置 DHCP 服务

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

```
<RouterB> system-view
[RouterB] dhcp enable
[RouterB] dhcp server relay information enable
```

配置接口 GigabitEthernet2/1/1 工作在 DHCP 服务器模式。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] dhcp select server
[RouterB-GigabitEthernet2/1/1] quit
```

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

```
[RouterB] dhcp class tt
[RouterB-dhcp-class-tt] if-match rule 1 option 82
[RouterB-dhcp-class-tt] 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。

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

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 Router 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。

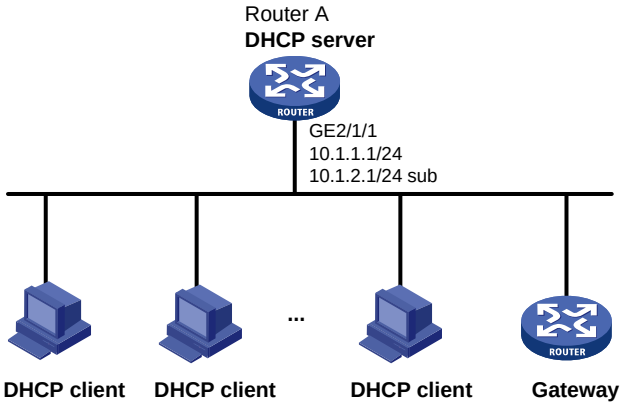
2.12.4 主从网段典型配置举例

1. 组网需求

- 作为 DHCP 服务器的 Router 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。
- Router 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2-4 主从网段组网图



3. 配置步骤

(1) 配置 DHCP 服务。

启用 DHCP 服务。

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

配置接口 GigabitEthernet2/1/1 的主从 IP 地址，并配置该接口工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/1/1] ip address 10.1.2.1 24 sub
[RouterA-GigabitEthernet2/1/1] dhcp select server
[RouterA-GigabitEthernet2/1/1] quit
```

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。

```
[RouterA] dhcp server ip-pool aa
[RouterA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-aa] gateway-list 10.1.1.254
[RouterA-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
[RouterA-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[RouterA-dhcp-pool-aa-secondary] quit
[RouterA-dhcp-pool-aa]
```

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。

2.12.5 自定义DHCP选项典型配置举例

1. 组网需求

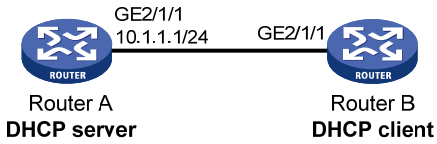
DHCP 客户端 Router B 从 DHCP 服务器 Router A 获取 IP 地址和 PXE 引导服务器地址信息：

- 客户端 IP 地址所在网段为 10.1.1.0/24；
- 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2-5 自定义 DHCP 选项典型配置举例



3. 配置步骤

(1) 配置接口 GigabitEthernet2/1/1 的 IP 地址（略）

(2) 配置 DHCP 服务

启用 DHCP 服务。

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

配置接口 GigabitEthernet2/1/1 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] dhcp select server
[RouterA-GigabitEthernet2/1/1] quit
```

配置 DHCP 地址池 0。

```
[RouterA] dhcp server ip-pool 0
[RouterA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-0] option 43 hex 800B0000020102030402020202
```

4. 验证配置

配置完成后，Router B 可以从 DHCP 服务器 Router 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。

2.13 DHCP服务器常见配置错误举例

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

3.1.1 DHCP中继的应用环境

由于在 IP 地址动态获取过程中采用广播方式发送请求报文，因此 DHCP 只适用于 DHCP 客户端和服务器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

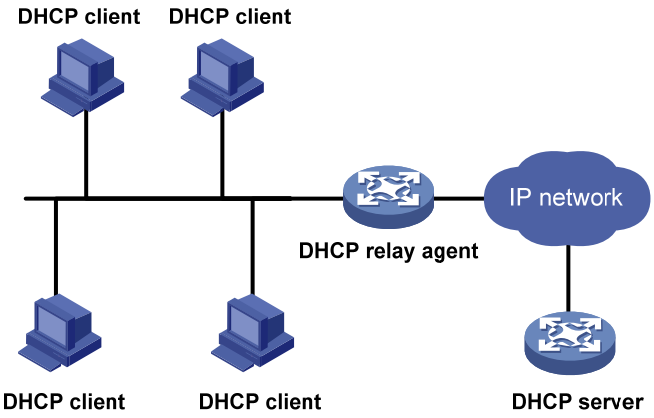
DHCP 中继功能的引入解决了这一难题：客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

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“MPLS 配置指导”中的“MPLS L3VPN”。

3.1.2 DHCP中继的基本原理

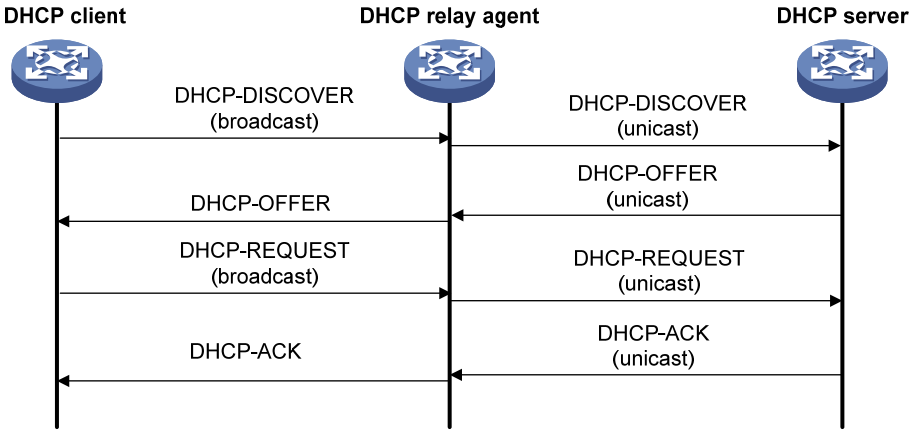
图 3-1 是DHCP中继的典型应用示意图。

图3-1 DHCP 中继的典型组网应用



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，并根据配置将报文单播转发给指定的 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“1.4.3 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

3.2 DHCP中继配置任务简介

表3-2 DHCP 中继配置任务简介

配置任务	说明	详细配置
启用DHCP服务	必选	3.3.1
配置接口工作在DHCP中继模式	必选	3.3.2
指定DHCP服务器的地址	必选	3.3.3
配置DHCP中继的安全功能	可选	3.3.4
配置通过DHCP中继释放客户端的IP地址	可选	3.3.5
配置DHCP中继支持Option 82功能	可选	3.3.6
配置DHCP中继发送DHCP报文的DSCP优先级	可选	3.3.7

3.3 配置DHCP中继

3.3.1 启用DHCP服务

只有启用 DHCP 服务后，其它相关的 DHCP 中继配置才能生效。

表3-3 启用 DHCP 服务

操作	命令	说明
进入系统视图	**system-view**	-
启用DHCP服务	**dhcp enable**	缺省情况下，DHCP服务处于禁止状态

3.3.2 配置接口工作在DHCP中继模式

配置接口工作在中继模式后，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。

表3-4 配置接口工作在 DHCP 中继模式

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口工作在DHCP中继模式	**dhcp select relay**	缺省情况下，启用DHCP服务后，接口工作在DHCP服务器模式

3.3.3 指定DHCP服务器的地址

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。

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。

表3-5 指定 DHCP 服务器的地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定DHCP服务器的地址	**dhcp relay server-address** *ip-address*	缺省情况下，没有在DHCP中继上指定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

3.3.4 配置DHCP中继的安全功能

1. 配置DHCP中继用户地址表项记录功能

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。

启用该功能后，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。

表3-6 配置 DHCP 中继用户地址表项记录功能

操作	命令	说明
进入系统视图	**system-view**	-
启用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

说明

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。

2. 配置DHCP中继动态用户地址表项定时刷新功能

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 地址和 DHCP 中继接口的 MAC 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没有接收到 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。

表3-7 配置 DHCP 中继动态用户地址表项定时刷新功能

操作	命令	说明
进入系统视图	**system-view**	-
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
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. 配置防止DHCP饿死攻击

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，需要启用 DHCP 中继的 MAC 地址检查功能。启用该功能后，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 中继设备上启用 MAC 地址检查功能。在非第一跳 DHCP 中继设备上启用 MAC 地址检查功能，会使 DHCP 中继设备错误地丢弃报文，导致客户端地址申请不成功。

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。

表3-8 启用 DHCP 中继的 MAC 地址检查功能

操作	命令	说明
进入系统视图	**system-view**	-
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**命令启用DHCP中继的MAC地址检查功能，则本命令的配置不会生效
进入接口视图	**interface** *interface-type interface-number*	-
启用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

3.3.5 配置通过DHCP中继释放客户端的IP地址

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。

表3-9 配置通过 DHCP 中继释放客户端的 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
向DHCP服务器请求释放客户端申请到的IP地址	**dhcp relay release ip** *client-ip* [**vpn-instance** *vpn-instance-name*]	-

3.3.6 配置DHCP中继支持Option 82 功能

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“2.8 配置Option 82 的处理方式”。

表3-10 配置 DHCP 中继支持 Option 82 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启用DHCP中继支持Option 82功能	**dhcp relay information enable**	缺省情况下，禁止DHCP中继支持Option 82功能

操作	命令	说明
（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**
（可选）配置Circuit ID子选项的填充内容和填充格式	**dhcp relay information circuit-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中继添加或替换Option 82失败
（可选）配置Remote ID子选项的填充内容和填充格式	**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

3.3.7 配置DHCP中继发送DHCP报文的DSCP优先级

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。

表3-11 配置 DHCP 中继发送 DHCP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
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

3.4 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3-12 DHCP 中继显示和维护

操作	命令
显示工作在DHCP中继模式的接口上指定的DHCP服务器地址信息	**display dhcp relay server-address** [**interface** *interface-type interface-number*]
显示DHCP中继上的Option 82配置信息	**display dhcp relay information** [**interface** *interface-type interface-number*]
显示DHCP中继的用户地址表项信息	**display dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]
显示DHCP中继的相关报文统计信息	**display dhcp relay statistics** [**interface** *interface-type interface-number*]

操作	命令
显示DHCP中继的MAC地址检查表项	**display dhcp relay check mac-address**
清除DHCP中继的用户地址表项信息	**reset dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]
清除DHCP中继的相关报文统计信息	**reset dhcp relay statistics** [**interface** *interface-type interface-number*]

3.5 DHCP中继典型配置举例

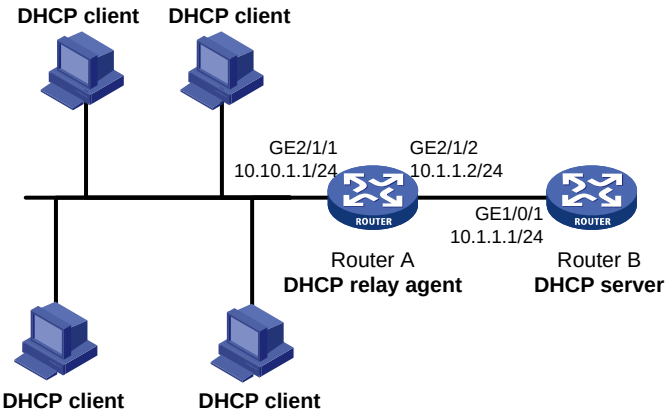
3.5.1 DHCP中继配置举例

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；
- Router A 作为 DHCP 中继通过 GigabitEthernet2/1/1 接口连接到 DHCP 客户端所在的网络，GigabitEthernet2/1/1 接口的 IP 地址为 10.10.1.1/24，GigabitEthernet2/1/2 接口的 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）。

启用 DHCP 服务。

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

配置 GigabitEthernet2/1/1 接口工作在 DHCP 中继模式。

```
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] dhcp select relay
```

指定 DHCP 服务器的地址。

```
[RouterA-GigabitEthernet2/1/1] 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** 命令启用了 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 DHCP 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“2.12 DHCP服务器典型配置举例”。

3.5.2 DHCP中继支持Option 82 配置举例

1. 组网需求

- 在 DHCP 中继 Router A 上启用 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；
- Router A 将添加 Option 82 的 DHCP 请求报文转发给 DHCP 服务器 Router 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）。

启用 DHCP 服务。

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

配置 GigabitEthernet2/1/1 接口工作在 DHCP 中继模式。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] dhcp select relay
```

指定 DHCP 服务器的地址。

```
[RouterA-GigabitEthernet2/1/1] dhcp relay server-address 10.1.1.1
```

配置 Option 82 的处理策略和填充内容。

```
[RouterA-GigabitEthernet2/1/1] dhcp relay information enable
[RouterA-GigabitEthernet2/1/1] dhcp relay information strategy replace
[RouterA-GigabitEthernet2/1/1] dhcp relay information circuit-id string company001
[RouterA-GigabitEthernet2/1/1] 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。

3.6 DHCP中继常见配置错误举例

1. 故障现象

客户端不能通过 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 中继是否启用了 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。

DHCP 客户端中对于接口的相关配置，目前只能在三层以太网接口（包括子接口）、VLAN 接口和三层聚合接口上进行。

4.2 配置接口通过DHCP协议获取IP地址

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。

表4-1 配置接口通过 DHCP 协议获取 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口通过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

4.3 配置接口使用的DHCP客户端ID

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，用户可以通过以下三种方法指定 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 的取值为十六进制字符串时，对应的类型值为该十六进制字符串的前两个字符；当客户端 ID 使用指定接口的 MAC 地址时，对应的类型值为 01。以上三种方式都需要由用户保证不同客户端的客户端 ID 不会相同。

表4-2 配置接口使用的 DHCP 客户端 ID

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置接口使用的DHCP客户端ID	**dhcp client identifier** { **ascii** *string* | **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

4.4 使能地址冲突检查功能

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。

表4-3 使能地址冲突检查功能

操作	命令	说明
进入系统视图	**system-view**	-
使能地址冲突检查功能	**dhcp client dad enable**	缺省情况下，地址冲突检查功能处于开启状态

4.5 配置DHCP客户端发送DHCP报文的DSCP优先级

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。

表4-4 配置 DHCP 客户端发送 DHCP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
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

4.6 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4-5 DHCP 客户端显示和维护

操作	命令
显示DHCP客户端的相关信息	**display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

4.7 DHCP客户端典型配置举例

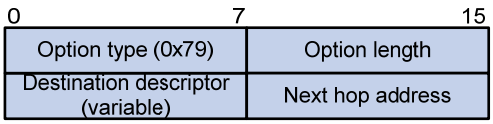
1. 组网需求

Router B 的以太网接口 GigabitEthernet2/1/1 接入局域网，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。

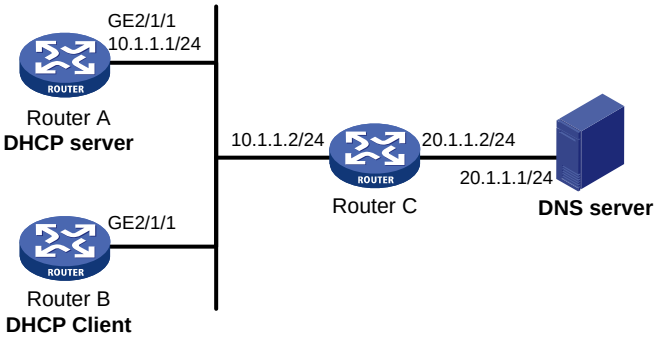
DHCP服务器需要通过自定义选项的方式配置Option 121 的内容，以便为客户端分配静态路由信息。Option 121 的格式如 图 4-1 所示。其中，目的描述符由子网掩码长度和目的网络地址两部分组成。在本例中，目的描述符字段取值为 18 14 01 01（十六进制数值，表示子网掩码长度为 24，目的网络地址为 20.1.1.0）；下一跳地址字段取值为 0A 01 01 02（十六进制数值，表示下一跳地址为 10.1.1.2）。

图4-1 Option 121 选项格式



2. 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 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/1/1] quit
```

启用 DHCP 服务。

```
[RouterA] dhcp enable
```

配置不参与自动分配的 IP 地址。

```
[RouterA] 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。

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

(2) 配置 DHCP 客户端 Router B

配置接口 GigabitEthernet2/1/1 通过 DHCP 动态获取地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address dhcp-alloc
[RouterB-GigabitEthernet2/1/1] quit
```

4. 验证配置

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

```
[RouterB] display dhcp client verbose
gigabitEthernet2/1/1 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: acsii(type value=00)
 Client ID value: 000c.29d3.8659-GE2/1/1
 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 Router B 的路由表中添加了到达 20.1.1.0/24 网络的静态路由。

```
[RouterB] 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	GE2/1/1
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	GE2/1/1
10.1.1.255/32	Direct	0	0	10.1.1.3	GE2/1/1
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

说明

- 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。
- 本特性仅在安装了二层交换卡的款型和 MSR3600-28/MSR3600-51 的固定二层接口上支持。

5.1 DHCP Snooping简介

5.1.1 DHCP Snooping作用

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

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

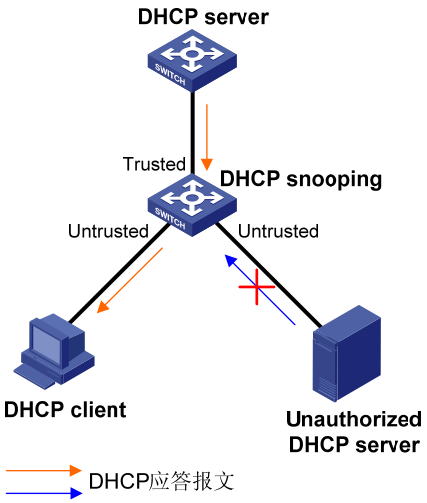
DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现：

- 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”。
- 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”。

5.1.2 信任端口的典型应用环境

1. 连接DHCP服务器

图5-1 信任端口和非信任端口



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。

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

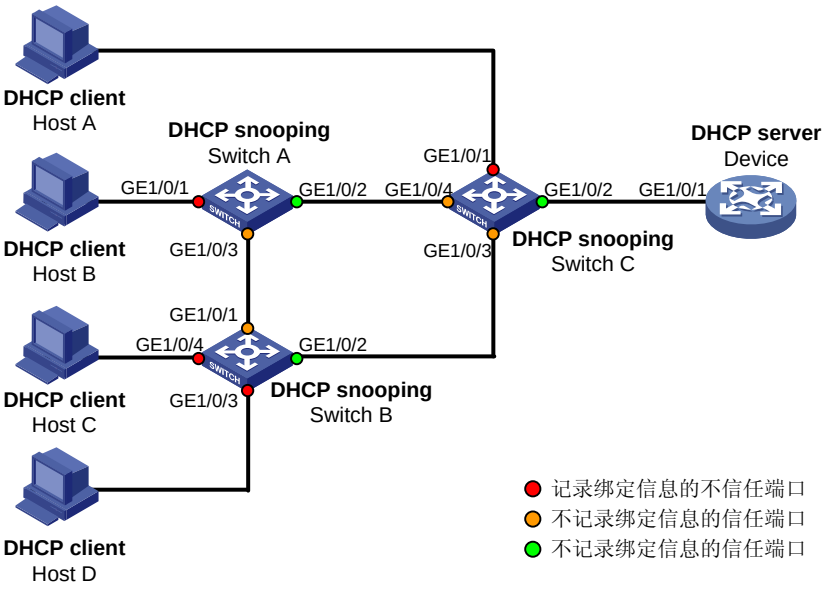


图 5-2 中设备各端口的角色如 表 5-1 所示。

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	不记录绑定信息的信任端口
Switch A	GE1/0/1	GEt1/0/3	GE1/0/2
Switch B	GE1/0/3和GE1/0/4	GE1/0/1	GE1/0/2
Switch C	GE1/0/1	GE1/0/3和GE1/0/4	GE1/0/2

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“1.4.3 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配置任务简介

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。

表5-3 DHCP Snooping 配置任务简介

配置任务	说明	详细配置
配置DHCP Snooping基本功能	必选	5.3
配置DHCP Snooping支持Option 82功能	可选	5.4
配置DHCP Snooping表项备份功能	可选	5.5

配置任务	说明	详细配置
配置防止DHCP饿死攻击	可选	5.6
配置防止伪造DHCP请求方向报文攻击	可选	5.7
配置接口动态学习DHCP Snooping表项的最大数目	可选	5.8

5.3 配置DHCP Snooping基本功能

配置 DHCP Snooping 基本功能时，需要注意：

- 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。
- DHCP Snooping 功能可以与 QinQ 功能同时使用，通过 DHCP Snooping 表项记录客户端发送 DHCP 报文的 VLAN Tag 信息。QinQ 功能的详细介绍，请参见“二层技术-以太网交换”中的“QinQ”。

表5-4 配置 DHCP Snooping 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
启用DHCP Snooping功能	**dhcp snooping enable**	缺省情况下，DHCP Snooping功能处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	此接口为连接DHCP服务器的接口
配置端口为信任端口	**dhcp snooping trust**	缺省情况下，在启用DHCP Snooping功能后，设备的所有端口均为不信任端口
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	此接口为连接DHCP客户端的接口
（可选）启用端口的DHCP Snooping表项记录功能	**dhcp snooping binding record**	缺省情况下，在启用DHCP Snooping功能后，端口的DHCP Snooping表项记录功能处于关闭状态

5.4 配置DHCP Snooping支持Option 82功能

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“2.8 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”。

表5-5 配置 DHCP Snooping 支持 Option 82 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启用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
（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的填充格式；处理策略为**keep**或**drop**时，不需要配置Option 82的填充格式。
（可选）配置Circuit ID子选项的填充内容和填充格式	**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
（可选）配置Remote ID子选项的填充内容和填充格式	**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

5.5 配置DHCP Snooping表项备份功能

DHCP Snooping 设备重启后，设备上记录的 DHCP Snooping 表项将丢失。如果 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 表项备份功能将 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。

表5-6 配置 DHCP Snooping 表项备份功能

操作	命令	说明
进入系统视图	**system-view**	-
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** } *key*]] }	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。之后，如果未配置**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**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
（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
（可选）配置DHCP Snooping表项存储文件的刷新时间间隔	**dhcp snooping binding database update interval** *seconds*	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

说明

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。

5.6 配置防止DHCP饿死攻击

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，需要启用 DHCP Snooping 的 MAC 地址检查功能。启用该功能后，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”。

表5-7 启用 DHCP Snooping 的 MAC 地址检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启用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

5.7 配置防止伪造DHCP请求方向报文攻击

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 设备上启用 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。如果启用了该功能，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。

表5-8 启用 DHCP Snooping 的 DHCP 请求方向报文检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启用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 只能在二层以太网接口上启用DHCP Snooping的DHCP请求方向报文检查功能

5.8 配置接口动态学习DHCP Snooping表项的最大数目

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。

表5-9 配置接口动态学习 DHCP Snooping 表项的最大数目

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

5.9 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5-10 DHCP Snooping 显示和维护

操作	命令
显示DHCP Snooping表项信息	**display dhcp snooping binding** [**ip** *ip-address* [**vlan** *vlan-id*]]
显示DHCP Snooping上Option 82的配置信息	**display dhcp snooping information** { **all** | **interface** *interface-type interface-number* }
显示DHCP Snooping设备上的DHCP报文统计信息（MSR 2600/MSR 3600）	**display dhcp snooping packet statistics**
显示DHCP Snooping设备上的DHCP报文统计信息（MSR 5600）	**display dhcp snooping packet statistics** [**slot** *slot-number*]
显示信任端口信息	**display dhcp snooping trust**
显示DHCP Snooping表项备份信息	**display dhcp snooping binding database**
清除DHCP Snooping表项	**reset dhcp snooping binding** { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }
清除DHCP Snooping设备上的DHCP报文统计信息（MSR 2600/MSR 3600）	**reset dhcp snooping packet statistics**
清除DHCP Snooping设备上的DHCP报文统计信息（MSR 5600）	**reset dhcp snooping packet statistics** [**slot** *slot-number*]

5.10 DHCP Snooping典型配置举例

5.10.1 DHCP Snooping配置举例

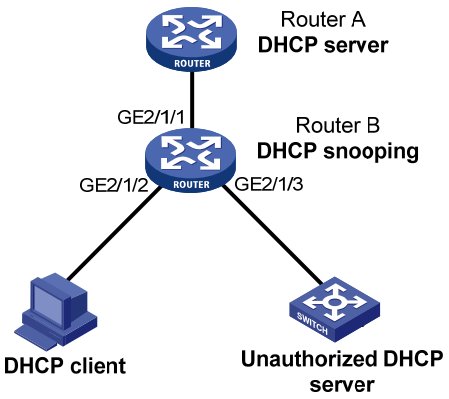
1. 组网需求

Router B 通过以太网端口 GigabitEthernet2/1/1 连接到合法 DHCP 服务器，通过以太网端口 GigabitEthernet2/1/3 连接到非法 DHCP 服务器，通过 GigabitEthernet2/1/2 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

启用 DHCP Snooping 功能。

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

设置 GigabitEthernet2/1/1 端口为信任端口。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] dhcp snooping trust
[RouterB-GigabitEthernet2/1/1] quit
```

在 GigabitEthernet2/1/2 上启用 DHCP Snooping 表项功能。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] dhcp snooping binding record
[RouterB-GigabitEthernet2/1/2] 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。

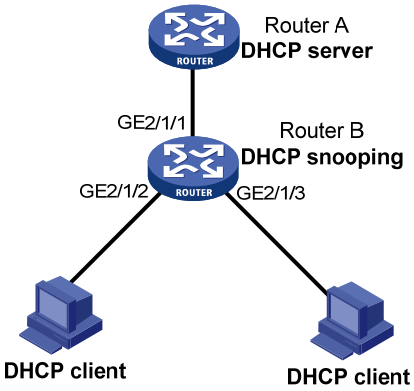
5.10.2 DHCP Snooping支持Option 82 配置举例

1. 组网需求

- Router B 上启用 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 GigabitEthernet2/1/2 上配置 Circuit ID 填充内容为 company001，Remote ID 填充内容为 device001；
- 在 GigabitEthernet2/1/3 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5-4 DHCP Snooping 支持 Option 82 配置示意图



3. 配置步骤

启用 DHCP Snooping 功能。

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

设置 GigabitEthernet2/1/1 端口为信任端口。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] dhcp snooping trust
[RouterB-GigabitEthernet2/1/1] quit
```

在 GigabitEthernet2/1/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] dhcp snooping information enable
[RouterB-GigabitEthernet2/1/2] dhcp snooping information strategy replace
[RouterB-GigabitEthernet2/1/2] dhcp snooping information circuit-id string company001
[RouterB-GigabitEthernet2/1/2] dhcp snooping information remote-id string device001
[RouterB-GigabitEthernet2/1/2] quit
```

在端口 GigabitEthernet2/1/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] dhcp snooping information enable
[RouterB-GigabitEthernet2/1/3] dhcp snooping information strategy replace
```

```
[RouterB-GigabitEthernet2/1/3] dhcp snooping information circuit-id verbose node-identifier sysname format ascii
[RouterB-GigabitEthernet2/1/3] 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 GigabitEthernet2/1/2 和 GigabitEthernet2/1/3 上 Option 82 的配置信息。

6 BOOTP客户端

BOOTP 客户端中对于接口的相关配置，目前只能在三层以太网接口（包括子接口）、三层聚合接口和 VLAN 接口上进行。

多个具有相同 MAC 地址的 VLAN 接口通过中继以 BOOTP 方式申请 IP 地址时，不能用 Windows 2000 Server 和 Windows 2003 Server 作为 BOOTP 服务器。

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

表6-1 配置接口通过 BOOTP 协议获取 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口通过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6-2 BOOTP 客户端显示和维护

操作	命令
显示BOOTP客户端的相关信息	**display bootp client** [**interface** *interface-type interface-number*]

6.4 BOOTP客户端典型配置举例

1. 组网需求

Router B 的以太网接口 GigabitEthernet2/1/1 接入局域网，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Router B的配置。

配置接口 GigabitEthernet2/1/1 通过 BOOTP 动态获取地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] 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“2.12 DHCP服务器典型配置举例”。

目 录

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。

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。

1.1.1 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。

1.1.2 动态域名解析

1. 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：

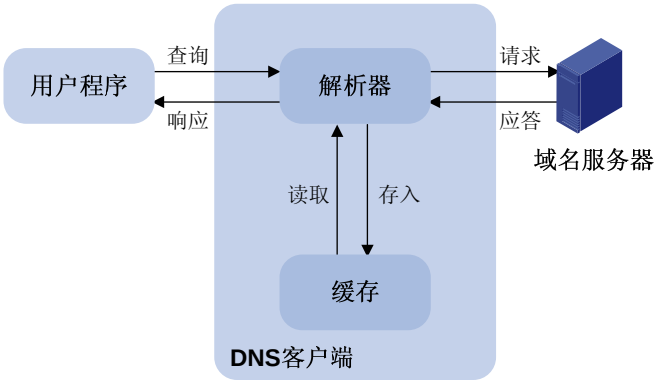
(1) 当用户使用域名进行某些应用时，用户程序首先向 DNS 客户端中的解析器发出请求。

(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；如果没有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。

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。

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。

2. 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）。

目前，设备支持静态域名解析和动态域名解析的 DNS 客户端功能。

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。

1.1.3 DNS代理

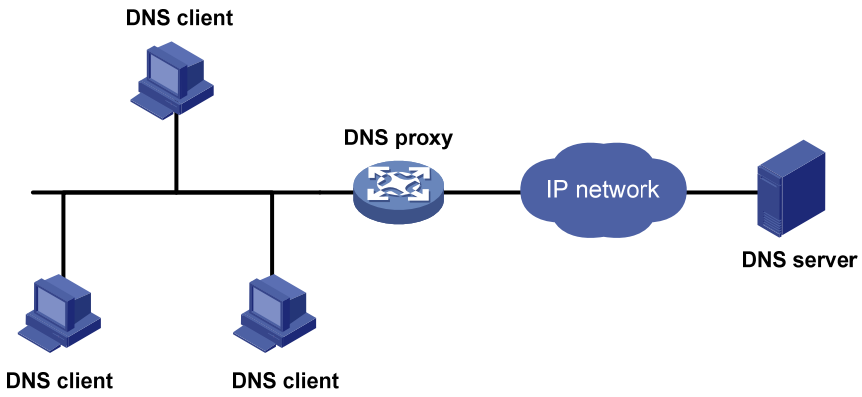
1. DNS代理简介

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



2. DNS代理的工作机制

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，即请求报文的目的地址为 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。

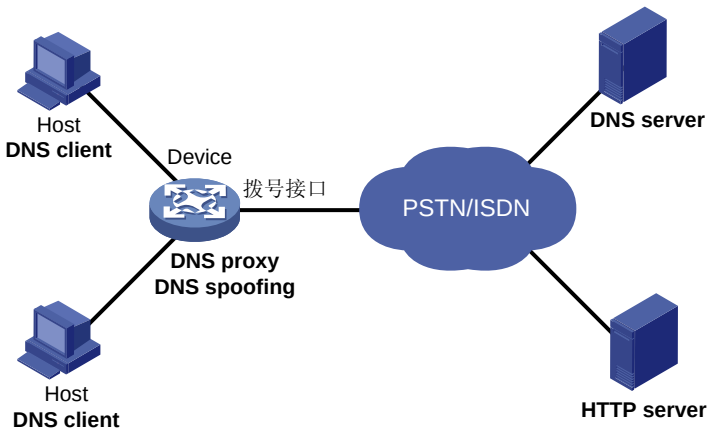
(3) 如果不存在请求的信息，则 DNS proxy 将报文转发给 DNS server，通过 DNS server 进行域名解析。

(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。

1.1.4 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 上没有使能 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“1.1.3 2. DNS代理的工作机制”。

(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

表1-1 域名解析配置任务简介

配置任务	说明	详细配置
配置IPv4 DNS client	二者必选其一	1.3
配置IPv6 DNS client		1.4
配置DNS proxy	可选	1.5
配置DNS spoofing	可选	1.6
配置DNS报文的源端口	可选	1.7
配置DNS信任接口	可选	1.8
配置DNS/IPv6 DNS报文的DSCP优先级	可选	1.9

1.3 配置IPv4 DNS client

1.3.1 配置静态域名解析

配置静态域名解析就是通过配置使主机名与 IPv4 地址相互对应。当使用 Telnet 等应用时，可以直接使用主机名，由系统解析为 IPv4 地址。

在配置静态域名解析时，需要注意：

- 在公网或单个 VPN 内，一个主机名只能对应一个 IPv4 地址。重复配置时，新的配置会覆盖原有配置。
- 公网或单个 VPN 内最多可以配置 1024 个主机名和 IPv4 地址的对应关系。可以同时在公网和最多 1024 个 VPN 内配置主机名和 IPv4 地址的对应关系。

表1-2 配置静态域名解析

操作	命令	说明
进入系统视图	**system-view**	-
配置主机名和对应的IPv4地址	**ip host** *host-name ip-address* [**vpn-instance** *vpn-instance-name*]	缺省情况下，静态域名解析表中不存在主机名及IPv4地址的对应关系

1.3.2 配置动态域名解析

1. 功能简介

如果用户要使用动态域名解析功能，则需要配置域名服务器的地址，这样才能将请求报文发送到正确的服务器进行解析。

用户还可以配置域名后缀，以便实现只输入域名的部分字段，而由系统自动加上预先设置的后缀进行解析。

2. 配置限制和指导

- 公网或单个 VPN 内最多可以配置 6 个域名服务器的 IPv4 地址。可以为公网和最多 1024 个 VPN 配置域名服务器的 IPv4 地址。
- 公网或单个 VPN 内最多可以配置 6 个域名服务器的 IPv6 地址。可以为公网和最多 1024 个 VPN 配置域名服务器的 IPv6 地址。
- 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。
- 域名服务器的优先级顺序为：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。
- 公网或单个 VPN 内最多可以配置 16 个域名后缀。可以为公网和最多 1024 个 VPN 配置域名后缀。
- 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。

3. 配置步骤

表1-3 配置动态域名解析

操作		命令	说明
进入系统视图		**system-view**	-
配置域名服务器地址	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，没有配置域名服务器的地址
	配置域名服务器的IPv6地址	**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	
（可选）配置域名后缀		**dns domain** *domain-name* [**vpn-instance** *vpn-instance-name*]	缺省情况下，没有配置域名后缀，即只根据用户输入的域名信息进行解析

1.4 配置IPv6 DNS client

1.4.1 配置静态域名解析

配置静态域名解析就是通过配置使主机名与 IPv6 地址相互对应。当使用 Telnet 等应用时，可以直接使用主机名，由系统解析为 IPv6 地址。

在配置静态域名解析时，需要注意：

- 在公网或同一个 VPN 内，一个主机名只能对应一个 IPv6 地址。重复配置时，新的配置会覆盖原有配置。
- 公网或单个 VPN 内最多可配置 1024 个主机名与 IPv6 地址的对应关系。可以为公网和最多 1024 个 VPN 配置主机名和 IPv6 地址的对应关系。

表1-4 配置静态域名解析

操作	命令	说明
进入系统视图	**system-view**	-
配置主机名和对应的IPv6地址	**ipv6 host** *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]	缺省情况下，静态域名解析表中不存在主机名及IPv6地址的对应关系

1.4.2 配置动态域名解析

1. 功能简介

如果用户要使用动态域名解析功能，则需要配置域名服务器的地址，这样才能将查询请求报文发送到正确的服务器进行解析。

用户还可以配置域名后缀，以便实现只输入域名的部分字段，而由系统自动加上预先设置的后缀进行解析。

2. 配置限制和指导

- 公网或单个 VPN 内最多可以配置 6 个域名服务器 IPv4 地址。可以为公网和最多 1024 个 VPN 配置域名服务器 IPv4 地址。
- 公网或单个 VPN 内最多可以配置 6 个域名服务器 IPv6 地址。可以为公网和最多 1024 个 VPN 配置域名服务器 IPv6 地址。
- 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：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，失败后再依次向其他域名服务器发送查询请求。
- 公网或单个 VPN 内最多可以配置 16 个域名后缀。最多可以为公网和 1024 个 VPN 配置域名后缀。
- 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，查询失败后再依次添加其他域名后缀。

3. 配置步骤

表1-5 配置动态域名解析

操作		命令	说明
进入系统视图		**system-view**	-
配置域名服务器地址	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，没有配置域名服务器的地址
	配置域名服务器的IPv6地址	**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	
（可选）配置域名后缀		**dns domain** *domain-name* [**vpn-instance** *vpn-instance-name*]	缺省情况下，没有配置域名后缀，即只根据用户输入的域名信息进行解析

1.5 配置DNS proxy

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。

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。

表1-6 配置 DNS proxy

操作		命令	说明
进入系统视图		**system-view**	-
开启DNS proxy功能		**dns proxy enable**	缺省情况下，DNS proxy功能处于关闭状态
配置域名服务器地址	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，没有配置域名服务器的地址
	配置域名服务器的IPv6地址	**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	

1.6 配置DNS spoofing

1. 配置准备

只有在以下条件均满足的情况下，DNS spoofing 功能才会生效：

- 设备上启用了 DNS proxy 功能
- 设备上没有指定域名服务器地址或不存在到达域名服务器的路由

因此，配置 DNS spoofing 前，需要先启用 DNS proxy 功能。

配置 DNS spoofing 功能时，需要注意：

- 公网或单个 VPN 内只能配置 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。
- 可以为公网和最多 1024 个 VPN 配置 DNS spoofing 功能。

2. 配置步骤

表1-7 配置 DNS spoofing

操作		命令	说明
进入系统视图		**system-view**	-
启用DNS proxy功能		**dns proxy enable**	缺省情况下，DNS proxy功能处于关闭状态
指定DNS spoofing应答地址	指定DNS spoofing应答的IPv4地址	**dns spoofing** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，没有指定DNS spoofing应答地址
	指定DNS spoofing应答的IPv6地址	**ipv6 dns spoofing** *ipv6-address* [**vpn-instance** *vpn-instance-name*]	

1.7 配置DNS报文的源接口

提示

无论配置的源接口是否属于指定的 VPN，该配置都会生效。不建议为 VPN 配置不属于该 VPN 的接口作为源接口。否则，设备会使用不属于该 VPN 的地址作为 DNS 报文源地址，导致无法收到 DNS 应答。

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。

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。如果源接口上没有配置对应的地址，则将导致报文发送失败。

公网或单个 VPN 内只能配置 1 个源接口。重复配置时，新的配置会覆盖原有配置。可以为公网和最多 1024 个 VPN 配置源接口。

表1-8 配置 DNS 报文的源接口

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
指定DNS报文的源接口	**dns source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定DNS报文的源接口

1.8 配置DNS信任接口

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。

表1-9 配置 DNS 信任接口

操作	命令	说明
进入系统视图	**system-view**	-
指定DNS信任接口	**dns trust-interface** *interface-type interface-number*	缺省情况下，没有指定任何接口为信任接口

说明

设备最多可以配置 128 个 DNS 信任接口。

1.9 配置DNS报文的DSCP优先级

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。

本命令的配置同时用于 DNS 客户端和 DNS proxy。

表1-10 配置 DNS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DNS报文的DSCP优先级	**dns dscp** *dscp-value*	缺省情况下，DNS报文的DSCP优先级为0，IPv6 DNS报文的DSCP优先级为0
配置IPv6 DNS报文的DSCP优先级	**ipv6 dns dscp** *dscp-value*	

1.10 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1-11 域名解析显示和维护

操作	命令
显示域名解析表信息	**display dns host** [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]
显示域名服务器的IPv4地址信息	**display dns server** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
显示域名服务器的IPv6地址信息	**display ipv6 dns server** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
显示域名后缀信息	**display dns domain** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
清除动态域名解析缓存信息	**reset dns host** [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

1.11 IPv4域名解析典型配置举例

1.11.1 静态域名解析配置举例

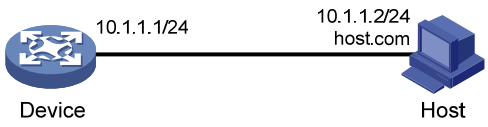
1. 组网需求

为了避免记忆复杂的 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
```

1.11.2 动态域名解析配置举例

1. 组网需求

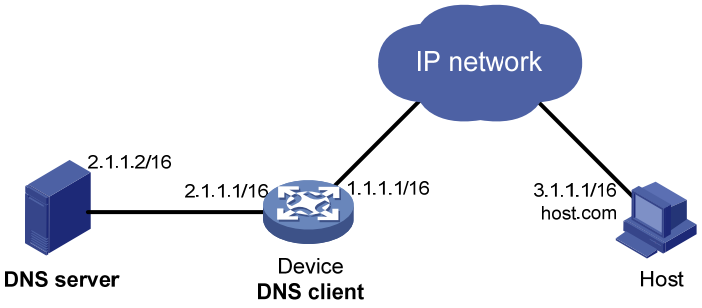
为了避免记忆复杂的 IP 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

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 2000 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。

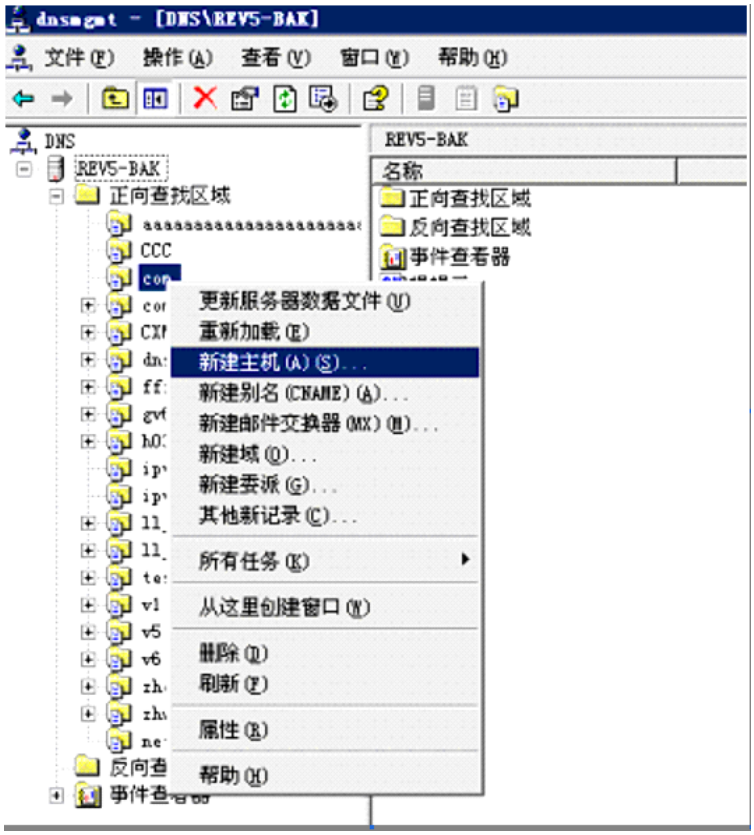
如 图 1-6 所示，右键点击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

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

(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
```

1.11.3 DNS proxy典型配置举例

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。

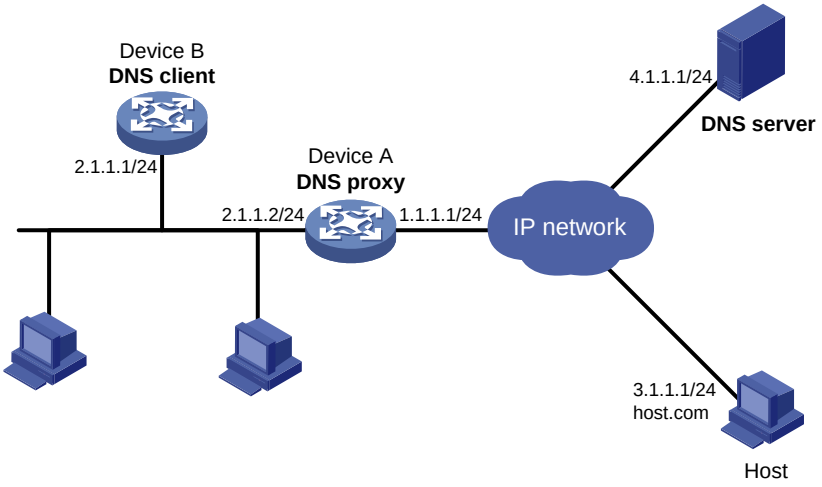
在本例中，具体配置步骤为：

(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 2000 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 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
```

1.12 IPv6域名解析典型配置举例

1.12.1 静态域名解析配置举例

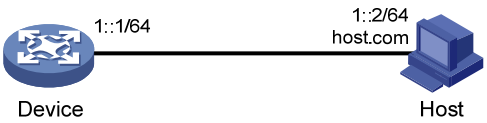
1. 组网需求

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
```

1.12.2 动态域名解析配置举例

1. 组网需求

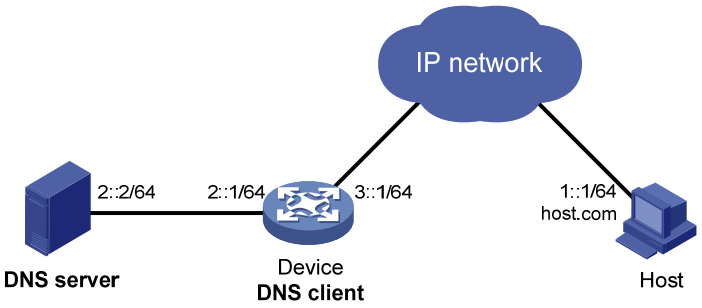
为了避免记忆复杂的 IPv6 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

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 2003 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。

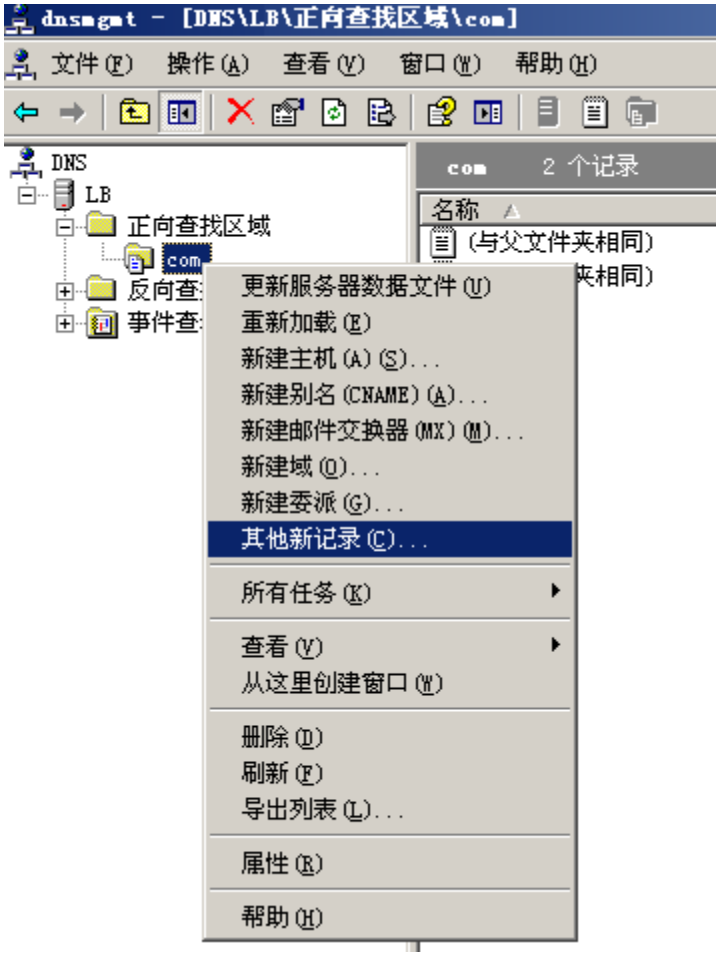
如 图 1-12 所示，右键点击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

图1-12 创建区域

添加域名和 IPv6 地址的映射。

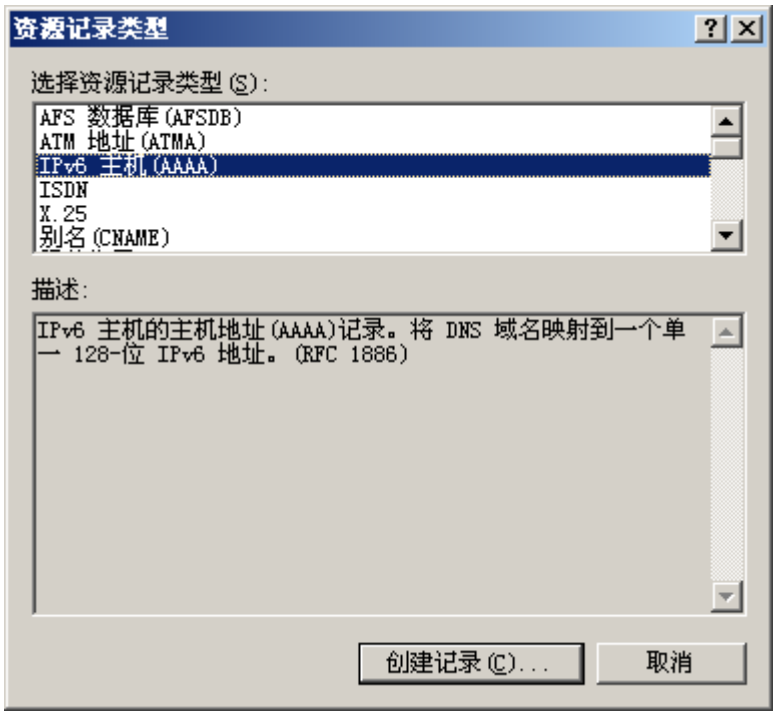
如 图 1-13 所示，右键点击区域[com]。

图1-13 创建记录



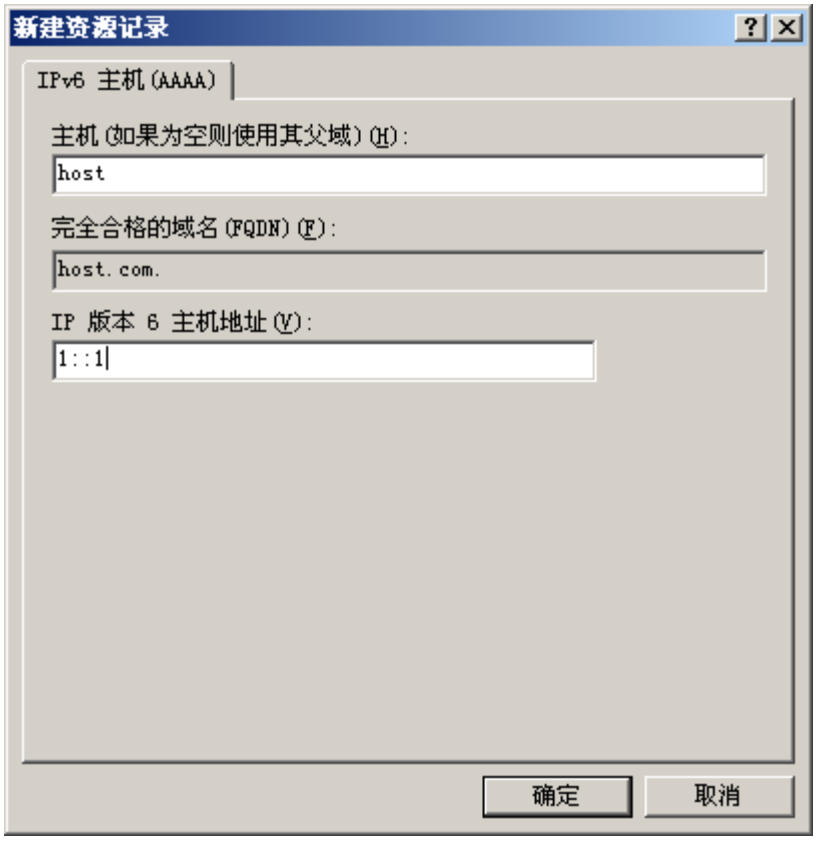
选择[其他新记录]，弹出如 图 1-14 的对话框，选择资源记录类型为“IPv6 主机（AAAA）”。

图1-14 选择资源记录类型



按照 图 1-15 输入域名host和IPv6 地址 1::1。点击<确定>按钮，添加域名和IPv6 地址的映射。

图1-15 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
```

1.12.3 DNS proxy典型配置举例

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。

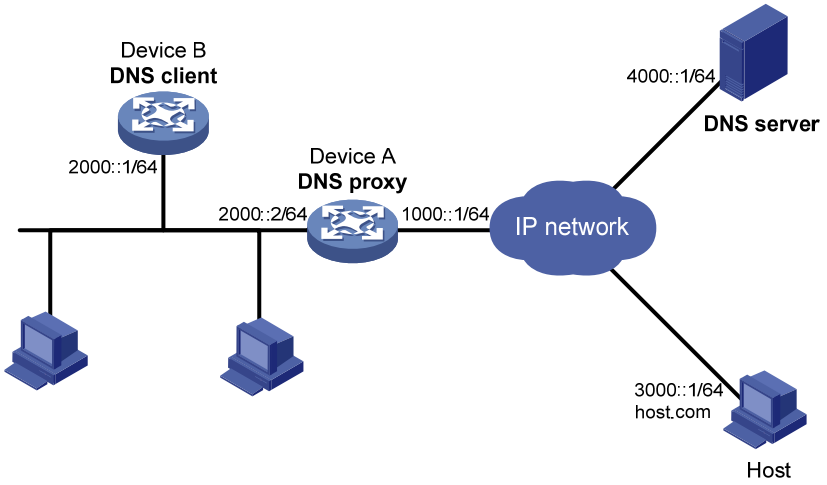
在本例中，具体配置步骤为：

(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1-16 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 2003 作为域名服务器时，配置方法请参见“1.12.2 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
```

1.13 常见配置错误举例

1.13.1 IPv4 域名解析常见配置错误举例

1. 现象描述

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. 故障排除

- 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。

1.13.2 IPv6 域名解析常见配置错误举例

1. 现象描述

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. 故障排除

- 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。

2 DDNS

2.1 DDNS简介

2.1.1 概述

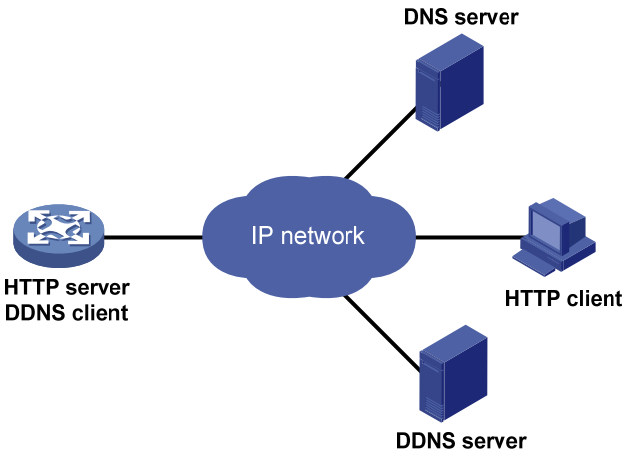
利用 DNS 可以将域名解析为 IP 地址，从而实现使用域名来访问网络中的节点。但是，DNS 仅仅提供了域名和 IP 地址之间的静态对应关系，当节点的 IP 地址发生变化时，DNS 无法动态地更新域名和 IP 地址的对应关系。此时，如果仍然使用域名访问该节点，通过域名解析得到的 IP 地址是错误的，从而导致访问失败。

DDNS（Dynamic Domain Name System，动态域名系统）用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。

目前，只有 IPv4 域名解析支持 DDNS，IPv6 域名解析不支持 DDNS，即只能通过 DDNS 动态更新域名和 IPv4 地址之间的对应关系。

2.1.2 DDNS典型组网应用

图2-1 DDNS 典型组网图



DDNS的典型组网环境如 图 2-1 所示，DDNS采用客户端/服务器模式：

- DDNS 客户端：IP 地址变化时，需要在 DNS 服务器上动态更新其域名和 IP 地址对应关系的设备。Internet 用户通常通过域名访问提供应用层服务的服务器，如 HTTP、FTP 服务器。为了保证 IP 地址变化时，仍然可以通过域名访问这些服务器，当服务器的 IP 地址发生变化时，服务器将作为 DDNS 客户端，向 DDNS 服务器发送更新域名和 IP 地址对应关系的 DDNS 更新请求。
- DDNS 服务器：负责通知 DNS 服务器动态更新域名和 IP 地址之间的对应关系。接收到 DDNS 客户端的更新请求后，DDNS 服务器通知 DNS 服务器重新建立 DDNS 客户端的域名和 IP 地址之间的对应关系。从而保证即使 DDNS 客户端的 IP 地址改变，Internet 用户仍然可以通过同样的域名访问 DDNS 客户端。

说明

- 目前，DDNS 更新过程没有统一的标准，向不同的 DDNS 服务器请求更新的过程各不相同。
- 设备可以作为 DDNS 客户端，通过 www.3322.org(www.pubyun.com)、花生壳等 DDNS 服务器动态更新 DNS 服务器上域名和 IP 地址之间的对应关系。

2.2 设备作为DDNS客户端配置任务简介

表2-1 设备作为 DDNS 客户端配置任务简介

配置任务	说明	详细配置
配置DDNS策略	必选	2.3
在接口上应用DDNS策略	必选	2.4
配置DDNS报文的DSCP优先级	可选	2.5

2.3 配置DDNS策略

1. 功能简介

DDNS 策略是 DDNS 服务器的地址、端口号、登录用户名、密码、时间间隔、关联的 SSL 客户端策略和更新时间间隔等信息的集合。创建 DDNS 策略后，可以在不同的接口上应用相同的 DDNS 策略，从而简化 DDNS 的配置。

2. 配置限制和指导

设备向不同DDNS服务器请求更新的过程各不相同，因此，DDNS更新请求的URL地址的配置方式也存在差异，如 表 2-2 所示。

表2-2 常见的 DDNS 更新请求 URL 地址格式列表

DDNS 服务器	DDNS 更新请求的 URL 地址格式
www.3322.org(www.pubyun.com)	http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
DYNDNS	http://members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
DYNS	http://www.dyns.cx/postscript.php?host=<h>&ip=<a>
ZONEEDIT	http://dynamic.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
TZO	http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>IPAddress=<a>
EASYDNS	http://members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&host_id=<h>
HEIPV6TB	http://dyn.dns.he.net/nic/update?hostname=<h>&myip=<a>
CHANGE-IP	http://nic.changeip.com/nic/update?hostname=<h>&offline=1
NO-IP	http://dynupdate.no-ip.com/nic/update?hostname=<h>&myip=<a>

DDNS 服务器	DDNS 更新请求的 URL 地址格式
DHS	http://members.dhs.org/nic/hosts?domain=dyn.dhs.org&hostname=<h>&hostscmd=edit&hostscmdstage=2&type=1&ip=<a>
HP	https://server-name/nic/update?group=group-name&myip=<a>
ODS	ods://update.ods.org
GNUDIP	gnudip://*server-name*
花生壳	oray://phservice2.oray.net

其中：

- URL 地址中不支持携带用户名和密码，配置用户名和密码请配合 **username** 和 **password** 命令使用，请根据实际情况修改。
- HP 和 GNUDIP 是通用的 DDNS 更新协议，*server-name* 是使用对应 DDNS 更新协议的服务提供商的服务器域名或地址。
- DDNS 更新请求的 URL 地址可以以“http://”开头，表示基于 HTTP 与 DDNS 服务器通信；以“https://”开头，表示基于 HTTPS 与 DDNS 服务器通信；以“ods://”开头，表示基于 TCP 与 ODS 服务器通信；以“gnudip://”开头，表示基于 TCP 与 GNUDIP 服务器通信；以“oray://”开头，表示基于 TCP 与花生壳 DDNS 服务器通信。
- members.3322.org 和 phservice2.oray.net 是服务提供商提供 DDNS 服务的域名。花生壳提供 DDNS 服务的域名可能是 phservice2.oray.net、phddns60.oray.net、client.oray.net 和 ph031.oray.net 等，请根据实际情况修改域名。
- URL 地址中的端口号是可选项，如果不包含端口号则使用缺省端口号：HTTP 是 80，HTTPS 是 443，花生壳 DDNS 服务器是 6060。
- <h>由系统根据接口上应用DDNS策略时指定的FQDN自动填写，<a>由系统根据应用DDNS策略的接口的主IP地址自动填写。用户也可以手工输入需要更新的FQDN和IP地址，代替URL中的<h>和<a>，此时，应用DDNS策略时指定的FQDN将不会生效。建议不要修改URL中的<h>和<a>，以免配置错误的FQDN和IP地址。应用DDNS策略的详细介绍，请参见“2.4 在接口上应用DDNS策略”。
- 花生壳 DDNS 服务器的 URL 地址中不能指定用于更新的 FQDN 和 IP 地址。用户可在接口上应用 DDNS 策略时指定 FQDN；用于更新的 IP 地址是应用 DDNS 策略的接口的主 IP 地址。

说明

FQDN 是节点在网络中的唯一标识，由主机名和域名组成，可被解析为 IP 地址。

3. 配置准备

登录 DDNS 服务提供商的网站，注册帐户，并为 DDNS 客户端申请域名。通过 DDNS 服务器更新域名和 IP 地址的对应关系时，DDNS 服务器将检查 DDNS 更新请求中的帐户信息是否正确、需要更新的域名是否属于该帐户。

4. 配置步骤

与 DHS 通信时，需要通过 **method** 命令指定 HTTP 使用 http-post 参数传输方式进行 DDNS 更新。

基于 HTTPS 与 DDNS 服务器通信时，需要通过 **ssl client policy** 命令指定与 DDNS 策略关联的 SSL 客户端策略，SSL 客户端策略的配置方法请参见“安全配置指导”中的“SSL”。

表2-3 配置 DDNS 策略

操作	命令	说明
进入系统视图	**system-view**	-
创建DDNS策略，并进入DDNS策略视图	**ddns policy** *policy-name*	缺省情况下，设备上不存在任何DDNS策略
指定DDNS更新请求的URL地址	**url** *request-url*	缺省情况下，未指定DDNS更新请求的URL地址
指定DDNS更新请求的URL地址中的用户名	**username** *username*	缺省情况下，未指定DDNS更新请求的URL地址中的用户名
指定DDNS更新请求的URL地址中的密码	**password** { **cipher** | **simple** } *password*	缺省情况下，未指定DDNS更新请求的URL地址中的密码
（可选）配置DDNS更新请求的方法	**method** { **http-get** | **http-post** }	缺省情况下，使用**http-get**方法 本命令仅在基于HTTP或HTTPS与DDNS服务器通信时生效
（可选）指定与DDNS策略关联的SSL客户端策略	**ssl-client-policy** *policy-name*	缺省情况下，未指定与DDNS策略关联的SSL客户端策略 SSL客户端策略只对URL为HTTPS地址的DDNS更新请求有效
（可选）指定DDNS更新启动后，定时发起更新请求的时间间隔	**interval** *days* [*hours* [*minutes*]]	缺省情况下，定时发起DDNS更新请求的时间间隔是1小时

2.4 在接口上应用DDNS策略

在接口上应用 DDNS 策略，并指定需要更新的 FQDN 与 IP 地址对应关系后，DDNS 客户端才会向 DDNS 服务器发起更新域名和接口主 IP 地址对应关系的请求。

1. 配置准备

- 配置该接口的主 IP 地址，使之与 DDNS 服务器路由可达。
- 配置IPv4 静态或动态域名解析功能，以便将DDNS服务器的域名解析为IP地址。域名解析功能的配置方法请参见“1.3 配置IPv4 DNS client”。

2. 配置步骤

表2-4 配置接口应用 DDNS 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
在接口上应用指定的DDNS策略来更新指定的FQDN与IP地址的对应关系，并启动DDNS更新	**ddns apply policy** *policy-name* [**fqdn** *domain-name*]	除花生壳DDNS服务器外，其他的DDNS服务器均需要指定更新的FQDN，否则会导致DDNS更新失败 缺省情况下，没有为接口指定任何DDNS策略和需要更新的FQDN，且未启动DDNS更新

对于花生壳 DDNS 服务器，如果没有指定更新的 FQDN，则 DDNS 服务器将更新 DDNS 客户端的帐户对应的所有域名；如果指定了更新的 FQDN，则 DDNS 服务器只更新指定的 FQDN。

2.5 配置DDNS报文的DSCP优先级

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 DDNS 服务器发送的 DDNS 报文的 DSCP 优先级。

表2-5 配置 DDNS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DDNS报文的DSCP优先级	**ddns dscp** *dscp-value*	缺省情况下，DDNS报文的DSCP优先级为0

2.6 DDNS显示和维护

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

表2-6 DDNS 显示和维护

操作	命令
显示DDNS策略的配置情况	**display ddns policy** [*policy-name*]

2.7 DDNS典型配置举例

2.7.1 与www.3322.org(www.pubyun.com)互通的配置举例

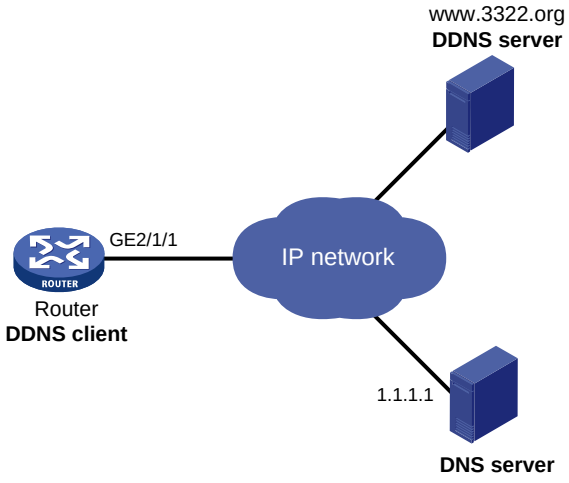
1. 组网需求

- Router 为 Internet 上的用户提供 Web 服务，使用的域名为 whatever.3322.org。

- Router 通过 DHCP 获得 IP 地址，为保证 Router 的 IP 地址变化后，Internet 上的用户仍然可以利用域名 whatever.3322.org 访问 Router，Router 通过 www.3322.org 提供的 DDNS 服务及时通知 DNS 服务器更新域名和 IP 地址的对应关系。
- DNS 服务器的 IP 地址为 1.1.1.1。Router 通过该 DNS 服务器将 DDNS 服务器的域名 www.3322.org(www.pubyun.com)解析为 IP 地址。

2. 组网图

图2-2 与 www.3322.org(www.pubyun.com)互通配置举例组网图



3. 配置步骤

说明

配置之前，请登录 http://www.3322.org(www.pubyun.com)申请帐户（帐户名为 steven，密码为 nevets），在 DNS 服务器上创建域名和 IP 地址的对应关系，并保证各个设备之间的路由可达。

创建名称为 3322.org 的 DDNS 策略，并进入 DDNS 策略视图。

```
<Router> system-view
[Router] ddns policy 3322.org
```

为 DDNS 策略 3322.org 指定 DDNS 更新请求的 URL 地址，登录用户名为 steven，密码为明文字段 nevets。

```
[Router-ddns-policy-3322.org] url http://
members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
[Router-ddns-policy-3322.org] username steven
[Router-ddns-policy-3322.org] password simple nevets
```

为 DDNS 策略 3322.org 指定定时发起更新请求的时间间隔为 15 分钟。

```
[Router-ddns-policy-3322.org] interval 0 0 15
[Router-ddns-policy-3322.org] quit
```

配置 DNS 服务器的 IP 地址为 1.1.1.1。

```
[Router] dns server 1.1.1.1
```

在 GigabitEthernet2/1/1 接口下指定应用 DDNS 策略 3322.org，更新域名 whatever.3322.org 与接口主 IP 地址的对应关系，并启动 DDNS 更新功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ddns apply policy 3322.org fqdn whatever.3322.org
```

配置完成后，Router 的接口 IP 地址变化时，它将通过 DDNS 服务提供商 www.3322.org(www.pubyun.com)通知 DNS 服务器建立域名 whatever.3322.org 和新的 IP 地址的对应关系，从而保证 Internet 上的用户可以通过域名 whatever.3322.org 解析到最新的 IP 地址，访问 Router 提供的 Web 服务。

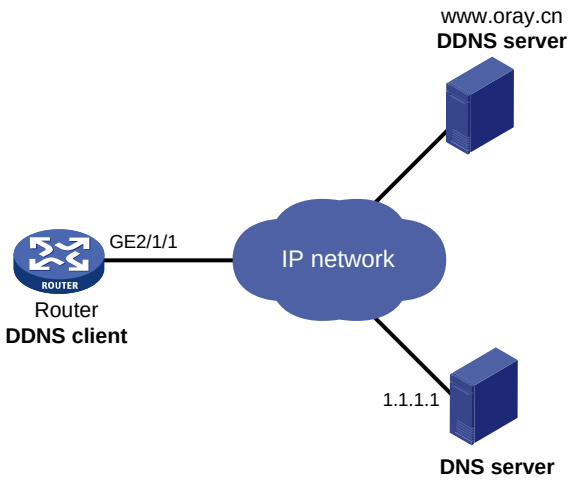
2.7.2 与花生壳DDNS服务器互通的配置举例

1. 组网需求

- Router 为 Internet 上的用户提供 Web 服务，使用的域名为 whatever.gicp.cn。
- Router 通过 DHCP 获得 IP 地址，为保证 Router 的 IP 地址变化后，Internet 上的用户仍然可以利用域名 whatever.gicp.cn 访问 Router，Router 通过花生壳提供的 DDNS 服务及时通知 DNS 服务器更新域名和 IP 地址的对应关系。
- DNS 服务器的 IP 地址为 1.1.1.1。Router 通过该 DNS 服务器将花生壳 DDNS 服务器的域名解析为 IP 地址。

2. 组网图

图2-3 与花生壳 DDNS 服务器互通配置举例组网图



3. 配置步骤

说明

配置之前，请登录 http://www.oray.cn 申请帐户（用户名为 steven，密码为 nevets），在 DNS 服务器上创建域名和 IP 地址的对应关系，并保证各个设备之间的路由可达。

创建名称为 oray.cn 的 DDNS 策略，并进入 DDNS 策略视图。

```
<Router> system-view
```

```
[Router] ddns policy oray.cn
```
为 DDNS 策略 oray.cn 指定 DDNS 更新请求的 URL 地址，登录用户名为 steven，密码为明文字段 nevets。
```
[Router-ddns-policy-oray.cn] url oray://phservice2.oray.net
[Router-ddns-policy-oray.cn] username steven
[Router-ddns-policy-oray.cn] password simple nevets
```
为 DDNS 策略 oray.cn 指定定时发起更新请求的时间间隔为 12 分钟。
```
[Router-ddns-policy-oray.cn] interval 0 0 12
[Router-ddns-policy-oray.cn] quit
```
配置 DNS 服务器的 IP 地址为 1.1.1.1。
```
[Router] dns server 1.1.1.1
```
在 GigabitEthernet2/1/1 接口下指定应用 DDNS 策略 oray.cn，更新域名 whatever.gicp.cn 与接口主 IP 地址的对应关系，并启动 DDNS 更新功能。
```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ddns apply policy oray.cn fqdn whatever.gicp.cn
```
配置完成后，Router 的接口 IP 地址变化时，它将通过花生壳 DDNS 服务器通知 DNS 服务器建立域名 whatever.gicp.cn 和新的 IP 地址的对应关系，从而保证 Internet 上的用户可以通过域名 whatever.gicp.cn 解析到最新的 IP 地址，访问 Router 提供的 Web 服务。

目 录

1 NAT

1.1 NAT简介

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。

NAT 可以让少量的外网网络 IP 地址代表较多的内部网络 IP 地址，这种地址转换能力具备以下优点：

- 私有网络内部的通信利用私网地址，如果私有网络需要与外部网络通信或访问外部资源，则可通过将大量的私网地址转换成少量的公网地址来实现，这在一定程度上缓解了 IPv4 地址空间日益枯竭的压力。
- 地址转换可以利用端口信息，将私网地址和端口作为地址端口对映射成公网地址和端口组合，使得多个私网用户可共用一个公网地址与外部网络通信，节省了公网地址。
- 通过静态映射，不同的内部服务器可以映射到同一个公网地址。外部用户可通过公网地址和端口访问不同的内部服务器，同时还隐藏了内部服务器的真实 IP 地址，从而防止外部对内部服务器乃至内部网络的攻击。
- 方便网络管理，例如私网服务器迁移时，无需过多配置的改变，仅仅通过调整内部服务器的映射表就可将这一变化体现出来。

1.1.1 NAT工作机制

配置了 NAT 功能的连接内部网络和外部网络的边缘设备，通常被称为 NAT 设备。当内部网络访问外部网络的报文经过 NAT 设备时，NAT 设备会用一个合法的公网地址替换原报文中的源 IP 地址，并对这种转换进行记录；之后，当报文从外网侧返回时，NAT 设备查找原有的记录，将报文的目的地址再替换回原来的私网地址，并转发给内网侧主机。这个过程，在私网侧或公网侧设备看来，与普通的网络访问并没有任何的区别。

1. 基本概念

- NAT 接口：NAT 设备上应用了 NAT 相关配置的接口。
- NAT 地址：用于进行地址转换的 IP 地址，与外部网络路由可达，可静态指定或动态分配。
- NAT 表项：NAT 设备上用于记录网络地址转换映射关系的表项。
- Easy IP 功能：NAT 转换时直接使用设备上接口的 IP 地址作为 NAT 地址。设备上接口的地址可通过 DHCP 或 PPPoE 等协议动态获取，因此对于支持 Easy IP 的 NAT 配置，不直接指定 NAT 地址，而是指定对应的接口或当前接口。

2. NAT的基本组网类型

(1) 传统 NAT

报文经过 NAT 设备时，在 NAT 接口上仅进行一次源 IP 地址转换或一次目的 IP 地址转换。对于内网访问外网的报文，在出接口上进行源 IP 地址转换；对于外网访问内网的报文，在入接口上进行目的地址 IP 地址转换。

(2) 两次 NAT

报文入接口和出接口均为 NAT 接口。报文经过 NAT 设备时，先后进行两次 NAT 转换。对于内网访问外网的报文和外网访问内网的报文，均在入接口进行目的 IP 地址转换，在出接口进行源 IP 地址转换。这种方式常用于支持地址重叠的 VPN 间互访。

(3) 双向 NAT

报文经过 NAT 设备时，在 NAT 接口上同时进行一次源 IP 地址转换和一次目的 IP 地址转换。对于内网访问外网的报文，在出接口上同时进行源 IP 地址和目的 IP 地址的转换；对于外网访问内网的报文，同时在入接口上进行目的地址 IP 地址和源 IP 地址的转换。这种方式常用于支持内网用户主动访问与之地址重叠的外网资源。

(4) NAT hairpin

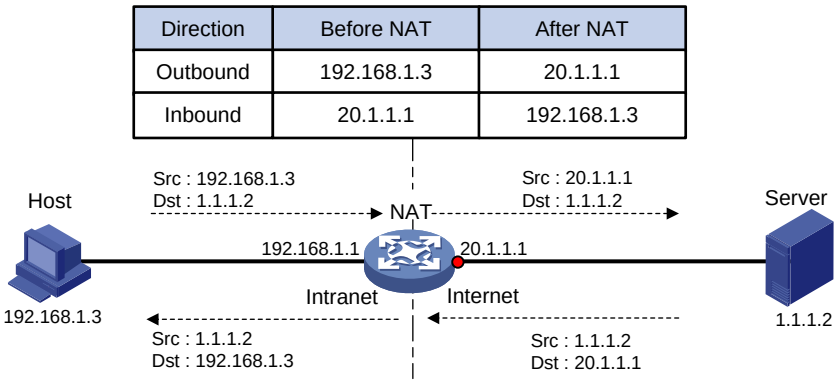
NAT hairpin 功能用于满足位于内网侧的用户之间或内网侧的用户与服务器之间通过 NAT 地址进行访问的需求。使能 NAT hairpin 的内网侧接口上会对报文同时进行源地址和目的地址的转换。它支持两种组网模式：

- P2P：位于内网侧的用户之间通过动态分配的 NAT 地址互访。
- C/S：位于内网侧的用户使用静态配置的 NAT 地址访问内网服务器。

3. 传统NAT的典型工作过程

如 图 1-1 所示，一台NAT设备连接内网和外网，连接外网的接口为NAT接口，当有报文经过NAT设备时，NAT的基本工作过程如下。

图1-1 NAT 基本工作过程示意图



(1) 当内网用户主机（192.168.1.3）向外网服务器（1.1.1.2）发送的 IP 报文通过 NAT 设备时，NAT 设备查看报文的 IP 头内容，发现该报文是发往外网的，则将其源 IP 地址字段的内网地址 192.168.1.3 转换成一个可路由的外网地址 20.1.1.1，并将该报文发送给外网服务器，同时在 NAT 设备上建立表项记录这一映射。

(2) 外网服务器给内网用户发送的应答报文到达 NAT 设备后，NAT 设备使用报文信息匹配建立的表项，然后查找匹配到的表项记录，用内网私有地址 192.168.1.3 替换初始的目的 IP 地址 20.1.1.1。

上述的 NAT 过程对终端（如图中的 Host 和 Server）来说是透明的。对外网服务器而言，它认为内网用户主机的 IP 地址就是 20.1.1.1，并不知道有 192.168.1.3 这个地址。因此，NAT“隐藏”了企业的私有网络。

1.1.2 NAT转换控制

在实际应用中，我们可能希望某些内部网络的主机可以访问外部网络，而某些主机不允许访问；或者希望某些外部网络的主机可以访问内部网络，而某些主机不允许访问。即 NAT 设备只对符合要求的报文进行地址转换。

NAT 设备可以利用 ACL（Access Control List，访问控制列表）来对地址转换的使用范围进行控制，通过定义 ACL 规则，并将其与 NAT 配置相关联，实现只对匹配指定的 ACL permit 规则的报文才进行地址转换的目的。而且，NAT 仅使用规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例这几个元素进行报文匹配，忽略其它元素。

1.1.3 NAT实现方式

1. 静态方式

静态地址转换是指外部网络和内部网络之间的地址映射关系由配置确定，该方式适用于内部网络与外部网络之间存在固定访问需求的组网环境。静态地址转换支持双向互访：内网用户可以主动访问外网，外网用户也可以主动访问内网。

2. 动态方式

动态地址转换是指内部网络和外部网络之间的地址映射关系在建立连接的时候动态产生。该方式通常适用于内部网络有大量用户需要访问外部网络的组网环境。动态地址转换存在两种转换模式：

- NO-PAT 模式

NO-PAT（Not Port Address Translation）模式下，一个外网地址同一时间只能分配给一个内网地址进行地址转换，不能同时被多个内网地址共用。当使用某外网地址的内网用户停止访问外网时，NAT 会将其占用的外网地址释放并分配给其他内网用户使用。

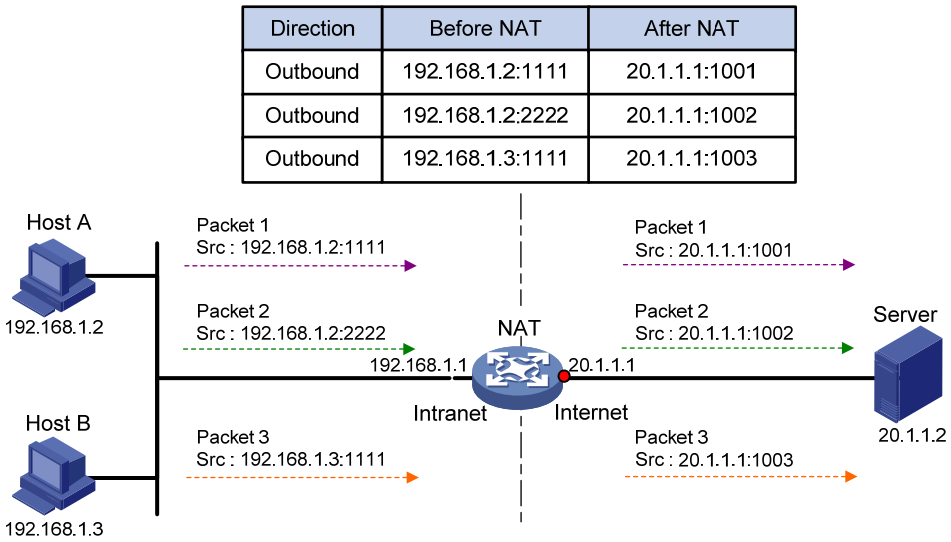
该模式下，NAT 设备只对报文的 IP 地址进行 NAT 转换，同时会建立一个 NO-PAT 表项用于记录 IP 地址映射关系，并可支持所有 IP 协议的报文。

- PAT 模式

PAT（Port Address Translation）模式下，一个 NAT 地址可以同时分配给多个内网地址共用。该模式下，NAT 设备需要对报文的 IP 地址和传输层端口同时进行转换，且只支持 TCP、UDP 和 ICMP（Internet Control Message Protocol，因特网控制消息协议）查询报文。

图 1-2 描述了PAT的基本原理。

图1-2 PAT 基本原理示意图



如 图 1-2 所示，三个带有内网地址的报文到达NAT设备，其中报文 1 和报文 2 来自同一个内网地址但有不同的源端口号，报文 1 和报文 3 来自不同的内网地址但具有相同的源端口号。通过PAT映射，三个报文的源IP地址都被转换为同一个外网地址，但每个报文都被赋予了不同的源端口号，因而仍保留了报文之间的区别。当各报文的回应报文到达时，NAT设备仍能够根据回应报文的目的IP地址和目的端口号来区别该报文应转发到的内部主机。

采用 PAT 方式可以更加充分地利用 IP 地址资源，实现更多内部网络主机对外部网络的同时访问。目前，PAT 支持两种不同的地址转换模式：

- Endpoint-Independent Mapping（不关心对端地址和端口转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过 PAT 映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个 EIM 表项；并且 NAT 设备允许所有外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同 NAT 网关之后的主机进行互访。
- Address and Port-Dependent Mapping（关心对端地址和端口转换模式）：对于来自相同源地址和源端口号的报文，相同的源地址和源端口号并不要求被转换为相同的外部地址和端口号，若其目的地址或目的端口号不同，通过 PAT 映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。与 Endpoint-Independent Mapping 模式不同的是，NAT 设备只允许这些目的地址对应的外部网络的主机可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但由于同一个内网主机地址转换后的外部地址不唯一，因此不便于位于不同 NAT 网关之后的主机使用内网主机转换后的地址进行互访。

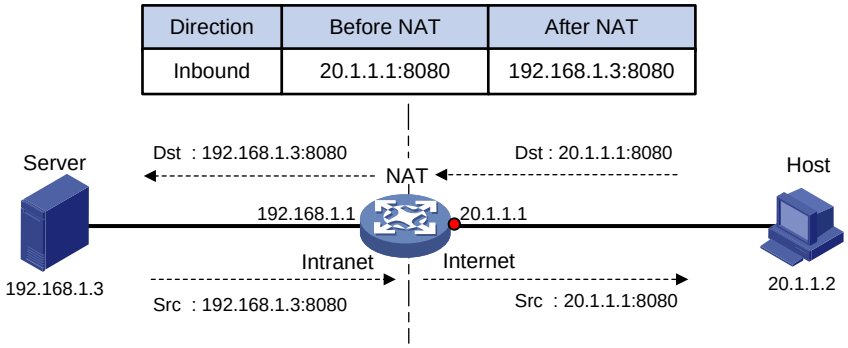
3. 内部服务器

在实际应用中，内网中的服务器可能需要对外部网络提供一些服务，例如给外部网络提供 Web 服务，或是 FTP 服务。这种情况下，NAT 设备允许外网用户通过指定的 NAT 地址和端口访问这些内部服务器，NAT 内部服务器的配置就定义了 NAT 地址和端口与内网服务器地址和端口的映射关系。

如 图 1-3 所示，外部网络用户访问内部网络服务器的数据报文经过NAT设备时，NAT设备将报文的目的地址与接口上的NAT内部服务器配置进行匹配，并将匹配上的访问内部服务器的请求报文的目

的IP地址和端口号转换成内部服务器的私有IP地址和端口号。当内部服务器回应该报文时，NAT设备再根据已有的地址映射关系将回应报文的源IP地址和端口号转换成外网IP地址和端口号。

图1-3 内部服务器基本原理示意图

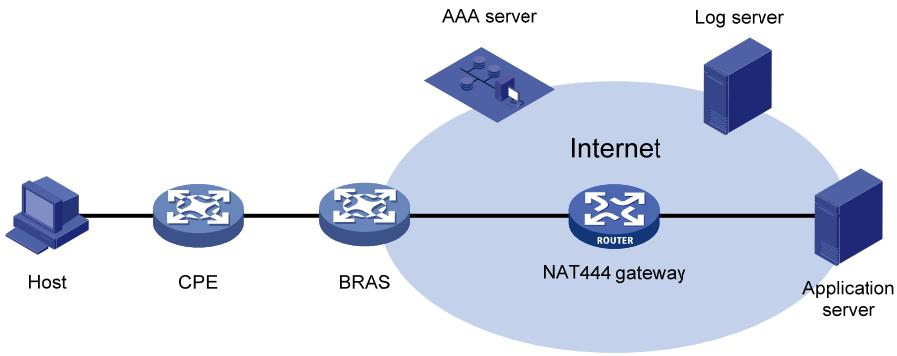


4. NAT444 端口块方式

NAT444 是运营商网络部署 NAT 转换的整体解决方案，它基于 NAT444 网关，结合 AAA 服务器、日志服务器等配套系统，提供运营商级的 NAT 转换，并支持用户溯源等功能。在众多 IPv4 向 IPv6 网络过渡的技术中，NAT444 仅需在运营商侧引入二次 NAT，对终端和服务的更改较小，并且 NAT444 通过端口块分配方式解决用户溯源等问题，因此成为了运营商的首选过渡方案。

NAT444 解决方案的架构如 图 1-4 所示。

图1-4 NAT444 解决方案架构



- CPE：实现用户侧地址转换。
- BRAS：负责接入终端，并配合 AAA 完成用户认证、授权和计费。
- NAT444 网关：实现运营商级地址转换。
- AAA 服务器：负责用户认证、授权和计费等。
- 日志服务器：接受和记录用户访问信息，响应用户访问信息查询。

NAT444 网关设备进行的地址转换（以下称为“NAT444 地址转换”）是一种 PAT 方式的动态地址转换，但与普通动态地址转换不同的是，NAT444 地址转换是基于端口块的方式来复用公网 IP 地址的，即一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。例如：假设私网 IP 地址 10.1.1.1 独占公网 IP 地址 202.1.1.1 的一个端口块 10001～10256，则该私网 IP 向公网发起的所有

连接，源 IP 地址都将被转换为同一个公网 IP 地址 202.1.1.1，而源端口将被转换为端口块 10001～10256 之内的一个端口。

端口块的分配支持静态映射和动态映射两种方式。

(2) 端口块静态映射

端口块静态映射是指，NAT 网关设备根据手动配置的命令行，自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，并创建静态端口块表项。当私网 IP 地址成员中的某个私网 IP 地址向公网发起新建连接时，根据私网 IP 地址匹配静态端口块表项，获取对应的公网 IP 地址和端口块，并从端口块中动态为其分配一个公网端口，对报文进行地址转换。

配置端口块静态映射时，需要创建一个端口块组，并在端口块组中配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小。假设端口块组中每个公网 IP 地址的可用端口块数为 m（即端口范围除以端口块大小），则端口块静态映射的算法如下：按照从小到大的顺序对私网 IP 地址成员中的所有 IP 地址进行排列，最小的 m 个私网 IP 地址对应最小的公网 IP 地址及其端口块，端口块按照起始端口号从小到大的顺序分配；次小的 m 个私网 IP 地址对应次小的公网 IP 地址及其端口块，端口块的分配顺序相同；依次类推。

(3) 端口块动态映射

端口块动态映射融合了普通 NAT 动态地址转换和 NAT444 端口块静态映射的特点。当内网用户向公网发起连接时，首先根据动态地址转换中的 ACL 规则进行过滤，决定是否需要进行源地址转换。对于需要进行源地址转换的连接，当该连接为该用户的首次连接时，从所匹配的动态地址转换配置引用的 NAT 地址组中获取一个公网 IP 地址，从该公网 IP 地址中动态分配一个端口块，创建动态端口块表项，然后从端口块表项中动态分配一个公网端口，进行地址转换。对该用户后续连接的转换，均从生成的动态端口块表项中分配公网端口。当该用户的所有连接都断开时，回收为其分配的端口块资源，删除相应的动态端口块表项。

端口块动态映射支持增量端口块分配。当为某私网 IP 地址分配的端口块资源耗尽（端口块中的所有端口都被使用）时，如果该私网 IP 地址向公网发起新的连接，则无法再从端口块中获取端口，无法进行地址转换。此时，如果预先在相应的 NAT 地址组中配置了增量端口块数，则可以为该私网 IP 地址分配额外的端口块，进行地址转换。

1.1.4 NAT表项

1. NAT会话表项

NAT 设备处理一个连接的首报文时便确定了相应的地址转换关系，并同时创建会话表项，该会话表项中添加了 NAT 扩展信息（例如接口信息、转换方式）。会话表项中记录了首报文的地址转换信息。这类经过 NAT 处理的会话表项，也称为 NAT 会话表项。

当该连接的后续报文经过 NAT 设备时，将与 NAT 会话表项进行匹配，NAT 设备从匹配到的会话表项中得到首报文的转换方式，并根据首报文的转换方式对后续报文进行处理。后续报文方向与首报文相同时，源和目的的转换方式与首报文相同；方向相反时，转换方式与首报文相反。即，如果首报文转换了源地址，则后续报文需要转换目的地址；如果首报文转换了目的地址，则后续报文需要转换源地址。

NAT 会话表项的更新和老化由会话管理模块维护，关于会话管理的相关介绍请参见“安全配置指导”中的“会话管理”。

2. EIM表项

如果 NAT 设备上使能了 Endpoint-Independent Mapping 模式，则在 PAT 方式的动态地址转换过程中，会首先创建一个 NAT 会话表项，然后创建一个 EIM 表项用于记录地址和端口的转换关系（内网地址和端口<-->NAT 地址和端口），该表项有以下两个作用：

- 保证后续来自相同源地址和源端口的新建连接与首次连接使用相同的转换关系。
- 允许外网主机向 NAT 地址和端口发起的新建连接根据 EIM 表项进行反向地址转换。

该表项在与其相关联的所有 NAT 会话表项老化后老化。

3. NO-PAT表项

在NO-PAT方式进行源地址的动态转换过程中，NAT设备首先创建一个NAT会话表项，然后建立一个NO-PAT表项用于记录该转换关系（内网地址<-->NAT地址）。除此之外，在NAT设备进行ALG处理时，也会触发创建NO-PAT表项。NAT ALG的相关介绍请参见“1.1.7 NAT支持ALG”。

NO-PAT 表项有以下两个作用：

- 保证后续来自相同源地址的新建连接与首次连接使用相同的转换关系。
- 配置了 **reversible** 参数的情况下，允许满足指定条件的主机向 NAT 地址发起的新建连接根据 NO-PAT 表项进行反向地址转换。

该表项在与其相关联的所有 NAT 会话表项老化后老化。

4. NAT444 端口块表项

NAT444 端口块表项记录 1 个用户在 NAT444 网关转换前的私网 IP 地址、转换后对应的公网 IP 地址及其端口块。

端口块表项分为静态端口块表项和动态端口块表项：

- 静态端口块表项在配置了 NAT444 端口块静态映射的相关命令时由系统自动创建，在删除相关配置时删除。
- 动态端口块表项在收到某私网 IP 地址的首次连接时创建，在该私网 IP 地址的所有连接都已关闭，即表项中的所有端口都已回收时删除。

1.1.5 NAT支持多VPN实例

支持多 VPN 实例的 NAT 允许 VPN 实例内的用户访问外部网络，同时允许分属于不同 VPN 实例的用户互访。例如，当某 VPN 实例内的用户经过 NAT 设备访问外部网络时，NAT 将内部网络主机的 IP 地址和端口替换为 NAT 地址和端口，同时还记录了用户的 VPN 实例信息（如 VPN 实例名称）。外部网络的回应报文到达 NAT 设备时，NAT 将外部网络地址和端口还原为内部网络主机的 IP 地址和端口，同时可得知该回应报文应该转发给哪一个 VPN 实例内的用户。另外，NAT 还可利用外部网络地址所携带的 VPN 实例信息，支持多个 VPN 实例之间的互访。

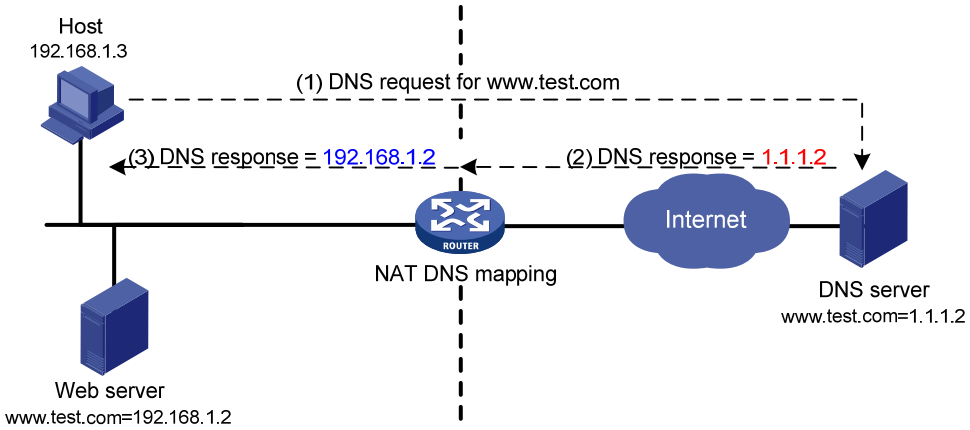
同时，NAT 内部服务器也支持多 VPN 实例，这给外部网络提供了访问 VPN 实例内服务器的机会。例如，VPN1 内提供 Web 服务的主机地址是 10.110.1.1，可以使用 202.110.10.20 作为 Web 服务器的外部地址，Internet 的用户使用 202.110.10.20 的地址就可以访问到 VPN1 提供的 Web 服务。

1.1.6 DNS mapping

一般情况下，DNS（Domain Name System，域名系统）服务器和访问私网服务器的用户都在公网，通过在NAT设备的公网接口上配置内部服务器，可以将公网地址、端口等信息映射到私网内的服务

器上，使得公网用户可以通过内部服务器的域名或公网地址来访问内部服务器。但是，如 图 1-5 所示，如果DNS服务器在公网，私网用户希望通过域名来访问私网的Web服务器，则会由于DNS服务器向私网用户发送的响应报文中包含的是私网服务器的公网地址，而导致收到响应报文的私网用户无法利用域名访问私网服务器。通过在设备上配置DNS mapping可以解决该问题。

图1-5 NAT DNS mapping 工作示意图



DNS mapping 功能是指，通过配置“域名+公网 IP 地址+公网端口号+协议类型”的映射表，建立内部服务器域名与内部服务器公网信息的对应关系。在配置了 NAT 的接口上，设备检查接收到的 DNS 响应报文，根据报文中的域名查找用户配置的 DNS mapping 映射表，并根据表项内的“公网地址+公网端口+协议类型”信息查找内部服务器地址映射表中该信息对应的私网地址，替换 DNS 查询结果中的公网地址。这样，私网用户收到的 DNS 响应报文中就包含了要访问的内部服务器的私网地址，也就能够使用内部服务器域名访问同一私网内的内部服务器。

1.1.7 NAT支持ALG

ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的解析和处理。通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析和处理。然而对于一些应用层协议，它们的报文的数据载荷中可能包含 IP 地址或端口信息，这些载荷信息也必须进行有效的转换，否则可能导致功能不正常。

例如，FTP（File Transfer Protocol，文件传输协议）应用由 FTP 客户端与 FTP 服务器之间建立的数据连接和控制连接共同实现，而数据连接使用的地址和端口由控制连接协商报文中的载荷信息决定，这就需要 ALG 利用 NAT 的相关转换配置完成载荷信息的转换，以保证后续数据连接的正确建立。

1.2 NAT配置任务简介

若接口上同时存在普通 NAT 静态地址转换、普通 NAT 动态地址转换、NAT444 端口块静态映射、NAT444 端口块动态映射和内部服务器的配置，则在地址转换过程中，它们的优先级从高到低依次为：

(1) 内部服务器。

(2) 普通 NAT 静态地址转换。

(3) NAT444 端口块静态映射。

(4) NAT444 端口块动态映射和普通 NAT 动态地址转换，系统对二者不做区分，统一按照 ACL 编号由大到小的顺序匹配。

表1-1 NAT 配置任务简介

配置任务	说明	详细配置
配置静态地址转换	根据实际的组网需求，选择其中一种或多种转换方式 (1) 静态地址转换适用于：转换关系完全确定 (2) 动态地址转换	1.3
配置动态地址转换	• PAT 方式适用于大量内网用户通过少量 NAT 地址访问外网 • NO-PAT 方式，通常仅用于配合内部服务器或静态地址转换实现双向 NAT 应用	1.4
配置内部服务器	(3) 内部服务器：内网服务器向外网提供服务 (4) NAT444 地址转换：	1.5
配置NAT444地址转换	• NAT444 端口块静态映射适用于：用户私网 IP 地址确定 • NAT444 端口块动态映射适用于：用户私网 IP 地址不确定	1.6
配置DNS mapping	可选	1.7
配置NAT hairpin	可选	1.8
配置NAT ALG功能	可选	1.9
配置NAT日志功能	可选	1.10

1.3 配置静态地址转换

配置静态地址转换时，需要首先在系统视图下配置静态地址转换映射，然后在接口下使该转换映射生效。

静态地址转换映射支持两种方式：一对一静态转换映射、网段对网段静态转换映射。静态地址转换可以支持配置在接口的出方向（**nat static outbound**）或入方向（**nat static inbound**）上，入方向的静态地址转换通常用于与其他 NAT 转换方式配合以实现双向 NAT，不建议单独配置。

1.3.1 配置准备

- 配置控制地址转换范围的 ACL。ACL 配置的相关介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其它元素。
- 对于入方向静态地址转换，需要手添加路由：目的地址为静态地址转换配置中指定的 *local-ip* 或 *local-network*；下一跳为静态地址转换配置中指定的外网地址，或者报文出接口的实际下一跳地址。

1.3.2 配置出方向一对一静态地址转换

出方向一对一静态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其源 IP 地址与指定的内网 IP 地址 *local-ip* 进行匹配，并将匹配的源 IP 地址转换为 *global-ip*。
- 对于该接口接收到的外网访问内网的报文，将其目的 IP 地址与指定的外网 IP 地址 *global-ip* 进行匹配，并将匹配的目的 IP 地址转换为 *local-ip*。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-2 配置出方向一对一静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置出方向一对一静态地址转换映射	**nat static outbound** *local-ip* [**vpn-instance** *local-name*] *global-ip* [**vpn-instance** *global-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.3.3 配置出方向网段对网段静态地址转换

出方向网段对网段静态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络到一个外部公有网络的地址转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其源 IP 地址与指定的内网网络地址进行匹配，并将匹配的源 IP 地址转换为指定外网网络地址之一。
- 对于该接口接收到的外网访问内网的报文，将其目的 IP 地址与指定的外网网络地址进行匹配，并将匹配的目的 IP 地址转换为指定的内网网络地址之一。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-3 配置出方向网段对网段静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置出方向网段对网段静态地址转换映射	**nat static outbound net-to-net** *local-start-address local-end-address* [**vpn-instance** *local-name*] **global** *global-network* { *mask-length* | *mask* } [**vpn-instance** *global-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射

操作	命令	说明
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.3.4 配置入方向一对一静态地址转换

入方向一对一静态地址转换用于实现一个内部私有网络地址与一个外部公有网络地址之间的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其目的 IP 地址与指定的内网 IP 地址 *local-ip* 进行匹配，并将匹配的目的 IP 地址转换为 *global-ip*。
- 对于该接口接收到的外网访问内网的报文，将其源 IP 地址与指定的外网 IP 地址 *global-ip* 进行匹配，并将匹配的源 IP 地址转换为 *local-ip*。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-4 配置入方向一对一静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置入方向一对一静态地址转换映射	**nat static inbound** *global-ip* [**vpn-instance** *global-name*] *local-ip* [**vpn-instance** *local-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.3.5 配置入方向网段对网段静态地址转换

入方向网段对网段静态地址转换用于实现一个内部私有网络与一个外部公有网络之间的地址转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其目的 IP 地址与指定的内网网络地址进行匹配，并将匹配的目的 IP 地址转换为指定的外网网络地址之一。
- 对于该接口接收到的外网访问内网的报文，将其源 IP 地址与指定的外网网络地址进行匹配，并将匹配的源 IP 地址转换为指定的内网网络地址之一。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-5 配置入方向网段对网段静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置入方向网段对网段静态地址转换映射	**nat static inbound net-to-net** *global-start-address global-end-address* [**vpn-instance** *global-name*] **local** *local-network* { *mask-length* | *mask* } [**vpn-instance** *local-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.4 配置动态地址转换

通过在接口上配置 ACL 和地址组（或接口地址）的关联即可实现动态地址转换。

- 直接使用接口的 IP 地址作为转换后的地址，即实现 Easy IP 功能。
- 选择使用地址组中的地址作为转换后的地址，根据地址转换过程中是否转换端口信息可将动态地址转换分为 NO-PAT 和 PAT 两种方式。

1.4.1 配置限制和指导

在同时配置了多条动态地址转换的情况下：

- 指定了 ACL 参数的动态地址转换配置的优先级高于未指定 ACL 参数的动态地址转换配置；
- 对于指定了 ACL 参数的动态地址转换配置，其优先级由 ACL 编号的大小决定，编号越大，优先级越高。

1.4.2 配置准备

- 配置控制地址转换范围的 ACL。ACL 配置的相关介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其它元素。
- 确定是否直接使用接口的 IP 地址作为转换后的报文源地址。
- 配置根据实际网络情况，合理规划可用于地址转换的公网 IP 地址组。
- 确定地址转换过程中是否使用端口信息。
- 对于入方向动态地址转换，如果指定了 **add-route** 参数，则有报文命中该配置时，设备会自动添加路由表项：目的地址为本次地址转换使用的地址组中的地址，出接口为本配置所在接口，下一跳地址为报文的源地址；如果没有指定 **add-route** 参数，则用户需要在设备上手工添加路由。由于自动添加路由表项速度较慢，通常建议手工添加路由。

1.4.3 配置出方向动态地址转换

出方向动态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将与指定 ACL permit 规则匹配的报文源 IP 地址转换为地址组中的地址。
- 在指定了 **no-pat reversible** 参数，并且已经存在 NO-PAT 表项的情况下，对于经过该接口收到的外网访问内网的首报文，将其目的 IP 地址与 NO-PAT 表项进行匹配，并将目的 IP 地址转换为匹配的 NO-PAT 表项中记录的内网地址。

表1-6 配置出方向动态地址转换

操作		命令	说明
进入系统视图		**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图		**nat address-group** *group-number*	缺省情况下，不存在地址组
添加地址组成员		**address** *start-address end-address*	缺省情况下，不存在地址组成员 可通过多次执行本命令添加多个地址组成员 当前地址组成员的IP地址段不能与该地址组中或者其它地址组中已有的地址成员组成员重叠
进入接口视图		**interface** *interface-type interface-number*	-
配置出方向动态地址转换	NO-PAT方式	**nat outbound** [*acl-number*] **address-group** *group-number* [**vpn-instance** *vpn-instance-name*] **no-pat** [**reversible**]	二者至少选其一 缺省情况下，不存在出方向动态地址转换配置 一个接口下可配置多个出方向的动态地址转换
	PAT方式	**nat outbound** [*acl-number*] [**address-group** *group-number*] [**vpn-instance** *vpn-instance-name*] [**port-preserved**]	
（可选）配置PAT方式地址转换的模式		**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	缺省情况下，PAT方式地址转换的模式为Address and Port-Dependent Mapping 该配置只对PAT方式的出方向动态地址转换有效

1.4.4 配置入方向动态地址转换

入方向动态地址转换功能通常与接口上的出方向动态地址转换（**nat outbound**）、内部服务器（**nat server**）或出方向静态地址转换（**nat static outbound**）配合，用于实现双向 NAT 应用，不建议单独使用。

入接口动态地址转换的具体过程如下：

- 对于该接口接收到的外网访问内网的首报文，将与指定的 ACL permit 规则匹配的报文的源 IP 地址转换为地址组中的地址。

- 在指定了 **no-pat reversible** 参数，并且已经存在 NO-PAT 表项的情况下，对于经过该接口发送的内网访问外网的首报文，将其目的 IP 地址与 NO-PAT 表项进行匹配，并将目的 IP 地址转换为匹配的 NO-PAT 表项中记录的外网地址。

需要注意的是，该方式下的地址转换不支持 Easy IP 功能。

表1-7 配置入方向动态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图	**nat address-group** *group-number*	缺省情况下，不存在NAT地址组
添加地址组成员	**address** *start-address end-address*	缺省情况下，不存在地址组成员 可通过多次执行本命令添加多个地址组成员 当前地址组成员的IP地址段不能与该地址组中或者其它地址组中已有的地址组成员重叠
进入接口视图	**interface** *interface-type interface-number*	-
配置入方向动态地址转换	**nat inbound** *acl-number* **address-group** *group-number* [**vpn-instance** *vpn-instance-name*] [**no-pat** [**reversible**] [**add-route**]]	缺省情况下，不存在入方向动态地址转换配置 一个接口下可配置多个入方向的动态地址转换

1.5 配置内部服务器

通过在 NAT 设备上配置内部服务器，建立一个或多个内网服务器内网地址和端口与外网地址和端口的映射关系，使外部网络用户能够通过配置的外网地址和端口来访问内网服务器。内部服务器可以位于一个普通的内网内，也可以位于一个 VPN 实例内。

内部服务器通常配置在外网侧接口上。

若内部服务器配置中引用了 **acl** 参数，则表示与指定的 ACL permit 规则匹配的报文才可以使用内部服务器的映射表进行地址转换。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其它元素。

1.5.1 配置普通内部服务器

普通的内部服务器是将内网服务器的地址和端口映射为外网地址和端口，允许外部网络中的主机通过配置的外网地址和端口访问位于内网的服务器。

表1-8 配置普通内部服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作		命令	说明
配置普通内部服务器	外网地址单一，未使用外网端口或外网端口单一	**nat server protocol** *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-name*] [**acl** *acl-number*]	四者至少选其一 缺省情况下，不存在内部服务器 一个接口下可以配置多个普通内部服务器
	外网地址单一，外网端口连续	**nat server protocol** *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* [**vpn-instance** *global-name*] **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port1 local-port2* } [**vpn-instance** *local-name*] [**acl** *acl-number*]	
	外网地址连续，未使用外网端口或外网端口单一	**nat server protocol** *pro-type* **global** *global-address1 global-address2* [*global-port*] [**vpn-instance** *global-name*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**vpn-instance** *local-name*] [**acl** *acl-number*]	
	外网地址连续，外网端口单一	**nat server protocol** *pro-type* **global** *global-address1 global-address2 global-port* [**vpn-instance** *global-name*] **inside** *local-address local-port1 local-port2* [**vpn-instance** *local-name*] [**acl** *acl-number*]	

1.5.2 配置负载分担内部服务器

负载分担内部服务器是指在配置内部服务器时，将内部服务器的内网信息指定为一个内部服务器组，组内的多台主机可以共同对外提供某种服务。外网用户向内部服务器指定的外网地址发起应用请求时，NAT 设备可根据内网服务器的权重和当前连接数，选择其中一台内网服务器作为目的服务器，实现内网服务器负载分担。

表1-9 配置负载分担内部服务器

操作	命令	说明
进入系统视图	**system-view**	-
配置内部服务器组，并进入服务器组视图	**nat server-group** *group-number*	缺省情况下，不存在内部服务器组
添加内部服务器组成员	**inside ip** *inside-ip* **port** *port-number* [**weight** *weight-value*]	缺省情况下，内部服务器组内没有内部服务器组成员 一个内部服务器组内可以添加多个组成员
进入接口视图	**interface** *interface-type interface-number*	-
配置负载分担内部服务器	**nat server protocol** *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } [**vpn-instance** *global-name*] **inside server-group** *group-number* [**vpn-instance** *local-name*] [**acl** *acl-number*]	缺省情况下，不存在内部服务器 一个接口下可以配置多个负载分担内部服务器

1.6 配置NAT444地址转换

通过在 NAT444 网关设备上配置 NAT444 地址转换，可以实现基于端口块的公网 IP 地址复用，使一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。

NAT444 是出方向地址转换，通常配置在外网侧接口上。

1.6.1 配置NAT444 端口块静态映射

配置 NAT444 端口块静态映射需要创建一个端口块组，并在接口的出方向上应用该端口块组。端口块组中需要配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小，系统会根据端口块组中的配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，创建静态端口块表项，并根据表项进行 NAT444 地址转换。

表1-10 配置 NAT444 端口块静态映射

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT端口块组，并进入NAT端口块组视图	**nat port-block-group** *group-number*	缺省情况下，不存在NAT端口块组
添加私网地址成员	**local-ip-address** *start-address end-address*	缺省情况下，不存在私网地址成员 一个端口块组内，可以配置多个私网地址成员，但各私网地址成员之间的IP地址不能重叠
添加公网地址成员	**global-ip-pool** *start-address end-address*	缺省情况下，不存在公网地址成员 一个端口块组内，可以配置多个公网地址成员，但各公网地址成员之间的IP地址不能重叠
（可选）配置公网地址的端口范围	**port-range** *start-port-number end-port-number*	缺省情况下，公网地址的端口范围为1-65535
（可选）配置端口块大小	**block-size** *block-size*	缺省情况下，端口块大小为256
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置NAT444端口块静态映射	**nat outbound port-block-group** *group-number*	缺省情况下，不存在NAT444端口块静态映射配置 一个接口下可配置多条基于不同端口块组的NAT444端口块静态映射
退回系统视图	**quit**	-
（可选）配置PAT方式出方向动态地址转换的模式	**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	缺省情况下，PAT方式出方向动态地址转换的模式为Address and Port-Dependent Mapping

1.6.2 配置NAT444 端口块动态映射

NAT444 端口块动态映射的配置方式与普通的 PAT 方式出方向动态地址转换的配置基本相同，只要在接口的出方向上配置 ACL 和 NAT 地址组的关联即可。所不同的是，对于 NAT444 端口动态映射，必须在 NAT 地址组中配置端口块参数，以实现基于端口块的 NAT444 地址转换。

表1-11 配置 NAT444 端口块动态映射

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图	**nat address-group** *group-number*	缺省情况下，不存在地址组
添加地址组成员	**address** *start-address end-address*	缺省情况下，不存在地址组成员 可通过多次执行本命令添加多个地址组成员 当前地址组成员的IP地址段不能与该地址组中或者其它地址组中已有的地址成员组成员重叠
配置端口范围	**port-range** *start-port-number end-port-number*	缺省情况下，端口范围为1-65535 该配置仅对PAT方式地址转换生效
配置端口块参数	**port-block block-size** *block-size* [**extended-block-number** *extended-block-number*]	缺省情况下，不存在端口块参数 该配置仅对PAT方式地址转换生效
进入接口视图	**interface** *interface-type interface-number*	-
配置PAT方式出方向动态地址转换	**nat outbound** [*acl-number*] [**address-group** *group-number*] [**vpn-instance** *vpn-instance-name*] [port-preserved]	缺省情况下，不存在PAT方式出方向动态地址转换配置。 **port-preserved**参数对NAT444端口块动态映射
（可选）配置PAT方式地址转换的模式	**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	缺省情况下，PAT方式出方向动态地址转换的模式为Address and Port-Dependent Mapping

1.7 配置DNS mapping

通过配置 DNS mapping，可以在 DNS 服务器位于外网的情况下，实现内网用户可通过域名访问位于同一内网的内部服务器的功能。DNS mapping 功能需要和内部服务器配合使用，由 **nat server** 配置定义内部服务器对外提供服务的外网 IP 地址和端口号，由 DNS mapping 建立“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。

NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，由于载荷中只包含域名和应用服务器的外网 IP 地址（不包含传输协议类型和端口号），当接口上存在多条 NAT 服务器配置且使用相同的外网地址而内网地址不同时，DNS ALG 仅使用 IP 地址来匹配内部服务器可能会得到错误的匹配结果。因此需要借助 DNS mapping 的配置，指定域名与应用服务器的外网 IP 地址、端口和协议的

映射关系，由域名获取应用服务器的外网 IP 地址、端口和协议，进而（在当前 NAT 接口上）精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

表1-12 配置 DNS mapping

操作	命令	说明
进入系统视图	**system-view**	-
配置一条域名到内部服务器的映射	**nat dns-map domain** *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*	缺省情况下，不存在域名到内部服务器的映射 可配置多条域名到内部服务器的映射

1.8 配置NAT hairpin功能

通过在内网侧接口上使能 NAT hairpin 功能，可以实现内网用户使用 NAT 地址访问内网服务器或内网其它用户。NAT hairpin 功能需要与内部服务器（**nat server**）、出方向动态地址转换（**nat outbound**）或出方向静态地址转换（**nat static outbound**）配合工作。

该功能在不同工作方式下的具体转换过程如下：

- C/S 方式：NAT 在内网接口上同时转换访问内网服务器的报文的源和目的 IP 地址，其中，目的 IP 地址转换通过匹配某外网接口上的内部服务器配置来完成，源地址转换通过匹配内部服务器所在接口上的出方向动态地址转换或出方向静态地址转换来完成。
- P2P 方式：内网各主机首先向外网服务器注册自己的内网地址信息，该地址信息为外网侧出方向地址转换的 NAT 地址，然后内网主机之间通过使用彼此向外网服务器注册的外网地址进行互访。该方式下，外网侧的出方向地址转换必须配置为 PAT 转换方式，并使能 EIM 模式。

表1-13 配置 NAT hairpin 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能NAT hairpin功能	**nat hairpin enable**	缺省情况下，NAT hairpin功能处于关闭状态

1.9 配置NAT ALG

通过开启指定应用协议类型的 ALG 功能，实现对应用层报文数据载荷字段的分析和 NAT 处理。

表1-14 配置 NAT ALG 功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启指定或所有协议类型的NAT ALG功能	**nat alg** { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }	缺省情况下，所有协议类型的NAT ALG功能均处于开启状态

1.10 配置NAT日志功能

1.10.1 配置NAT会话日志功能

NAT 会话日志是为了满足网络管理员安全审计的需要，对 NAT 会话（报文经过设备时，源或目的信息被 NAT 进行过转换的连接）信息进行的记录，包括 IP 地址及端口的转换信息、用户的访问信息以及用户的网络流量信息。

有三种情况可以触发设备生成 NAT 会话日志：

- 新建 NAT 会话。
- 删除 NAT 会话。新增高优先级的配置、删除配置、报文匹配规则变更、NAT 会话老化以及执行删除 NAT 会话的命令时，都可能导致 NAT 会话被删除。
- 存在 NAT 活跃流。NAT 活跃流是指在一定时间内存在的 NAT 会话。当设置的生成活跃流日志的时间间隔到达时，当前存在的 NAT 会话信息就被记录并生成日志。

表1-15 配置 NAT 会话日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NAT日志功能	**nat log enable** [**acl** *acl-number*]	缺省情况下，NAT日志功能处于关闭状态
开启NAT新建会话的日志功能	**nat log flow-begin**	三者至少选其一 缺省情况下，创建、删除NAT会话或存在NAT活跃流时，均不生成NAT日志
开启NAT删除会话的日志功能	**nat log flow-end**	
开启NAT活跃流的日志功能，并设置生成活跃流日志的时间间隔	**nat log flow-active** *time-value*	

1.10.2 配置NAT444 用户日志功能

NAT444 用户日志是为了满足互联网用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

有两种情况可以触发设备输出 NAT444 用户日志：

- 端口块分配：端口块静态映射方式下，在某私网 IP 地址的第一个新建连接通过端口块进行地址转换时输出日志；端口块动态映射方式下，在为某私网 IP 地址分配端口块或增量端口块时输出日志。

- 端口块回收：端口块静态映射方式下，在某私网 IP 地址的最后一个连接拆除时输出日志；端口块动态映射方式下，在释放端口块资源（并删除端口块表项）时输出日志。

在配置 NAT444 用户日志功能前，必须先配置将用户定制日志发送到日志主机的功能，否则无法产生 NAT444 用户日志。详细配置请参见“网络管理和监控配置指导”中的“信息中心”。

表1-16 配置 NAT444 用户日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NAT日志功能	**nat log enable** [**acl** *acl-number*]	缺省情况下，NAT日志功能处于关闭状态 ACL参数对NAT444用户日志功能无效
开启端口块分配的NAT444用户日志功能	**nat log port-block-assign**	二者至少选其一 缺省情况下，分配和回收端口块时，均不输出NAT444用户日志
开启端口块回收的NAT444用户日志功能	**nat log port-block-withdraw**	

1.10.3 配置NAT444 告警信息日志功能

在 NAT444 地址转换中，如果可为用户分配的公网 IP 地址、端口块或端口块中的端口都被占用，则该用户的后续连接由于没有可用的资源无法对其进行地址转换，相应的报文将被丢弃。为了监控公网 IP 地址和端口块资源的使用情况，可以对端口用满和资源用满两种情况记录告警信息日志。

- 端口用满告警：在私网 IP 地址对应的端口块中的所有端口都被占用的情况下，输出告警信息日志。对于端口块动态映射方式，如果配置了增量端口块分配，则当首次分配的端口块中的端口都被占用时，并不输出日志；只有当增量端口块中的端口也都被私用时，才会输出日志。
- 资源用满告警：在 NAT444 端口块动态映射中，如果所有资源（公网 IP 地址、端口块）都占用，则输出日志。

在配置 NAT444 告警信息日志功能前，必须先配置将用户定制日志发送到日志主机的功能，否则无法产生 NAT444 告警信息日志。详细配置请参见“网络管理和监控配置指导”中的“信息中心”。

表1-17 配置 NAT444 告警信息日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NAT日志功能	**nat log enable**[**acl** *acl-number*]	缺省情况下，NAT日志功能处于关闭状态 ACL参数对NAT444告警信息日志功能无效
开启NAT444告警信息的日志功能	**nat log alarm**	缺省情况下，NAT444告警信息日志功能处于关闭状态

1.11 NAT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 NAT 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 NAT 表项。

表1-18 NAT 显示和维护

操作	命令
显示所有的NAT配置信息	**display nat all**
显示NAT地址组的配置信息	**display nat address-group** [*group-number*]
显示NAT DNS mapping的配置信息	**display nat dns-map**
显示NAT EIM表项信息（MSR 2600/MSR 3600）	**display nat eim**
显示NAT EIM表项信息（MSR 5600）	**display nat eim** [**slot** *slot-number*]
显示NAT入接口动态地址转换关系的配置信息	**display nat inbound**
显示NAT日志功能的配置信息	**display nat log**
显示NAT NO-PAT表项信息（MSR 2600/MSR 3600）	**display nat no-pat**
显示NAT NO-PAT表项信息（MSR 5600）	**display nat no-pat** [**slot** *slot-number*]
显示NAT出接口动态地址转换关系的配置信息	**display nat outbound**
显示NAT内部服务器的配置信息	**display nat server**
显示NAT内部服务器组的配置信息	**display nat server-group** [*group-number*]
显示NAT会话（MSR 2600/MSR 3600）	**display nat session** [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } * [**vpn-instance** *vpn-name*]] [**verbose**]
显示NAT会话（MSR 5600）	**display nat session** [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } * [**vpn-instance** *vpn-name*]] [**slot** *slot-number*] [**verbose**]
显示NAT静态地址转换的配置信息	**display nat static**
显示NAT统计信息（MSR 2600/MSR 3600）	**display nat statistics**
显示NAT统计信息（MSR 5600）	**display nat statistics** [**slot** *slot-number*]
显示NAT444端口块静态映射的配置信息	**display nat outbound port-block-group**
显示NAT端口块组配置信息	**display nat port-block-group** [*group-number*]
显示端口块表项（MSR 2600/MSR 3600）	**display nat port-block** { **dynamic** | **static** }
显示端口块表项（MSR 5600）	**display nat port-block** { **dynamic** | **static** } [**slot** *slot-number*]
删除NAT会话（MSR 2600/MSR 3600）	**reset nat session**
删除NAT会话（MSR 5600）	**reset nat session** [**slot** *slot-number*]

1.12 NAT典型配置举例

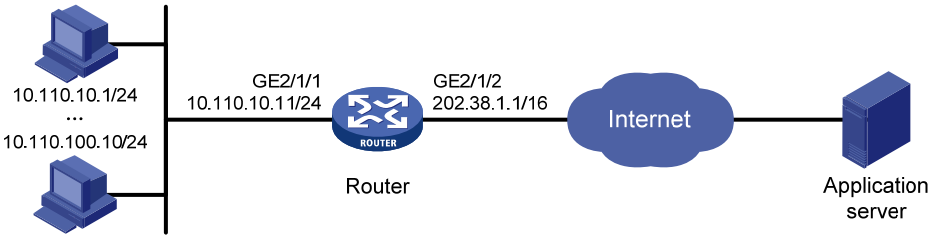
1.12.1 内网用户通过NAT地址访问外网（静态地址转换）

1. 组网需求

内部网络用户 10.110.10.8/24 使用外网地址 202.38.1.100 访问 Internet。

2. 组网图

图1-6 静态地址转换典型配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态地址转换映射。

```
<Router> system-view
[Router] nat static outbound 10.110.10.8 202.38.1.100
```

使配置的静态地址转换在接口 GigabitEthernet2/1/2 上生效。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat static enable
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，内网主机可以访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat static
Static NAT mappings:
  There are 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP  : 10.110.10.8
    Global IP : 202.38.1.100

Interfaces enabled with static NAT:
  There are 1 interfaces enabled with static NAT.
  Interface: GigabitEthernet2/1/2
```

通过以下显示命令，可以看到 Host 访问某外网服务器时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 10.110.10.8/42496
  Destination IP/port: 202.38.1.111/2048
  DS-Lite tunnel peer: -
```

```
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 202.38.1.111/42496
  Destination IP/port: 202.38.1.100/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2012-08-16 09:30:49  TTL: 27s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/2
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

1.12.2 内网用户通过NAT地址访问外网（地址不重叠）

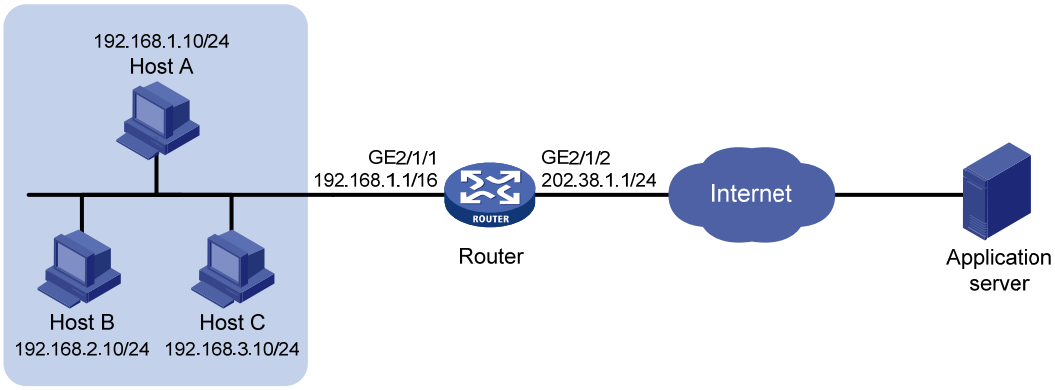
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

需要实现，内部网络中 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。使用的外网地址为 202.38.1.2 和 202.38.1.3。

2. 组网图

图1-7 内网用户通过 NAT 访问外网（地址不重叠）



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3。

```
<Router> system-view
[Router] nat address-group 0
[Router-nat-address-group-0] address 202.38.1.2 202.38.1.3
```

```
[Router-nat-address-group-0] quit
```

配置 ACL 2000，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/1/2 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat outbound 2000 address-group 0
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，Host A 能够访问 WWW server，Host B 和 Host C 无法访问 WWW server。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT address group information:
  There are 1 NAT address groups.
  Address group 0:
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.3

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 0      Port-preserved: N
    NO-PAT: N         Reversible: N

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
```

```
  NBT         : Enabled
  PPTP        : Enabled
  RTSP        : Enabled
  RSH         : Enabled
  SCCP        : Enabled
  SIP         : Enabled
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : Enabled
```

通过以下显示命令，可以看到 Host A 访问 WWW server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/52992
  Destination IP/port: 200.1.1.10/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 200.1.1.10/4
  Destination IP/port: 202.38.1.3/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2012-08-15 14:53:29  TTL: 12s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/2
Initiator->Responder:            1 packets         84 bytes
Responder->Initiator:            1 packets         84 bytes

Total sessions found: 1
```

1.12.3 内网用户通过NAT地址访问外网（地址重叠）

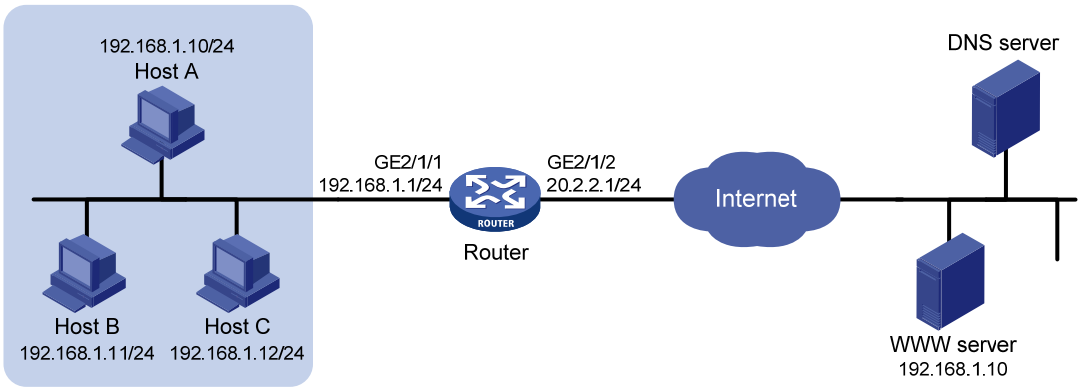
1. 组网需求

- 某公司内网网段地址为 192.168.1.0/24，该网段与要访问的外网 Web 服务器所在网段地址重叠。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

需要实现，内网用户可以通过域名访问外网的 Web 服务器。

2. 组网图

图1-8 内网用户通过 NAT 访问外网（地址重叠）



3. 配置思路

这是一个典型的双向 NAT 应用，具体配置思路如下。

- 内网主机通过域名访问外网 Web 服务器时，首先需要向外网的 DNS 服务器发起 DNS 查询请求。由于外网 DNS 服务器回复给内网主机的 DNS 应答报文载荷中的携带的 Web 服务器地址与内网主机地址重叠，因此 NAT 设备需要将载荷中的 Web 服务器地址转换为动态分配的一个 NAT 地址。动态地址分配可以通过入方向动态地址转换实现，载荷中的地址转换需要通过 DNS ALG 功能实现。
- 内网主机得到外网 Web 服务器的 IP 地址之后（该地址为临时分配的 NAT 地址），通过该地址访问外网 Web 服务器。由于内网主机的地址与外网 Web 服务器的真实地址重叠，因此也需要为其动态分配一个的 NAT 地址，可以通过出方向动态地址转换实现。
- 外网 Web 服务器对应的 NAT 地址在 NAT 设备上没有路由，因此需要手工添加静态路由，使得目的地址为外网服务器 NAT 地址的报文出接口为 GigabitEthernet2/1/2。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 的 NAT ALG 功能。

```
<Router> system-view
[Router] nat alg dns
```

配置 ACL 2000，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

```
[Router] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

```
[Router] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet2/1/2 上配置入方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的外网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat inbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet2/1/2 上配置出方向动态地址转换，允许使用地址组 2 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router-GigabitEthernet2/1/2] nat outbound 2000 address-group 2
[Router-GigabitEthernet2/1/2] quit
```

配置静态路由，目的地址为外网服务器 NAT 地址 202.38.1.2，出接口为 GigabitEthernet2/1/2，下一跳地址为 20.2.2.2（20.2.2.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准）。

```
[Router] ip route-static 202.38.1.2 32 gigabitethernet 2/1/2 20.2.2.2
```

5. 验证配置

以上配置完成后，Host A 能够通过域名访问 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT address group information:
  There are 2 NAT address groups.
  Address group 1:
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.2

  Address group 2:
    Address information:
      Start address         End address
      202.38.1.3            202.38.1.3

NAT inbound information:
  There are 1 NAT inbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 1      Add route: N
    NO-PAT: Y         Reversible: Y

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 2      Port-preserved: N
    NO-PAT: N         Reversible: N

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
```

```
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS         : Enabled
  FTP         : Enabled
  H323        : Enabled
  ICMP-ERROR  : Enabled
  ILS         : Enabled
  MGCP        : Enabled
  NBT         : Enabled
  PPTP        : Enabled
  RTSP        : Enabled
  RSH         : Enabled
  SCCP        : Enabled
  SIP         : Enabled
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : Enabled
```

通过以下显示命令，可以看到 Host A 访问 WWW server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/1694
  Destination IP/port: 202.38.1.2/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.10/8080
  Destination IP/port: 202.38.1.3/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2012-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/2
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.4 外网用户通过外网地址访问内网服务器

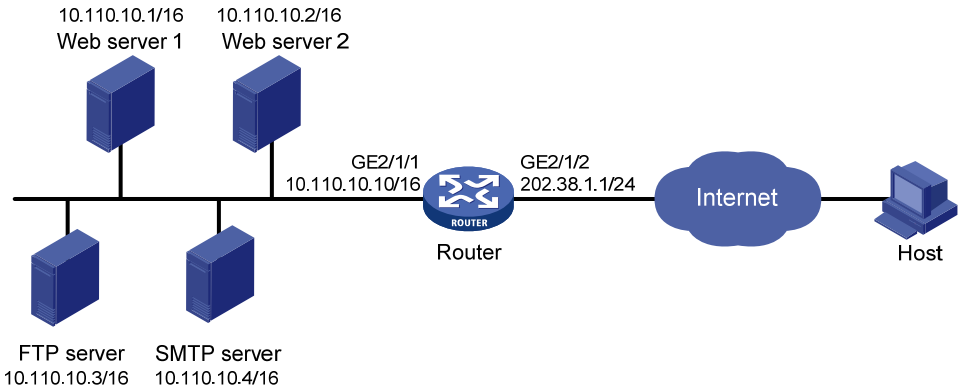
1. 组网需求

某公司内部对外提供 Web、FTP 和 SMTP 服务，而且提供两台 Web 服务器。公司内部网址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.3/16，内部 Web 服务器 1 的 IP 地址为 10.110.10.1/16，内部 Web 服务器 2 的 IP 地址为 10.110.10.2/16，内部 SMTP 服务器 IP 地址为 10.110.10.4/16。公司拥有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。需要实现如下功能：

- 外部的主机可以访问内部的服务器。
- 选用 202.38.1.1 作为公司对外提供服务的 IP 地址，Web 服务器 2 对外采用 8080 端口。

2. 组网图

图1-9 外网用户通过外网地址访问内网服务器



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

进入接口 GigabitEthernet2/1/2。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/2
```

配置内部 FTP 服务器，允许外网主机使用地址 202.38.1.1、端口号 21 访问内网 FTP 服务器。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.1 21 inside
10.110.10.3 ftp
```

配置内部 Web 服务器 1，允许外网主机使用地址 202.38.1.1、端口号 80 访问内网 Web 服务器 1。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.1 80 inside
10.110.10.1 http
```

配置内部 Web 服务器 2，允许外网主机使用地址 202.38.1.1、端口号 8080 访问内网 Web 服务器 2。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.1 8080 inside
10.110.10.2 http
```

配置内部 SMTP 服务器，允许外网主机使用地址 202.38.1.1 以及 SMTP 协议定义的端口访问内网 SMTP 服务器。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.1 smtp inside
10.110.10.4 smtp
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，外网 Host 能够通过 NAT 地址访问各内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT internal server information:
  There are 4 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/21
    Local  IP/port: 10.110.10.3/21

  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/25
    Local  IP/port: 10.110.10.4/25

  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/80
    Local  IP/port: 10.110.10.1/80

  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/8080
    Local  IP/port: 10.110.10.2/80

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
```

```
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到 Host 访问 FTP server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 202.38.1.10/1694
  Destination IP/port: 202.38.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.10.3/21
  Destination IP/port: 202.38.1.10/1694
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2012-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet2/1/2
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.5 外网用户通过域名访问内网服务器（地址不重叠）

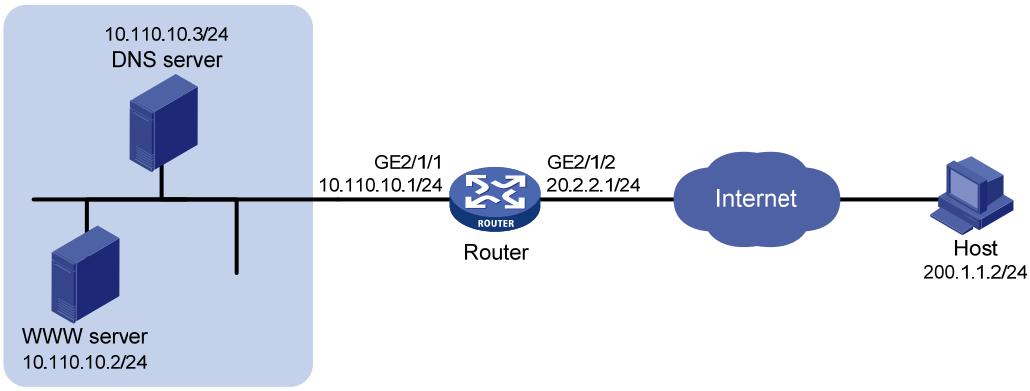
1. 组网需求

- 某公司内部对外提供 Web 服务，Web 服务器地址为 10.110.10.2/24。
- 该公司在内网有一台 DNS 服务器，IP 地址为 10.110.10.3/24，用于解析 Web 服务器的域名。
- 该公司拥有两个外网 IP 地址：202.38.1.2 和 202.38.1.3。

需要实现，外网主机可以通过域名访问内网的 Web 服务器。

2. 组网图

图1-10 外网用户通过域名访问内网服务器（地址不重叠）



3. 配置思路

- 外网主机通过域名访问 Web 服务器，首先需要通过访问内网 DNS 服务器获取 Web 服务器的 IP 地址，因此需要通过配置 NAT 内部服务器将 DNS 服务器的内网 IP 地址和 DNS 服务端口映射为一个外网地址和端口。
- DNS 服务器回应给外网主机的 DNS 报文载荷中携带了 Web 服务器的内网 IP 地址，因此需要将 DNS 报文载荷中的内网 IP 地址转换为一个外网 IP 地址。外网地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过 DNS ALG 功能实现。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 协议的 ALG 功能。

```
<Router> system-view
[Router] nat alg dns
```

配置 ACL 2000，允许对内部网络中 10.110.10.2 的报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 10.110.10.2 0
[Router-acl-basic-2000] quit
```

创建地址组 1。

```
[Router] nat address-group 1
```

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-1] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-1] quit
```

在接口 GigabitEthernet2/1/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.2 访问内网 DNS 服务器。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat server protocol udp global 202.38.1.2 inside 10.110.10.3
domain
```

在接口 GigabitEthernet2/1/2 上配置出方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Router-GigabitEthernet2/1/2] nat outbound 2000 address-group 1 no-pat reversible
```

```
[Router-GigabitEthernet2/1/2] quit
```

5. 验证配置

以上配置完成后，外网 Host 能够通过域名访问内网 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT address group information:
  There are 1 NAT address groups.
  Address group 1:
    Address information:
      Start address         End address
      202.38.1.3            202.38.1.3

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 1      Port-preserved: N
    NO-PAT: Y         Reversible: Y

NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 17(UDP)
    Global IP/port: 202.38.1.2/53
    Local  IP/port: 10.110.10.3/53

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS         : Enabled
  FTP         : Enabled
  H323        : Enabled
  ICMP-ERROR  : Enabled
  ILS         : Enabled
  MGCP        : Enabled
  NBT         : Enabled
  PPTP        : Enabled
```

```
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 202.1.1.2/1694
  Destination IP/port: 202.38.1.3/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.10.2/8080
  Destination IP/port: 202.1.1.2/1694
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2012-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet2/1/2
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.6 外网用户通过域名访问内网服务器（地址重叠）

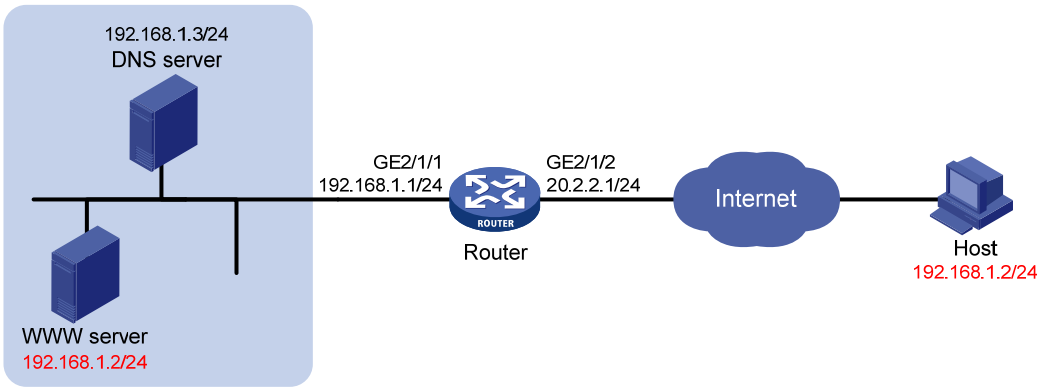
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.1.0/24。
- 该公司内部对外提供 Web 服务，Web 服务器地址为 192.168.1.2/24。
- 该公司在内网有一台 DNS 服务器，IP 地址为 192.168.1.3/24，用于解析 Web 服务器的域名。
- 该公司拥有三个外网 IP 地址：202.38.1.2、202.38.1.3 和 202.38.1.4。

需要实现，外网主机可以通过域名访问与其地址重叠的内网 Web 服务器。

2. 组网图

图1-11 外网用户通过域名访问内网服务器（地址重叠）



3. 配置思路

这是一个典型的双向 NAT 应用，具体配置思路如下。

- 外网主机通过域名访问 Web 服务器，首先需要访问内部的 DNS 服务器获取 Web 服务器的 IP 地址，因此需要通过配置 NAT 内部服务器将 DNS 服务器的内网 IP 地址和 DNS 服务端口映射为一个外网地址和端口。
- DNS 服务器回应给外网主机的 DNS 报文载荷中携带了 Web 服务器的内网 IP 地址，该地址与外网主机地址重叠，因此在出方向上需要为内网 Web 服务器动态分配一个 NAT 地址，并将载荷中的地址转换为该地址。NAT 地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过 DNS ALG 功能实现。
- 外网主机得到内网 Web 服务器的 IP 地址之后（该地址为 NAT 地址），使用该地址访问内网 Web 服务器，因为外网主机的地址与内网 Web 服务器的真实地址重叠，因此在入方向上也需要为外网主机动态分配一个 NAT 地址，可以通过入方向动态地址转换实现。
- NAT 设备上没有目的地址为外网主机对应 NAT 地址的路由，因此需要手工添加静态路由，使得目的地址为外网主机 NAT 地址的报文的出接口为 GigabitEthernet2/1/2。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 协议的 ALG 功能。

```
<Router> system-view
[Router] nat alg dns
```

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

```
[Router] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

```
[Router] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet2/1/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.4 访问内网 DNS 服务器。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat server protocol udp global 202.38.1.4 inside 192.168.1.3 domain
```

在接口 GigabitEthernet2/1/2 上配置出方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Router-GigabitEthernet2/1/2] nat outbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet2/1/2 上配置入方向动态地址转换，允许使用地址组 2 中的地址对外网访问内网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router-GigabitEthernet2/1/2] nat inbound 2000 address-group 2
[Router-GigabitEthernet2/1/2] quit
```

配置到达 202.38.1.3 地址的静态路由，出接口为 GigabitEthernet2/1/2，下一跳地址为 20.2.2.2（20.2.2.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准）。

```
[Router] ip route-static 202.38.1.3 32 gigabitethernet 2/1/2 20.2.2.2
```

5. 验证配置

以上配置完成后，外网 Host 能够通过域名访问内网相同 IP 地址的 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT address group information:
  There are 2 NAT address groups.
  Address group 1:
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.2

  Address group 2:
    Address information:
      Start address         End address
      202.38.1.3            202.38.1.3

NAT inbound information:
  There are 1 NAT inbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 2      Add route: N
    NO-PAT: N         Reversible: N

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
```

```
    ACL: 2000         Address group: 1      Port-preserved: N
    NO-PAT: Y         Reversible: Y

NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 17(UDP)
    Global IP/port: 202.38.1.4/53
    Local  IP/port: 200.1.1.3/53

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS         : Enabled
  FTP         : Enabled
  H323        : Enabled
  ICMP-ERROR  : Enabled
  ILS         : Enabled
  MGCP        : Enabled
  NBT         : Enabled
  PPTP        : Enabled
  RTSP        : Enabled
  RSH         : Enabled
  SCCP        : Enabled
  SIP         : Enabled
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : Enabled
```

通过以下显示命令，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.2/1694
  Destination IP/port: 202.38.1.2/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
```

```
  Source      IP/port: 192.168.1.2/8080
  Destination IP/port: 202.38.1.3/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2012-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet2/1/2
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.7 内网用户通过NAT地址访问内网服务器

1. 组网需求

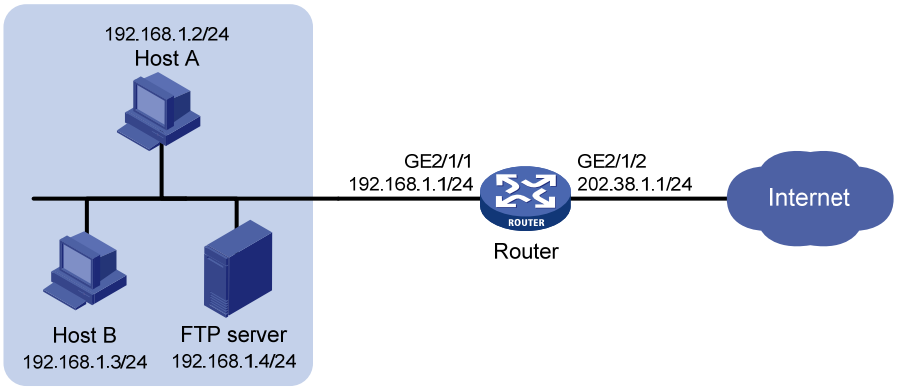
- 某公司内部网络中有一台 FTP 服务器，地址为 192.168.1.4/24。
- 该公司拥有两个外网 IP 地址：202.38.1.1 和 202.38.1.2。

需要实现如下功能：

- 外网主机可以通过 202.38.1.2 访问内网中的 FTP 服务器。
- 内网主机也可以通过 202.38.1.2 访问内网中的 FTP 服务器。

2. 组网图

图1-12 内网用户通过 NAT 地址访问内网服务器



3. 配置思路

该需求为典型的 C-S 模式的 NAT hairpin 应用，具体配置思路如下。

- 为使外网主机可以通过外网地址访问内网 FTP 服务器，需要在外网侧接口配置 NAT 内部服务器。
- 为使内网主机通过外网地址访问内网 FTP 服务器，需要在内网侧接口使能 NAT hairpin 功能。其中，目的 IP 地址转换通过匹配外网侧接口上的内部服务器配置来完成，源地址转换通过匹

配内部服务器所在接口上的出方向动态地址转换或出方向静态地址转换来完成，本例中采用出方向动态地址转换配置。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
<Router> system-view
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/1/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.2 访问内网 FTP 服务器，同时使得内网主机访问内网 FTP 服务器的报文可以进行目的地址转换。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.2 inside 192.168.1.4
ftp
```

在接口 GigabitEthernet2/1/2 上配置 Easy IP 方式的出方向动态地址转换，使得内网主机访问内网 FTP 服务器的报文可以使用接口 GigabitEthernet2/1/2 的 IP 地址进行源地址转换。

```
[Router-GigabitEthernet2/1/2] nat outbound 2000
[Router-GigabitEthernet2/1/2] quit
```

在接口 GigabitEthernet2/1/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] nat hairpin enable
[Router-GigabitEthernet2/1/1] quit
```

5. 验证配置

以上配置完成后，内网主机和外网主机均能够通过外网地址访问内网 FTP Server。通过查看如下显示信息，可以验证以上配置成功。

```
[Router]display nat all
NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N
NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/21
    Local  IP/port: 192.168.1.4/21

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
```

```
  Alarm               : Disabled

NAT hairpinning:
  There are 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet2/1/1

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS         : Enabled
  FTP         : Enabled
  H323        : Enabled
  ICMP-ERROR  : Enabled
  ILS         : Enabled
  MGCP        : Enabled
  NBT         : Enabled
  PPTP        : Enabled
  RTSP        : Enabled
  RSH         : Enabled
  SCCP        : Enabled
  SIP         : Enabled
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : Enabled
```

通过以下显示命令，可以看到 Host A 访问 FTP server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.2/1694
  Destination IP/port: 202.38.1.2/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.4/21
  Destination IP/port: 202.38.1.1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2012-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes
```

```
Total sessions found: 1
```

1.12.8 内网用户通过NAT地址互访

1. 组网需求

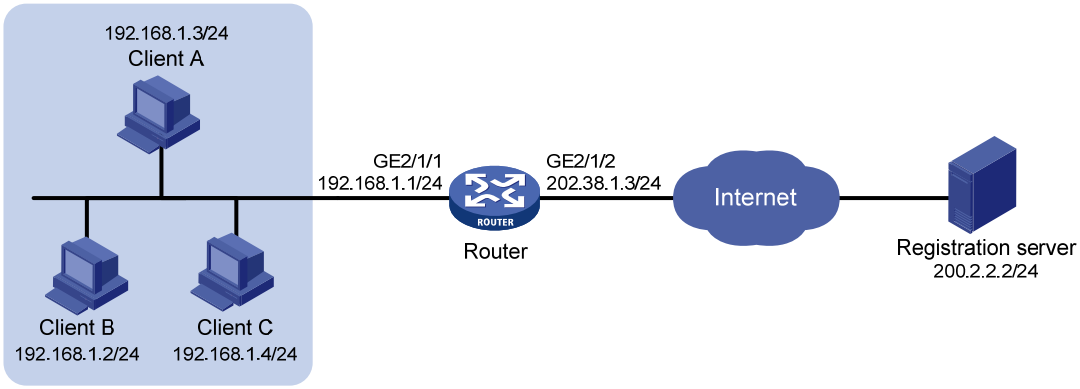
某 P2P 应用环境中，内网中的客户端首先需要向外网服务器进行注册，外网服务器会记录客户端的 IP 地址和端口号。如果内网的一个客户端要访问内网的另一个客户端，首先需要向服务器获取对方的 IP 地址和端口号。

需要实现如下功能：

- 内网客户端可以向外网中的服务器注册，且注册为一个相同的外网地址。
- 内网客户端能够通过从服务器获得的 IP 地址和端口进行互访。

2. 组网图

图1-13 内网用户通过 NAT 地址互访



3. 配置思路

该需求为典型的 P2P 模式的 NAT hairpin 应用，具体配置思路如下。

- 内网中的客户端需要向外网中的服务器注册，因此需要进行源地址转换，可以通过在外网侧接口配置出方向动态地址转换实现。
- 服务器记录客户端的 IP 地址和端口号，且该地址和端口号是 NAT 转换后的。由于服务器记录的客户端 IP 地址和端口号需要供任意源地址访问，因此客户端地址的转换关系必须不关心对端地址，这可以通过配置 EIM 模式的动态地址转换实现。
- 内部主机通过外网地址进行互访，需要在内网侧接口使能 NAT hairpin 功能。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
<Router> system-view
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在外网侧接口 GigabitEthernet2/1/2 上配置 Easy IP 方式的出方向动态地址转换，允许使用接口 GigabitEthernet2/1/2 的 IP 地址对内网访问外网的报文进行源地址转换，因为多个内部主机共用一个外网地址，因此需要配置为 PAT 方式，即转换过程中使用端口信息。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat outbound 2000
[Router-GigabitEthernet2/1/2] quit
```

配置 PAT 方式下的地址转换模式为 EIM，即只要是来自相同源地址和源端口号的且匹配 ACL 2000 的报文，不论其目的地址是否相同，通过 PAT 转换后，其源地址和源端口号都被转换为同一个外部地址和端口号。

```
[Router] nat mapping-behavior endpoint-independent acl 2000
```

在内网侧接口 GigabitEthernet2/1/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] nat hairpin enable
[Router-GigabitEthernet2/1/1] quit
```

5. 验证配置

以上配置完成后，Host A、Host B 和 Host C 分别向外网服务器注册之后，它们之间可以相互访问。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT hairpinning:
  There are 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet2/1/1

NAT mapping behavior:
  Mapping mode: Endpoint-Independent
  ACL         : 2000

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
```

```
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到 Client A 访问 Client B 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.3/44929
  Destination IP/port: 202.38.1.3/1
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
Responder:
  Source      IP/port: 192.168.1.2/69
  Destination IP/port: 202.38.1.3/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
State: UDP_READY
Application: TFTP
Start time: 2012-08-15 15:53:36  TTL: 46s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            1 packets         56 bytes
Responder->Initiator:            1 packets         72 bytes

Total sessions found: 1
```

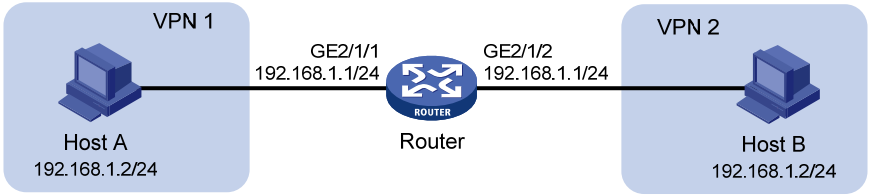
1.12.9 地址重叠的两个VPN之间互访

1. 组网需求

某公司两个部门由于需要业务隔而分属不同的 VPN 实例，且两个部门内部使用了相同的子网地址空间。现在要求这两个部门的主机 Host A 和 Host B 之间能够通过 NAT 地址互相访问。

2. 组网图

图1-14 地址重叠的两个内网之间互访



3. 配置思路

这是一个典型的两次 NAT 应用：两个 VPN 之间主机交互的报文的源 IP 地址和目的 IP 地址都需要转换，即需要在连接两个 VPN 的接口上先后进行两次 NAT，这可以通过在 NAT 设备的两侧接口上分别配置静态地址转换实现。

4. 配置步骤

按照组网图配置各接口的 VPN 实例和 IP 地址，具体配置过程略。

配置 VPN 1 内的 IP 地址 192.168.1.2 到 VPN 2 内的 IP 地址 172.16.1.2 之间的静态地址转换映射。

```
<Router> system-view
[Router] nat static outbound 192.168.1.2 vpn-instance vpn1 172.16.1.2 vpn-instance vpn2
```

配置 VPN 2 内的 IP 地址 192.168.1.2 到 VPN 1 内的 IP 地址 172.16.2.2 之间的静态地址转换映射。

```
[Router] nat static outbound 192.168.1.2 vpn-instance vpn2 172.16.2.2 vpn-instance vpn1
```

在接口 GigabitEthernet2/1/2 上使能静态地址转换。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat static enable
[Router-GigabitEthernet2/1/2] quit
```

在接口 GigabitEthernet2/1/1 上使能静态地址转换。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] nat static enable
[Router-GigabitEthernet2/1/1] quit
```

5. 验证配置

以上配置完成后，Host A 和 Host B 可以互通，且 Host A 的对外地址为 172.16.1.2，Host B 的对外地址为 172.16.2.2。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
Static NAT mappings:
  There are 2 outbound static NAT mappings.
  IP-to-IP:
    Local IP  : 192.168.1.2
    Global IP : 172.16.1.2
    Local VPN : vpn1
    Global VPN: vpn2

  IP-to-IP:
    Local IP  : 192.168.1.2
    Global IP : 172.16.2.2
    Local VPN : vpn2
```

```
    Global VPN: vpn1

Interfaces enabled with static NAT:
  There are 2 interfaces enabled with static NAT.
  Interface: GigabitEthernet2/1/1
             GigabitEthernet2/1/2

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到 Host A 访问 Host B 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.2/42496
  Destination IP/port: 172.16.2.2/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: vpn1/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 192.168.1.2/42496
  Destination IP/port: 172.16.1.2/0
  DS-Lite tunnel peer: -
```

```
  VPN instance/VLAN ID/VLL ID: vpn2/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2012-08-16 09:30:49  TTL: 27s
Interface(in) : GigabitEthernet2/1/1
Interface(out): GigabitEthernet2/1/2
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

1.12.10 负载分担内部服务器典型配置举例

1. 组网需求

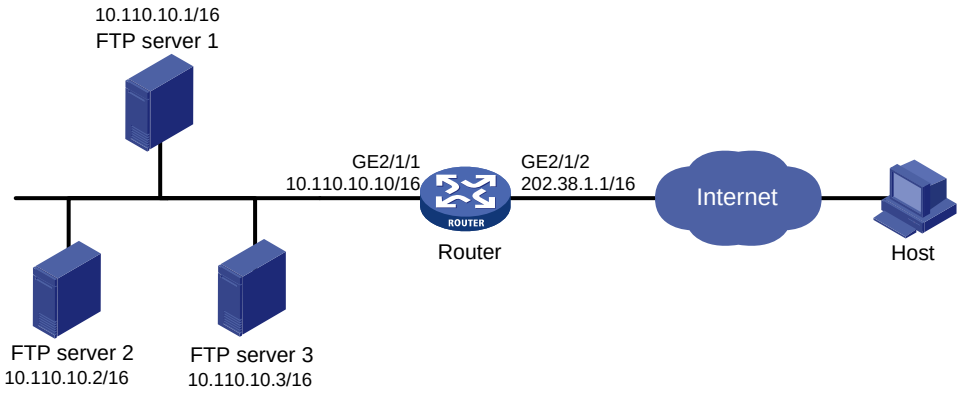
某公司内部拥有 3 台 FTP 服务器对外提供 FTP 服务。

需要实现如下功能：

- 使用 IP 地址为 202.38.1.1 作为公司对外提供服务的 IP 地址。
- 3 台 FTP 服务器可以同时对外提供服务，并进行负载分担。

2. 组网图

图1-15 负载分担内部服务器典型配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置内部服务器组 0 及其成员 10.110.10.1、10.110.10.2 和 10.110.10.3。

```
<Router> system-view
[Router] nat server-group 0
[Router-nat-server-group-0] inside ip 10.110.10.1 port 21
[Router-nat-server-group-0] inside ip 10.110.10.2 port 21
[Router-nat-server-group-0] inside ip 10.110.10.3 port 21
[Router-nat-server-group-0] quit
```

在接口 Gigabitethernet2/1/2 上配置负载分担内部服务器，引用内部服务器组 0，该组内的主机共同对外提供 FTP 服务。

```
[Router] interface gigabitethernet 2/1/2
```

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.1 ftp inside
server-group 0
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，外网主机可以访问内网 FTP 服务器组。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT server group information:
  There are 1 NAT server groups.
  Group Number      Inside IP             Port    Weight
  0                 10.110.10.1           21      100
                    10.110.10.2           21      100
                    10.110.10.3           21      100

NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/21
    Local  IP/port: server group 0
                    10.110.10.1/21         (Connections: 1)
                    10.110.10.2/21         (Connections: 2)
                    10.110.10.3/21         (Connections: 2)

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
```

```
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到外网主机访问内网某 FTP server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 202.38.1.25/53957
  Destination IP/port: 202.38.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.10.3/21
  Destination IP/port: 202.38.1.25/53957
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2012-08-16 11:06:07  TTL: 26s
Interface(in) : GigabitEthernet2/1/2
Interface(out): GigabitEthernet2/1/1
Initiator->Responder:            1 packets         60 bytes
Responder->Initiator:            2 packets        120 bytes

Total sessions found: 5
```

1.12.11 NAT DNS mapping典型配置举例

1. 组网需求

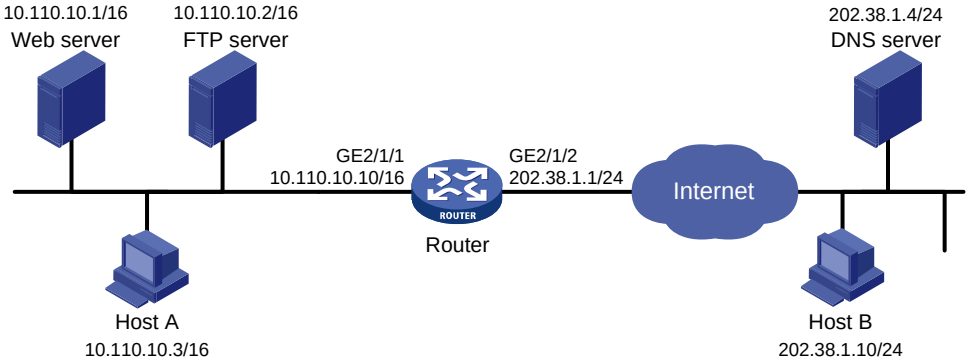
某公司内部对外提供 Web 和 FTP 服务。公司内部网址为 10.110.0.0/16。其中，Web 服务器地址为 10.110.10.1/16，FTP 服务器地址为 10.110.10.2/16。公司具有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。另外公司在外网有一台 DNS 服务器，IP 地址为 202.38.1.4。

需要实现如下功能：

- 选用 202.38.1.2 作为公司对外提供服务的 IP 地址。
- 外网用户可以通过域名或 IP 地址访问内部服务器。
- 内网用户可以通过域名访问内部服务器。

2. 组网图

图1-16 NAT DNS mapping 典型配置组网图



3. 配置思路

- 内网服务器对外提供服务，需要配置 NAT 内部服务器将各服务器的内网 IP 地址和端口映射为一个外网地址和端口。
- 内网主机通过域名访问内网服务器时，首先需要通过出接口地址转换分配的外网地址访问外网的 DNS 服务器，并获取内网服务器的内网 IP 地址。由于 DNS 服务器向内网主机发送的响应报文中包含的是内网服务器的外网地址，因此 NAT 设备需要将 DNS 报文载荷内的外网地址转换为内网地址，这可以通过查找 DNS mapping 映射表配合 DNS ALG 功能实现。DNS mapping 映射表用于实现根据“域名+外网 IP 地址+外网端口号+协议类型”查找到对应的“内网 IP+内网端口号”。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 的 NAT ALG 功能。

```
<Router> system-view
[Router] nat alg dns
```

进入接口 GigabitEthernet2/1/2。

```
[Router] interface gigabitethernet 2/1/2
```

配置 NAT 内部 Web 服务器，允许外网主机使用地址 202.38.1.2 访问内网 Web 服务器。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.2 inside 10.110.10.1
http
```

配置 NAT 内部 FTP 服务器，允许外网主机使用地址 202.38.1.2 访问内网 FTP 服务器。

```
[Router-GigabitEthernet2/1/2] nat server protocol tcp global 202.38.1.2 inside 10.110.10.2
ftp
```

在接口 GigabitEthernet2/1/2 上配置 Easy IP 方式的出方向动态地址转换。

```
[Router-GigabitEthernet2/1/2] nat outbound
[Router-GigabitEthernet2/1/2] quit
```

配置两条 DNS mapping 表项：Web 服务器的域名 www.server.com 对应 IP 地址 202.38.1.2；FTP 服务器的域名 ftp.server.com 对应 IP 地址 202.38.1.2。

```
[Router] nat dns-map domain www.server.com protocol tcp ip 202.38.1.2 port http
[Router] nat dns-map domain ftp.server.com protocol tcp ip 202.38.1.2 port ftp
[Router] quit
```

5. 验证配置

以上配置完成后，内网主机和外网主机均可以通过域名访问内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Router] display nat all
NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: ---          Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N

NAT internal server information:
  There are 2 internal servers.
  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/21
    Local  IP/port: 10.110.10.2/21

  Interface: GigabitEthernet2/1/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/80
    Local  IP/port: 10.110.10.1/80

NAT DNS mapping information:
  There are 2 NAT DNS mappings.
  Domain name: ftp.server.com
  Global IP  : 202.38.1.2
  Global port: 21
  Protocol   : TCP(6)

  Domain name: www.server.com
  Global IP  : 202.38.1.2
  Global port: 80
  Protocol   : TCP(6)

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
```

```
  DNS          : Enabled
  FTP          : Enabled
  H323         : Enabled
  ICMP-ERROR   : Enabled
  ILS          : Enabled
  MGCP         : Enabled
  NBT          : Enabled
  PPTP         : Enabled
  RTSP         : Enabled
  RSH          : Enabled
  SCCP         : Enabled
  SIP          : Enabled
  SQLNET       : Enabled
  TFTP         : Enabled
  XDMCP        : Enabled
```

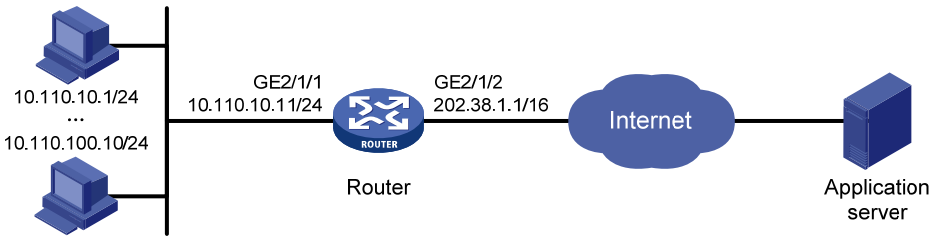
1.12.12 NAT444 端口块静态映射配置举例

1. 组网需求

内部网络用户 10.110.10.1～10.110.10.10 使用外网地址 202.38.1.100 访问 Internet。内网用户地址基于 NAT444 端口块静态映射方式复用外网地址 202.38.1.100，外网地址的端口范围为 10001～15000，端口块大小为 500。

2. 组网图

图1-17 NAT444 端口块静态映射配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

创建 NAT 端口块组 1。

```
<Router> system-view
[Router] nat port-block-group 1
```

添加私网地址成员 10.110.10.1～10.110.10.10。

```
[Router-port-block-group-1] local-ip-address 10.110.10.1 10.110.10.10
```

添加公网地址成员为 202.38.1.100。

```
[Router-port-block-group-1] global-ip-pool 202.38.1.100 202.38.1.100
```

配置端口块大小为 500，公网地址的端口范围为 10001～15000。

```
[Router-port-block-group-1] block-size 500
[Router-port-block-group-1] port-range 10001 15000
[Router-port-block-group-1] quit
```

在接口 GigabitEthernet2/1/2 上配置 NAT444 端口块静态映射，引用端口块组 1。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat outbound port-block-group 1
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，内网主机可以访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Router]display nat all
NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled

NAT port block group information:
  There are 1 NAT port block groups.
  Port block group 1:
    Port range: 10001-15000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.110.10.1          10.110.10.10         ---
    Global IP pool information:
```

```
      Start address         End address
      202.38.1.100          202.38.1.100

NAT outbound port block group information:
  There are 1 outbound port block group items.
  Interface: GigabitEthernet2/1/2
    Port block group: 1
```

通过以下显示命令，可以看到系统生成的静态端口块表项信息。

```
[Router]display nat port-block static
Local VPN      Local IP         Global IP        Port block     Connections
---            10.110.10.1      202.38.1.100     10001-10500    2
---            10.110.10.2      202.38.1.100     10501-11000    0
---            10.110.10.3      202.38.1.100     11001-11500    0
---            10.110.10.4      202.38.1.100     11501-12000    0
---            10.110.10.5      202.38.1.100     12001-12500    1
---            10.110.10.6      202.38.1.100     12501-13000    0
---            10.110.10.7      202.38.1.100     13001-13500    0
---            10.110.10.8      202.38.1.100     13501-14000    0
---            10.110.10.9      202.38.1.100     14001-14500    0
---            10.110.10.10     202.38.1.100     14501-15000    0
```

1.12.13 NAT444 端口块动态映射配置举例

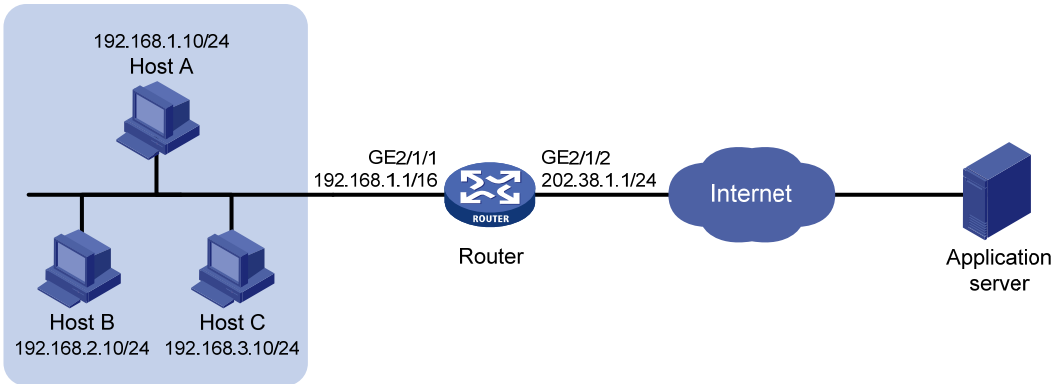
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

需要实现，内部网络中的 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。基于 NAT444 端口块动态映射方式复用两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024～65535，端口块大小为 300。当为某用户分配的端口块资源耗尽时，再为其增量分配 1 个端口块。

2. 组网图

图1-18 NAT444 端口块动态映射配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024～65535，端口块大小为 300，增量端口块数为 1。

```
<Router> system-view
[Router] nat address-group 0
[Router-address-group-0] address 202.38.1.2 202.38.1.3
[Router-address-group-0] port-range 1024 65535
[Router-address-group-0] port-block block-size 300 extended-block-number 1
[Router-address-group-0] quit
```

配置 ACL 2000，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/1/2 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] nat outbound 2000 address-group 0
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，Host A 能够访问外网服务器，Host B 和 Host C 无法访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Router]display nat all
NAT address group information:
  There are 1 NAT address groups.
  Address group 0:
    Port range: 1024-65535
    Port block size: 300
    Extended block number: 1
    Address iniformation:
      Start address         End address
      202.38.1.2            202.38.1.3

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet2/1/2
    ACL: 2000         Address group: 0      Port-preserved: N
    NO-PAT: N         Reversible: N

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
```

```
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RSH        : Enabled
  RTSP       : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到系统当前可分配的动态端口块总数和已分配的动态端口块个数。

```
[Router]display nat statistics
  Total session entries: 0
  Total EIM entries: 0
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 0
  Total dynamic port block entries: 430
  Active static port block entries: 0
  Active dynamic port block entries: 1
```

目 录

1 IP转发基础

1.1 IP转发概述

1.1.1 IP转发简介

不同网络之间通常使用网络层地址（即 IP 地址）来进行通信。路由器收到一个 IP 报文后，根据报文的目的地址查找转发表，指导 IP 报文进行转发。

1.1.2 IP转发表

1. 简介

转发表，即 FIB（Forwarding Information Base，转发信息库）表。

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”。

2. IP转发表内容

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:Useable   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        GE2/1/1                  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 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	**display fib** [**topology** *topo-name* | **vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]]

目 录

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，根据报文的目的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。

快速转发使用 5 元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号）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。

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。

1.2 配置快速转发

表1-1 配置快速转发

操作	命令	说明
进入系统视图	**system-view**	-
开启快速转发负载分担功能	**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
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

1.3 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1-2 快速转发显示和维护

操作	命令
显示快速转发表信息（MSR 2600/MSR 3600）	**display ip fast-forwarding cache** [*ip-address*]
显示快速转发表信息（MSR 5600）	**display ip fast-forwarding cache** [*ip-address*] [**slot** *slot-number*]
显示分片报文快速转发表信息（MSR 2600/MSR 3600）	**display ip fast-forwarding fragcache** [*ip-address*]
显示分片报文快速转发表信息（MSR 5600）	**display ip fast-forwarding fragcache** [*ip-address*] [**slot** *slot-number*]

操作	命令
显示快速转发表项的老化时间	**display ip fast-forwarding aging-time**
清除快速转发表信息（MSR 2600/MSR 3600）	**reset ip fast-forwarding cache**
清除快速转发表信息（MSR 5600）	**reset ip fast-forwarding cache** [**slot** *slot-number*]

1.4 快速转发典型配置举例

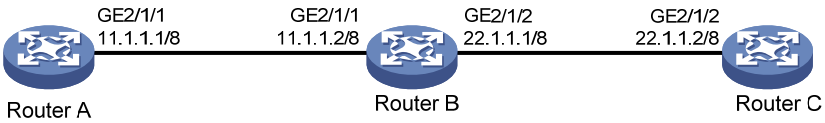
1.4.1 快速转发典型配置举例

1. 组网需求

在 Router B 上实现快速转发。

2. 组网图

图1-1 配置快速转发组网图



3. 配置步骤

(1) 配置 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 11.1.1.1 255.0.0.0
[RouterA-GigabitEthernet2/1/1] quit
```

配置静态路由。

```
[RouterA] ip route-static 22.1.1.0 255.0.0.0 11.1.1.2
```

(2) 配置 Router C

配置接口的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] ip address 22.1.1.2 255.0.0.0
[RouterC-GigabitEthernet2/1/2] quit
```

配置静态路由。

```
[RouterC] ip route-static 11.1.1.0 255.0.0.0 22.1.1.1
```

(3) 配置 Router B

开启快速转发功能。

```
<RouterB> system-view
[RouterB] ip fast-forwarding load-sharing
```

配置接口的 IP 地址。

```
[RouterB] interface gigabitethernet2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 11.1.1.2 255.0.0.0
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 22.1.1.1 255.0.0.0
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

在 Router B 查看快速转发表，这时未建立快转表项，结果如下：

```
[RouterB] display ip fast-forwarding cache
No fast-forwarding entries.
```

从 Router A 上 ping Router C 的 GigabitEthernet2/1/2 接口 IP 地址，能收到应答报文。

```
[RouterA] ping 22.1.1.2
  PING 22.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 22.1.1.2: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 22.1.1.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 22.1.1.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 22.1.1.2: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 22.1.1.2: bytes=56 Sequence=5 ttl=254 time=2 ms

  --- 22.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```

在 Router B 查看快速转发表，已建立快转表项，显示信息如下：

```
[RouterB] display ip fast-forwarding cache
Total number of fast-forwarding entries: 2
SIP            SPort DIP            DPort Pro Input_If   Output_If   Flg
22.1.1.2       0     11.1.1.1       0     1   GE2/1/2    GE2/1/1      7
11.1.1.1       8     22.1.1.2       0     1   GE2/1/1    GE2/1/2      7
```

目 录

1 流分类

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	流分类	不支持
MSR 3600		MSR 36-10/MSR 36-20/MSR 36-40/MSR 36-60支持 MSR3600-28/MSR3600-51不支持
MSR 5600		支持

1.1 流分类简介

流分类采用一定的规则识别符合某类特征的报文，是有区别地进行服务的前提和基础。

多核处理中，对于接收到的报文可以基于流或基于报文进行处理，具体含义如下：

- 基于流处理：用五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号）来区分和划定一条流，同一条流被分配到同一个 CPU 进行处理，处理过程保证先进先出。
- 基于报文处理：将报文依次发送到不同的 CPU 进行处理，不保证报文的处理顺序。

1.2 配置流分类策略

表1-1 配置流分类策略

操作	命令	说明
进入系统视图	**system-view**	-
配置流分类策略	**forwarding policy** { **per-flow** | **per-packet** }	缺省情况下，采用基于流处理的流分类策略

说明

当流分类策略配置为基于报文处理时，同一条流的报文会被发送到不同的 CPU 进行处理，这样无法保证报文的处理顺序。当启动某些业务时，该业务可能无法处理在不同的 CPU 的同一条流的报文而将报文丢弃。

目 录

1 邻接表

1.1 邻接表简介

1.1.1 邻接表介绍

邻接表用于管理各种链路层协议（如 PPP、ATM）的邻居信息。此处的邻居，是指 IP 层面的邻居，即对于三层转发来说一跳可达，不需要经过中间设备进行三层转发。

各种链路层协议通过协商（如 PPP 动态协商）或配置（如 ATM 静态配置）生成邻居信息后，将其下发给邻接表，生成邻接表表项。邻接表中记录了邻居的网络层地址（下一跳）、路由出接口、链路层协议类型、链路层地址（对 ATM 可以是 PVC，PPP 则没有这个信息）等信息。邻接表表项的更新、删除也由各链路层协议模块通知完成。

IP/IPv6 转发时，设备通过查找 FIB（Forwarding Information Base，转发信息库）/IPv6 FIB 表项得到报文的出接口和下一跳信息，再以此出接口和下一跳为索引查找邻接表，获取到该下一跳的链路层转发信息，如链路层协议（PPP、HDLC 等）及介质类型（P2P、NBMA）、封装报文的链路层头信息等，然后根据此信息对报文进行封装后转发。

说明

以太网类型邻居信息和非以太网类型邻居信息统一存储和管理，本文所描述的邻接表特指管理非以太网类型的邻居信息。

1.1.2 邻接表内容

通过 **display adjacent-table** 和 **display ipv6 adjacent-table** 命令可以查看邻接表的信息，例如：

显示所有 IPv4 邻接表项的详细信息。

```
<Sysname> display adjacent-table all verbose
 IP address                  : 0.0.0.0
 Routing interface           : Pos2/2/0
 Physical interface          : Pos2/2/0
 Logical interface           : N/A
 Service type                : PPP
 Action type                 : Forwarding
 Link media type             : P2P
 Slot                        : 2
 Virtual circuit information : N/A
 Link head information(IP)   : ff030021
 Link head information(MPLS) : ff030281
```

显示所有 IPv6 邻接表项的详细信息。

```
<Sysname> display ipv6 adjacent-table all verbose
 IPv6 address                : N/A
 Routing interface           : Pos2/2/0
```

```
Physical interface          : Pos2/2/0
Logical interface           : N/A
Service type                : PPP
Action type                 : Forwarding
Link media type             : P2P
Slot                        : 2
Virtual circuit information : N/A
Link head information(IPv6) : ff030057
```

邻接表中部分字段的含义如下：

- IP address：查找 FIB 表项得到的报文转发下一跳的地址，以此为索引来查找邻接表。
- Routing interface：路由出接口。查找 FIB 表项得到的报文转发的出接口，以此为索引来查找邻接表。该接口可能是逻辑接口，也可能是物理接口。
- Physical interface：路由出接口对应的实际发送报文的物理接口。如果 Routing interface 为物理接口，则 Routing interface、Physical interface 二者相同；如果 Routing interface 为逻辑接口，则 Routing interface、Physical interface 二者会不同。
- Logical interface：发送报文的逻辑接口。如：ATM 中的 Virtual-Ethernet 接口、MP 中的 Virtual-Template 接口等。
- Service type：链路层协议类型。如：PPP、HDLC 等。
- Action type：报文处理类型。表示匹配上此表项的报文应该做的动作。如：Forwarding 表示转发，Drop 表示丢弃。
- Link media type：链路介质类型。与路由出接口当前封装的链路层协议有关。如：P2P 表示点到点链路，NBMA 表示点对多点链路。
- Link head information (IP)：IPv4 协议对应的链路层头信息，用于 IP 转发时对报文进行封装。
- Link head information(IPv6)：IPv6 协议对应的链路层头信息，用于 IPv6 转发时对报文进行封装。
- Slot：单板所在的槽位号。
- Virtual circuit information：虚链路信息，如 PVC、DLCI 等（如果没有此信息，则显示为 N/A）
- Link head information(MPLS)：MPLS 协议对应的链路层头信息，用于 MPLS 转发时对报文进行封装。

1.2 邻接表显示和维护

在任意视图下执行 **display** 命令可以显示邻接表项的信息。

表1-1 邻接表显示和维护

操作	命令
显示IPv4邻接表项（MSR 2600/MSR 3600）	**display adjacent-table** { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* } [**count** | **verbose**]
显示IPv4邻接表项（MSR 5600）	**display adjacent-table** { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* | **slot** *slot-number* } [**count** | **verbose**]

操作	命令
显示IPv6邻接表项（MSR 2600/MSR 3600）	**display ipv6 adjacent-table** { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* } [**count** | **verbose**]
显示IPv6邻接表项（MSR 5600）	**display ipv6 adjacent-table** { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* | **slot** *slot-number* } [**count** | **verbose**]

目 录

1 IRDP


说明

- 本文提到的主机表示支持 IRDP 功能的主机。
- 本文提到的路由器表示具有路由功能的网络设备。

1.1 IRDP简介

1.1.1 IRDP的产生背景

一个网络中的主机如果要发送报文到网络外部，它至少需要获取本网络内的一台路由器的 IP 地址，由路由器把报文转发出去。主机通常有两种方式获取路由器的 IP 地址：一是在主机上配置默认网关，二是让主机侦听网络内的路由协议报文，从报文中获取路由器的 IP 地址。

这两种方式都有缺点。第一种要求静态配置，必须要手工维护，而且不能适应网络的动态变化；第二种方式要求主机能够识别各种路由协议的报文，这对于一台主机来说要求太高了，而且有时路由器上不运行动态路由协议，此时主机便无法侦听到路由协议报文。

为了解决上述问题，出现了 IRDP（ICMP Router Discovery Protocol，ICMP 路由器发现协议）。IRDP 是 ICMP 协议的一个扩展，它采用两种新的 ICMP 消息类型来实现主机对路由器的发现，使得主机能够动态地发现本地网络中路由器的 IP 地址，并设置自己的缺省路由。IRDP 可以动态适应网络的变化，也不用手工维护大量的配置，并且不依赖于任何一种具体的路由协议。

1.1.2 IRDP的工作机制

IRDP 中用到两种 ICMP 消息：

- 路由公告消息 RA（Router Advertisements）：由路由器发送，用于公告该路由器的 IP 地址、优先级等信息。
- 路由请求消息 RS（Router Solicitations）：由主机发送，用于主动向网络中的路由器请求其 IP 地址。

IRDP 的工作机制如下：

- 路由器周期性的从接口发送 RA，公告该接口的 IP 地址（包括接口的主 IP 地址和从 IP 地址）。主机接收到 RA 后，就会获取到网络中路由器的 IP 地址。
- 当一台主机刚刚连接到网络上，它可以主动发送 RS 来请求路由器的 IP 地址，而不是被动等待 RA。如果主机发送的 RS 没有回应，它可以重传几次 RS。如果主机通过上述主动方式不能获取路由器的IP地址，那么还可以通过后续路由器周期性公告RA来获取路由器的IP地址。
- 主机接收到 RA 后，将根据 RA 中包含的 IP 地址，添加本地路由。如果主机希望缺省路由也从 RA 中获取，那么主机将从收到的所有 RA 包含的 IP 地址中选择一个优先级最高的 IP 地址作为本机缺省路由。

IRDP 功能只能使主机获取路由器的 IP 地址，但并不能帮主机判断出通过哪台路由器到达目的地址是最优的。如果主机选中了一台到达某目的地非最优的路由器作为报文转发路由器，一旦报文转发到那台路由器后，主机会收到从那台路由器发来的一个 ICMP 重定向报文，让主机发往这个目的地的报文重定向到一台更优的路由器上。

1.1.3 IRDP基本概念

1. IP地址的优先级

RA 中每一个被公告的 IP 地址都对应一个“优先级”值，这个优先级是主机选择缺省路由的依据。当主机希望从 RA 中获取缺省路由时，它将从收到的所有 RA 包含的 IP 地址中选择一个优先级最高的 IP 地址作为本机缺省路由。

用户可以对路由器公告的 IP 地址的优先级进行配置，以控制主机优先选择哪个 IP 地址作为缺省路由。

优先级值越大表示优先级越高。最小的优先级值（-2147483648）表示主机不要使用这个地址作为缺省路由。

2. IP地址的生命周期

生命周期表示路由器公告的 IP 地址可以在主机上存在的时间。如果在生命周期内主机没有收到包含该 IP 地址的新的 RA，那么该 IP 地址将被删除。

通过同一个接口公告出去的所有 IP 地址具有相同的生命周期。

3. 周期性发送RA的时间间隔

使能 IRDP 功能后，路由器会周期性发送 RA。发送 RA 不是完全周期性的，每两次发送 RA 的时间间隔是在最小时间间隔和最大时间间隔之间的一个随机值，从而避免同一链路上多个路由器同时发送 RA 对网络性能的影响。

在丢包严重的链路上，建议缩短 RA 的发送周期。

4. RA消息的目的地址

RA 消息的目的 IP 地址可以有两种：广播地址 255.255.255.255、组播地址 224.0.0.1（本地链路所有主机）。

缺省情况下，RA 消息的目的 IP 地址采用广播地址。如果发送 RA 的接口支持组播报文，那么建议使用组播地址 224.0.0.1 作为 RA 消息的目的 IP 地址。

5. 代理公告IP地址

缺省情况下，接口仅向外公告接口的主 IP 地址和从 IP 地址，如果用户希望接口公告其他 IP 地址，可以通过命令行手工配置该接口代理公告的 IP 地址。

1.1.4 协议规范

与 IRDP 相关的协议规范有：

- RFC 1256：ICMP Router Discovery Messages

1.2 配置IRDP

表1-1 配置 IRDP

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	支持配置IP地址的三层接口，不包括loopback口
使能接口的IRDP功能	**ip irdp**	只有使能接口的IRDP功能，其他IRDP相关配置才生效，设备才会从该接口发送路由公告消息RA 缺省情况下，接口的IRDP功能处于关闭状态
（可选）配置接口公告的接口IP地址的优先级	**ip irdp preference** *preference-value*	缺省情况下，接口公告的接口IP地址的优先级为0 本配置对接口公告出去的所有接口IP地址（包括接口主IP地址和从IP地址）有效
（可选）配置接口公告的IP地址的生命周期	**ip irdp lifetime** *lifetime-value*	缺省情况下，接口公告的IP地址的生命周期为1800秒 本配置对接口公告出去的所有IP地址（包括接口IP地址和代理公告的IP地址）有效 接口公告的IP地址的生命周期必须大于等于接口发送周期性RA的最大时间间隔
（可选）配置接口发送周期性RA的最大时间间隔和最小时间间隔	**ip irdp interval** *max-interval-value* [*min-interval-value*]	缺省情况下，接口发送周期性RA的最大时间间隔为600秒，最小时间间隔为最大时间间隔的0.75倍
（可选）配置接口发送的RA消息的目的IP地址为组播地址224.0.0.1	**ip irdp multicast**	缺省情况下，接口发送的RA消息的目的IP地址为广播地址255.255.255.255
（可选）配置接口代理公告的IP地址	**ip irdp address** *ip-address preference-value*	该命令支持重复配置，设备上接口最多支持配置4个代理公告的IP地址 缺省情况下，未设置接口代理公告的IP地址

1.3 IRDP典型配置举例

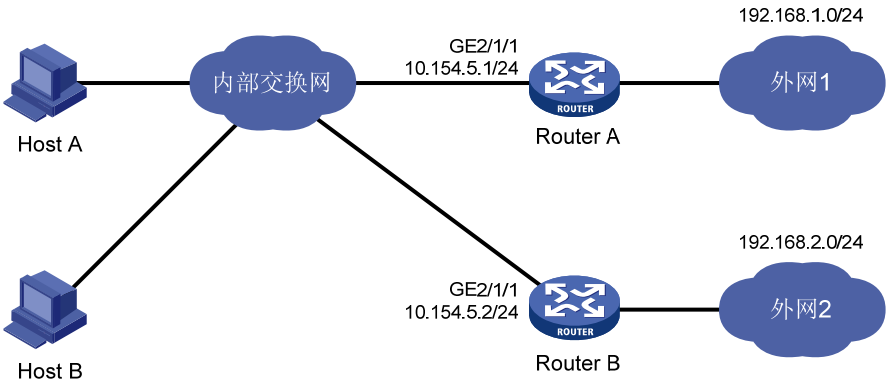
1. 组网需求

- 公司内部网络中有两台 Linux 系统的主机 Host A 和 Host B，支持 IRDP 功能。
- 内部交换网连接了两台出口路由器 Router A 和 Router B，分别到达外网 192.168.1.0/24 和 192.168.2.0/24。

用户希望两台主机使用 Router A 作为缺省路由器，并且到两个外网的报文能正确路由。

2. 组网图

图1-1 配置 IRDP 组网图



3. 配置步骤

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.154.5.1 24
```

使能接口 GigabitEthernet2/1/1 的 IRDP 功能。

```
[RouterA-GigabitEthernet2/1/1] ip irdp
```

配置接口 GigabitEthernet2/1/1 公告的接口 IP 地址的优先级为 1000。

```
[RouterA-GigabitEthernet2/1/1] ip irdp preference 1000
```

配置接口 GigabitEthernet2/1/1 发送的 RA 消息的目的 IP 地址为组播地址。

```
[RouterA-GigabitEthernet2/1/1] ip irdp multicast
```

配置接口 GigabitEthernet2/1/1 代理公告 IP 地址为 192.168.1.0，优先级为 400。

```
[RouterA-GigabitEthernet2/1/1] ip irdp address 192.168.1.0 400
```

(2) 配置 Router B

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 10.154.5.2 24
```

使能接口 GigabitEthernet2/1/1 的 IRDP 功能。

```
[RouterB-GigabitEthernet2/1/1] ip irdp
```

配置接口 GigabitEthernet2/1/1 公告的接口 IP 地址的优先级为 500。

```
[RouterB-GigabitEthernet2/1/1] ip irdp preference 500
```

配置接口 GigabitEthernet2/1/1 发送的 RA 消息的目的 IP 地址为组播地址。

```
[RouterB-GigabitEthernet2/1/1] ip irdp multicast
```

配置接口 GigabitEthernet2/1/1 代理公告 IP 地址为 192.168.2.0，优先级为 400。

```
[RouterB-GigabitEthernet2/1/1] ip irdp address 192.168.2.0 400
```

4. 验证配置

Host A 和 Host B 打开 IRDP 功能后，查看 Host A 的路由表。

```
[HostA@localhost ~]$ netstat -rne
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.154.5.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
0.0.0.0         10.154.5.1      0.0.0.0         UG    0      0        0 eth1
```

从上面的信息可以看出，Host A 的缺省路由是 10.154.5.1，并且有到达外网 192.168.1.0/24、192.168.2.0/24 的路由。

查看 Host B 的路由表。

```
[HostB@localhost ~]$ netstat -rne
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.154.5.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
0.0.0.0         10.154.5.1      0.0.0.0         UG    0      0        0 eth1
```

从上面的信息可以看出，Host B 的缺省路由是 10.154.5.1，并且有到达外网 192.168.1.0/24、192.168.2.0/24 的路由。

目 录

1 IP性能优化

1.1 IP性能优化简介

在一些特定的网络环境里，可以通过调整 IP 的参数，以使网络性能达到最佳。IP 性能的优化配置包括：

- 配置允许接收和发送定向广播报文
- 配置接口 MTU
- 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
- 配置 TCP 的 SYN Cookie 功能
- 配置 TCP 连接的缓冲区大小
- 配置 TCP 定时器
- 配置 ICMP 差错报文发送功能
- 配置 ICMP 分片报文转发功能
- 配置指定时间内发送 ICMP 差错报文的最大个数
- 配置 ICMP 报文指定源地址功能

1.2 配置允许接口接收和转发直连网段的定向广播报文

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。

接口接收和转发直连网段的定向广播报文包括以下几种情况：

- 在接收定向广播报文的情况下，如果在接口上配置了此命令，设备允许接收此接口直连网段的定向广播报文。
- 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，设备接口需要接收或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接收和转发直连网段的定向广播报文。

1.2.1 配置允许接口接收和转发直连网段的定向广播报文

表1-1 配置允许接口接收和转发直连网段的定向广播报文

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置允许接口接收和转发面向直连网段的定向广播报文	**ip forward-broadcast**	缺省情况下，设备禁止转发直连网段的定向广播报文

1.2.2 允许接口接收和转发直连网段的定向广播报文配置举例

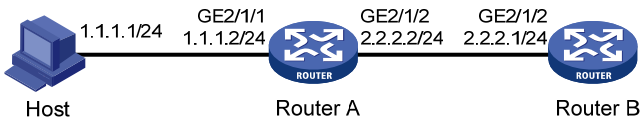
1. 组网需求

如 图 1-1 所示，Host的接口和Router A的接口GigabitEthernet2/1/1 处于同一个网段（1.1.1.0/24），Router A的接口GigabitEthernet2/1/2 和Router B的接口GigabitEthernet2/1/2 处于另外一个网段（2.2.2.0/24）。Host上配置默认网关为Router A的接口GigabitEthernet2/1/1 的地址（1.1.1.2/24），Router B上配置静态路由使得Host与Router B之间路由可达。

要求通过配置使得 Router B 可以收到 Host 发送的定向广播报文。

2. 组网图

图1-1 配置收发定向广播报文组网图



3. 配置步骤

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 1.1.1.2 24
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 2.2.2.2 24
```

配置允许接口 GigabitEthernet2/1/2 转发直连网段的定向广播报文。

```
[RouterA-GigabitEthernet2/1/2] ip forward-broadcast
```

(2) 配置 Router B

配置 Router B 到 Host 的静态路由。

```
<RouterB> system-view
[RouterB] ip route-static 1.1.1.1 24 2.2.2.2
```

配置接口 GigabitEthernet2/1/2 的 IP 地址。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 2.2.2.1 24
```

配置允许接口 GigabitEthernet2/1/2 接收直连网段的定向广播报文。

```
[RouterB-GigabitEthernet2/1/2] ip forward-broadcast
```

配置完成以后，在 Host 上 ping Router A 的接口 GigabitEthernet2/1/2 所在子网网段的广播地址（2.2.2.255）时，Router B 的接口 GigabitEthernet2/1/2 可以收到该报文。取消掉 **ip forward-broadcast** 的配置，Router B 的接口 GigabitEthernet2/1/2 就不能收到该报文。

1.3 配置接口MTU

当设备收到一个报文后，如果发现报文长度比转发接口的 MTU 值大，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。

表 1-4 配置接口 MTU

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口MTU	**ip mtu** *mtu-size*	缺省情况下，没有配置接口MTU

1.4 配置接口的TCP最大报文段长度

TCP 最大报文段长度（Max 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。

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，当接口上配置了 MPLS 功能后，不建议再配置本功能。

表1-2 配置接口的 TCP 最大报文段长度

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口的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

1.5 配置TCP连接的Path MTU探测功能

RFC 1191 中规定的 TCP 连接的 Path MTU 探测功能，可以探测 TCP 路径上从源端到目的端的最小 MTU，其探测机制如下：

(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＝最小 MTU 值－IP 头部长度－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）。

用户通过命令行开启 TCP 连接的 Path MTU 探测功能后，新建的 TCP 连接均会携带 Path MTU 探测属性，可以通过上述探测机制确定 Path MTU，按照数据路径上的最小 MTU 组织 TCP 分段长度，最大限度利用网络资源，避免 IP 分片的发生。

Path MTU 值可以老化，这样当 Path MTU 增大时可以充分利用网络资源，尽量按照转发路径可以容忍的最大报文长度发送数据。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。
- 当该定时器超时后，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 分钟内没有收到 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。

表1-3 配置 TCP 连接的 Path MTU 探测功能

操作	命令	说明
进入系统视图	**system-view**	-
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

说明

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 unreachables enable**），以确保 ICMP 差错报文可以发送到 TCP 源端。

1.6 配置TCP的SYN Cookie功能

一般情况下，TCP 连接的建立需要经过三次握手，即：

(1) TCP 连接请求的发起者向目标服务器发送 SYN 报文；

(2) 目标服务器收到 SYN 报文后，建立处于 SYN_RECEIVED 状态的 TCP 半连接，并向发起者回复 SYN ACK 报文，等待发起者的回应；

(3) 发起者收到 SYN ACK 报文后，回应 ACK 报文，这样 TCP 连接就建立起来了。

利用 TCP 连接的建立过程，一些恶意的攻击者可以进行 SYN Flood 攻击。攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。在服务器上配置此功能后，当服务器收到 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。服务器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，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

表1-4 配置 TCP 的 SYN Cookie 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SYN Cookie功能	**tcp syn-cookie enable**	缺省情况下，SYN Cookie功能处于关闭状态

1.7 配置TCP连接的缓冲区大小

表1-5 配置 TCP 连接的缓冲区大小

操作	命令	说明
进入系统视图	**system-view**	-
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64KB

1.8 配置TCP定时器

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，如果 synwait 超时前未收到回应报文，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没有收到报文，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。

表1-6 配置 TCP 定时器

操作	命令	说明
进入系统视图	**system-view**	-
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
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

1.9 配置ICMP差错报文发送功能

发送差错报文是 ICMP（Internet Control Message Protocol，互联网控制报文协议）的主要功能之一。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。

重定向报文、超时报文、目的不可达报文是 ICMP 差错报文中的三种。下面分别介绍这三种差错报文发送的条件及作用。

(1) ICMP 重定向报文发送功能

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) ICMP 超时报文发送功能

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。

(3) ICMP 目的不可达报文发送功能

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“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。

ICMP 差错报文的发送虽然方便了网络的控制管理，但是也存在缺限：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，可以关闭设备的 ICMP 差错报文发送功能，从而减少网络流量、防止遭到恶意攻击。

表1-7 配置 ICMP 差错报文发送功能

操作	命令	说明
进入系统视图	**system-view**	-
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
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
开启ICMP目的不可达报文发送功能	**ip unreachables enable**	缺省情况下，ICMP目的不可达报文发送功能处于关闭状态

说明

- 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。
- 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”。

1.10 配置指定时间内发送ICMP差错报文的最大个数

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，即每隔多长时间将令牌桶内的令牌个数刷新为所配置的容量。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。

表1-8 配置指定时间内发送 ICMP 差错报文的最大个数

操作	命令	说明
进入系统视图	**system-view**	-
配置指定时间内发送ICMP差错报文的最大个数	**ip icmp error-interval** *milliseconds* [*bucketsize*]	缺省情况下，令牌桶容量为10，令牌桶的刷新周期为100毫秒，即每一个刷新周期内最多可以发送10个ICMP差错报文 刷新周期为0时，表示不限制ICMP差错报文的发送

1.11 配置ICMP报文指定源地址功能

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，可以配置 ICMP 报文指定源地址功能。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。

表1-9 配置 ICMP 报文指定源地址功能

操作	命令	说明
进入系统视图	**system-view**	-
开启设备的ICMP报文指定源地址功能	**ip icmp source** [**vpn-instance** *vpn-instance-name*] *ip-address*	缺省情况下，ICMP报文指定源地址功能处于关闭状态

说明

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。

1.12 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1-10 IP 性能优化显示和维护

操作	命令
显示RawIP连接摘要信息（MSR 2600/MSR 3600）	**display rawip**
显示RawIP连接摘要信息（MSR 5600）	**display rawip** [**slot** *slot-number*]

操作	命令
显示RawIP连接详细信息（MSR 2600/MSR 3600）	**display rawip verbose** [**pcb** *pcb-index*]
显示RawIP连接详细信息（MSR 5600）	**display rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示TCP连接摘要信息（MSR 2600/MSR 3600）	**display tcp**
显示TCP连接摘要信息（MSR 5600）	**display tcp** [**slot** *slot-number*]
显示TCP连接详细信息（MSR 2600/MSR 3600）	**display tcp verbose** [**pcb** *pcb-index*]
显示TCP连接详细信息（MSR 5600）	**display tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示UDP连接摘要信息（MSR 2600/MSR 3600）	**display udp**
显示UDP连接摘要信息（MSR 5600）	**display udp** [**slot** *slot-number*]
显示UDP连接详细信息（MSR 2600/MSR 3600）	**display udp verbose** [**pcb** *pcb-index*]
显示UDP连接详细信息（MSR 5600）	**display udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示IP报文统计信息（MSR 2600/MSR 3600）	**display ip statistics**
显示IP报文统计信息（MSR 5600）	**display ip statistics** [**slot** *slot-number*]
显示TCP连接的流量统计信息（MSR 2600/MSR 3600）	**display tcp statistics**
显示TCP连接的流量统计信息（MSR 5600）	**display tcp statistics** [**slot** *slot-number*]
显示UDP流量统计信息（MSR 2600/MSR 3600）	**display udp statistics**
显示UDP流量统计信息（MSR 5600）	**display udp statistics** [**slot** *slot-number*]
显示ICMP流量统计信息（MSR 2600/MSR 3600）	**display icmp statistics**
显示ICMP流量统计信息（MSR 5600）	**display icmp statistics** [**slot** *slot-number*]
清除IP报文统计信息（MSR 2600/MSR 3600）	**reset ip statistics**
清除IP报文统计信息（MSR 5600）	**reset ip statistics** [**slot** *slot-number*]
清除TCP连接的流量统计信息	**reset tcp statistics**
清除UDP流量统计信息	**reset udp statistics**

目 录

1 UDP Helper

1.1 UDP Helper简介

UDP Helper（UDP 中继转发）功能包括三部分：

- 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。
- 组播 UDP Helper：将指定 UDP 端口的组播报文转换为广播报文或单播报文。

UDP 广播报文可以分为以下两类：

- 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 地址中网络号为特定网络的网络号，主机号为全 1。譬如一个 B 类 IP 地址 128.1.1.1 的定向广播地址就是 128.1.255.255。
- 受限广播报文是指发送给接口所在子网主机的广播报文，该报文的目的 IP 地址为 255.255.255.255。

1.1.1 广播转单播UDP Helper

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。

使能广播转单播 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。

1.1.2 广播转组播UDP Helper

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。

1.1.3 组播UDP Helper

组播 UDP Helper 包括组播转单播和组播转广播。

在某些特定组网下，网络中的中间设备通过组播转发报文，边缘设备通过广播或单播转发报文，在组播转发的最后一跳可以通过配置组播 MAP 将组播报文转换成广播或单播报文。

配置 UDP Helper 组播 MAP 功能后，当设备收到组播报文时，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，则查找配置的组播 MAP 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 MAP 映射的 IP 地址，将报文转发出去。

1.2 配置广播转单播UDP Helper

提示

一些支持定向广播报文抑制功能的设备，缺省情况下禁止接收接口所在子网的定向广播报文，此类设备只有在接口视图下配置 **ip forward-broadcast** 命令后，UDP Helper 功能才可用。有些支持定向广播报文抑制功能的设备，缺省情况下允许接收接口所在子网的定向广播报文，此类设备不需配置 **ip forward-broadcast** 命令，UDP Helper 功能也可以使用。定向广播报文抑制功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“IP 性能优化”。

表1-1 配置广播转单播 UDP Helper

操作	命令	说明
进入系统视图	**system-view**	-
使能UDP Helper功能	**udp-helper enable**	缺省情况下，UDP Helper功能处于关闭状态
配置需要中继转发的UDP端口	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	缺省情况下，没有配置中继转发的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
进入接口视图	**interface** *interface-type interface-number*	-
配置广播转单播中继转发的目的服务器	**udp-helper server** *ip-address* [**global** | **vpn-instance** *vpn-instance-name*]	缺省情况下，没有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）

1.3 配置广播转组播UDP Helper

提示

一些支持定向广播报文抑制功能的设备，缺省情况下禁止接收接口所在子网的定向广播报文，此类设备只有在接口视图下配置 **ip forward-broadcast** 命令后，UDP Helper 功能才可用。有些支持

定向广播报文抑制功能的设备，缺省情况下允许接收接口所在子网的定向广播报文，此类设备不需配置 **ip forward-broadcast** 命令，UDP Helper 功能也可以使用。定向广播报文抑制功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“IP 性能优化”。

表1-2 配置广播转组播 UDP Helper

操作	命令	说明
进入系统视图	**system-view**	-
使能UDP Helper功能	**udp-helper enable**	缺省情况下，UDP Helper功能处于关闭状态
配置需要中继转发的UDP端口	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	缺省情况下，没有配置中继转发的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
进入接口视图	**interface** *interface-type interface-number*	-
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，没有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）

1.4 配置组播 UDP Helper

表1-3 配置组播 UDP Helper

操作	命令	说明
进入系统视图	**system-view**	-
使能UDP Helper功能	**udp-helper enable**	缺省情况下，UDP Helper功能处于关闭状态
配置需要中继转发的UDP端口	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	缺省情况下，没有配置中继转发的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
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置组播MAP映射	**udp-helper multicast-map** *multicast-address ip-address* [**global** | **vpn-instance** *vpn-instance-name*] [**acl** *acl-number*]	缺省情况下，没有配置组播MAP映射 请在接收组播报文的入接口上配置组播MAP映射 当*ip-address*配置为单播地址时将实现组播转单播，当*ip-address*为定向广播时将实现组播转广播

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1-4 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	**display udp-helper interface** *interface-type interface-number*
清除广播转单播中继转发的报文统计数目	**reset udp-helper statistics**

1.6 UDP Helper典型配置举例

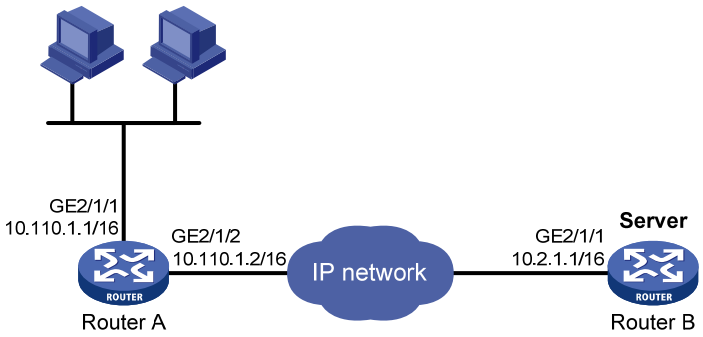
1.6.1 广播转单播UDP Helper典型配置举例

1. 组网需求

如 图 1-1 所示，Router A的GigabitEthernet2/1/1 接口的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 Router A 到网段 10.2.0.0/16 路由可达。

开启 UDP Helper 功能。

```
<RouterA> system-view
[RouterA] udp-helper enable
```

配置将目的 UDP 端口号为 55 的广播报文进行中继转发。

```
[RouterA] udp-helper port 55
```

将 Router A 的接口 GigabitEthernet2/1/2 加入私网 VPN a。

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip binding vpn-instance a
[RouterA-GigabitEthernet2/1/2] quit
```

配置中继转发的目的服务器为 10.2.1.1。

```
[RouterA] interface GigabitEthernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.110.1.1 16
[RouterA-GigabitEthernet2/1/1] udp-helper server 10.2.1.1 vpn-instance a
```

4. 验证配置

显示 GigabitEthernet2/1/1 接口的广播转单播 UDP Helper 的相关信息。

```
[RouterA-GigabitEthernet2/1/1] display udp-helper interface gigabitethernet 2/1/1
Interface                Server VPN instance           Server address   Packets sent
GigabitEthernet2/1/1     a                             10.2.1.1         5
```

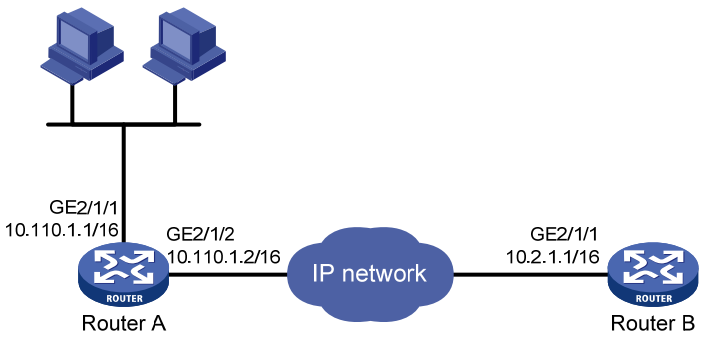
1.6.2 广播转组播UDP Helper典型配置举例

1. 组网需求

如 图 1-2 所示，Router A的GigabitEthernet2/1/1 接口的IP地址为 10.110.1.1/16，连接到网段 10.110.0.0/16，Router B在组播组 225.1.1.1 中。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 Router A 到网段 10.2.0.0/16 路由可达。

开启 UDP Helper 功能。

```
<RouterA> system-view
[RouterA] udp-helper enable
```

配置将目的 UDP 端口号为 55 的广播报文进行中继转发。

```
[RouterA] udp-helper port 55
```

在广播报文的入接口上配置广播到组播映射。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.110.1.1 16
[RouterA-GigabitEthernet2/1/1] udp-helper broadcast-map 225.1.1.1
[RouterA-GigabitEthernet2/1/1] quit
```

在路由器 A 上全局使能组播路由，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。

```
[RouterA] multicast routing
[Sysname-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim dm
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] igmp static-group 225.1.1.1
```

在路由器 A 的接口 GigabitEthernet2/1/2 上配置组播协议，允许转换后的组播报文从该口出。

```
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] igmp enable
[RouterA-GigabitEthernet2/1/2] igmp static-group 225.1.1.1
```

4. 验证配置

通过抓包，分析发现 Router B 能接收到来自 Router A 转发的组播报文。

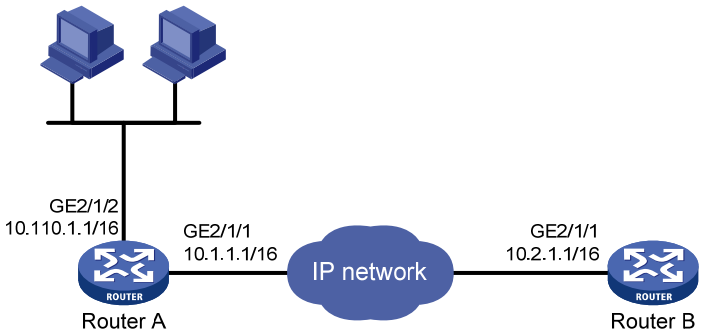
1.6.3 组播UDP Helper典型配置举例

1. 组网需求

Router A 的 GigabitEthernet2/1/2 接口的 IP 地址为 10.110.1.1/16，连接到网段 10.110.0.0/16，Router B 的接口 GigabitEthernet2/1/1 在组播组 225.1.1.1 中。配置将 Router B 发送过来的目的 UDP 端口号为 55、目的组播地址为 225.1.1.1 的组播报文广播到 10.110.0.0/16 网段的所有主机。

2. 组网图

图1-3 UDP Helper 组播 MAP 配置举例组网图



3. 配置步骤

说明

用户需保证 Router A 到网段 10.2.0.0/16 路由可达。

开启 UDP Helper 功能。

```
<RouterA> system-view
[RouterA] udp-helper enable
```

配置将目的 UDP 端口号为 55 的组播报文进行中继转发。

```
[RouterA] udp-helper port 55
```

配置组播 MAP 映射。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] udp-helper multicast-map 225.1.1.1 10.110.255.255
```

4. 验证配置

通过抓包，分析发现 Router A 中接口 GigabitEthernet2/1/2 所在网段 10.110.0.0/16 的所有主机能收到转发后的广播报文。

目 录

1 IPv6 基础

1.1 IPv6简介

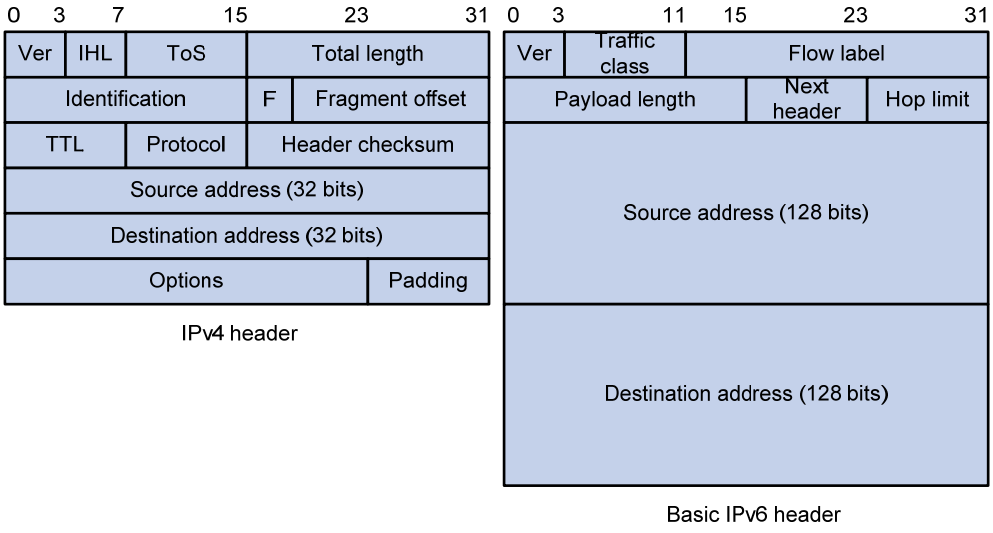
IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。

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 3.4×10^{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 的互联网控制报文协议）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：

FF02:0:0:0:0:1:FFXX:XXXX

其中，FF02:0:0:0:0:1:FF 为 104 位固定格式；XX:XXXX 为单播或任播 IPv6 地址的后 24 位。

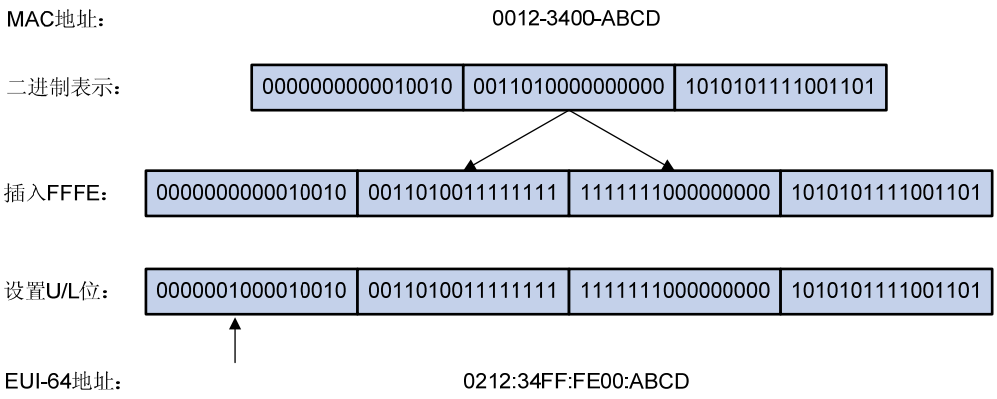
5. IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来标识链路上的一个唯一的接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。

不同接口的 IEEE EUI-64 格式的接口标识符的生成方法不同，分别介绍如下：

- 所有 IEEE 802 接口类型（例如，以太网接口、VLAN 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（1111111111111110）。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



- Tunnel 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”。
- 其他接口类型（例如，Serial 接口）：IEEE EUI-64 格式的接口标识符由设备随机生成。

1.1.3 IPv6 邻居发现协议介绍

IPv6 邻居发现（Neighbor Discovery，ND）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功能。

邻居发现协议使用的ICMPv6 消息的类型及作用如 表 1-3 所示。

表1-3 邻居发现协议使用的 ICMPv6 消息类型及作用

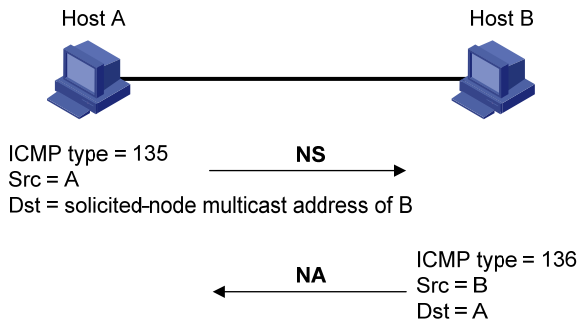
ICMPv6 消息	类型号	作用
邻居请求消息NS（Neighbor Solicitation）	135	获取邻居的链路层地址
		验证邻居是否可达
		进行重复地址检测
邻居通告消息NA（Neighbor Advertisement）	136	对NS消息进行响应
		节点在链路层变化时主动发送NA消息，向邻居节点通告本节点的变化信息
路由器请求消息RS（Router Solicitation）	133	节点启动后，通过RS消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息RA（Router Advertisement）	134	对RS消息进行响应
		在没有抑制RA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

邻居发现协议提供的主要功能如下：

1. 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 1-3 所示，节点A要获取节点B的链路层地址。

图1-3 地址解析示意图



(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。

2. 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。

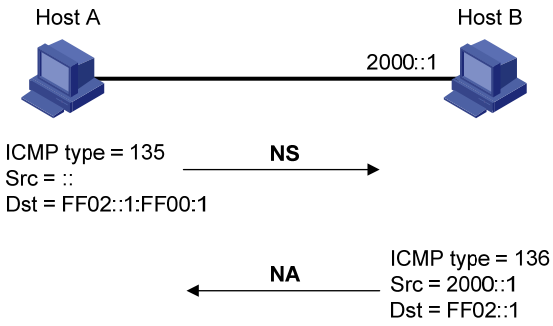
(1) 节点发送 NS 消息，其中目的地址是邻居节点的 IPv6 地址。

(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。

3. 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）。通过NS和NA可以实现重复地址检测，如 图 1-4 所示。

图1-4 重复地址检测示意图



(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。

4. 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。

5. 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：

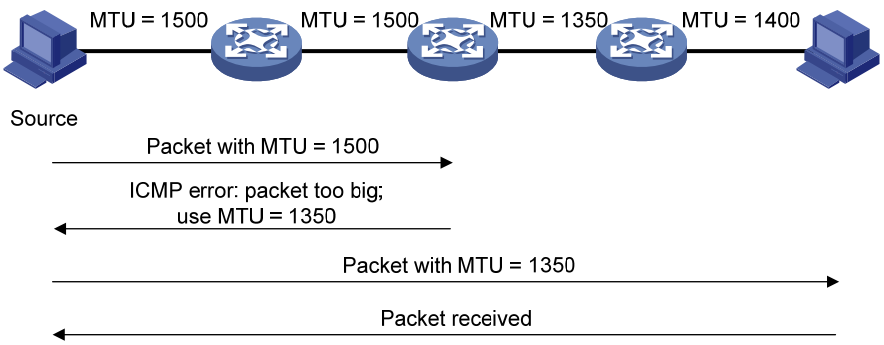
- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMPv6 重定向报文创建或修改过；
- 被选择的路由不是设备的缺省路由；
- 被转发的 IPv6 数据报文中不包含路由扩展头。

1.1.4 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。PMTU的工作过程如 图 1-5 所示。

图1-5 PMTU 发现工作过程



(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。

(4) 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。

1.1.5 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。

目前解决过渡问题的基本技术主要有 4 种：双协议栈（RFC 2893）、隧道技术（RFC 2893）、NAT-PT（RFC 2766）、6PE。

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

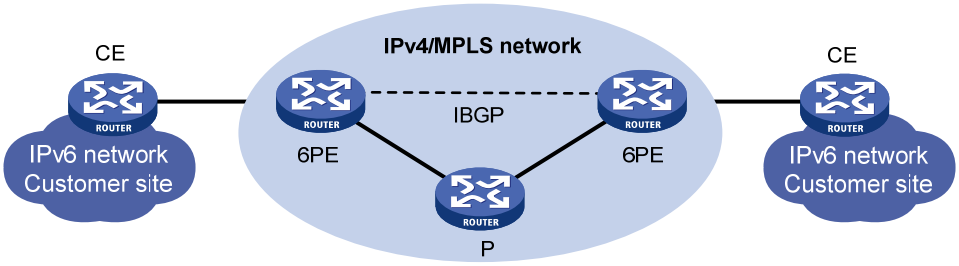
NAT-PT（Network Address Translation-Protocol Translation，附带协议转换的网络地址转换）作用于 IPv4 和 IPv6 网络边缘的设备上，用于实现 IPv6 与 IPv4 报文的转换。NAT-PT 在 IPv4 和 IPv6 网络之间转换 IP 报头的地址，同时根据协议不同对报文做相应的语义翻译，使纯 IPv4 节点和纯 IPv6 节点之间能够透明通信。这种技术适用于仅运行 IPv6 的节点和仅运行 IPv4 的节点之间的通信，具有一定的局限性。关于 NAT-PT 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“NAT-PT”。

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。有关 6PE 的详细介绍及配置请参见“三层技术-IP 路由配置指导”中的“IPv6 BGP”。

图1-6 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。

1.1.6 协议规范

与 IPv6 基础相关的协议规范有：

- 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
- RFC 4861：Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862：IPv6 Stateless Address Autoconfiguration

1.2 IPv6基础配置任务简介

表1-4 IPv6 基础配置任务简介

配置任务		说明	详细配置
配置IPv6基本功能	配置IPv6全球单播地址	三者至少选其一	1.3.1
	配置IPv6链路本地地址		1.3.2
	配置IPv6任播地址		1.3.3
配置IPv6邻居发现协议	配置静态邻居表项	可选	1.4.1

配置任务		说明	详细配置
	配置接口上允许动态学习的邻居的最大个数	可选	1.4.2
	配置STALE状态ND表项的老化时间	可选	1.4.3
	配置链路本地ND表项资源占用最小化	可选	1.4.4
	配置设备的跳数限制	可选	1.4.5
	配置RA消息的相关参数	可选	1.4.6
	配置重复地址检测时发送邻居请求消息的次数	可选	1.4.7
	配置ND Proxy功能	可选	1.4.8
配置PMTU发现	配置接口MTU	可选	1.5.1
	配置指定地址的静态PMTU	可选	1.5.2
	配置PMTU老化时间	可选	1.5.3
配置ICMPv6报文发送	配置指定时间内发送ICMPv6差错报文的最大个数	可选	1.6.1
	配置允许回复组播形式的Echo request报文	可选	1.6.2
	配置ICMPv6目的不可达差错报文发送功能	可选	1.6.3
	配置ICMPv6超时差错报文发送功能	可选	1.6.4
	配置ICMPv6重定向报文发送功能	可选	1.6.5
	配置ICMPv6报文指定源地址功能	可选	1.6.6

1.3 配置IPv6基本功能

1.3.1 配置IPv6 全球单播地址

IPv6 全球单播地址可以通过下面三种方式配置：

- 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，而接口标识符则由接口自动生成。
- 手工配置：用户手工配置 IPv6 全球单播地址。
- 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。

手工配置的全球单播地址（包括采用 EUI-64 格式形成的全球单播地址）的优先级高于自动生成的全球单播地址。如果在接口已经自动生成全球单播地址的情况下，手工配置前缀相同的全球单播地址，不会覆盖之前自动生成的全球单播地址。如果删除手工配置的全球单播地址，设备还可以使用自动生成的全球单播地址进行通信。

1. 采用EUI-64 格式形成IPv6 地址

表1-5 采用 EUI-64 格式形成 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
采用EUI-64格式形成IPv6地址	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-addressIprefix-length* } **eui-64**	缺省情况下，接口上没有配置IPv6全球单播地址

2. 手工指定IPv6 地址

表1-6 手工指定 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
手工指定IPv6地址	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }	缺省情况下，接口上没有配置IPv6全球单播地址

3. 无状态自动配置IPv6 地址

表1-7 无状态自动配置 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
无状态自动配置IPv6地址	**ipv6 address auto**	缺省情况下，接口上没有配置IPv6全球单播地址 在接口上执行**undo ipv6 address auto**命令，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

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”。

表1-8 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

操作	命令	说明
进入系统视图	**system-view**	-
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
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

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。

4. 手工配置静态IPv6 前缀

表1-9 手工配置静态 IPv6 前缀

操作	命令	说明
进入系统视图	**system-view**	-
手工配置静态IPv6前缀	**ipv6 prefix** *prefix-number ipv6-prefix/prefix-length*	缺省情况下，设备上不存在任何IPv6前缀

1.3.2 配置IPv6 链路本地地址

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。

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。

表1-10 配置自动生成链路本地地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置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

表1-11 手工指定接口的链路本地地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
手工指定接口的链路本地地址	**ipv6 address** *ipv6-address* **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

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。

1.3.3 配置IPv6 任播地址

用户需要手工配置接口的 IPv6 任播地址。

表1-12 配置 IPv6 任播地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv6任播地址	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **anycast**	缺省情况下，接口上没有配置任播地址

1.4 配置IPv6邻居发现协议

1.4.1 配置静态邻居表项

将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态实现，也可以通过手工配置静态邻居表项来实现。

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对应的邻居节点的 IPv6 地址、链路层地址；
- 配置本节点 VLAN 中的端口对应的邻居节点的 IPv6 地址、链路层地址。

表1-13 配置静态邻居表项

操作	命令	说明
进入系统视图	**system-view**	-
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* } [**vpn-instance** *vpn-instance-name*]	缺省情况下，设备上不存在静态邻居表项

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，设备还需要解析 VLAN 对应的二层端口信息。
- 采用第二种方式配置静态邻居表项后，需要保证 VLAN 所对应的 VLAN 接口已经存在，且 *port-type port-number* 指定的二层端口属于 *vlan-id* 指定的 VLAN。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。

1.4.2 配置接口上允许动态学习的邻居的最大个数

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。

表1-14 配置接口上允许学习的动态邻居表项的最大个数

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口上允许学习的动态邻居表项的最大个数	**ipv6 neighbors max-learning-num** *number*	缺省情况： MSR2600缺省值为2048，MSR 36-10/ MSR 36-20/ MSR 36-40/ MSR 36-60缺省值为4096，MSR3600-28/MSR3600-51缺省值为2048，MSR 5600缺省值为4096

1.4.3 配置STALE状态ND表项的老化时间

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。

表1-15 配置 STALE 状态 ND 表项的老化时间

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.4 配置链路本地ND表项资源占用最小化

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。

表1-16 配置链路本地 ND 表项资源占用最小化

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.5 配置设备的跳数限制

设备的跳数限制有以下两个作用：

- 决定了设备发送的 IPv6 数据报文的跳数，即 IPv6 数据报文的 Hop Limit 字段的值。
- 如果用户配置了在 RA 消息中发布本设备的跳数限制（配置命令 **undo ipv6 nd ra hop-limit unspecified**），则设备发送的 RA 消息中将携带此处配置的跳数限制值。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。

表1-17 配置设备的跳数限制

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.6 配置RA消息的相关参数

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 1-18 所示。

表1-18 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。
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。

表1-19 配置允许发布 RA 消息

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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

操作	命令	说明
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 RA消息周期性发布时，相邻两次的时间间隔是在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布RA消息的时间间隔 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

表1-20 配置 RA 消息中的相关参数

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置RA消息中的前缀信息	**ipv6 nd ra prefix** { *ipv6-prefix prefix-length* | *ipv6-prefixIprefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *	缺省情况下，没有配置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
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
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
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
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
配置RA消息中路由器的生存时间	**ipv6 nd ra router-lifetime** *value*	缺省情况下，RA消息中路由器的生存时间为1800秒
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
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**
配置保持邻居可达状态的时间	**ipv6 nd nud reachable-time** *value*	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

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。

1.4.7 配置重复地址检测时发送邻居请求消息的次数

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。

表1-21 配置重复地址检测时发送邻居请求消息的次数

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置重复地址检测时发送邻居请求消息的次数	**ipv6 nd dad attempts** *value*	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*value*值为0时，表示禁止重复地址检测

1.4.8 配置ND Proxy功能

1. ND Proxy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。

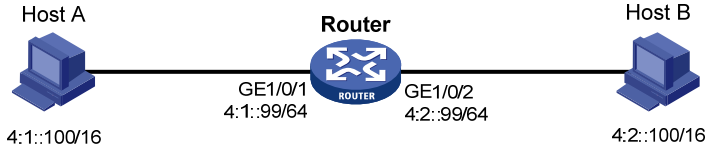
说明

如无特殊说明，本章后续描述中的 ND Proxy 均指普通 ND Proxy。

(1) ND Proxy

ND Proxy的典型应用环境如 图 1-7 所示。设备Router通过两个三层接口GigabitEthernet1/0/1 和GigabitEthernet1/0/2 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1-7 ND Proxy 的应用环境



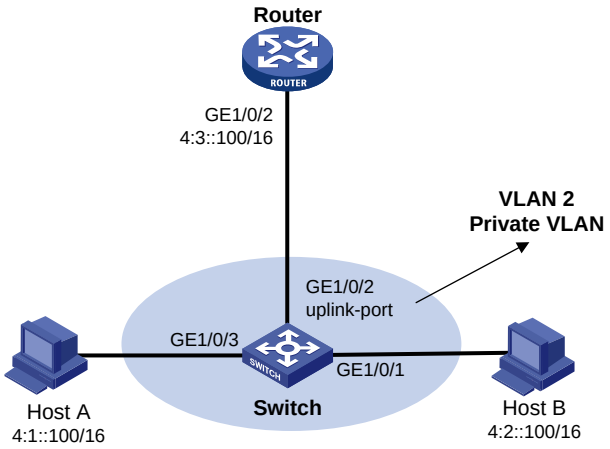
在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，此时的两台主机处于不同的广播域中，Host B 无法收到 Host A 的 NS 请求报文，当然也就无法应答。

通过在 Router 上启用 ND Proxy 功能，可以解决此问题。在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上启用 ND Proxy 后，Router 可以应答 Host A 的 NS 请求。同时，Router 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 1-8 所示。Host A和Host B属于同一个VLAN 2，但它们分别连接到被二层隔离的端口GigabitEthernet1/0/3 和GigabitEthernet1/0/1 上。

图1-8 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，因为连接两台主机的端口处于端口隔离状态，Host B 无法收到 Host A 的 NS 请求报文。

通过在 Router 上启用本地 ND Proxy 功能，可以解决此问题。在接口 GigabitEthernet1/0/2 上启用本地 ND Proxy 后，Router 会代替 Host B 回应 NA，Host A 发给 Host B 的报文就会通过 Router 进行转发，从而实现 Host A 与 Host B 之间的通信。

本地 ND Proxy 可以在下列三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个 VLAN 中的不同二层隔离端口下；
- 使能 Super VLAN 功能后，想要互通的主机属于不同的 Sub VLAN；
- 使能 Private VLAN 功能后，想要互通的主机属于不同的 Secondary VLAN。

2. 配置ND Proxy功能

ND Proxy 和本地 ND Proxy 功能均可在 VLAN 接口视图/三层以太网接口/三层以太网子接口视图下进行配置。

表1-22 配置 ND Proxy 功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
开启ND Proxy功能	**proxy-nd enable**	缺省情况下，ND Proxy功能处于关闭状态

表1-23 配置本地 ND Proxy 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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

1.5 配置PMTU发现

1.5.1 配置接口MTU

由于 IPv6 路由器不支持对报文进行分片，当路由器接口收到一个报文后，如果发现报文长度比转发接口的 MTU 值大，则会将其丢弃；同时将转发接口的 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。

表1-24 配置接口 MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口MTU	**ipv6 mtu** *mtu-size*	缺省情况下，没有配置接口MTU

1.5.2 配置指定地址的静态PMTU

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“1.1.4 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。

表1-25 配置指定地址的静态 PMTU

操作	命令	说明
进入系统视图	**system-view**	-
配置指定IPv6地址对应的静态PMTU值	**ipv6 pathmtu** [**vpn-instance** *vpn-instance-name*] *ipv6-address value*	缺省情况下，没有配置静态PMTU值

1.5.3 配置PMTU老化时间

通过“1.1.4 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。

该配置对静态 PMTU 不起作用。

表1-26 配置 PMTU 老化时间

操作	命令	说明
进入系统视图	**system-view**	-
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

1.6 配置ICMPv6报文发送功能

1.6.1 配置指定时间内发送ICMPv6 差错报文的最大个数

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，即每隔多长时间将令牌桶内的令牌个数刷新为所配置的容量。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。

表1-27 配置指定时间内发送 ICMPv6 差错报文的最大个数

操作	命令	说明
进入系统视图	**system-view**	-
配置指定时间内发送ICMPv6差错报文的最大个数	**ipv6 icmpv6 error-interval** *milliseconds* [*bucketsize*]	缺省情况下，令牌桶容量为10，令牌桶的刷新周期为100毫秒，即每一个刷新周期内最多可以发送10个ICMPv6差错报文 刷新周期为0时，表示不限制ICMPv6差错报文的发送

1.6.2 配置允许回复组播形式的Echo request报文

缺省情况下，不允许设备回复组播形式的 Echo request 报文。

在某些应用场景下，可能需要使用组播形式的 Echo request 报文来获取信息，此时可以通过下面的命令，配置允许设备回复组播形式的 Echo request 报文。

表1-28 配置允许回复组播形式的 Echo request 报文

操作	命令	说明
进入系统视图	**system-view**	-
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

1.6.3 配置ICMPv6 目的不可达差错报文发送功能

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。

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。

表1-29 配置 ICMPv6 目的不可达报文发送功能

操作	命令	说明
进入系统视图	**system-view**	-
开启设备的ICMPv6目的不可达报文的发送功能	**ipv6 unreachables enable**	缺省情况下，ICMPv6目的不可达报文发送功能处于关闭状态

1.6.4 配置ICMPv6 超时差错报文发送功能

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。

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。

表1-30 配置 ICMPv6 超时差错报文发送功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.6.5 配置ICMPv6 重定向报文发送功能

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。

表1-31 配置 ICMPv6 重定向报文发送功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.6.6 配置ICMPv6 报文指定源地址功能

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。

表1-32 配置 ICMPv6 报文指定源地址功能

操作	命令	说明
进入系统视图	**system-view**	-
开启设备的ICMPv6报文指定源地址功能	**ipv6 icmpv6 source** [**vpn-instance** *vpn-instance-name*] *ipv6-address*	缺省情况下，ICMPv6报文指定源地址功能处于关闭状态

说明

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。

1.7 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。

表1-33 IPv6 基础显示和维护

操作	命令
显示IPv6 FIB信息	**display ipv6 fib** [**vpn-instance** *vpn-instance-name*] [*ipv6-address* [*prefix-length*]]
显示接口的IPv6信息	**display ipv6 interface** [*interface-type* [*interface-number*]] [**brief**]
显示接口的IPv6前缀信息	**display ipv6 interface** *interface-type interface-number* **prefix**
显示邻居信息（MSR 2600/MSR 3600）	**display ipv6 neighbors** { *ipv6-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id* } [**verbose**]
显示邻居信息（MSR 5600）	**display ipv6 neighbors** { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]
显示邻居表项的个数（MSR 2600/MSR 3600）	**display ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id* } **count**
显示邻居表项的个数（MSR 5600）	**display ipv6 neighbors** { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**
显示指定VPN实例的邻居信息	**display ipv6 neighbors vpn-instance** *vpn-instance-name* [**count**]
显示IPv6的PMTU信息	**display ipv6 pathmtu** [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }
显示IPv6前缀信息	**display ipv6 prefix** [*prefix-number*]
显示IPv6报文及ICMPv6报文的统计信息（MSR 2600/MSR 3600）	**display ipv6 statistics**

操作	命令
显示IPv6报文及ICMPv6报文的统计信息（MSR 5600）	**display ipv6 statistics** [**slot** *slot-number*]
显示IPv6 RawIP连接摘要信息（MSR 2600/MSR 3600）	**display ipv6 rawip**
显示IPv6 RawIP连接摘要信息（MSR 5600）	**display ipv6 rawip** [**slot** *slot-number*]
显示IPv6 RawIP连接详细信息（MSR 2600/MSR 3600）	**display ipv6 rawip verbose** [**pcb** *pcb-index*]
显示IPv6 RawIP连接详细信息（MSR 5600）	**display ipv6 rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示IPv6 TCP连接摘要信息（MSR 2600/MSR 3600）	**display ipv6 tcp**
显示IPv6 TCP连接摘要信息（MSR 5600）	**display ipv6 tcp** [**slot** *slot-number*]
显示IPv6 TCP连接详细信息（MSR 2600/MSR 3600）	**display ipv6 tcp verbose** [**pcb** *pcb-index*]
显示IPv6 TCP连接详细信息（MSR 5600）	**display ipv6 tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示IPv6 UDP连接摘要信息（MSR 2600/MSR 3600）	**display ipv6 udp**
显示IPv6 UDP连接摘要信息（MSR 5600）	**display ipv6 udp** [**slot** *slot-number*]
显示IPv6 UDP连接详细信息（MSR 2600/MSR 3600）	**display ipv6 udp verbose** [**pcb** *pcb-index*]
显示IPv6 UDP连接详细信息（MSR 5600）	**display ipv6 udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
显示IPv6 ICMP流量统计信息（MSR 2600/MSR 3600）	**display ipv6 icmp statistics**
显示IPv6 ICMP流量统计信息（MSR 5600）	**display ipv6 icmp statistics** [**slot** *slot-number*]
显示IPv6 TCP连接的流量统计信息（MSR 2600/MSR 3600）	**display tcp statistics**
显示IPv6 TCP连接的流量统计信息（MSR 5600）	**display tcp statistics** [**slot** *slot-number*]
显示IPv6 UDP流量统计信息（MSR 2600/MSR 3600）	**display udp statistics**
显示IPv6 UDP流量统计信息（MSR 5600）	**display udp statistics** [**slot** *slot-number*]
清除IPv6邻居信息（MSR 2600/MSR 3600）	**reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }
清除IPv6邻居信息（MSR 5600）	**reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }
清除PMTU值	**reset ipv6 pathmtu** { **all** | **dynamic** | **static** }
清除IPv6报文及ICMPv6报文的统计信息（MSR 2600/MSR 3600）	**reset ipv6 statistics**

操作	命令
清除IPv6报文及ICMPv6报文的统计信息（MSR 5600）	**reset ipv6 statistics** [**slot** *slot-number*]
清除IPv6 TCP连接的流量统计信息	**reset tcp statistics**
清除IPv6 UDP流量统计信息	**reset udp statistics**

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”。

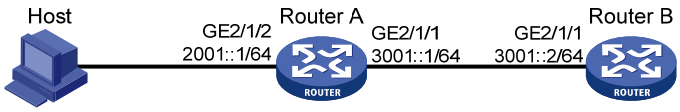
1.8 IPv6基础典型配置举例

1. 组网需求

- 如 图 1-9 所示，Host、Router A和Router B之间通过以太网接口相连，在接口上配置IPv6 地址，验证它们之间的互通性。
- Router 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 Router B 的路由。

2. 组网图

图1-9 IPv6 地址配置组网图



3. 配置步骤

(1) 配置 Router A

手工指定接口 GigabitEthernet2/1/1 的全球单播地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 3001::1/64
[RouterA-GigabitEthernet2/1/1] quit
```

手工指定接口 GigabitEthernet2/1/2 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）

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 address 2001::1/64
[RouterA-GigabitEthernet2/1/2] undo ipv6 nd ra halt
[RouterA-GigabitEthernet2/1/2] quit
```

(2) 配置 Router B

手工指定接口 GigabitEthernet2/1/1 的全球单播地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 3001::2/64
```

```
[RouterB-GigabitEthernet2/1/1] 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。

```
[RouterB] 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 Router A 上查看接口 GigabitEthernet2/1/2 的邻居信息。

```
[RouterA] display ipv6 neighbors interface gigabitethernet 2/1/2
         Type: S-Static    D-Dynamic    O-Openflow    I-Invalid
IPv6 Address                    Link Layer     VID  Interface      State T Age
FE80::215:E9FF:FEA6:7D14        0015-e9a6-7d14 N/A  GE2/1/2        STALE D 1238
2001::15B:E0EA:3524:E791        0015-e9a6-7d14 N/A  GE2/1/2        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 Router A 的接口信息，可以看到各接口配置的 IPv6 全球单播地址。

```
[RouterA] display ipv6 interface gigabitethernet 2/1/1
GigabitEthernet2/1/1 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
[RouterA] display ipv6 interface gigabitethernet 2/1/2
GigabitEthernet2/1/2 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 Router B 的接口信息，可以看到接口配置的 IPv6 全球单播地址。

```
[RouterB] display ipv6 interface gigabitethernet 2/1/1
GigabitEthernet2/1/1 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:FF00:1
    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 Router A 及 Router B 的互通性；在 Router B 上使用 Ping 测试和 Router 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。

```
[RouterB] 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
[RouterB] 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 Router B 和 Router A，证明它们是互通的。

1.9 常见配置错误举例

1. 故障现象

无法 Ping 通对端的 IPv6 地址。

2. 故障排除

- 在任意视图下使用 **display ipv6 interface** 命令检查接口配置的 IPv6 地址是否正确，接口状态是否为 up。
- 在用户视图下使用 **debugging ipv6 packet** 命令打开 IPv6 报文调试开关，根据调试信息进行判断。

目 录

1 DHCPv6 简介

1.1 DHCPv6概述

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

与其他 IPv6 地址分配方式（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。

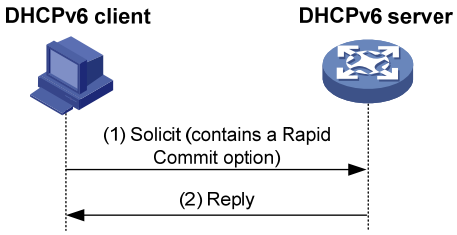
1.2 DHCPv6地址/前缀分配过程

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：

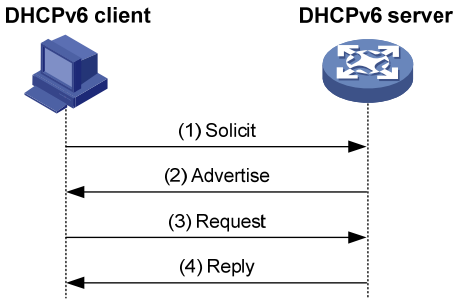
(1) DHCPv6 客户端在向 DHCPv6 服务器发送的 Solicit 消息中携带 Rapid Commit 选项，标识客户端希望服务器能够快速为其分配地址/前缀和其他网络配置参数。

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

1.2.2 交互四个消息的分配过程

交互四个消息的分配过程如 图 1-2 所示。

图1-2 交互四个消息的分配过程



交互四个消息分配过程的简述如 表 1-1。

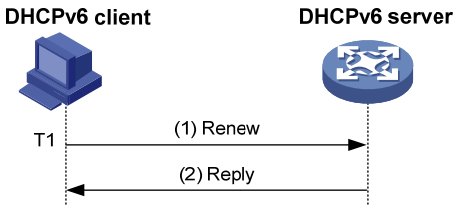
表1-1 交互四个消息的分配过程

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

1.3 地址/前缀租约更新过程

DHCPv6 服务器分配给客户端的 IPv6 地址/前缀具有一定的租借期限，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。

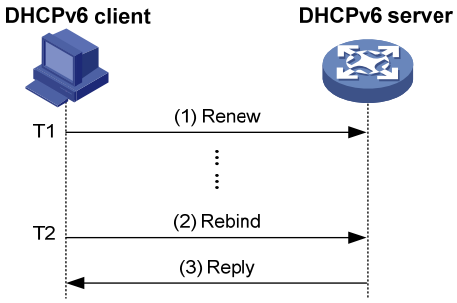
图1-3 通过 Renew 更新地址/前缀租约



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，但是没有收到DHCPv6 服务器的回应报文，则DHCPv6 客户端会在T2（推荐值为首选生命期的 0.8 倍）时，向所有DHCPv6 服务器组播发送Rebind报文请求更新租约。如果客户端可以继续使用该地址/前缀，则DHCPv6 服务器回应续约成功的Reply报文，通知DHCPv6 客户端已经成功更新地址/前缀租约；如果该地址/前缀不可以再分配给该客户端，则DHCPv6 服务器回应续约失败的Reply报文，通知客户端不能获得新的租约；如果DHCPv6 客户端没有收到服务器的应答报文，则到达有效生命期后，客户端停止使用该地址/前缀。有效生命期和首选生命期的详细介绍请参见“三层技术-IP业务配置指导”中的“IPv6 基础”。

1.4 DHCPv6无状态配置

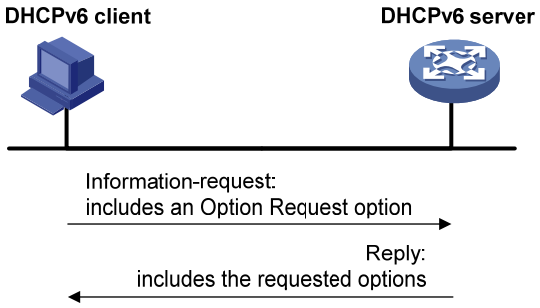
1.4.1 DHCPv6 无状态配置简介

DHCPv6 服务器可以为已经具有 IPv6 地址/前缀的客户端分配其他网络配置参数，该过程称为DHCPv6 无状态配置。地址无状态自动配置是指节点根据路由器发现/前缀发现所获取的信息，自动配置 IPv6 地址。详细介绍请参见“三层技术-IP 业务配置指导”的“IPv6 基础”。

DHCPv6 客户端通过地址无状态自动配置功能成功获取 IPv6 地址后，如果接收到的 RA（Router Advertisement，路由器通告）报文中 M 标志位（Managed address configuration flag，被管理地址配置标志位）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。

1.4.2 DHCPv6 无状态配置过程

图1-5 DHCPv6 无状态配置工作过程



如 图 1-5 所示，DHCPv6 无状态配置的具体过程为：

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

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

(3) 客户端检查 Reply 报文中提供的信息，如果与 Information-request 报文中请求的配置参数相符，则按照 Reply 报文中提供的参数进行网络配置；否则，忽略该参数。如果接收到多个与请求相符的 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 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

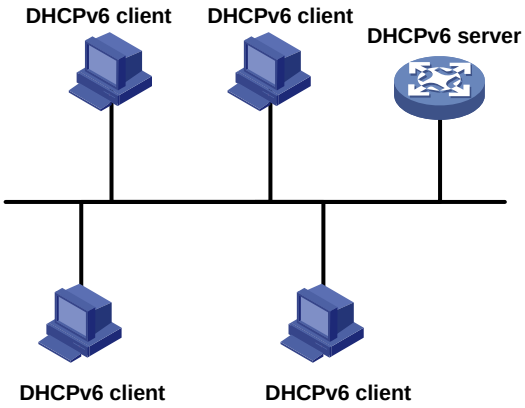
2.1 DHCPv6服务器简介

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 服务器地址和其他网络配置参数分配应用环境



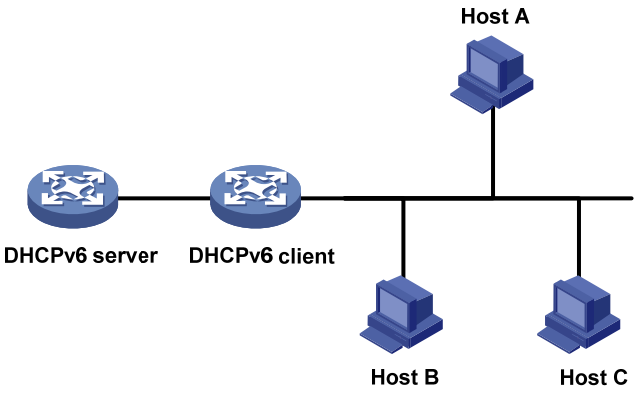
如 图 2-1 所示，为了便于集中管理IPv6 地址，简化网络配置，DHCPv6 服务器可以用来为DHCPv6 客户端提供诸如IPv6 地址、域名后缀、DNS服务器地址等网络配置参数。DHCPv6 客户端根据服务器分配的参数来实现主机的配置。

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

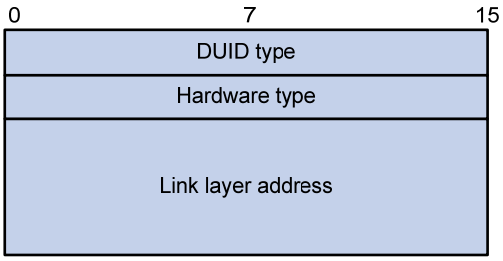
1. DHCPv6 采用的组播地址

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，即通过将客户端 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，即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，即通过将客户端 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，即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，地址池的选择原则如下：

(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) 如果不存在静态绑定的地址池，且接收到 DHCPv6 请求报文的接口没有引用地址池，则按照以下方法选择地址池：

- 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) 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；

(7) 地址池/前缀池中的其他空闲地址/前缀；

(8) 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 配置DHCPv6服务器

2.2.1 DHCPv6 服务器配置任务简介

表2-1 DHCPv6 服务器配置任务简介

配置任务	说明	详细配置
配置为DHCPv6客户端分配IPv6前缀	根据实际情况选择	2.2.2
配置为DHCPv6客户端分配IPv6地址		2.2.3
配置为DHCPv6客户端分配网络参数		2.2.4
配置接口工作在DHCPv6服务器模式，并配置地址/前缀分配策略	必选	2.2.5
配置DHCPv6服务器发送DHCPv6报文的DSCP优先级	可选	2.2.6

2.2.2 配置为DHCPv6 客户端分配IPv6 前缀

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，没有指定静态绑定的 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。

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。

表2-2 配置为 DHCPv6 客户端分配 IPv6 前缀

操作	命令	说明
进入系统视图	**system-view**	-
（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 多次执行**ipv6 dhcp server forbidden-prefix**命令，可以配置多个不参与自动分配的IPv6前缀段
创建前缀池	**ipv6 dhcp prefix-pool** *prefix-pool-number* **prefix** *prefix/prefix-len* **assign-len** *assign-len*	缺省情况下，没有配置DHCPv6前缀池 DHCPv6服务器为DHCPv6客户端动态分配IPv6前缀时，为必选；其他情况下，不需要进行本配置

操作	命令	说明
创建DHCPv6地址池，并进入DHCPv6地址池视图	**ipv6 dhcp pool** *pool-name*	缺省情况下，设备上不存在任何DHCPv6地址池
配置动态分配的IPv6地址网段	**network** *prefix/prefix-length* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	缺省情况下，没有配置动态分配的IPv6地址网段
配置静态绑定前缀	**static-bind prefix** *prefix/prefix-len* **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	二者至少选其一 缺省情况下，没有指定地址池的静态绑定前缀和可动态分配的前缀 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*]	

2.2.3 配置为DHCPv6 客户端分配IPv6 地址

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，没有指定静态绑定的 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，如果没有在地址池下通过 **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，如果没有在地址池下通过 **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。

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。

表2-3 配置为 DHCPv6 客户端分配 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
（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 多次执行**ipv6 dhcp server forbidden-address**命令，可以配置多个不参与自动分配的IPv6地址段
创建DHCPv6地址池，并进入DHCPv6地址池视图	**ipv6 dhcp pool** *pool-name*	缺省情况下，设备上不存在任何DHCPv6地址池
配置动态分配的IPv6地址网段	**network** *prefix/prefix-length* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	缺省情况下，没有配置动态分配的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
（可选）配置动态分配的IPv6非临时地址范围	**address range** *start-ipv6-address end-ipv6-adddress* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	缺省情况下，没有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
（可选）配置动态分配的IPv6临时地址范围	**temporary address range** *start-ipv6-address end-ipv6-adddress* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	缺省情况下，没有配置动态分配的IPv6临时地址范围，不能分配IPv6临时地址
（可选）配置静态绑定的IPv6地址	**static-bind address** *ipv6-address/addr-prefix-length* **duid** *duid* [**iaid** *iaid*] [**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

2.2.4 配置为DHCPv6 客户端分配网络参数

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 个域名后缀、8 个 SIP 服务器地址和 8 个 SIP 服务器域名等。

表2-4 配置为 DHCPv6 客户端分配网络参数

操作	命令	说明
进入系统视图	**system-view**	-
创建DHCPv6地址池，并进入DHCPv6地址池视图	**ipv6 dhcp pool** *pool-name*	缺省情况下，设备上不存在任何DHCPv6地址池
配置动态分配的IPv6地址网段	**network** *prefix/prefix-length* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]	缺省情况下，没有配置动态分配的IPv6地址网段
（可选）配置为客户端分配的DNS服务器地址	**dns-server** *ipv6-address*	缺省情况下，没有指定为客户端分配的DNS服务器地址
（可选）配置为客户端分配的域名后缀	**domain-name** *domain-name*	缺省情况下，没有指定为客户端分配的域名后缀
（可选）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，没有指定为客户端分配的SIP服务器地址或域名
（可选）配置DHCPv6自定义选项	**option** *code* **hex** *hex-string*	缺省情况下，没有配置DHCPv6自定义选项

2.2.5 配置接口工作在DHCPv6 服务器模式，并配置地址/前缀分配策略

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。

配置接口工作在 DHCPv6 服务器模式，并配置地址/前缀分配策略时，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。

表2-5 配置接口工作在 DHCPv6 服务器模式，并配置地址/前缀分配策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
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
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策略	**ipv6 dhcp server** { **allow-hint** | **preference** *preference-value* | **rapid-commit** } *	两者必选其一 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 多次执行**ipv6 dhcp server**命令，新的配置会覆盖已有配置 一个接口上最多只能引用一个地址池，如果多次执行**ipv6 dhcp server apply pool**命令，新的配置会覆盖已有配置
配置接口引用DHCP地址池	**ipv6 dhcp server apply pool** *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *	

2.2.6 配置DHCPv6 服务器发送DHCPv6 报文的DSCP优先级

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。

表2-6 配置 DHCPv6 服务器发送 DHCPv6 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DHCPv6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

2.3 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2-7 DHCPv6 服务器显示和维护

操作	命令
显示本设备的DUID	**display ipv6 dhcp duid**
显示DHCPv6地址池的信息	**display ipv6 dhcp pool** [*pool-name*]
显示前缀池的信息	**display ipv6 dhcp prefix-pool** [*prefix-pool-number*]
显示接口上的DHCPv6服务器信息	**display ipv6 dhcp server** [**interface** *interface-type interface-number*]

操作	命令
显示DHCPv6地址冲突信息	**display ipv6 dhcp server conflict** [**address** *ipv6-address*]
显示租约过期的DHCPv6地址绑定信息	**display ipv6 dhcp server expired** [**address** *ipv6-address* | **pool** *pool-name*]
显示DHCPv6地址绑定信息	**display ipv6 dhcp server ip-in-use** [**address** *ipv6-address* | **pool** *pool*-name]
显示DHCPv6前缀绑定信息	**display ipv6 dhcp server pd-in-use** [**pool** *pool-name* | **prefix** *prefix/prefix-len*]
显示DHCPv6服务器的报文统计信息	**display ipv6 dhcp server statistics** [**pool** *pool-name*]
清除DHCPv6地址冲突信息	**reset ipv6 dhcp server conflict** [**address** *ipv6-address*]
清除租约过期的DHCPv6地址绑定信息	**reset ipv6 dhcp server expired** [**address** *ipv6-address* | **pool** *pool-name*]
清除DHCPv6的正式地址绑定和临时地址绑定信息	**reset ipv6 dhcp server ip-in-use** [**address** *ipv6-address* | **pool** *pool-name*]
清除DHCPv6正式前缀绑定和临时前缀绑定信息	**reset ipv6 dhcp server pd-in-use** [**pool** *pool-name* | **prefix** *prefix/prefix-len*]
清除DHCPv6服务器的报文统计信息	**reset ipv6 dhcp server statistics**

2.4 DHCPv6服务器典型配置举例

2.4.1 动态分配IPv6 前缀典型配置举例

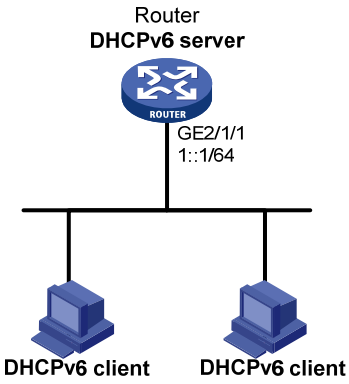
1. 组网需求

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：

- Router 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

配置接口 GiagbitEthernet2/1/1 的 IPv6 地址。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ipv6 address 1::1/64
[Router-GigabitEthernet2/1/1] 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。

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

创建地址池 1。

```
[Router] ipv6 dhcp pool 1
```

配置地址池 1 网段为 1::/64，与接口地址所属的网段相同。

```
[Router-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。

```
[Router-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。

```
[Router-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。

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

配置为客户端分配的域名为 aaa.com。

```
[Router-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。

```
[Router-dhcp6-pool-1] sip-server address 2:2::4
[Router-dhcp6-pool-1] sip-server domain-name bbb.com
[Router-dhcp6-pool-1] quit
```

配置接口 GigabitEthernet2/1/1 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。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ipv6 dhcp select server
[Router-GigabitEthernet2/1/1] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

4. 验证配置

完成上述配置后，查看接口 GigabitEthernet2/1/1 上的 DHCPv6 服务器配置信息。

```
[Router-GigabitEthernet2/1/1] display ipv6 dhcp server interface gigabitethernet 2/1/1
Using pool: global
Preference value: 255
Allow-hint: Enabled
Rapid-commit: Enabled
```

显示地址池 1 的信息。

```
[Router-GigabitEthernet2/1/1] 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: 00030001ca0006a4
    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。

```
[Router-GigabitEthernet2/1/1] 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。

```
[Router-GigabitEthernet2/1/1] 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。

```
[Router-GigabitEthernet2/1/1] 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
```

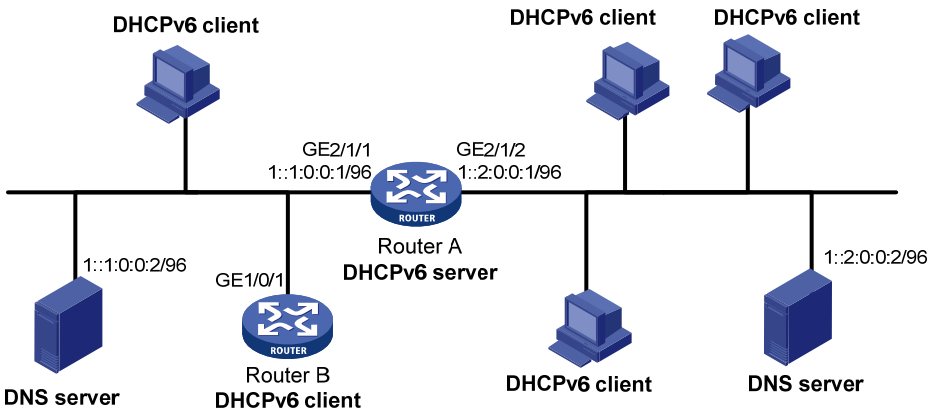
2.4.2 动态分配IPv6 地址典型配置举例

1. 组网需求

- 作为 DHCPv6 服务器的 Router A 为网段 1::1:0:0:0/96 和 1::2:0:0:0/96 的客户端动态分配 IPv6 地址；
- Router A 的两个以太网接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 的地址分别为 1::1:0:0:1/96 和 1::2:0:0:1/96；
- 1::1:0:0:0/96 网段内的地址租约时长为 172800 秒（2 天），有效时长为 345600 秒（4 天），域名为 aabbcc.com，DNS 服务器地址为 1::1:0:0:2/96；
- 1::2:0:0:0/96 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（略）

(2) 配置 DHCPv6 服务

配置接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 工作在 DHCPv6 服务器模式。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 dhcp select server
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 dhcp select server
[RouterA-GigabitEthernet2/1/2] 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。

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

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

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

4. 验证配置

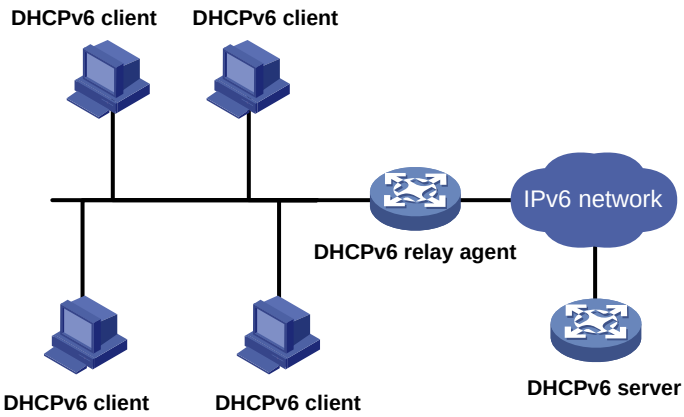
配置完成后，1::1:0:0:0/96 和 1::2:0:0:0/96 网段的客户端可以从 DHCPv6 服务器 Router A 申请到相应网段的 IPv6 地址和网络配置参数。通过 **display ipv6 dhcp server ip-in-use** 命令可以查看 DHCPv6 服务器为客户端分配的 IPv6 地址。

3 DHCPv6 中继

3.1 DHCPv6中继简介

3.1.1 应用环境

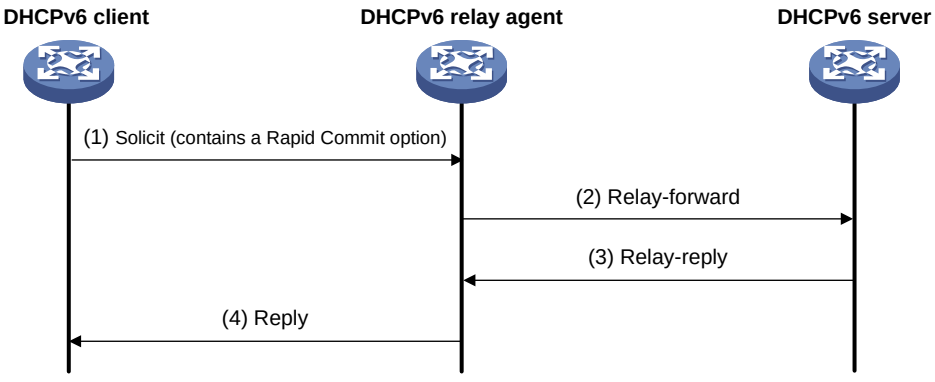
图3-1 DHCPv6 中继应用组网图



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。

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 配置DHCPv6中继

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。建议不要在一个接口上同时配置 DHCPv6 中继和 DHCPv6 客户端功能。

表3-1 配置 DHCPv6 中继

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口工作在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
指定DHCPv6服务器的地址	**ipv6 dhcp relay server-address** *ipv6-address* [**interface** *interface-type interface-number*]	缺省情况下，未指定任何DHCPv6服务器 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

操作	命令	说明
配置DHCPv6中继发送DHCPv6报文的DSCP优先级	**ipv6 dhcp dscp** *dscp-value*	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 缺省情况下，DHCPv6中继发送的DHCPv6报文的DSCP优先级为56

3.3 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3-2 DHCPv6 中继显示和维护

操作	命令
显示本设备DUID	**display ipv6 dhcp duid**
显示DHCPv6中继上指定的DHCPv6服务器地址信息	**display ipv6 dhcp relay server-address** [**interface** *interface-type interface-number*]
显示DHCPv6中继的相关报文统计信息	**display ipv6 dhcp relay statistics** [**interface** *interface-type interface-number*]
清除DHCPv6中继的相关报文统计信息	**reset ipv6 dhcp relay statistics** [**interface** *interface-type interface-number*]

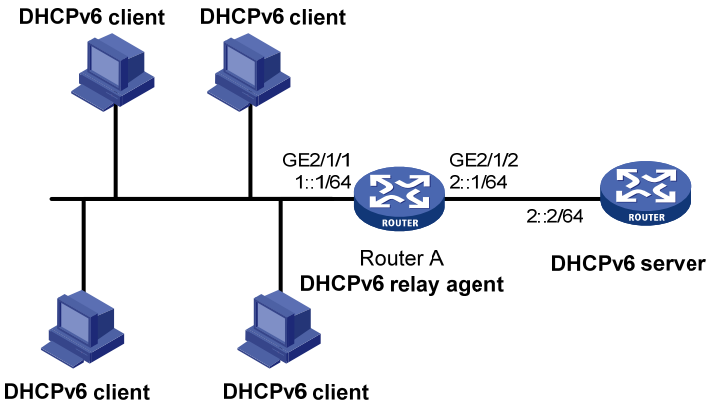
3.4 DHCPv6中继典型配置举例

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。客户端和服务器不在同一个链路范围，需要通过 DHCPv6 中继转发报文。
- Router A 作为 DHCPv6 中继，为客户端和服务器转发报文。
- Router 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

(1) 配置 Router A 作为 DHCPv6 中继

配置接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 address 2::1 64
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 1::1 64
```

配置接口 GigabitEthernet2/1/1 工作在 DHCPv6 中继模式，并指定 DHCPv6 服务器地址。

```
[RouterA-GigabitEthernet2/1/1] ipv6 dhcp select relay
[RouterA-GigabitEthernet2/1/1] ipv6 dhcp relay server-address 2::2
```

(2) 配置 Router A 作为网关

配置发布 RA 消息，并配置 M 和 O 标志位。

```
[RouterA-GigabitEthernet2/1/1] undo ipv6 nd ra halt
[RouterA-GigabitEthernet2/1/1] ipv6 nd autoconfig managed-address-flag
[RouterA-GigabitEthernet2/1/1] ipv6 nd autoconfig other-flag
```

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。

```
[RouterA-GigabitEthernet2/1/1] display ipv6 dhcp relay server-address
Interface: GigabitEthernet2/1/1
 Server address                              Outgoing Interface
 2::2
```

查看 DHCPv6 中继相关报文的统计信息。

```
[RouterA-GigabitEthernet2/1/1] 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，并根据获取的网络配置参数自动创建 DHCPv6 选项组。
- 通过 DHCPv6 获取 IPv6 前缀和网络配置参数，并根据获取的前缀自动创建 IPv6 前缀、根据获取的网络配置参数自动创建 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 配置DHCPv6客户端

提示

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。

4.2.1 DHCPv6 客户端配置任务简介

表4-1 DHCPv6 客户端配置任务简介

配置任务	说明	详细配置
配置DHCPv6客户端获取IPv6地址和网络配置参数	根据实际情况选择其一	4.2.2
配置DHCPv6客户端获取IPv6前缀和网络配置参数		4.2.3
配置DHCPv6客户端获取除地址/前缀外的其他网络配置参数		4.2.4
配置DHCPv6客户端发送DHCPv6报文的DSCP优先级	可选	4.2.5

4.2.2 配置DHCPv6 客户端获取IPv6 地址和网络配置参数

表4-2 配置 DHCPv6 客户端获取 IPv6 地址和网络配置参数

操作		命令	说明
进入系统视图		**system-view**	-
进入接口	三层以太网接口视图	**interface** *interface-type interface-number*	-

操作		命令	说明
视图	三层聚合接口视图	**interface route-aggregation** *interface-number*	
	VLAN接口视图	**interface vlan-interface** *interface-number*	
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

4.2.3 配置DHCPv6 客户端获取IPv6 前缀和网络配置参数

表4-3 配置 DHCPv6 客户端获取 IPv6 前缀和网络配置参数

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网接口视图	**interface** *interface-type interface-number*	-
	三层聚合接口视图	**interface route-aggregation** *interface-number*	
	VLAN接口视图	**interface vlan-interface** *interface-number*	
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

4.2.4 配置DHCPv6 客户端获取除地址/前缀外的其他网络配置参数

表4-4 配置 DHCPv6 客户端获取除地址/前缀外的其他网络配置参数

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网接口视图	**interface** *interface-type interface-number*	-
	三层聚合接口视图	**interface route-aggregation** *interface-number*	
	VLAN接口视图	**interface vlan-interface** *interface-number*	
使能IPv6地址无状态自动配置功能		**ipv6 address auto**	二者至少选其一 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
使能DHCPv6无状态配置功能		**ipv6 dhcp client stateless enable**	

说明

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

4.2.5 配置DHCPv6 客户端发送DHCPv6 报文的DSCP优先级

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。

表4-5 配置 DHCPv6 客户端发送 DHCPv6 报文的 DSCP 优先级

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

4.3 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4-6 DHCPv6 客户端显示和维护

操作	命令
显示DHCPv6客户端的信息	**display ipv6 dhcp client** [**interface** *interface-type interface-number*]
显示DHCPv6客户端的统计信息	**display ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]
清除DHCPv6客户端的统计信息	**reset ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]

4.4 DHCPv6客户端典型配置举例

4.4.1 DHCPv6 客户端申请地址及网络参数配置举例

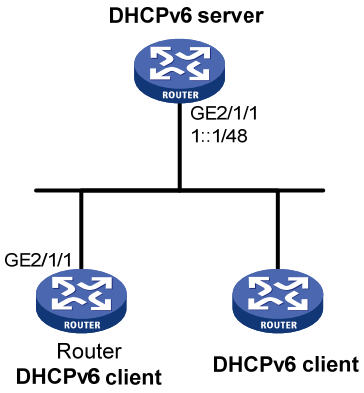
1. 组网需求

DHCPv6 客户端 Router 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。DHCPv6 服务器的配置方法，请参见“三层技术-IP 业务配置指导”中的“DHCPv6 服务器”。

配置接口 GigabitEthernet2/1/1 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。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ipv6 address dhcp-alloc rapid-commit option-group 1
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置

显示 DHCPv6 客户端的信息。

```
[Router] display ipv6 dhcp client
GigabitEthernet2/1/1:
  Type: Stateful client requesting address
    State: OPEN
    IAID: 0xf0019
    Client DUID: 00030001000fe2ff0000
    Preferred server:
      Reachable via address: FE80::200:5EFF:FE0A:2303
      Server DUID: 00030001000fe20a0a00
    Address: 1:2::2
       Preferred lifetime 60 sec, valid lifetime 60 sec
       T1 30 sec, T2 48 sec
       Will expire on Feb 4 2013 at 15:37:20（50 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 DHCPv6 选项组 1 的信息。

```
[Router-GigabitEthernet2/1/1] display ipv6 dhcp option-group 1
DHCPv6 option group: 1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet2/1/1
    2000::FF
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet2/1/1
    example.com
  SIP server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet2/1/1
    2:2::4
  SIP server domain names:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet2/1/1
    bbb.com
```

查看获取到的 IPv6 地址。

```
[Router] display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                          Physical   Protocol   IPv6 Address
GigabitEthernet2/1/1               up         up         1:2::2
```

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。

4.4.2 DHCPv6 客户端申请前缀及网络参数配置举例

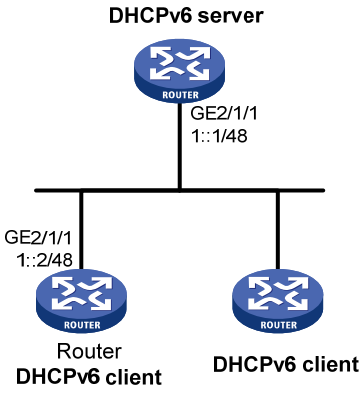
1. 组网需求

DHCPv6 客户端 Router 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 Router 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 DHCPv6 客户端连接到 DHCPv6 服务器的接口 GigabitEthernet2/1/1 上配置 IPv6 地址。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ipv6 address 1::2/48
```

配置接口 GigabitEthernet2/1/1 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。

```
[Router-GigabitEthernet2/1/1] ipv6 dhcp client pd 1 rapid-commit option-group 1
[Router-GigabitEthernet2/1/1] 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。

```
[Router] display ipv6 dhcp client
GigabitEthernet2/1/1:
  Type: Stateful client requesting prefix
    State: OPEN
    IAID: 0xf0019
    Client DUID: 00030001000fe2ff0000
    Preferred server:
      Reachable via address: FE80::200:5EFF:FE0A:2303
      Server DUID: 00030001000fe20a0a00
    Prefix: 12:34::/32
      Preferred lifetime 90 sec, valid lifetime 90 sec
      T1 45 sec, T2 72 sec
```

```
      Will expire on Feb 4 2013 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。

```
[Router] display ipv6 prefix 1
Number: 1
Type  : Dynamic
Prefix: 12:34::/32
Preferred lifetime 90 sec, valid lifetime 90 sec
```

显示动态创建的 DHCPv6 选项组 1 的信息。

```
[Router] display ipv6 dhcp option-group 1
DHCPv6 option group: 1
  DNS server addresses:
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: GigabitEthernet2/1/1
    2000::FF
  Domain name:
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: GigabitEthernet2/1/1
    example.com
  SIP server addresses:
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: GigabitEthernet2/1/1
    2:2::4
  SIP server domain names:
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: GigabitEthernet2/1/1
    bbb.com
```

以上两条 **display** 命令可以看到客户端获取到的前缀信息和网络参数。

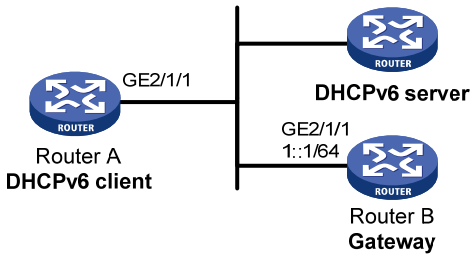
4.4.3 DHCPv6 无状态配置典型配置举例

1. 组网需求

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

2. 组网图

图4-3 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 Router B

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 1::1 64
```

配置 RA 消息中 O 标志位为 1。

```
[RouterB-GigabitEthernet2/1/1] ipv6 nd autoconfig other-flag
```

配置允许发送 RA 消息。

```
[RouterB-GigabitEthernet2/1/1] undo ipv6 nd ra halt
```

(2) 配置 DHCPv6 客户端 Router A

在接口 GigabitEthernet2/1/1 上使能 IPv6 地址无状态自动配置功能。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address auto
```

执行此命令后，如果 GigabitEthernet2/1/1 下没有配置地址，Router 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 Router 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，Router 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。

```
[RouterA-GigabitEthernet2/1/1] display ipv6 dhcp client interface gigabitethernet 2/1/1
GigabitEthernet2/1/1:
  Type: Stateless client
    State: OPEN
    IAID: 0xf0019
    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
```

如果从服务器成功获取了配置，将会有以上的显示信息。

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

```
[RouterA-GigabitEthernet2/1/1] display ipv6 dhcp client statistics
Interface                     :  GigabitEthernet2/1/1
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

说明

- 设备只有位于 DHCPv6 客户端与 DHCPv6 服务器之间，或 DHCPv6 客户端与 DHCPv6 中继之间时，DHCPv6 Snooping 功能配置后才能正常工作；设备位于 DHCPv6 服务器与 DHCPv6 中继之间时，DHCPv6 Snooping 功能配置后不能正常工作。
- 本特性仅在安装了二层交换卡的款型和 MSR3600-28/MSR3600-51 的固定二层接口上支持。

5.1 DHCPv6 Snooping简介

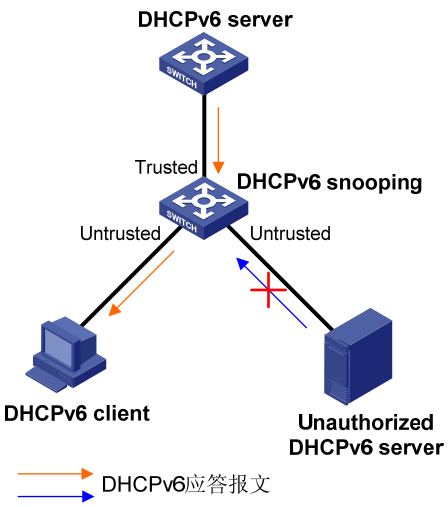
DHCPv6 Snooping 是 DHCPv6 的一种安全特性，具有如下功能：

1. 保证客户端从合法的服务器获取IPv6 地址

网络中如果存在私自架设的非法 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。

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。

5.2 DHCPv6 Snooping配置任务简介

表5-1 DHCPv6 Snooping 配置任务简介

配置任务	说明	详细配置
配置DHCPv6 Snooping基本功能	必选	5.3
配置DHCPv6 Snooping支持Option 18与Option 37功能	可选	5.4
配置DHCPv6 Snooping表项备份功能	可选	5.5
配置接口动态学习DHCPv6 Snooping 表项的最大数目	可选	5.6
启用DHCPv6 Snooping的DHCPv6请求方向报文检查功能	可选	5.7

5.3 配置DHCPv6 Snooping基本功能

启用 DHCPv6 Snooping 功能，并正确地配置信任端口和非信任端口后，可以保证客户端从合法的服务器获取 IPv6 地址，配置 DHCPv6 Snooping 基本功能时，需要注意，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。

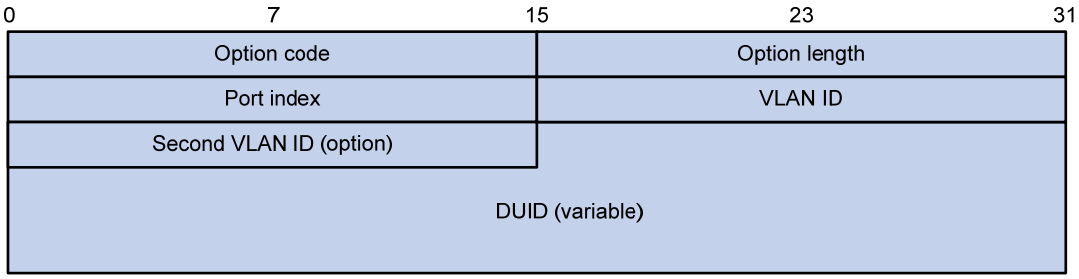
表5-2 配置 DHCPv6 Snooping 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
启用DHCPv6 Snooping功能	**ipv6 dhcp snooping enable**	缺省情况下，DHCPv6 Snooping功能处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	此接口为连接DHCPv6服务器的接口
配置DHCPv6 Snooping信任端口	**ipv6 dhcp snooping trust**	缺省情况下，启用DHCPv6 Snooping功能后，设备的所有端口均为不信任端口
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	此接口为连接DHCPv6客户端的接口
（可选）启用端口的DHCPv6 Snooping表项记录功能	**ipv6 dhcp snooping binding record**	缺省情况下，在启用DHCPv6 Snooping功能后， 端口的DHCPv6 Snooping表项记录功能处于关闭状态

5.4 配置DHCPv6 Snooping支持Option 18和Option 37功能

Option 18 称为接口ID选项（Interface ID），DHCPv6 Snooping设备接收到DHCPv6 客户端发送给DHCPv6 服务器的请求报文后，在该报文中添加Option 18 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 5-2 为Option 18 选项格式。

图5-2 Option 18 选项格式

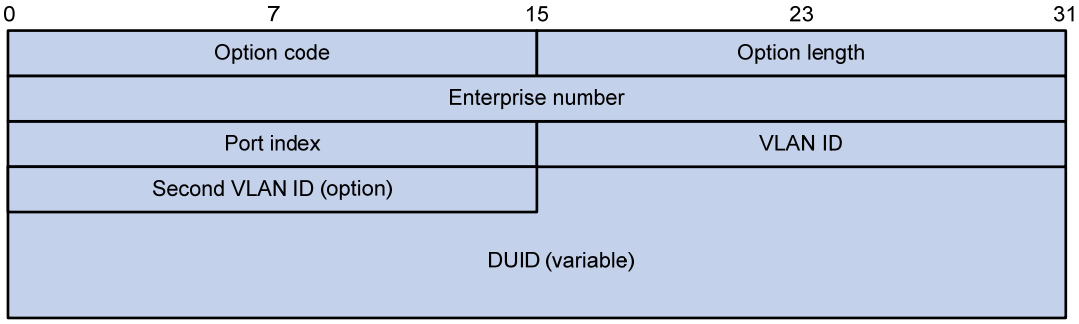


各字段的解释如下：

- Option code：Option 编号。
- Option length：Option 字段长度。
- Port index：DHCPv6 Snooping 设备收到客户端请求报文的端口信息。
- VLAN ID：第一层 VLAN 信息。
- Second VLAN ID：第二层 VLAN 信息。
- DUID：DHCPv6 客户端的 DUID 信息。

Option 37 称为远程ID选项（Remote ID），DHCPv6 Snooping设备接收到DHCPv6 客户端发送给DHCPv6 服务器的请求报文后，在该报文中添加Option 37 选项，并转发给DHCPv6 服务器。服务器可根据Option37选项中的信息对DHCPv6客户端定位，对分配IPv6地址提供帮助。图 5-3 为Option 37 选项格式。

图5-3 Option 37 选项格式



各字段的解释如下：

- Option code：Option 编号。

- Option length：Option 字段长度。
- Enterprise number：企业编号。
- Port index：DHCPv6 Snooping 设备收到客户端请求报文的端口信息。
- VLAN ID：第一层 VLAN 信息。
- Second VLAN ID：第二层 VLAN 信息。
- DUID：DHCPv6 客户端的 DUID 信息。

说明

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 或 Option 37 中也不包含 Second VLAN ID 内容。

表5-3 配置 DHCPv6 Snooping 支持 Option 18 和 Option 37 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
启用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
（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
启用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
（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

5.5 配置DHCPv6 Snooping表项备份功能

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。

表5-4 配置 DHCPv6 Snooping 表项备份功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
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** } *key*]] }	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。之后，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
（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
（可选）启用DHCPv6 Snooping表项存储文件的刷新时间间隔	**ipv6 dhcp snooping binding database update interval** *seconds*	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

说明

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。

5.6 配置接口动态学习DHCPv6 Snooping表项的最大数目

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

表5-5 配置接口动态学习 DHCPv6 Snooping 表项的最大数目

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

5.7 启用DHCPv6 Snooping的DHCPv6请求方向报文检查功能

本功能用来检查 DHCPv6-Renew、DHCPv6-Decline 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-Decline/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-Decline/DHCPv6-Release 报文，导致 DHCPv6 服务器错误终止 IPv6 地址租约。

在 DHCPv6 Snooping 设备上启用 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。如果启用了该功能，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。

表5-6 启用 DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启用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 只能在二层以太网接口上启用DHCPv6 Snooping的DHCPv6请求方向报文检查功能

5.8 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5-7 DHCPv6 Snooping 显示和维护

操作	命令
显示DHCPv6 Snooping信任端口信息	**display ipv6 dhcp snooping trust**
显示DHCPv6 Snooping表项信息	**display ipv6 dhcp snooping binding** [**address** *ipv6-address* [**vlan** *vlan-id*]]
显示DHCPv6 Snooping表项备份信息	**display ipv6 dhcp snooping binding database**
显示DHCPv6 Snooping设备上的DHCPv6报文统计信息（MSR 2600/MSR 3600）	**display ipv6 dhcp snooping packet statistics**
显示DHCPv6 Snooping设备上的DHCPv6报文统计信息（MSR 5600）	**display ipv6 dhcp snooping packet statistics** [**slot** *slot-number*]

操作	命令
清除DHCPv6 Snooping表项	**reset ipv6 dhcp snooping binding** { **all** | **address** *ipv6-address* [**vlan** *vlan-id*] }
清除DHCPv6 Snooping设备上的DHCPv6报文统计信息（MSR 2600/MSR 3600）	**reset ipv6 dhcp snooping packet statistics**
清除DHCPv6 Snooping设备上的DHCPv6报文统计信息（MSR 5600）	**reset ipv6 dhcp snooping packet statistics** [**slot** *slot-number*]

5.9 DHCPv6 Snooping典型配置举例

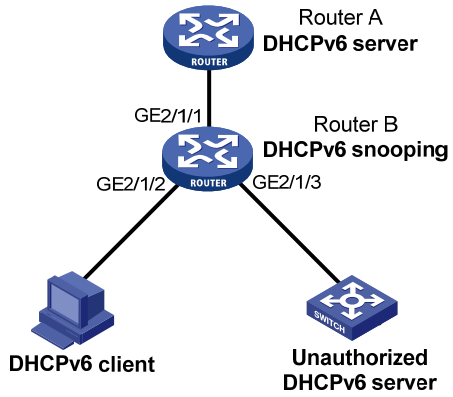
1. 组网需求

Router B 通过以太网端口 GigabitEthernet2/1/1 连接到合法 DHCPv6 服务器，通过以太网端口GigabitEthernet2/1/3连接到非法服务器，通过GigabitEthernet2/1/2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5-4 DHCPv6 Snooping 组网示意图



3. 配置步骤

启用 DHCPv6 Snooping 功能。

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

配置 GigabitEthernet2/1/1 端口为信任端口。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 dhcp snooping trust
[RouterB-GigabitEthernet2/1/1] quit
```

在 GigabitEthernet2/1/2 上启用安全表项功能。

```
[RouterB]interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 dhcp snooping binding record
```

```
[RouterB-GigabitEthernet2/1/2] 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 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，根据报文的目的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 快速转发使用 6 元组（源 IPv6 地址、目的 IPv6 地址、源端口号、目的端口号、协议号和 VPN 实例名称）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1-1 配置 IPv6 快速转发

操作	命令	说明
进入系统视图	**system-view**	-
开启IPv6快速转发负载分担功能	**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
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 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1-2 IPv6 快速转发显示和维护

操作	命令
显示IPv6快速转发表信息（MSR 2600/MSR 3600）	**display ipv6 fast-forwarding cache** [*ipv6-address*]
显示IPv6快速转发表信息（MSR 5600）	**display ipv6 fast-forwarding cache** [*ipv6-address*] [**slot** *slot-number*]
显示IPv6快速转发表项的老化时间	**display ipv6 fast-forwarding aging-time**
清除IPv6快速转发表信息（MSR 2600/MSR 3600）	**reset ipv6 fast-forwarding cache**

操作	命令
清除IPv6快速转发表信息（MSR 5600）	**reset ipv6 fast-forwarding cache** [**slot** *slot-number*]

1.4 IPv6快速转发典型配置举例

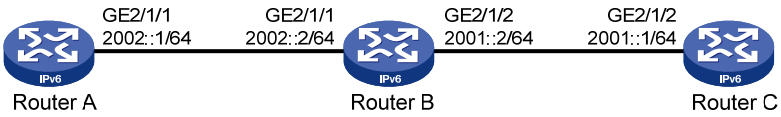
1.4.1 IPv6 快速转发典型配置举例

1. 组网需求

在 Router B 上实现 IPv6 快速转发。

2. 组网图

图1-1 配置 IPv6 快速转发组网图



3. 配置步骤

(1) 配置 Router A

配置接口的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 2002::1 64
[RouterA-GigabitEthernet2/1/1] quit
```

配置静态路由。

```
[RouterA] ipv6 route-static 2001:: 64 2002::2
```

(2) 配置 Router C

配置接口的 IPv6 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] ipv6 address 2001::1 64
[RouterC-GigabitEthernet2/1/2] quit
```

配置静态路由。

```
[RouterC] ipv6 route-static 2002:: 64 2001::2
```

(3) 配置 Router B

使能 IPv6 快速转发功能。

```
<RouterB> system-view
[RouterB] ipv6 fast-forwarding
```

配置接口的 IPv6 地址。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 2002::2 64
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
```

```
[RouterB-GigabitEthernet2/1/2] ipv6 address 2001::2 64
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

在 Router B 查看 IPv6 快速转发表，这时未建立快转表项，结果如下：

```
[RouterB] display ipv6 fast-forwarding cache
No IPv6 fast-forwarding entries.
```

从 Router A 上 ping Router C 的 GigabitEthernet2/1/2 接口 IPv6 地址，能收到应答报文。

```
[RouterA] ping ipv6 2001::1
  PING 2001::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64  time = 69 ms
    Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64  time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64  time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64  time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=5 hop limit=64  time = 1 ms

  --- 2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/14/69 ms
```

在 Router B 查看 IPv6 快速转发表，已建立快转表项，显示信息如下：

```
[RouterB] display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
Src IP: 2002::1                                        Src port: 129
Dst IP: 2001::1                                        Dst port: 0
Protocol: 58
VPN instance: N/A
Input interface: GE2/1/1
Output interface: GE2/1/2

Src IP: 2001::1                                        Src port: 128
Dst IP: 2002::1                                        Dst port: 0
Protocol: 58
VPN instance: N/A
Input interface: GE2/1/2
Output interface: GE2/1/1
```

目 录

1 隧道

1.1 隧道概述

隧道技术是一种封装技术，即一种网络协议将其他网络协议的数据报文封装在自己的报文中，然后在网络中传输。封装后的数据报文在网络中传输的路径，称为隧道。隧道是一条虚拟的点对点连接，隧道的两端需要对数据报文进行封装及解封装。隧道技术就是指包括数据封装、传输和解封装在内的全过程。

隧道技术具有以下用途：

- 作为过渡技术，实现 IPv4 和 IPv6 网络互通，如 IPv6 over IPv4 隧道技术。
- 创建 VPN（Virtual Private Network，虚拟专用网络），如 IPv4 over IPv4 隧道、IPv4/IPv6 over IPv6 隧道、GRE（Generic Routing Encapsulation，通用路由封装）、DVPN（Dynamic Virtual Private Network，动态虚拟专用网络）和 IPsec 隧道技术。GRE、DVPN 的相关介绍和配置请分别参见“三层技术-IP 业务配置指导”中的“GRE”和“DVPN”；IPsec 的相关介绍和配置请参见“安全配置指导”中的“IPsec”。
- 实现流量工程，避免由于负载不均衡导致网络拥塞，如 MPLS TE（Multiprotocol Label Switching Traffic Engineering，多协议标记交换流量工程）。MPLS TE 的相关介绍和配置请参见“MPLS 配置指导”中的“MPLS TE”。

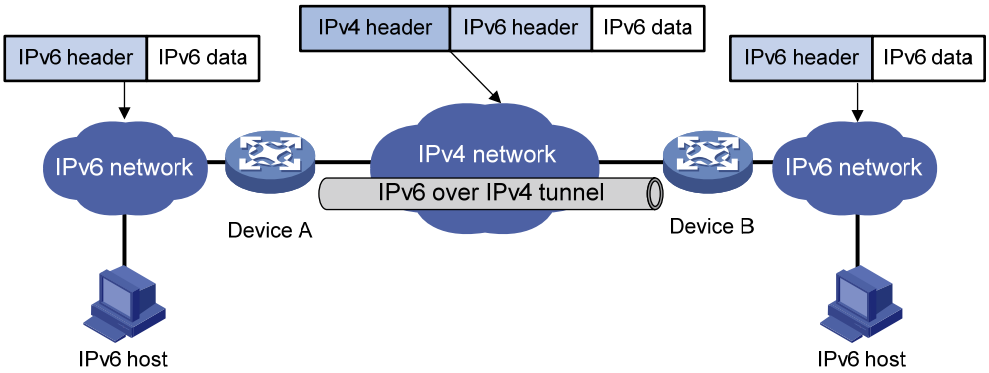
本文只介绍 IPv6 over IPv4 隧道、IPv4 over IPv4 隧道、IPv4 over IPv6 隧道和 IPv6 over IPv6 隧道。如无特殊说明，下文中的隧道技术均指此类隧道。

1.1.1 IPv6 over IPv4 隧道

1. IPv6 over IPv4 隧道原理

如 图 1-1 所示，IPv6 over IPv4 隧道是在IPv6 数据报文前封装上IPv4 的报文头，通过隧道使IPv6 报文穿越IPv4 网络，实现隔离的IPv6 网络互通。IPv6 over IPv4 隧道两端的设备必须支持IPv4/IPv6 双协议栈，即同时支持IPv4 协议和IPv6 协议。

图1-1 IPv6 over IPv4 隧道原理图



IPv6 over IPv4 隧道对报文的处理过程如下：

(1) IPv6 网络中的主机发送 IPv6 报文，该报文到达隧道的源端设备 Device A。

(2) Device A 根据路由表判定该报文要通过隧道进行转发后，在 IPv6 报文前封装上 IPv4 的报文头，通过隧道的实际物理接口将报文转发出去。IPv4 报文头中的源 IP 地址为隧道的源端地址，目的 IP 地址为隧道的目的端地址。

(3) 封装报文通过隧道到达隧道目的端设备（或称隧道终点）Device B，Device B 判断该封装报文的目的地是本设备后，将对报文进行解封装。

(4) Device B 根据解封装后的 IPv6 报文的目的地址处理该 IPv6 报文。如果目的地就是本设备，则将 IPv6 报文转给上层协议处理；否则，查找路由表转发该 IPv6 报文。

2. IPv6 over IPv4 隧道模式

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为“配置隧道”和“自动隧道”。

- 如果 IPv6 over IPv4 隧道终点的 IPv4 地址不能从 IPv6 报文的目的地址中自动获取，需要进行手工配置，这样的隧道称为“配置隧道”。
- 如果 IPv6 报文的目的地址中嵌入了 IPv4 地址，则可以从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址，这样的隧道称为“自动隧道”。

如 表 1-1 所示，根据对IPv6 报文的封装方式的不同，IPv6 over IPv4 隧道分为以下几种模式。

表1-1 IPv6 over IPv4 隧道模式

隧道类型	隧道模式	隧道源端/目的端地址	IPv6 报文目的地址格式
配置隧道	IPv6 over IPv4手动隧道	源端/目的端地址为手工配置的IPv4地址	普通的IPv6地址
自动隧道	IPv4兼容IPv6自动隧道	源端地址为手工配置的IPv4地址，目的端地址不需配置	IPv4兼容IPv6地址，其格式为： ::IPv4-destination-address/96 其中，IPv4-destination-address表示隧道的目的端地址
	6to4隧道	源端地址为手工配置的IPv4地址，目的端地址不需配置	6to4地址，其格式为： 2002:IPv4-destination-address::/48 其中，IPv4-destination-address表示隧道的目的端地址
	ISATAP（Intra-Site Automatic Tunnel Addressing Protocol，站点内自动隧道寻址协议）隧道	源端地址为手工配置的IPv4地址，目的端地址不需配置	ISATAP地址，其格式为： Prefix:0:5EFE:IPv4-destination-address/64 其中，IPv4-destination-address表示隧道的目的端地址

(1) IPv6 over IPv4 手动隧道

IPv6 over IPv4 手动隧道是点到点之间的链路。建立手动隧道需要在隧道两端手工指定隧道的源端和目的端地址。

手动隧道可以建立在连接 IPv4 网络和 IPv6 网络的两个边缘路由器之间，实现隔离的 IPv6 网络跨越 IPv4 网络通信；也可以建立在边缘路由器和 IPv4/IPv6 双栈主机之间，实现隔离的 IPv6 网络跨越 IPv4 网络与双栈主机通信。

(2) IPv4 兼容 IPv6 自动隧道

IPv4 兼容 IPv6 自动隧道是点到多点的链路。隧道两端采用特殊的 IPv6 地址：IPv4 兼容 IPv6 地址，其格式为：0:0:0:0:0:0:a.b.c.d/96，其中 a.b.c.d 是 IPv4 地址。通过这个嵌入的 IPv4 地址可以自动确定隧道的目的端地址。

IPv4 兼容 IPv6 自动隧道的建立非常方便。但是，由于它使用 IPv4 兼容 IPv6 地址，采用 IPv4 兼容 IPv6 自动隧道通信的主机和路由器必须具有全球唯一的 IPv4 地址，无法解决 IPv4 地址空间耗尽的问题，存在一定的局限性。

(3) 6to4 隧道

- 普通 6to4 隧道

6to4 隧道是点到多点的自动隧道，主要建立在边缘路由器之间，用于通过 IPv4 网络连接多个 IPv6 孤岛。

6to4 隧道两端采用特殊的 6to4 地址，其格式为：2002:abcd:efgh:子网号::接口 ID/48。其中：2002 表示固定的 IPv6 地址前缀；abcd:efgh 为用 16 进制表示的 IPv4 地址（如 1.1.1.1 可以表示为 0101:0101），用来唯一标识一个 6to4 网络（如果 IPv6 孤岛中的主机都采用 6to4 地址，则该 IPv6 孤岛称为 6to4 网络），6to4 网络的边缘路由器上连接 IPv4 网络的接口地址需要配置为此 IPv4 地址；子网号用来在 6to4 网络内划分子网；子网号和接口 ID 共同标识了一个主机在 6to4 网络内的位置。通过 6to4 地址中嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

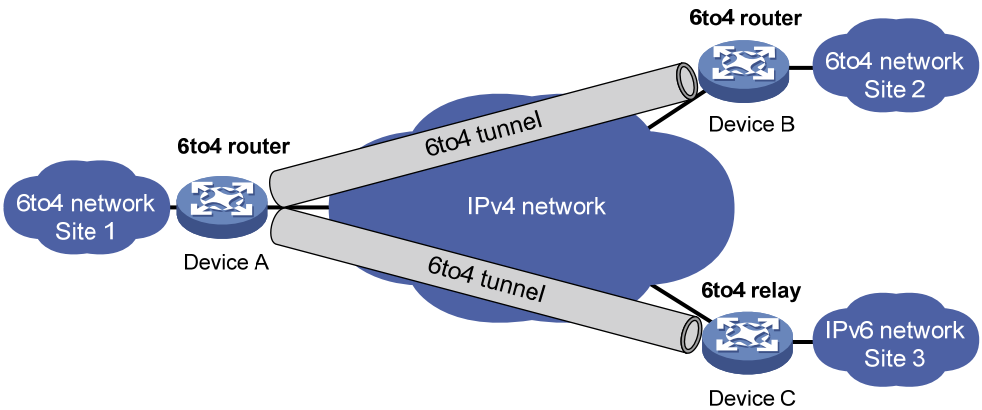
6to4 地址中采用一个全球唯一的 IPv4 地址标识了一个 6to4 网络，克服了 IPv4 兼容 IPv6 自动隧道的局限性。

- 6to4 中继

6to4 隧道只能用于前缀为 2002::/16 的 6to4 网络之间的通信，但在 IPv6 网络中也会使用像 2001::/16 这样的 IPv6 网络地址。为了实现 6to4 网络和其它 IPv6 网络的通信，必须有一台 6to4 路由器作为网关转发到 IPv6 网络的报文，这台路由器就叫做 6to4 中继（6to4 relay）路由器。

如下图所示，在 6to4 网络的边缘路由器 Device A 上配置一条到达 IPv6 网络（非 6to4 网络）的静态路由，下一跳地址指向 6to4 中继路由器 Device C 的 6to4 地址，这样，所有去往该 IPv6 网络的报文都会被转发到 6to4 中继路由器，之后再由 6to4 中继路由器转发到 IPv6 网络中，从而实现 6to4 网络与 IPv6 网络的互通。

图1-2 6to4 隧道和 6to4 中继原理图



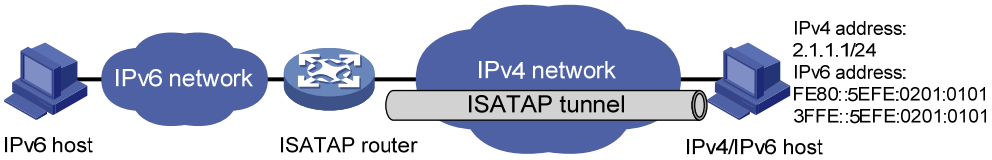
(4) ISATAP 隧道

ISATAP 隧道是点到多点的自动隧道技术，为 IPv6 主机通过 IPv4 网络接入 IPv6 网络提供了一个较好的解决方案。

使用 ISATAP 隧道时，IPv6 报文的目的地址要采用特殊的 ISATAP 地址。ISATAP 地址格式为：Prefix:0:5EFE:abcd:efgh/64。其中，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀；abcd:efgh 为用 16 进制表示的 32 位 IPv4 地址（如 1.1.1.1 可以表示为 0101:0101），该 IPv4 地址不要求全球唯一。通过 ISATAP 地址中嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

ISATAP 隧道主要用于跨越 IPv4 网络在 IPv6 主机与边缘路由器之间、两个边缘路由器之间建立连接。

图1-3 ISATAP 隧道原理图



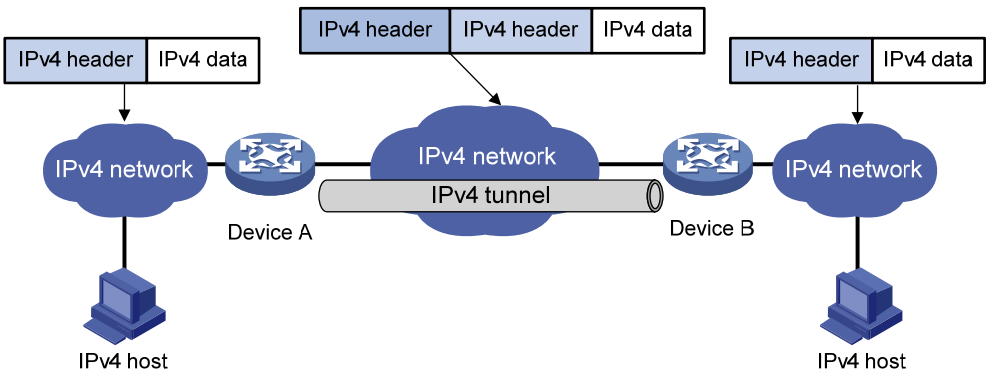
1.1.2 IPv4 over IPv4 隧道

1. IPv4 over IPv4 隧道简介

IPv4 over IPv4 隧道（RFC 1853）是对 IPv4 报文进行封装，使得一个 IPv4 网络的报文能够在另一个 IPv4 网络中传输。例如，运行 IPv4 协议的两个子网位于不同的区域，并且这两个子网都使用私网地址时，可以通过建立 IPv4 over IPv4 隧道，实现两个子网的互联。

2. 报文封装及解封装

图1-4 IPv4 over IPv4 隧道原理图



报文在隧道中传输经过封装与解封装两个过程，以 图 1-4 为例说明这两个过程：

- 封装过程

Device A 连接 IPv4 主机所在子网的接口收到 IPv4 报文后，首先交由 IPv4 协议栈处理。IPv4 协议栈根据 IPv4 报文头中的目的地址判断该报文需要通过隧道进行转发，则将此报文发给 Tunnel 接口。Tunnel 接口收到此报文后，在 IPv4 报文外再封装一个 IPv4 报文头，封装的报文头中源 IPv4 地址为隧道的源端地址，目的 IPv4 地址为隧道的目的端地址。封装完成后将报文重新交给 IPv4 协议栈处理，IPv4 协议栈根据添加的 IPv4 报文头查找路由表，转发报文。

- 解封装过程

解封装过程和封装过程相反。Device B 从接口收到 IPv4 报文后，将其送到 IPv4 协议栈处理。IPv4 协议栈检查接收到的 IPv4 报文头中的协议号。如果协议号为 4（表示封装的报文为 IPv4 报文），则

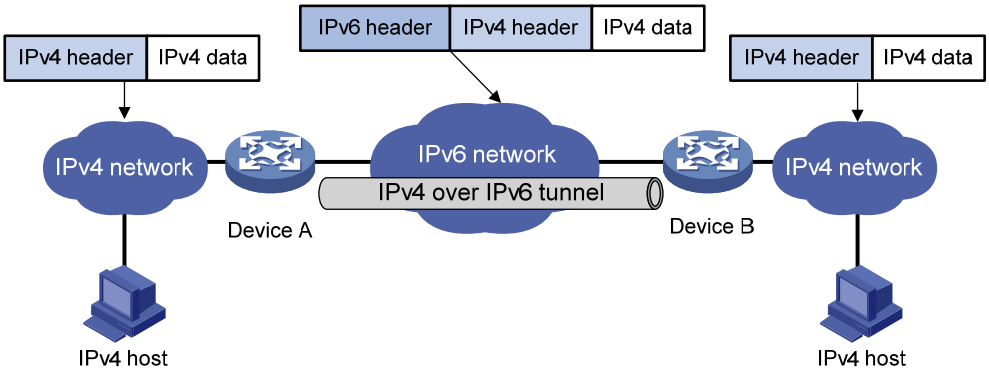
将此 IPv4 报文发送到隧道模块进行解封装处理。解封装之后的 IPv4 报文将重新被送到 IPv4 协议栈进行二次路由处理。

1.1.3 IPv4 over IPv6 隧道

1. IPv4 over IPv6 隧道原理

随着 IPv6 网络的广泛部署，IPv6 网络将逐渐取代 IPv4 网络，占据主导地位。尚未被 IPv6 网络取代的 IPv4 网络将形成孤岛，需要通过 IPv6 网络互通。IPv4 over IPv6 隧道在 IPv4 报文上封装 IPv6 的报文头，通过隧道使 IPv4 报文穿越 IPv6 网络，从而实现通过 IPv6 网络连接隔离的 IPv4 网络孤岛。

图1-5 IPv4 over IPv6 隧道原理图



IPv4 报文在隧道中传输经过封装与解封装两个过程，以 图 1-5 为例说明这两个过程：

- 封装过程

Device A 连接 IPv4 网络的接口收到 IPv4 报文后，首先交由 IPv4 协议栈处理。IPv4 协议栈根据 IPv4 报文头中的目的地址判断该报文需要通过隧道进行转发，则将此报文发给 Tunnel 接口。

Tunnel 接口收到此报文后添加 IPv6 报文头，IPv6 报文头中源 IPv6 地址为隧道的源端地址，目的 IPv6 地址为隧道的目的端地址。封装完成后将报文交给 IPv6 模块处理。IPv6 协议模块根据 IPv6 报文头的目的地址重新确定如何转发此报文。

- 解封装过程

解封装过程和封装过程相反。从连接 IPv6 网络的接口接收到 IPv6 报文后，将其送到 IPv6 协议模块。IPv6 协议模块检查 IPv6 报文封装的协议类型。若封装的协议为 IPv4，则报文进入隧道处理模块进行解封装处理。解封装之后的 IPv4 报文被送往 IPv4 协议模块进行二次路由处理。

2. IPv4 over IPv6 隧道模式

IPv4 over IPv6 隧道分为以下几种模式：

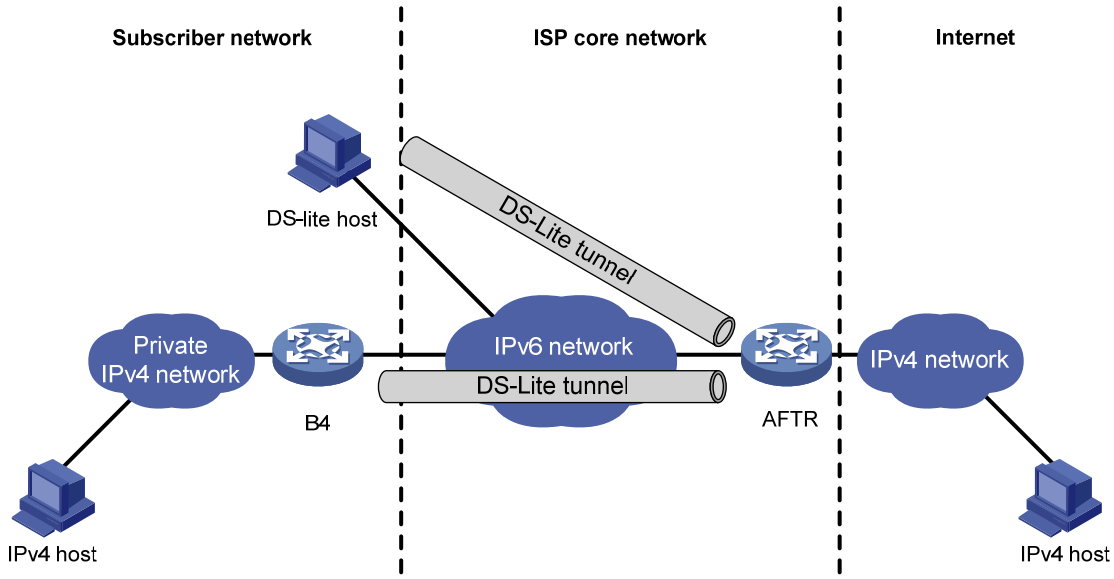
(1) IPv4 over IPv6 手动隧道

IPv4 over IPv6 手动隧道需要手动配置隧道的源和目的 IPv6 地址，以便根据配置的地址在 IPv4 报文上封装 IPv6 报文头，使报文能通过隧道穿越 IPv6 网络。IPv4 over IPv6 手动隧道是一种点到点的虚拟链路。

(2) DS-Lite 隧道

DS-Lite（Dual Stack Lite，轻量级双协议栈）技术综合了 IPv4 over IPv6 隧道技术和 NAT（Network Address Translation，网络地址转换）技术，利用隧道技术实现通过 IPv6 网络连接隔离的 IPv4 网络，利用 NAT 技术实现不同的用户网络共享相同的 IPv4 地址空间，减缓 IPv4 地址的耗尽速度。

图1-6 DS-Lite 组网图



如 图 1-6 所示，DS-Lite网络主要由几个部分组成：

- DS-Lite 隧道

DS-Lite 隧道是 B4 设备和 AFTR 之间的 IPv4 over IPv6 隧道，用来实现 IPv4 报文跨越 IPv6 网络传输。

- B4（Basic Bridging BroadBand，基本桥接宽带）设备

B4 设备是位于用户网络侧、用来连接 ISP（Internet Service Provider，互联网服务提供商）网络的设备，通常为用户网络的网关。B4 设备作为 DS-Lite 隧道的一个端点，负责将用户网络的 IPv4 报文封装成 IPv6 报文发送给隧道的另一个端点，同时将从隧道接收到的 IPv6 报文解封装成 IPv4 报文发送给用户网络。

某些用户网络的主机也可以作为 B4 设备，直接连接到 ISP 网络，这样的主机称为 DS-Lite 主机。

- AFTR（Address Family Transition Router，地址族转换路由器）

AFTR 是 ISP 网络中的设备。AFTR 同时作为 DS-Lite 隧道端点和 NAT 网关设备。

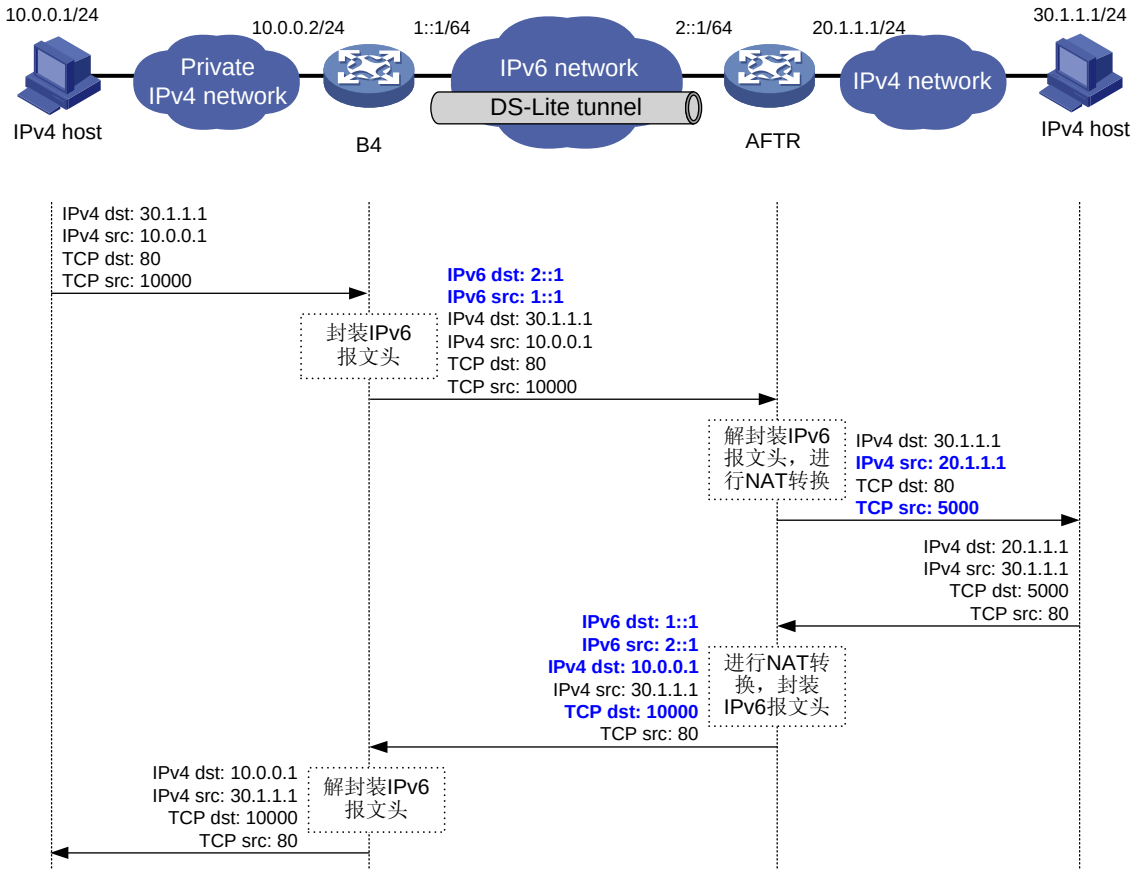
AFTR 从 DS-Lite 隧道接收到 B4 设备发送的 IPv6 报文后，为该 B4 设备分配 Tunnel ID，并记录 B4 设备的 IPv6 地址（报文中的源 IPv6 地址）与 Tunnel ID 的对应关系。AFTR 对 IPv6 报文进行解封装，将解封装后的用户网络报文的源 IPv4 地址（私网地址）转换为公网地址，并将转换后的报文发送给目的 IPv4 主机。AFTR 进行 NAT 转换时，同时记录 NAT 映射关系和 Tunnel ID，以便实现不同 B4 设备连接的用户网络地址可以重叠。

AFTR 接收到目的 IPv4 主机返回的应答报文后，将目的 IPv4 地址（公网地址）转换为对应的私网地址，并根据记录的 Tunnel ID 获取对应的 B4 设备的 IPv6 地址，作为封装后 IPv6 报文的目的地址。AFTR 将 NAT 转换后的报文封装成 IPv6 报文通过隧道发送给 B4 设备。

提示

DS-Lite 只支持用户网络内的 IPv4 主机主动访问公网上的 IPv4 主机；公网上的 IPv4 主机不能主动访问用户网络内的 IPv4 主机。

图1-7 DS-Lite 报文转发流程



采用独立的网关设备作为B4 设备时，报文转发过程中源和目的IP地址、源和目的端口号的变化如 图1-7 所示。报文转发过程的关键步骤为：

- B4 设备和 AFTR 对报文进行封装和解封装。
- AFTR 对 IPv4 报文进行 NAT 转换。

说明

DS-Lite隧道支持的NAT转换方式包括：静态地址转换、NO-PAT（Not Port Address Translation）模式和PAT（Port Address Translation）模式的动态地址转换。图 1-7 所示为PAT模式的动态地址转换。使用静态地址转换时不同B4 设备连接的用户网络地址不能重叠，因此DS-Lite隧道一般使用动态地址转换。有关NAT的详细介绍，请参见“三层技术-IP业务配置指导”中的“NAT”。

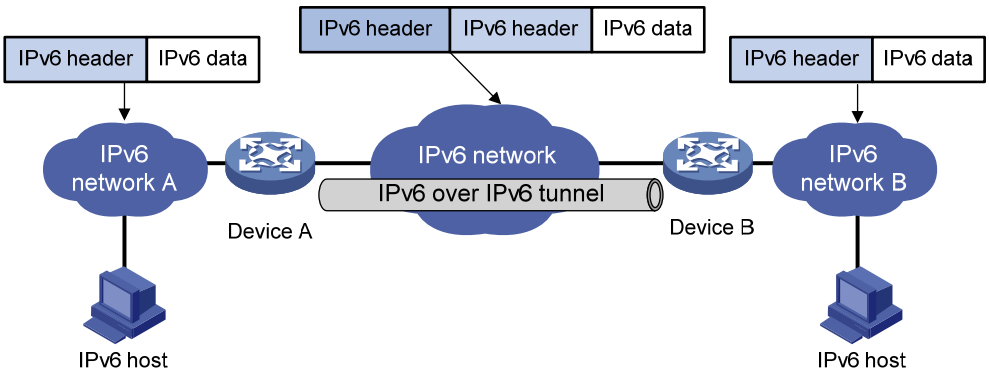
1.1.4 IPv6 over IPv6 隧道

1. IPv6 over IPv6 隧道简介

IPv6 over IPv6 隧道（RFC 2473）是对 IPv6 报文进行封装，使这些被封装的报文能够在另一个 IPv6 网络中传输，封装后的报文即 IPv6 隧道报文。例如，如果运行 IPv6 协议的两个子网的网络地址不希望泄露到 IPv6 网络中，则可以通过建立 IPv6 over IPv6 隧道，实现在两个子网的网络地址不被泄露的情况下，使两个子网互通。

2. 报文封装及解封装

图1-8 IPv6 over IPv6 隧道原理图



IPv6 报文在隧道中传输经过封装与解封装两个过程，以 图 1-8 为例说明这两个过程：

- 封装过程

Device A 连接网络 A 的接口收到 IPv6 报文后，首先交由 IPv6 协议模块处理。IPv6 协议模块根据报文的目的 IPv6 地址判断该报文需要通过隧道进行转发，则将此报文发给 Tunnel 接口。

Tunnel 接口收到此报文后，为 IPv6 报文再封装一个 IPv6 报文头，封装的 IPv6 报文头中源 IPv6 地址为隧道的源端地址，目的 IPv6 地址为隧道的目的端地址。封装完成后将报文交给 IPv6 模块处理。IPv6 协议模块根据添加的 IPv6 报文头的目的地址重新确定如何转发此报文。

- 解封装过程

解封装过程和封装过程相反。从 IPv6 网络接口接收的报文被送到 IPv6 协议模块。IPv6 协议模块检查 IPv6 报文封装的协议类型。若封装的协议为 IPv6，则报文进入隧道处理模块进行解封装处理；解封装之后的报文被送往相应的协议模块进行二次路由处理。

1.1.5 协议规范

与隧道技术相关的协议规范有：

- RFC 1853：IP in IP Tunneling
- RFC 2473：Generic Packet Tunneling in IPv6 Specification
- RFC 2893：Transition Mechanisms for IPv6 Hosts and Routers
- RFC 3056：Connection of IPv6 Domains via IPv4 Clouds
- RFC 4214：Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC 6333：Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

1.2 隧道配置任务简介

表1-2 隧道配置任务简介

配置任务		说明	详细配置
配置Tunnel接口		必选	1.3
配置IPv6 over IPv4隧道	配置IPv6 over IPv4手动隧道	根据组网情况，选择其一	1.4
	配置IPv4兼容IPv6自动隧道		1.5
	配置6to4隧道		1.6
	配置ISATAP隧道		1.7
配置IPv4 over IPv4隧道			1.8
配置IPv4 over IPv6隧道	配置IPv4 over IPv6手动隧道		1.9
	配置DS-Lite隧道		1.10
配置IPv6 over IPv6隧道			1.11

1.3 配置Tunnel接口

隧道两端的设备上，需要创建虚拟的三层接口，即 Tunnel 接口，以便隧道两端的设备利用 Tunnel 接口发送报文、识别并处理来自隧道的报文。

配置 Tunnel 接口时，需要注意在 MSR 5600 上，主备倒换或备板拔出时，建立在主控板或备板上的隧道接口不会被删除，若再配置相同的隧道接口，系统会提示隧道接口已经存在。如果需要删除隧道接口，请使用 **undo interface tunnel** 命令。

表1-3 配置 Tunnel 接口

操作	命令	说明
进入系统视图	**system-view**	-
创建Tunnel接口，指定隧道模式，并进入Tunnel接口视图	**interface tunnel** *number* **mode { ds-lite-aftr | gre [ipv6] | ipv4-ipv4 | ipv6 | ipv6-ipv4 [6to4 | auto-tunnel | isatap] | mpls-te }**	缺省情况下，设备上不存在任何Tunnel接口 创建Tunnel接口时，必须指定隧道的模式；进入已经创建的Tunnel接口视图时，可以不指定隧道模式 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败
（可选）配置接口描述信息	**description** *text*	缺省情况下，接口描述信息为“*该接口的接口名* Interface”
（可选）指定转发当前接口流量的业务处理板（MSR 5600）	**service slot** *slot-number*	缺省情况下，没有指定转发当前接口流量的业务处理板

操作	命令	说明
配置IPv4 MTU值	**mtu** *mtu-size*	缺省情况下，MTU值为64000字节
配置Tunnel接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，Tunnel接口的期望带宽为64kbps 接口的期望带宽会影响链路开销值。具体介绍请参见“三层技术-IP路由配置指导”中的“OSPF”、“OSPFv3”和“IS-IS”
设置封装后隧道报文的ToS	**tunnel tos** *tos-value*	缺省情况下，封装后隧道报文的ToS值与封装前原始IP报文的ToS值相同
设置封装后隧道报文的TTL值	**tunnel ttl** *ttl-value*	缺省情况下，封装后隧道报文的TTL值为255
配置隧道目的端地址所属的VPN	**tunnel vpn-instance** *vpn-instance-name*	缺省情况下，隧道目的端地址属于公网，设备查找公网路由表转发隧道封装后的报文 在隧道的源接口上通过**ip binding vpn-instance**命令可以指定隧道源端地址所属的VPN。隧道的源端地址和目的端地址必须属于相同的VPN，否则隧道接口链路状态无法UP **ip binding vpn-instance**命令的详细介绍，请参见“MPLS命令参考”中的“MPLS L3VPN”
（可选）恢复当前接口的缺省配置	**default**	-
（可选）关闭Tunnel接口	**shutdown**	缺省情况下，Tunnel接口是打开的

1.4 配置IPv6 over IPv4手动隧道

1.4.1 配置步骤

配置 IPv6 over IPv4 手动隧道时，需要注意：

- 在本端设备上为隧道指定的目的端地址，应该与在对端设备上为隧道指定的源端地址相同；在本端设备上为隧道指定的源端地址，应该与在对端设备上为隧道指定的目的端地址相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 如果封装前 IPv6 报文的目的 IPv6 地址与 Tunnel 接口的 IPv6 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达目的 IPv6 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址。用户也可以配置动态路由，在 Tunnel 接口使能动态路由协议。在隧道的两端都要进行此项配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 静态路由”或其他路由协议配置。

表1-4 配置 IPv6 over IPv4 手动隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为IPv6 over IPv4手动隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6-ipv4**]	-
设置Tunnel接口的IPv6地址	详细配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上不存在IPv6地址
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IP地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IP地址
设置隧道的目的端地址	**destination** *ip-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端接收报文的接口的地址，该地址将作为封装后隧道报文的目的地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
退回系统视图	**quit**	-
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

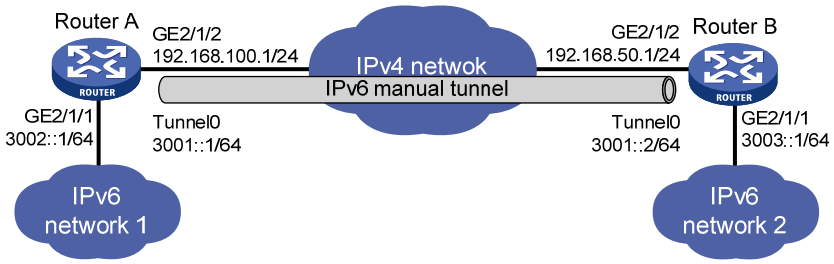
1.4.2 配置举例

1. 组网需求

如 图 1-9 所示，两个IPv6 网络分别通过Router A和Router B与IPv4 网络连接，要求在Router A和Router B之间建立IPv6 over IPv4 隧道，使两个IPv6 网络可以互通。由于隧道终点的IPv4 地址不能从IPv6 报文的目的地址中自动获取，因此，需要配置IPv6 over IPv4 手动隧道。

2. 组网图

图1-9 IPv6 over IPv4 手动隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv4 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/2 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 192.168.100.1 255.255.255.0
[RouterA-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 3002::1 64
[RouterA-GigabitEthernet2/1/1] quit
```

创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel0。

```
[RouterA] interface tunnel 0 mode ipv6-ipv4
```

配置 Tunnel0 接口的 IPv6 地址。

```
[RouterA-Tunnel0] ipv6 address 3001::1/64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterA-Tunnel0] source gigabitethernet 2/1/2
```

配置 Tunnel0 接口的目的端地址（Router B 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterA-Tunnel0] destination 192.168.50.1
[RouterA-Tunnel0] quit
```

配置从 Router A 经过 Tunnel0 接口到 IPv6 network 2 的静态路由。

```
[RouterA] ipv6 route-static 3003:: 64 tunnel 0
```

(2) 配置 Router B

配置接口 GigabitEthernet2/1/2 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 192.168.50.1 255.255.255.0
[RouterB-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 3003::1 64
[RouterB-GigabitEthernet2/1/1] quit
```

创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel0。

```
[RouterB] interface tunnel 0 mode ipv6-ipv4
```

配置 Tunnel0 接口的 IPv6 地址。

```
[RouterB-Tunnel0] ipv6 address 3001::2/64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterB-Tunnel0] source gigabitethernet 2/1/2
```

配置 Tunnel0 接口的目的端地址（Router A 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterB-Tunnel0] destination 192.168.100.1
[RouterB-Tunnel0] quit
```

配置从 Router B 经过 Tunnel0 接口到 IPv6 network 1 的静态路由。

```
[RouterB] ipv6 route-static 3002:: 64 tunnel 0
```

4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display ipv6 interface** 命令，可以看出 Tunnel0 接口处于 up 状态。（具体显示信息略）

从 Router A 和 Router B 上可以 Ping 通对端的 GigabitEthernet2/1/1 接口的 IPv6 地址。下面仅以 Router A 为例。

```
[RouterA] ping ipv6 3003::1
Ping6(56 data bytes) 3001::1 --> 3003::1, press CTRL_C to break
56 bytes from 3003::1, icmp_seq=0 hlim=64 time=45.000 ms
56 bytes from 3003::1, icmp_seq=1 hlim=64 time=10.000 ms
56 bytes from 3003::1, icmp_seq=2 hlim=64 time=4.000 ms
56 bytes from 3003::1, icmp_seq=3 hlim=64 time=10.000 ms
56 bytes from 3003::1, icmp_seq=4 hlim=64 time=11.000 ms

--- Ping6 statistics for 3003::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/16.000/45.000/14.711 ms
```

1.5 配置IPv4兼容IPv6自动隧道

1.5.1 配置步骤

配置 IPv4 兼容 IPv6 自动隧道时，需要注意：

- IPv4 兼容 IPv6 自动隧道不需要配置隧道的目的端地址，因为隧道的目的端地址可以通过 IPv4 兼容 IPv6 地址中嵌入的 IPv4 地址自动获得。
- 对于自动隧道，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址。

表1-5 配置 IPv4 兼容 IPv6 自动隧道

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入模式为IPv4兼容IPv6自动隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6-ipv4 auto-tunnel**]	-
设置Tunnel接口的IPv6地址	详细配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上不存在IPv6地址
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IP地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IP地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片

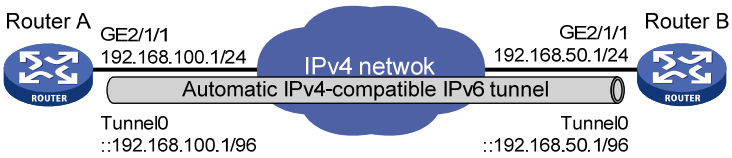
1.5.2 配置举例

1. 组网需求

如 图 1-10 所示，两台具有双协议栈的路由器Router A和Router B通过IPv4 网络连接。网络管理员希望建立IPv4 兼容IPv6 自动隧道，使得这两台设备能够通过IPv6 协议互通。

2. 组网图

图1-10 IPv4 兼容 IPv6 自动隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv4 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 192.168.100.1 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

创建模式为 IPv4 兼容 IPv6 自动隧道的接口 Tunnel0。

```
[RouterA] interface tunnel 0 mode ipv6-ipv4 auto-tunnel
```

配置 Tunnel0 接口的 IPv6 地址为 IPv4 兼容 IPv6 地址::192.168.100.1/96。

```
[RouterA-Tunnel0] ipv6 address ::192.168.100.1/96
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/1。

```
[RouterA-Tunnel0] source gigabitethernet 2/1/1
```

(2) 配置 Router B

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 192.168.50.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

创建模式为 IPv4 兼容 IPv6 自动隧道的接口 Tunnel0。

```
[RouterB] interface tunnel 0 mode ipv6-ipv4 auto-tunnel
```

配置 Tunnel0 接口的 IPv6 地址为 IPv4 兼容 IPv6 地址::192.168.50.1/96。

```
[RouterB-Tunnel0] ipv6 address ::192.168.50.1/96
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/1。

```
[RouterB-Tunnel0] source gigabitethernet 2/1/1
```

4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display ipv6 interface** 命令，可以看出 Tunnel0 接口处于 up 状态。（具体显示信息略）

从 Router A 和 Router B 上可以 Ping 通对端的 IPv4 兼容 IPv6 地址。下面仅以 Router A 为例。

```
[RouterA-Tunnel0] ping ipv6 ::192.168.50.1
Ping6(56 data bytes) ::192.168.100.1 --> ::192.168.50.1, press CTRL_C to break
56 bytes from ::192.168.50.1, icmp_seq=0 hlim=64 time=17.000 ms
56 bytes from ::192.168.50.1, icmp_seq=1 hlim=64 time=9.000 ms
56 bytes from ::192.168.50.1, icmp_seq=2 hlim=64 time=11.000 ms
56 bytes from ::192.168.50.1, icmp_seq=3 hlim=64 time=9.000 ms
56 bytes from ::192.168.50.1, icmp_seq=4 hlim=64 time=11.000 ms

--- Ping6 statistics for ::192.168.50.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 9.000/11.400/17.000/2.939 ms
```

1.6 配置6to4隧道

1.6.1 配置步骤

配置 6to4 隧道时，需要注意：

- 6to4 隧道不需要配置隧道的目的端地址，因为隧道的目的端地址可以通过 6to4 IPv6 地址中嵌入的 IPv4 地址自动获得。
- 对于自动隧道，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址。
- 如果封装前 IPv6 报文的目的 IPv6 地址与 Tunnel 接口的 IPv6 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。对于自动隧道，用户只能配置静态路由，指定到达目的 IPv6 地址的路由出接口为本端 Tunnel

接口或下一跳为对端 Tunnel 接口地址，不支持动态路由。在隧道的两端都要进行转发路由的配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 静态路由”。

表1-6 配置 6to4 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为6to4隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6-ipv4 6to4**]	-
设置Tunnel接口的IPv6地址	详细配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上不存在IPv6地址
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IP地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IP地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
退回系统视图	**quit**	-
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

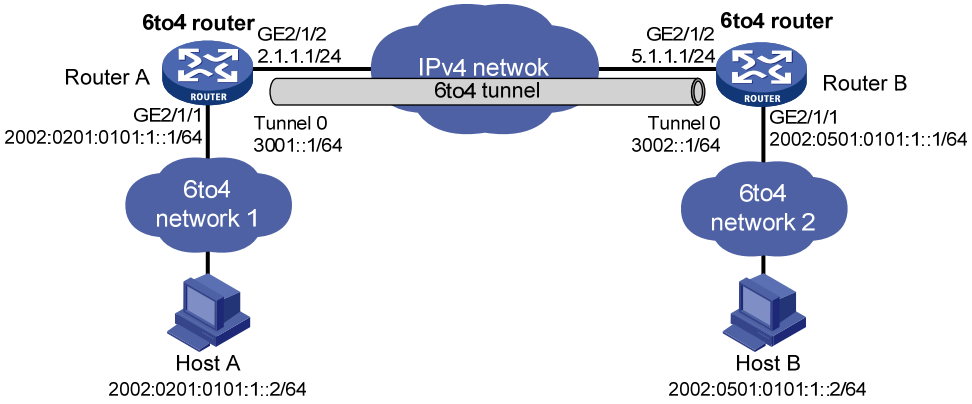
1.6.2 配置 6to4 隧道举例

1. 组网需求

如 图 1-11 所示，两个 6to4 网络通过网络边缘 6to4 router（Router A和Router B）与IPv4 网络相连。在Router A和Router B之间建立 6to4 隧道，实现 6to4 网络中的主机Host A和Host B之间的互通。

2. 组网图

图1-11 6to4 隧道组网图



3. 配置思路

为了实现 6to4 网络之间的互通，除了配置 6to4 隧道外，还需要为 6to4 网络内的主机及 6to4 router 配置 6to4 地址。

- Router A 上接口 GigabitEthernet2/1/2 的 IPv4 地址为 2.1.1.1/24，转换成 6to4 地址后的前缀为 2002:0201:0101::/48，Host A 的地址必须使用该前缀。
- Router B 上接口 GigabitEthernet2/1/2 的 IPv4 地址为 5.1.1.1/24，转换成 6to4 地址后的前缀为 2002:0501:0101::/48，Host B 的地址必须使用该前缀。

4. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv4 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/2 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 2.1.1.1 24
[RouterA-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的地址为 6to4 地址 2002:0201:0101:1::1/64。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 2002:0201:0101:1::1/64
[RouterA-GigabitEthernet2/1/1] quit
```

创建模式为 6to4 隧道的接口 Tunnel0。

```
[RouterA] interface tunnel 0 mode ipv6-ipv4 6to4
```

配置 Tunnel0 接口的 IPv6 地址。

```
[RouterA-Tunnel0] ipv6 address 3001::1/64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterA-Tunnel0] source gigabitethernet 2/1/2
```

```
[RouterA-Tunnel0] quit
```
配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。
```
[RouterA] ipv6 route-static 2002:: 16 tunnel 0
```
(2)　配置 Router B

配置接口 GigabitEthernet2/1/2 的地址。
```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 5.1.1.1 24
[RouterB-GigabitEthernet2/1/2] quit
```
配置接口 GigabitEthernet2/1/1 的地址为 6to4 地址 2002:0501:0101:1::1/64。
```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 2002:0501:0101:1::1/64
[RouterB-GigabitEthernet2/1/1] quit
```
创建模式为 6to4 隧道的接口 Tunnel0。
```
[RouterB] interface tunnel 0 mode ipv6-ipv4 6to4
```
配置 Tunnel0 接口的 IPv6 地址。
```
[RouterB-Tunnel0] ipv6 address 3002::1/64
```
配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。
```
[RouterB-Tunnel0] source gigabitethernet 2/1/2
[RouterB-Tunnel0] quit
```
配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。
```
[RouterB] ipv6 route-static 2002:: 16 tunnel 0
```
5. 验证配置

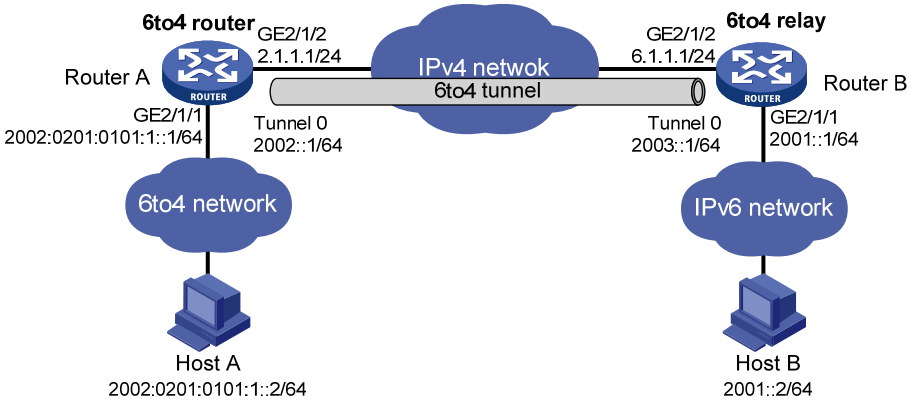
完成以上配置之后，Host A 与 Host B 可以互相 Ping 通。
```
D:\>ping6 -s 2002:201:101:1::2 2002:501:101:1::2

Pinging 2002:501:101:1::2
from 2002:201:101:1::2 with 32 bytes of data:

Reply from 2002:501:101:1::2: bytes=32 time=13ms
Reply from 2002:501:101:1::2: bytes=32 time=1ms
Reply from 2002:501:101:1::2: bytes=32 time=1ms
Reply from 2002:501:101:1::2: bytes=32 time<1ms

Ping statistics for 2002:501:101:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```
1.6.3 配置 6to4 中继举例

1. 组网需求

如 图 1-12 所示，Router A为 6to4 路由器，其IPv6 侧的网络使用 6to4 地址。Router B作为 6to4 中继路由器，它和IPv6 网络（2001::/16）相连。要求在Router A和Router B之间配置 6to4 隧道，使得 6to4 网络中的主机与IPv6 网络中的主机互通。

2. 组网图

图1-12 6to4 中继组网图



3. 配置思路

6to4 中继路由器的配置与 6to4 路由器的配置相同，但为实现 6to4 网络与 IPv6 网络的互通，需要在 6to4 路由器上配置到 IPv6 网络的路由，下一跳指向 6to4 中继路由器的 6to4 地址。6to4 中继路由器上接口 GigabitEthernet2/1/2 的 IPv4 地址为 6.1.1.1/24，转换成 6to4 地址后的前缀为 2002:0601:0101::/48，6to4 路由器上配置的到 IPv6 网络的路由下一跳可以是符合该前缀的任意一个地址。

4. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv4 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/2 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 2.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的地址为 6to4 地址 2002:0201:0101:1::1/64。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 2002:0201:0101:1::1/64
[RouterA-GigabitEthernet2/1/1] quit
```

创建模式为 6to4 隧道的接口 Tunnel0。

```
[RouterA] interface tunnel 0 mode ipv6-ipv4 6to4
```

配置 Tunnel0 接口的 IPv6 地址。

```
[RouterA-Tunnel0] ipv6 address 2002::1/64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterA-Tunnel0] source gigabitethernet 2/1/2
[RouterA-Tunnel0] quit
```

配置到 6to4 中继的静态路由。

```
[RouterA] ipv6 route-static 2002:0601:0101:: 64 tunnel 0
```

配置到纯 IPv6 网络的缺省路由，指定路由的下一跳地址为 6to4 中继路由器的 6to4 地址。

```
[RouterA] ipv6 route-static :: 0 2002:0601:0101::1
```

(2)　配置 Router B

配置接口 GigabitEthernet2/1/2 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 6.1.1.1 255.255.255.0
[RouterB-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的地址。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 2001::1/16
[RouterB-GigabitEthernet2/1/1] quit
```

创建模式为 6to4 隧道的接口 Tunnel0。

```
[RouterB] interface tunnel 0 mode ipv6-ipv4 6to4
```

配置 Tunnel0 接口的 IPv6 地址。

```
[RouterB-Tunnel0] ipv6 address 2003::1/64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterB-Tunnel0] source gigabitethernet 2/1/2
[RouterB-Tunnel0] quit
```

配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。

```
[RouterB] ipv6 route-static 2002:: 16 tunnel 0
```

5. 验证配置

完成以上配置之后，Host A 与 Host B 可以互相 Ping 通。

```
D:\>ping6 -s 2002:201:101:1::2 2001::2

Pinging 2001::2
from 2002:201:101:1::2 with 32 bytes of data:

Reply from 2001::2: bytes=32 time=13ms
Reply from 2001::2: bytes=32 time=1ms
Reply from 2001::2: bytes=32 time=1ms
Reply from 2001::2: bytes=32 time<1ms

Ping statistics for 2001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

1.7 配置ISATAP隧道

1.7.1 配置步骤

配置 ISATAP 隧道时，需要注意：

- ISATAP 隧道不需要配置隧道的目的端地址，因为隧道的目的端地址可以通过 ISATAP 地址中嵌入的 IPv4 地址自动获得。
- 对于自动隧道，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址。
- 如果封装前 IPv6 报文的目的 IPv6 地址与 Tunnel 接口的 IPv6 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。对于自动隧道，用户只能配置静态路由，指定到达目的 IPv6 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址，不支持动态路由。在隧道的两端都要进行转发路由的配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 静态路由”。

表1-7 配置 ISATAP 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为ISATAP隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6-ipv4 isatap**]	-
设置Tunnel接口的IPv6地址	详细配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上不存在IPv6地址
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IP地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IP地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
退回系统视图	**quit**	-
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

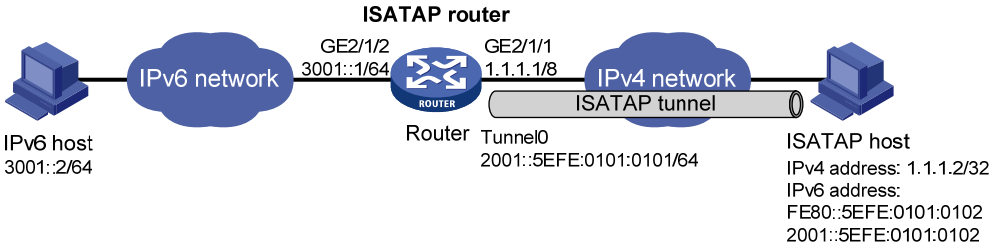
1.7.2 配置举例

1. 组网需求

如 图 1-13 所示，IPv6 网络和IPv4 网络通过ISATAP路由器相连，在IPv4 网络侧分布着一些IPv6 主机。要求将IPv4 网络中的IPv6 主机通过ISATAP隧道接入到IPv6 网络。

2. 组网图

图1-13 ISATAP 隧道组网图



3. 配置步骤

(1) 配置 Router

配置接口 GigabitEthernet2/1/2 的地址。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ipv6 address 3001::1/64
[Router-GigabitEthernet2/1/2] quit
```

配置接口 GigabitEthernet2/1/1 的地址。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 1.1.1.1 255.0.0.0
[Router-GigabitEthernet2/1/1] quit
```

创建模式为 ISATAP 隧道的接口 Tunnel0。

```
[Router] interface tunnel 0 mode ipv6-ipv4 isatap
```

配置 Tunnel0 接口采用 EUI-64 格式形成 IPv6 地址。

```
[Router-Tunnel0] ipv6 address 2001:: 64 eui-64
```

配置 Tunnel0 接口的源接口为 GigabitEthernet2/1/1。

```
[Router-Tunnel0] source gigabitethernet 2/1/1
```

取消对 RA 消息发布的抑制，使主机可以通过路由器发布的 RA 消息获取地址前缀等信息。

```
[Router-Tunnel0] undo ipv6 nd ra halt
[Router-Tunnel0] quit
```

(2) 配置 ISATAP 主机

ISATAP 主机上的具体配置与主机的操作系统有关，下面仅以 Windows XP 操作系统为例进行说明。

在主机上安装 IPv6 协议。

```
C:\>ipv6 install
```

在 Windows XP 上，ISATAP 接口通常为接口 2，查看这个 ISATAP 接口的信息。

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 0.0.0.0
  router link-layer address: 0.0.0.0
```

```
    preferred link-local fe80::5efe:1.1.1.2, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

配置 ISATAP 路由器的 IPv4 地址。

```
C:\>netsh interface ipv6 isatap set router 1.1.1.1
```

完成上述配置后，再来查看 ISATAP 接口的信息。

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  uses Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 1.1.1.2
  router link-layer address: 1.1.1.1
    preferred global 2001::5efe:1.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:1.1.1.2, life infinite
  link MTU 1500 (true link MTU 65515)
  current hop limit 255
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

对比前后的接口信息，我们可以看到主机获取了 2001::/64 的前缀，自动生成全球单播地址 2001::5efe:1.1.1.2，同时还有一行信息“uses Router Discovery”表明主机启用了路由器发现。

查看主机上的 IPv6 路由信息。

```
C:\>ipv6 rt
2001::/64 -> 2 pref 1if+8=9 life 29d23h59m43s (autoconf)
::/0 -> 2/fe80::5efe:1.1.1.1 pref 1if+256=257 life 29m43s (autoconf)
```

(3) 配置 IPv6 主机

配置一条到边界路由器隧道的路由。

```
C:\>netsh interface ipv6 set route 2001::/64 5 3001::1
```

4. 验证配置

在 ISATAP 主机上 Ping IPv6 主机的地址，可以 Ping 通，表明 ISATAP 隧道已经成功建立，ISATAP 主机可访问 IPv6 网络中的主机。

```
C:\>ping 3001::2

Pinging 3001::2 with 32 bytes of data:

Reply from 3001::2: time=1ms
Reply from 3001::2: time=1ms
Reply from 3001::2: time=1ms
Reply from 3001::2: time=1ms
```

```
Ping statistics for 3001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

1.8 配置IPv4 over IPv4隧道

1.8.1 配置步骤

配置 IPv4 over IPv4 隧道时，需要注意：

- 在本端设备上为隧道指定的目的端地址，应该与在对端设备上为隧道指定的源端地址相同；在本端设备上为隧道指定的源端地址，应该与在对端设备上为隧道指定的目的端地址相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 本端隧道接口的 IPv4 地址与隧道的目的端地址不能在同一个网段内。
- 如果封装前 IPv4 报文的目的 IPv4 地址与 Tunnel 接口的 IPv4 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv4 地址的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达目的 IPv4 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址。用户也可以配置动态路由，在 Tunnel 接口使能动态路由协议。在隧道的两端都要进行转发路由的配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“静态路由”或其他路由协议配置。
- 配置经过隧道接口的路由时，路由的目的地址不能与该隧道的目的端地址在同一个网段内。

表1-8 配置 IPv4 over IPv4 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为IPv4 over IPv4隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv4-ipv4**]	-
设置Tunnel接口的IPv4地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，Tunnel接口上不存在IPv4地址
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IP地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IP地址
设置隧道的目的端地址	**destination** *ip-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端接收报文的接口的地址，该地址将作为封装后隧道报文的目的地址

操作	命令	说明
（可选）设置封装后隧道报文的DF（Don't Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片

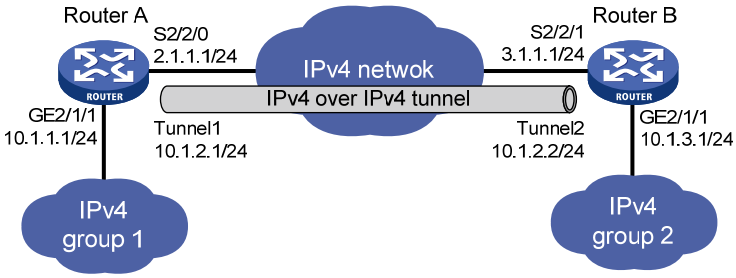
1.8.2 配置举例

1. 组网需求

运行 IP 协议的两个子网 Group 1 和 Group 2 位于不同的区域，这两个子网都使用私网地址。通过在路由器 Router A 和路由器 Router B 之间建立 IPv4 over IPv4 隧道，实现两个子网的互联。

2. 组网图

图1-14 IPv4 over IPv4 隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv4 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

配置接口 Serial2/2/0（隧道的实际物理接口）的地址。

```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ip address 2.1.1.1 255.255.255.0
[RouterA-Serial2/2/0] quit
```

创建模式为 IPv4 over IPv4 隧道的接口 Tunnel1。

```
[RouterA] interface tunnel 1 mode ipv4-ipv4
```

配置 Tunnel1 接口的 IP 地址。

```
[RouterA-Tunnel1] ip address 10.1.2.1 255.255.255.0
```

配置 Tunnel1 接口的源端地址（Serial2/2/0 的 IP 地址）。

```
[RouterA-Tunnel1] source 2.1.1.1
```
配置 Tunnel1 接口的目的端地址（RouterB 的 Serial2/2/1 的 IP 地址）。
```
[RouterA-Tunnel1] destination 3.1.1.1
[RouterA-Tunnel1] quit
```
配置从 Router A 经过 Tunnel1 接口到 Group 2 的静态路由。
```
[RouterA] ip route-static 10.1.3.0 255.255.255.0 tunnel 1
```
(2)　配置 Router B

配置接口 GigabitEthernet2/1/1 的地址。
```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 10.1.3.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```
配置接口 Serial2/2/1（隧道的实际物理接口）的地址。
```
[RouterB] interface serial 2/2/1
[RouterB-Serial2/2/1] ip address 3.1.1.1 255.255.255.0
[RouterB-Serial2/2/1] quit
```
创建模式为 IPv4 over IPv4 隧道的接口 Tunnel2。
```
[RouterB] interface tunnel 2 mode ipv4-ipv4
```
配置 Tunnel2 接口的 IP 地址。
```
[RouterB-Tunnel2] ip address 10.1.2.2 255.255.255.0
```
配置 Tunnel2 接口的源端地址（Serial2/2/1 的 IP 地址）。
```
[RouterB-Tunnel2] source 3.1.1.1
```
配置 Tunnel2 接口的目的端地址（Router A 的 Serial2/2/0 的 IP 地址）。
```
[RouterB-Tunnel2] destination 2.1.1.1
[RouterB-Tunnel2] quit
```
配置从 Router B 经过 Tunnel2 接口到 Group 1 的静态路由。
```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 tunnel 2
```
4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display interface tunnel** 命令，可以看出 Tunnel 接口处于 up 状态。（具体显示信息略）

从 Router A 和 Router B 上可以 Ping 通对端的 GigabitEthernet2/1/1 接口的 IPv4 地址。下面仅以 Router A 为例。
```
[RouterA] ping -a 10.1.1.1 10.1.3.1
Ping 10.1.3.1 (10.1.3.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.3.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 10.1.3.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.3.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.3.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.3.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 10.1.3.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/2.000/0.632 ms
```

1.9 配置IPv4 over IPv6手动隧道

1.9.1 配置步骤

配置 IPv4 over IPv6 手动隧道时，需要注意：

- 在本端设备上为隧道指定的目的端地址，应该与在对端设备上为隧道指定的源端地址相同；在本端设备上为隧道指定的源端地址，应该与在对端设备上为隧道指定的目的端地址相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 如果封装前 IPv4 报文的目的 IPv4 地址与 Tunnel 接口的 IPv4 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv4 地址的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达目的 IPv4 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址。用户也可以配置动态路由，在 Tunnel 接口使能动态路由协议。在隧道的两端都要进行转发路由的配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“静态路由”或其他路由协议配置。

表1-9 配置 IPv4 over IPv6 手动隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为IPv6隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6**]	-
设置Tunnel接口的IPv4地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，Tunnel接口上不存在IPv4地址
设置隧道的源端地址或源接口	**source** { *ipv6-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IPv6地址；如果设置的是隧道的源接口，则该接口的地址将作为封装后隧道报文的源IPv6地址
设置隧道的目的端地址	**destination** *ipv6-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端接收报文的接口的地址，该地址将作为封装后隧道报文的目的IPv6地址

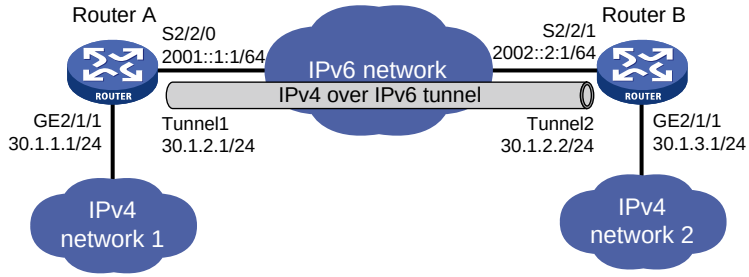
1.9.2 配置举例

1. 组网需求

两个 IPv4 网络分别通过 Router A 和 Router B 与 IPv6 网络连接。通过在 Router A 和 Router B 之间建立 IPv4 over IPv6 手动隧道，实现两个 IPv4 网络穿越 IPv6 网络互联。

2. 组网图

图1-15 IPv4 over IPv6 手动隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv6 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 30.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

配置接口 Serial2/2/0（隧道的实际物理接口）的地址。

```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ipv6 address 2001::1:1 64
[RouterA-Serial2/2/0] quit
```

创建模式为 IPv6 隧道的接口 Tunnel1。

```
[RouterA] interface tunnel 1 mode ipv6
```

配置 Tunnel1 接口的 IP 地址。

```
[RouterA-Tunnel1] ip address 30.1.2.1 255.255.255.0
```

配置 Tunnel1 接口的源端地址（Serial2/2/0 的 IP 地址）。

```
[RouterA-Tunnel1] source 2001::1:1
```

配置 Tunnel1 接口的目的端地址（Router B 的 Serial2/2/1 的 IP 地址）。

```
[RouterA-Tunnel1] destination 2002::2:1
[RouterA-Tunnel1] quit
```

配置从 Router A 经过 Tunnel1 接口到 IPv4 network 2 的静态路由。

```
[RouterA] ip route-static 30.1.3.0 255.255.255.0 tunnel 1
```

(2) 配置 Router B

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 30.1.3.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

配置接口 Serial2/2/1（隧道的实际物理接口）的地址。

```
[RouterB] interface serial 2/2/1
[RouterB-Serial2/2/1] ipv6 address 2002::2:1 64
[RouterB-Serial2/2/1] quit
```

创建模式为 IPv6 隧道的接口 Tunnel2。

```
[RouterB] interface tunnel 2 mode ipv6
```

配置 Tunnel2 接口的 IP 地址。

```
[RouterB-Tunnel2] ip address 30.1.2.2 255.255.255.0
```

配置 Tunnel2 接口的源端地址（Serial2/2/1 的 IP 地址）。

```
[RouterB-Tunnel2] source 2002::2:1
```

配置 Tunnel2 接口的目的端地址（Router A 的 Serial2/2/0 的 IP 地址）。

```
[RouterB-Tunnel2] destination 2001::1:1
[RouterB-Tunnel2] quit
```

配置从 Router B 经过 Tunnel2 接口到 IPv4 network 1 的静态路由。

```
[RouterB] ip route-static 30.1.1.0 255.255.255.0 tunnel 2
```

4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display interface tunnel** 命令，可以看出 Tunnel 接口处于 up 状态。（具体显示信息略）

从 Router A 和 Router B 可以 Ping 通对端的 GigabitEthernet2/1/1 接口的 IPv4 地址。下面仅以 Router A 为例。

```
[RouterA] ping -a 30.1.1.1 30.1.3.1
Ping 30.1.3.1 (30.1.3.1) from 30.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 30.1.3.1: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 30.1.3.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 30.1.3.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 30.1.3.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 30.1.3.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 30.1.3.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.200/3.000/0.980 ms
```

1.10 配置DS-Lite隧道

1.10.1 配置步骤

配置 DS-Lite 隧道时，需要注意：

- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址。
- 在 B4 设备上为隧道指定的目的端地址，应该与在 AFTR 设备上为隧道指定的源端地址相同。
- 在 AFTR 端不能配置 DS-Lite 隧道的目的端地址。AFTR 从隧道上接收到报文后，记录该报文的源 IPv6 地址（即 B4 设备的地址），将此地址作为隧道目的端的 IPv6 地址。
- B4 设备上的一个 Tunnel 接口只能和一个 AFTR 建立隧道连接；AFTR 上的一个 Tunnel 接口可以和多个 B4 设备建立隧道连接。

- 在 B4 端，如果封装前 IPv4 报文的目的 IPv4 地址与 Tunnel 接口的 IPv4 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv4 地址的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达目的 IPv4 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址。用户也可以配置动态路由，在 Tunnel 接口使能动态路由协议。配置的详细情况请参见“三层技术-IP 路由配置指导”中的“静态路由”或其他路由协议配置。
- 在 AFTR 端，不需要配置通过 Tunnel 接口到达目的 IPv4 地址的转发路由。
- AFTR 连接 IPv4 公网的接口上需要配置 NAT。

建立 DS-Lite 隧道时，需要进行以下配置：

- 在B4 端配置IPv4 over IPv6 手动隧道，并指定隧道目的端地址为AFTR的源端地址。配置方法请参见“1.9 配置IPv4 over IPv6 手动隧道”。
- 在AFTR端配置DS-Lite隧道，并在AFTR连接IPv4 公网的接口上使能DS-Lite隧道功能。配置方法请参见 表 1-10。

表1-10 配置 DS-Lite 隧道的 AFTR 端

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为AFTR端DS-Lite隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ds-lite-aftr**]	-
设置Tunnel接口的IPv4地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，Tunnel接口上不存在IPv4地址
设置隧道的源端地址或源接口	**source** { *ipv6-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IPv6地址；如果设置的是隧道的源接口，则该接口的地址将作为封装后隧道报文的源IPv6地址
退回系统视图	**quit**	-
进入AFTR连接IPv4公网的接口视图	**interface** *interface-type interface-number*	-
使能接口的DS-Lite隧道功能	**ds-lite enable**	缺省情况下，接口的DS-Lite隧道功能处于关闭状态 只有使能该功能后，AFTR从IPv4公网接口接收到的IPv4报文才能够通过DS-Lite隧道正确地转发到B4设备

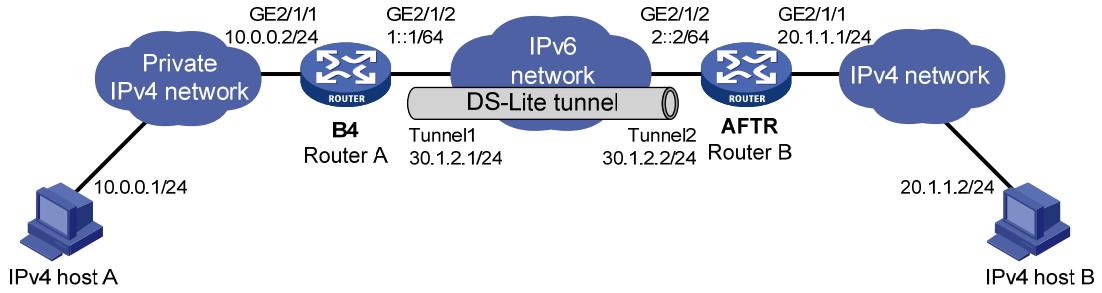
1.10.2 配置举例

1. 组网需求

运行 IPv4 协议的私网 Private IPv4 network 和公网 IPv4 network 通过 IPv6 网络相连。通过在 B4 设备（Router A）和 AFTR（Router B）之间建立 DS-Lite 隧道，并在 AFTR 连接 IPv4 network 接口上配置 NAT，实现 IPv4 私网主机穿越 IPv6 网络访问 IPv4 公网。

2. 组网图

图1-16 DS-Lite 隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv6 报文路由可达。

(1) 配置 B4 设备 Router A

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.0.0.2 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2（隧道的实际物理接口）的地址。

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 address 1::1 64
[RouterA-GigabitEthernet2/1/2] quit
```

创建模式为 IPv6 隧道的接口 Tunnel1。

```
[RouterA] interface tunnel 1 mode ipv6
```

配置 Tunnel1 接口的 IP 地址。

```
[RouterA-Tunnel1] ip address 30.1.2.1 255.255.255.0
```

配置 Tunnel1 接口的源端地址（GigabitEthernet2/1/2 的地址）。

```
[RouterA-Tunnel1] source 1::1
```

配置 Tunnel1 接口的目的端地址（Router B 的 GigabitEthernet2/1/2 的地址）。

```
[RouterA-Tunnel1] destination 2::2
[RouterA-Tunnel1] quit
```

配置从 Router A 经过 Tunnel1 接口到公网 IPv4 network 的静态路由。

```
[RouterA] ip route-static 20.1.1.0 255.255.255.0 tunnel 1
```

(2) 配置 AFTR 端 Router B

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 20.1.1.1 24
```

```
[RouterB-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2（隧道的实际物理接口）的地址。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 address 2::2 64
[RouterB-GigabitEthernet2/1/2] quit
```

创建模式为 AFTR 端 DS-Lite 隧道的接口 Tunnel2。

```
[RouterB] interface tunnel 2 mode ds-lite-aftr
```

配置 Tunnel2 接口的 IP 地址。

```
[RouterB-Tunnel2] ip address 30.1.2.2 255.255.255.0
```

配置 Tunnel2 接口的源接口为 GigabitEthernet2/1/2。

```
[RouterB-Tunnel2] source gigabitethernet 2/1/2
[RouterB-Tunnel2] quit
```

在接口 GigabitEthernet2/1/1 上使能 DS-Lite 隧道功能。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ds-lite enable
```

在接口 GigabitEthernet2/1/1 上配置 NAT，使用接口 GigabitEthernet2/1/1 的 IP 地址作为转换后的 IP 地址。

```
[RouterB-GigabitEthernet2/1/1] nat outbound
[RouterB-GigabitEthernet2/1/1] quit
```

(3) 配置 IPv4 host A

配置 IPv4 host A 的地址为 10.0.0.1，并在该主机上配置到达 20.1.1.0/24 网段的路由，路由下一跳为 10.0.0.2。（具体配置过程略）

(4) 配置 IPv4 host B

配置 IPv4 host B 的地址为 20.1.1.2。（具体配置过程略）

4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display interface tunnel** 命令，可以看出 Tunnel 接口处于 up 状态。（具体显示信息略）

从 IPv4 host A 上可以 ping 通 IPv4 host B。

```
C:\> ping 20.1.1.2
Pinging 20.1.1.2 with 32 bytes of data:
Reply from 20.1.1.2: bytes=32 time=51ms TTL=255
Reply from 20.1.1.2: bytes=32 time=44ms TTL=255
Reply from 20.1.1.2: bytes=32 time=1ms TTL=255
Reply from 20.1.1.2: bytes=32 time=1ms TTL=255
Ping statistics for 20.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 51ms, Average = 24ms
```

1.11 配置IPv6 over IPv6隧道

1.11.1 配置步骤

配置 IPv6 over IPv6 隧道时，需要注意：

- 在本端设备上为隧道指定的目的端地址，应该与在对端设备上为隧道指定的源端地址相同；在本端设备上为隧道指定的源端地址，应该与在对端设备上为隧道指定的目的端地址相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 本端隧道接口的 IPv6 地址与隧道的目的端地址不能在同一个网段内。
- 如果封装前 IPv6 报文的目的 IPv6 地址与 Tunnel 接口的 IPv6 地址不在同一个网段，则必须配置通过 Tunnel 接口到达目的 IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达目的 IPv6 地址的路由出接口为本端 Tunnel 接口或下一跳为对端 Tunnel 接口地址。用户也可以配置动态路由，在 Tunnel 接口使能动态路由协议。在隧道的两端都要进行转发路由的配置，配置的详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 静态路由”或其他路由协议配置。
- 配置经过隧道接口的路由时，路由的目的地址不能与该隧道的目的端地址在同一个网段内。

表1-11 配置 IPv6 over IPv6 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为IPv6隧道的Tunnel接口视图	**interface tunnel** *number* [**mode ipv6**]	-
设置Tunnel接口的IPv6地址	详细配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上不存在IPv6地址
设置隧道的源端地址或源接口	**source** { *ipv6-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IPv6地址；如果设置的是隧道的源接口，则该接口的地址将作为封装后隧道报文的源IPv6地址
设置隧道的目的端地址	**destination** *ipv6-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端接收报文的接口的地址，该地址将作为封装后隧道报文的目的IPv6地址
（可选）设置隧道允许的最大嵌套封装次数	**encapsulation-limit** *number*	缺省情况下，不限制隧道的最大嵌套封装次数
退回系统视图	**quit**	-
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

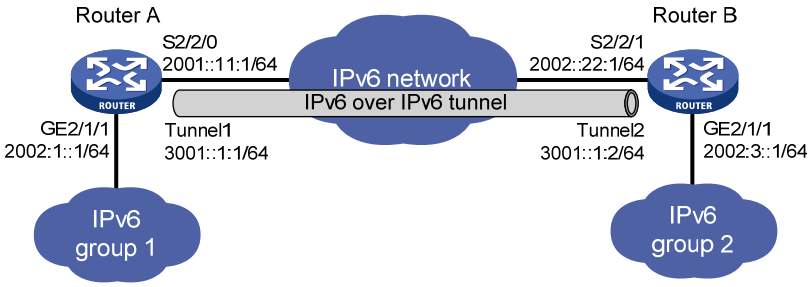
1.11.2 配置举例

1. 组网需求

运行 IPv6 协议的两个子网 Group 1 和 Group 2 的网络地址不希望泄露到 IPv6 网络中。网络管理员通过在路由器 Router A 和路由器 Router B 之间建立 IPv6 over IPv6 隧道，实现在 Group 1 和 Group 2 的网络地址不被泄露的情况下，确保 Group 1 和 Group 2 互通。

2. 组网图

图1-17 IPv6 over IPv6 隧道组网图



3. 配置步骤

说明

在开始下面的配置之前，请确保 Router A 和 Router B 之间 IPv6 报文路由可达。

(1) 配置 Router A

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 address 2002:1::1 64
[RouterA-GigabitEthernet2/1/1] quit
```

配置接口 Serial2/2/0（隧道的实际物理接口）的地址。

```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ipv6 address 2001::11:1 64
[RouterA-Serial2/2/0] quit
```

创建模式为 IPv6 隧道的接口 Tunnel1。

```
[RouterA] interface tunnel 1 mode ipv6
```

配置 Tunnel1 接口的 IP 地址。

```
[RouterA-Tunnel1] ipv6 address 3001::1:1 64
```

配置 Tunnel1 接口的源端地址（Serial2/2/0 的 IP 地址）。

```
[RouterA-Tunnel1] source 2001::11:1
```

配置 Tunnel1 接口的目的端地址（Router B 的 Serial2/2/1 的 IP 地址）。

```
[RouterA-Tunnel1] destination 2002::22:1
[RouterA-Tunnel1] quit
```

配置从 Router A 经过 Tunnel1 接口到 Group 2 的静态路由。

```
[RouterA] ipv6 route-static 2002:3:: 64 tunnel 1
```

(2) 配置 Router B

配置接口 GigabitEthernet2/1/1 的地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 2002:3::1 64
[RouterB-GigabitEthernet2/1/1] quit
```

配置接口 Serial2/2/1（隧道的实际物理接口）的地址。

```
[RouterB] interface serial 2/2/1
[RouterB-Serial2/2/1] ipv6 address 2002::22:1 64
[RouterB-Serial2/2/1] quit
```

创建模式为 IPv6 隧道的接口 Tunnel2。

```
[RouterB] interface tunnel 2 mode ipv6
```

配置 Tunnel2 接口的 IP 地址。

```
[RouterB-Tunnel2] ipv6 address 3001::1:2 64
```

配置 Tunnel2 接口的源端地址（Serial2/2/1 的 IP 地址）。

```
[RouterB-Tunnel2] source 2002::22:1
```

配置 Tunnel2 接口的目的端地址（Router A 的 Serial2/2/0 的 IP 地址）。

```
[RouterB-Tunnel2] destination 2001::11:1
[RouterB-Tunnel2] quit
```

配置从 Router B 经过 Tunnel2 接口到 Group 1 的静态路由。

```
[RouterB] ipv6 route-static 2002:1:: 64 tunnel 2
```

4. 验证配置

完成上述配置后，在 Router A 和 Router B 上分别执行 **display ipv6 interface** 命令，可以看出 Tunnel 接口处于 up 状态。（具体显示信息略）

从 Router A 和 Router B 上可以 Ping 通对端的 GigabitEthernet2/1/1 接口的 IPv6 地址。下面仅以 Router A 为例。

```
[RouterA] ping ipv6 -a 2002:1::1 2002:3::1
Ping6(56 data bytes) 2002:1::1 --> 2002:3::1, press CTRL_C to break
56 bytes from 2002:3::1, icmp_seq=0 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=3 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 2002:3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms
```

1.12 隧道显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示隧道配置后的运行情况，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 Tunnel 接口的统计信息。

表1-12 隧道显示和维护

操作	命令
显示Tunnel接口的相关信息	**display interface** [**tunnel** [*number*]] [**brief** [**description** | **down**]]
显示Tunnel接口的IPv6相关信息	**display ipv6 interface** [**tunnel** [*number*]] [**brief**]
清除Tunnel接口的统计信息	**reset counters interface** [**tunnel** [*number*]]

说明

display ipv6 interface 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”。

1.13 常见错误配置举例

1.13.1 故障现象

在 Tunnel 接口上配置了相关的参数后（例如隧道的源端地址、目的端地址和隧道模式），Tunnel 接口仍未处于 up 状态。

1.13.2 故障分析

Tunnel 接口未处于 up 状态的原因可能是隧道起点的物理接口没有处于 up 状态，或隧道的目的端地址不可达。

1.13.3 处理过程

(1) 使用 **display interface** 和 **display ipv6 interface** 命令查看隧道起点的物理接口状态为 up 还是 down。如果物理接口状态是 down 的，请检查网络连接。

(2) 使用 **display ipv6 routing-table** 和 **display ip routing-table** 命令查看是否目的端地址通过路由可达。如果路由表中没有保证隧道通讯的路由表项，请配置相关路由。

目 录

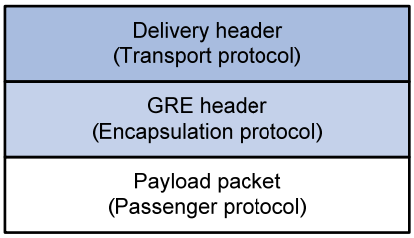
1 GRE

1.1 GRE简介

GRE（Generic Routing Encapsulation，通用路由封装）协议用来对任意一种网络层协议（如 IPv6）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络（如 IPv4）中传输。封装前后数据报文的网络层协议可以相同，也可以不同。封装后的数据报文在网络中传输的路径，称为 GRE 隧道。GRE 隧道是一个虚拟的点到点的连接，其两端的设备分别对数据报文进行封装及解封装。

1.1.1 GRE封装后的报文格式

图1-1 GRE 封装后的报文格式

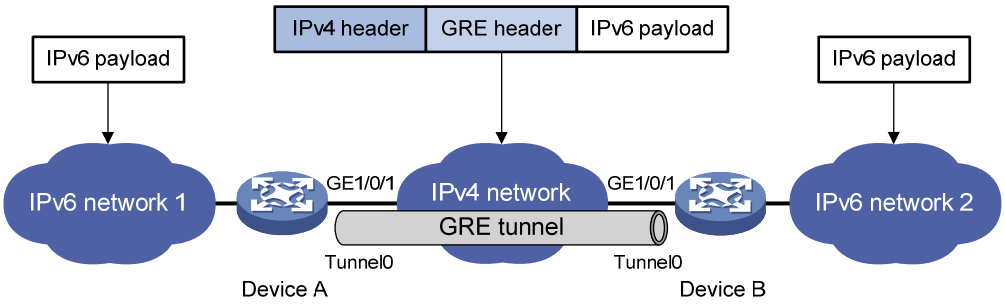


如 图 1-1 所示，GRE封装后的报文包括如下几个部分：

- 净荷数据（Payload packet）：需要封装和传输的数据报文。净荷数据的协议类型，称为乘客协议（Passenger Protocol）。乘客协议可以是任意的网络层协议。
- GRE 头（GRE header）：采用 GRE 协议对净荷数据进行封装所添加的报文头，包括封装层数、版本、乘客协议类型、校验和信息、Key 信息等内容。添加 GRE 头后的报文称为 GRE 报文。对净荷数据进行封装的 GRE 协议，称为封装协议（Encapsulation Protocol）。
- 传输协议的报文头（Delivery header）：在 GRE 报文上添加的报文头，以便传输协议对 GRE 报文进行转发处理。传输协议（Delivery Protocol 或者 Transport Protocol）是指负责转发 GRE 报文的网络层协议。设备支持 IPv4 和 IPv6 两种传输协议：当传输协议为 IPv4 时，GRE 隧道称为 GRE over IPv4 隧道；当传输协议为 IPv6 时，GRE 隧道称为 GRE over IPv6 隧道。

1.1.2 GRE隧道原理

图1-2 IPv6 协议网络通过 GRE 隧道互连



下面以 图 1-2 的网络为例说明IPv6 协议的报文通过GRE隧道穿越IPv4 网络进行传输的过程。

(1) Device A 从连接 IPv6 network 1 的接口收到 IPv6 报文后，查找路由表判定此报文需要通过 GRE 隧道模式的 Tunnel 接口（本例中为 Tunnel0）转发，并将报文发给相应的 Tunnel 接口。

(2) GRE 隧道模式的 Tunnel 接口收到此 IPv6 报文后，先在报文前封装上 GRE 头，再封装上 IPv4 头。IPv4 头中的源地址为隧道的源端地址（本例中为 Device A 的 GigabitEthernet1/0/1 接口的 IP 地址），目的地址为隧道的目的端地址（本例中为 Device B 的 GigabitEthernet1/0/1 接口的 IP 地址）。

(3) Device A 根据封装的 IPv4 头中的目的地址查找路由表，将封装后的 IPv4 报文通过 GRE 隧道的实际物理接口（GigabitEthernet1/0/1）转发出去。

(4) 封装后的 IPv4 报文通过 GRE 隧道到达隧道的目的端设备 Device B 后，由于报文的目的地是本设备，且 IPv4 头中的协议号为 47（表示封装的报文为 GRE 报文），Device B 将此报文交给 GRE 协议进行解封装处理。

(5) GRE 协议先剥离掉此报文的 IPv4 头，再对报文进行 GRE Key 验证、校验和验证、报文序列号检查等处理，处理通过后再剥离掉报文的 GRE 头，将报文交给 IPv6 协议进行后续的转发处理。

提示

GRE 收发双方的加封装、解封装处理，以及由于封装造成的数据量增加，会导致使用 GRE 后设备的数据转发效率有一定程度的下降。

1.1.3 GRE安全机制

GRE 支持 GRE Key 验证、校验和验证两种安全机制。

1. GRE Key验证

通过 GRE Key 验证可以检查报文的合法性。

发送方在发送的报文中携带其本地配置的 GRE Key。接收方收到报文后，将报文中的 GRE Key 与接收方本地配置的 GRE Key 进行比较，如果一致则对报文进行进一步处理，否则丢弃该报文。

2. GRE校验和验证

通过 GRE 校验和验证可以检查报文的完整性。

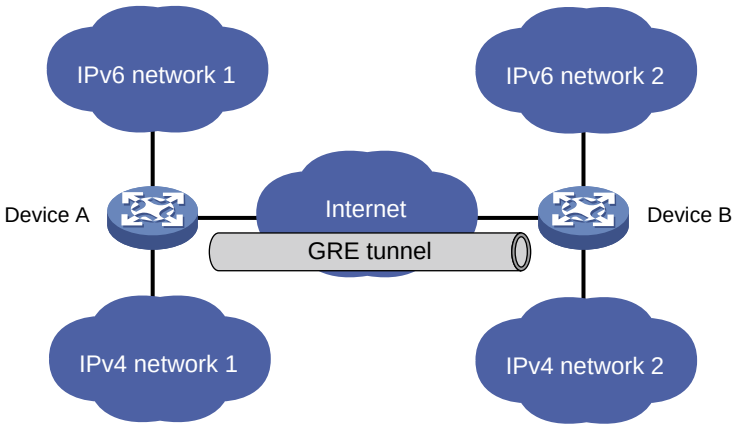
发送方根据 GRE 头及 Payload 信息计算校验和，并将包含校验和信息的报文发送给对端。接收方对接收到的报文计算校验和，并与报文中的校验和比较，如果一致则对报文进行进一步处理，否则丢弃该报文。

1.1.4 应用场景

GRE 主要有以下几种应用场景。

1. 通过单一协议的骨干网连接采用不同协议的网络

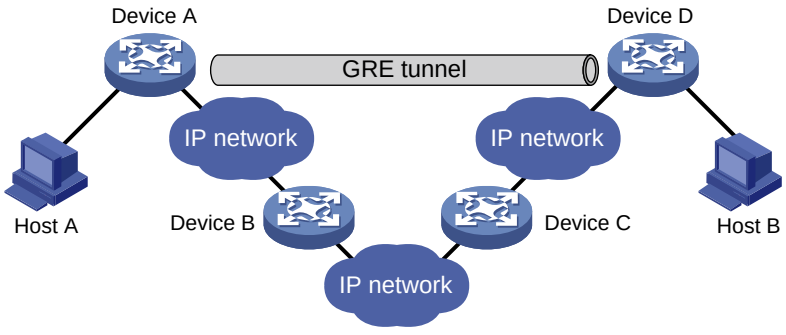
图1-3 通过单一协议的骨干网连接采用不同协议的网络



如 图 1-3 所示，IPv6 network 1 和IPv6 network 2 是运行IPv6 协议的网络，IPv4 network 1 和IPv4 network 2 是运行IPv4 协议的网络。在Device A和Device B之间建立GRE隧道，可以使IPv6 network 1 和IPv6 network 2、IPv4 network 1 和IPv4 network 2 通过骨干网互不影响地进行通信，实现两地互通。

2. 扩大网络的工作范围

图1-4 扩大网络的工作范围

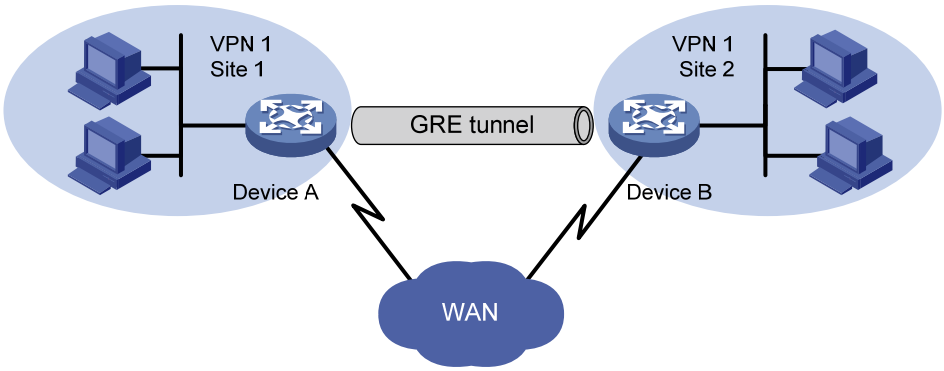


在IP网络中，报文的TTL值最大为 255。如果两台设备之间的跳数超过 255，它们将无法通信。通过在网络中使用GRE隧道可以隐藏一部分跳数，从而扩大网络的工作范围。如 图 1-4 所示，使用了

GRE隧道之后，Host A和Host B之间的跳数减少为 3 跳，GRE隧道经过的设备中只有隧道两端的设备（Device A和Device D）参与跳数计算。

3. 组建VPN

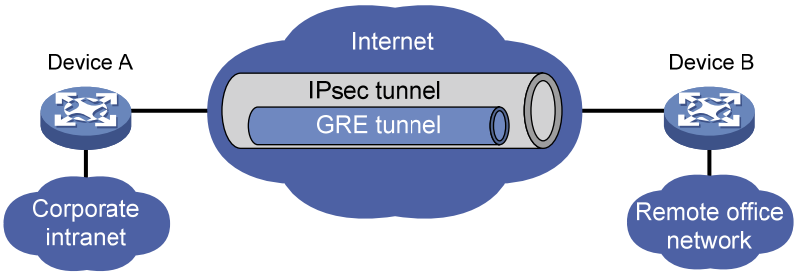
图1-5 组建 VPN



如 图 1-5 所示，属于VPN 1 的两个站点Site 1 和Site 2 分别位于不同的城市，通过使用GRE隧道可以实现跨越广域网连接VPN 1 的两个站点。

4. 与IPsec配合使用

图1-6 GRE over IPsec 隧道应用



如 图 1-6 所示，GRE可以和IPsec（IP Security，IP安全）配合使用，通过建立GRE over IPsec隧道，对路由协议、语音、视频等数据先进行GRE封装，再对封装后的报文进行IPsec处理。二者配合使用的优势如下：

- 提高数据在隧道中传输的安全性。
- 解决 IPsec 只能处理单播报文的问题。GRE 可以支持组播、广播和非 IP 报文，先对这些报文进行 GRE 封装，使其成为普通的单播报文。然后，IPsec 就可以对其进行进一步的处理。
- 简化 IPsec 的配置。由于所有报文都先经过 GRE 封装后再进行 IPsec 处理，因此只要根据 GRE 隧道的源/目的端地址来定义需要 IPsec 保护的数据流即可，不需要关注原始报文的源/目的地址，从而简化了 IPsec 的配置。

GRE 和 IPsec 还有另外一种配合方式，即 IPsec over GRE 隧道。但这种方式不能充分利用二者的优势，一般不推荐使用。

关于 IPsec 的详细介绍请参见“安全配置指导”中的“IPsec”。

1.1.5 协议规范

与 GRE 相关的协议规范有：

- RFC 1701：Generic Routing Encapsulation (GRE)
- RFC 1702：Generic Routing Encapsulation over IPv4 networks
- RFC 2784：Generic Routing Encapsulation (GRE)
- RFC 2890：Key and Sequence Number Extensions to GRE

1.2 配置GRE over IPv4隧道

配置 GRE over IPv4 隧道时，需要注意：

- 隧道两端必须都配置隧道的源端地址和目的端地址，且本端配置的源端地址（目的端地址）应该与对端配置的目的端地址（远端地址）相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 隧道两端可以根据各自的实际应用需要决定是否要开启 GRE 报文校验和功能。如果本端开启了 GRE 报文校验和功能，则会在发送的报文中携带校验和信息，由对端来对报文进行校验和验证。对端是否对收到的报文进行校验和验证，取决于报文中是否携带校验和信息，与对端的配置无关。
- 如果封装前报文的目的地址与 Tunnel 接口的地址不在同一个网段，则必须配置通过 Tunnel 接口到达报文目的地址的路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达报文目的地址的路由出接口为本端 Tunnel 接口；也可以配置动态路由，在 Tunnel 接口、与私网相连的接口上分别使能动态路由协议，由动态路由协议来建立通过 Tunnel 接口转发的路由表项。
- 在 Tunnel 接口上配置的隧道目的端地址不能与 Tunnel 接口的地址在同一网段。
- 关于 Tunnel 接口的详细介绍，关于 **interface tunnel**、**source**、**destination**、**tunnel dfbit enable** 和 **tunnel discard ipv4-compatible-packet** 命令以及 Tunnel 接口下更多配置命令的详细介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。

表1-1 配置 GRE over IPv4 隧道

操作	命令	说明
进入系统视图	**system-view**	-
创建模式为GRE over IPv4隧道的Tunnel接口，并进入该Tunnel接口视图	**interface tunnel** *interface-number* **mode gre**	缺省情况下，设备上不存在任何Tunnel接口 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败
设置Tunnel接口的IPv4地址或IPv6地址	IPv4地址的配置方法，请参见“三层技术-IP业务配置指导”中的“IP地址” IPv6地址的配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上没有设置IPv4地址和IPv6地址 乘客协议为IPv4时，需要配置Tunnel接口的IPv4地址；乘客协议为IPv6时，需要配置Tunnel接口的IPv6地址

操作	命令	说明
设置隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IPv4地址；如果设置的是隧道的源接口，则该接口的主IP地址将作为封装后隧道报文的源IPv4地址
设置隧道的目的端地址	**destination** *ip-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端从GRE隧道上接收报文的实际物理接口的地址，该地址将作为封装后隧道报文的目的IPv4地址
（可选）开启GRE的keepalive功能，并配置keepalive报文发送周期及最大发送次数	**keepalive** [*interval* [*times*]]	缺省情况下，GRE的keepalive功能处于关闭状态
（可选）开启GRE报文校验和功能	**gre checksum**	缺省情况下，GRE报文校验和功能处于关闭状态
（可选）设置GRE类型Tunnel接口的GRE Key	**gre key** *key-number*	缺省情况下，没有设置GRE类型Tunnel接口的GRE Key 隧道两端必须设置相同的GRE Key，或者都不设置GRE Key
（可选）设置封装后隧道报文的DF（Don't Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
退回系统视图	**quit**	-
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

1.3 配置GRE over IPv6隧道

配置 GRE over IPv6 隧道时，需要注意：

- 隧道两端必须都配置隧道的源端地址和目的端地址，且本端配置的源端地址（目的端地址）应该与对端配置的目的端地址（远端地址）相同。
- 在同一台设备上，隧道模式相同的 Tunnel 接口建议不要同时配置完全相同的源端地址和目的端地址。
- 隧道两端可以根据各自的实际应用需要决定是否要开启 GRE 报文校验和功能。如果本端开启了 GRE 报文校验和功能，则会在发送的报文中携带校验和信息，由对端来对报文进行校验和验证。对端是否对收到的报文进行校验和验证，取决于报文中是否携带校验和信息，与对端的配置无关。

- 如果封装前报文的目的地址与 Tunnel 接口的地址不在同一个网段，则必须配置通过 Tunnel 接口到达报文目的地址的路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达报文目的地址的路由出接口为本端 Tunnel 接口；也可以配置动态路由，在 Tunnel 接口、与私网相连的接口上分别使能动态路由协议，由动态路由协议来建立通过 Tunnel 接口转发的路由表项。
- 在 Tunnel 接口上配置的隧道目的端地址不能与 Tunnel 接口的地址在同一网段。
- 关于 Tunnel 接口的详细介绍，关于 **interface tunnel**、**source**、**destination** 和 **tunnel discard ipv4-compatible-packet** 命令以及 Tunnel 接口下更多配置命令的详细介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。

表1-2 配置 GRE over IPv6 隧道

操作	命令	说明
进入系统视图	**system-view**	-
创建模式为GRE over IPv6隧道的Tunnel接口，并进入该Tunnel接口视图	**interface tunnel** *interface-number* **mode gre ipv6**	缺省情况下，设备上不存在任何Tunnel接口 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败
设置Tunnel接口的IPv4地址或IPv6地址	IPv4地址的配置方法，请参见“三层技术-IP业务配置指导”中的“IP地址” IPv6地址的配置方法，请参见“三层技术-IP业务配置指导”中的“IPv6基础”	缺省情况下，Tunnel接口上没有设置IPv4地址和IPv6地址 乘客协议为IPv4时，需要配置Tunnel接口的IPv4地址；乘客协议为IPv6时，需要配置Tunnel接口的IPv6地址
设置隧道的源端地址或源接口	**source** { *ipv6-address* | *interface-type interface-number* }	缺省情况下，没有设置隧道的源端地址和源接口 如果设置的是隧道的源端地址，则该地址将作为封装后隧道报文的源IPv6地址；如果设置的是隧道的源接口，则该接口的地址将作为封装后隧道报文的源IPv6地址
设置隧道的目的端地址	**destination** *ipv6-address*	缺省情况下，没有设置隧道的目的端地址 隧道的目的端地址是对端从GRE隧道上接收报文的实际物理接口的地址，该地址将作为封装后隧道报文的目的IPv6地址
（可选）开启GRE报文校验和功能	**gre checksum**	缺省情况下，GRE报文校验和功能处于关闭状态
（可选）设置GRE类型Tunnel接口的GRE Key	**gre key** *key-number*	缺省情况下，没有设置GRE类型Tunnel接口的GRE Key 隧道两端必须设置相同的GRE Key，或者都不设置GRE Key
退回系统视图	**quit**	-

操作	命令	说明
（可选）配置丢弃含有IPv4兼容IPv6地址的IPv6报文	**tunnel discard ipv4-compatible-packet**	缺省情况下，不会丢弃含有IPv4兼容IPv6地址的IPv6报文

1.4 GRE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 GRE 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 Tunnel 接口的统计信息。

表1-3 GRE 显示和维护

操作	命令
显示Tunnel接口的相关信息（本命令的详细介绍，请参见“三层技术-IP业务命令参考”中的“隧道”）	**display interface** [**tunnel** [*number*]] [**brief** [**description** | **down**]]
显示Tunnel接口的IPv6相关信息（本命令的详细介绍，请参见“三层技术-IP业务命令参考”中的“IPv6基础”）	**display ipv6 interface** [**tunnel** [*number*]] [**brief**]
清除Tunnel接口的统计信息（本命令的详细介绍，请参见“三层技术-IP业务命令参考”中的“隧道”）	**reset counters interface** [**tunnel** [*number*]]

1.5 GRE典型配置举例

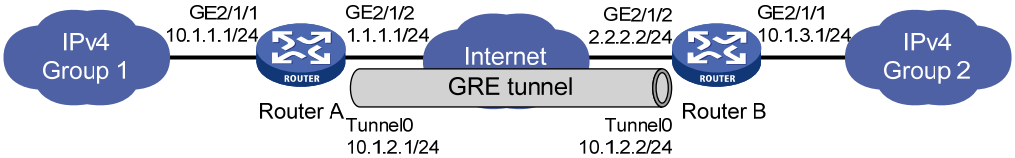
1.5.1 GRE over IPv4 隧道典型配置举例

1. 组网需求

Router A 和 Router B 分别连接 IPv4 私有网络 Group 1 和 Group 2。这两个私有网络都使用私网地址，且属于同一个 VPN。通过在 Router A 和 Router B 之间建立 GRE 隧道，实现两个私有网络的互联。

2. 组网图

图1-7 GRE over IPv4 隧道应用组网图



3. 配置步骤

说明

在开始下面的配置之前，假设设备各接口的地址都已配置完毕，并且 Router A 和 Router B 之间路由可达。

(1) 配置 Router A

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
<RouterA> system-view
[RouterA] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址。

```
[RouterA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

配置 Tunnel0 接口的源端地址（Router A 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterA-Tunnel0] source 1.1.1.1
```

配置 Tunnel0 接口的目的端地址（Router B 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterA-Tunnel0] destination 2.2.2.2
[RouterA-Tunnel0] quit
```

配置从 Router A 经过 Tunnel0 接口到 Group 2 的静态路由。

```
[RouterA] ip route-static 10.1.3.0 255.255.255.0 tunnel 0
```

(2) 配置 Router B

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
<RouterB> system-view
[RouterB] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址。

```
[RouterB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

配置 Tunnel0 接口的源端地址（Router B 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterB-Tunnel0] source 2.2.2.2
```

配置 Tunnel0 接口的目的端地址（Router A 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterB-Tunnel0] destination 1.1.1.1
[RouterB-Tunnel0] quit
```

配置从 Router B 经过 Tunnel0 接口到 Group 1 的静态路由。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

4. 验证配置

查看 Router A 的 Tunnel 接口状态。

```
[RouterA] display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.2.1/24 Primary
Tunnel source 1.1.1.1, destination 2.2.2.2
```

```
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

查看 Router B 的 Tunnel 接口状态。

```
[RouterB] display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.2.2/24 Primary
Tunnel source 2.2.2.2, destination 1.1.1.1
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

从 Router B 可以 Ping 通 Router A 上 GigabitEthernet2/1/1 接口的地址。

```
[RouterB] ping -a 10.1.3.1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1) from 10.1.3.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=11.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/2.400/11.000/4.317 ms
```

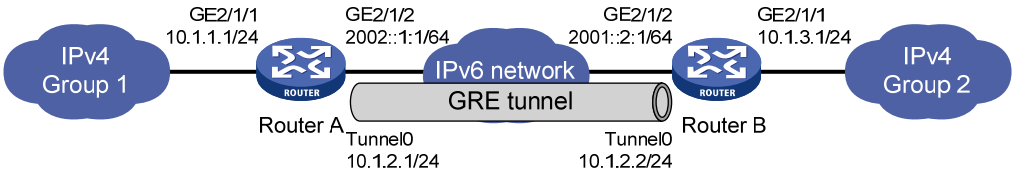
1.5.2 GRE over IPv6 隧道典型配置举例

1. 组网需求

运行 IPv4 协议的两个子网 Group 1 和 Group 2 通过 IPv6 网络相连。通过在 Router A 和 Router B 之间建立 GRE over IPv6 隧道，实现两个子网穿越 IPv6 网络互联。

2. 组网图

图1-8 GRE over IPv6 隧道应用组网图



3. 配置步骤

说明

在开始下面的配置之前，假设设备各接口的地址都已配置完毕，并且 Router A 和 Router B 之间路由可达。

(1) 配置 Router A

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv6 隧道。

```
<RouterA> system-view
[RouterA] interface tunnel 0 mode gre ipv6
```

配置 Tunnel0 接口的 IP 地址。

```
[RouterA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

配置 Tunnel0 接口的源端地址（Router A 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterA-Tunnel0] source 2002::1:1
```

配置 Tunnel0 接口的目的端地址（Router B 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterA-Tunnel0] destination 2001::2:1
[RouterA-Tunnel0] quit
```

配置从 Router A 经过 Tunnel0 接口到 Group 2 的静态路由。

```
[RouterA] ip route-static 10.1.3.0 255.255.255.0 tunnel 0
```

(2) 配置 Router B

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv6 隧道。

```
<RouterB> system-view
[RouterB] interface tunnel 0 mode gre ipv6
```

配置 Tunnel0 接口的 IP 地址。

```
[RouterB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

配置 Tunnel0 接口的源端地址（Router B 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterB-Tunnel0] source 2001::2:1
```

配置 Tunnel0 接口的目的端地址（Router A 的 GigabitEthernet2/1/2 的 IP 地址）。

```
[RouterB-Tunnel0] destination 2002::1:1
[RouterB-Tunnel0] quit
```

配置从 Router B 经过 Tunnel0 接口到 Group 1 的静态路由。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

4. 验证配置

查看 Router A 的 Tunnel 接口状态。

```
[RouterA] display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1456
Internet Address is 10.1.2.1/24 Primary
Tunnel source 2002::1:1, destination 2001::2:1
Tunnel TTL 255
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

查看 Router B 的 Tunnel 接口状态。

```
[RouterB] display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1456
Internet Address is 10.1.2.2/24 Primary
Tunnel source 2002::2:1, destination 2001::1:1
Tunnel TTL 255
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
```

```
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

从 Router B 可以 Ping 通 Router A 上 GigabitEthernet2/1/1 接口的地址。

```
[RouterB] ping -a 10.1.3.1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1) from 10.1.3.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/2.000/0.632 ms
```

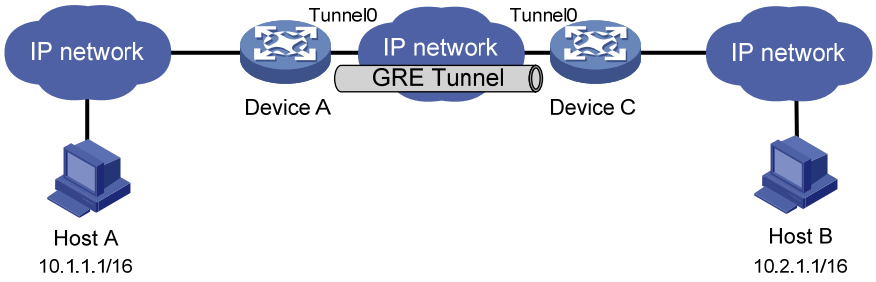
1.6 常见配置错误举例

GRE 的配置相对比较简单，但要注意配置的一致性，大部分的错误都可以使用调试命令 **debugging gre** 和 **debugging tunnel** 定位。这里仅就一种错误进行分析。

1. 故障现象

如 图 1-9 所示，Tunnel两端接口配置正确且Tunnel两端可以ping通，但Host A和Host B之间却无法ping通。

图1-9 GRE 排错示例



2. 故障分析

出现该故障的原因可能是 Device A 或 Device C 上没有到达对端网络的路由。

3. 故障排除

(1) 在 Device A 和 Device C 分别执行 **display ip routing-table** 命令，观察在 Device A 是否有经过 Tunnel0 接口到 10.2.0.0/16 的路由；在 Device C 是否有经过 Tunnel0 接口到 10.1.0.0/16 的路由。

(2) 如果不存在上述路由，则在系统视图下使用 **ip route-static** 命令添加静态路由。以 Device A 为例，配置如下：

```
[DeviceA] ip route-static 10.2.0.0 255.255.0.0 tunnel 0
```

目 录

1 ADVPN

1.1 ADVPN简介

越来越多的企业希望利用公共网络组建 VPN（Virtual Private Network，虚拟专用网络），连接地理位置不同的多个分支机构。然而，企业分支机构通常采用动态地址接入公共网络，通信一方无法事先知道对端的公网地址，这就为组建 VPN 提出了一个难题。

ADVPN（Auto Discovery Virtual Private Network，自发现虚拟专用网络）通过 VAM（VPN Address Management，VPN 地址管理）协议收集、维护和分发动态变化的公网地址等信息，解决了无法事先获得通信对端公网地址的问题。ADVPN 可以在企业网各分支机构使用动态地址接入公网的情况下，在各分支机构间建立 VPN。

ADVPN 把连接到公网上的各节点组成的网络看作 VPN 网络，公网作为 VPN 网络的链路层，ADVPN 隧道作为企业内部子网之间的虚通道，相当于网络层。企业各分支设备动态接入到公网中，其公网地址对于通信的另一端来说是未知的，而对于建立端到端的安全隧道，公网地址是必须的条件之一。ADVPN 通过 VAM 获取通信对端的公网地址。

VAM 协议是 ADVPN 方案的主要协议，负责收集、维护、分发公网地址等信息，帮助用户快捷、方便的建立起内部的安全隧道。企业内部子网之间转发的数据报文通过路由协议得到其私网下一跳，通过 VAM 协议查询到私网下一跳对应的公网地址，并利用该公网地址做为隧道的目的地址进行封装，最后交给已建立起的安全隧道发送到目的端用户。

1.1.1 ADVPN的基本概念

ADVPN 方案中有几个关键的角色：

1. ADVPN节点

ADVPN 节点为动态 VPN 隧道两端的设备，可以是网络设备或主机。ADVPN 节点参与隧道的建立，需要实现 VAM 的客户端功能。

2. VAM Server

VAM Server 是接受 ADVPN 节点向其注册信息的服务器，负责管理、维护各 ADVPN 节点的信息。目前 VAM Server 一般运行在较高性能的路由器设备上。

3. VAM Client

VAM Client 向 VAM Server 注册自己的私网地址、公网地址等信息，向 VAM Server 查询其它 VAM Client 的信息。ADVPN 节点上需要实现 VAM Client 功能。文中涉及到 VAM Client 的地方，如果不是特别说明，是指对 Hub 和 Spoke 的统称。

4. Hub

Hub 是一种 VAM Client，一个 ADVPN 网络的中心设备，它是路由信息交换的中心。在 Hub-Spoke 组网中，它也是数据转发的中心。

5. Spoke

Spoke 是一种 VAM Client，通常是企业分支机构的网关设备，该节点不会转发收到的其它 ADVPN 节点的数据。

6. Hub组

Hub 组将一个 ADVPN 网络划分为若干个逻辑区域。每个 Hub 组内可以规划一组 Hub 和 Spoke。一个 Hub 组内的 Spoke 只与本组的 Hub 建立 ADVPN 隧道，不与其他 Hub 组的 Hub 建立 ADVPN 隧道。当一个 ADVPN 网络中有大量 ADVPN 节点时，为了减轻 Hub 的负担，应该给 ADVPN 域划分 Hub 组。

7. AAA服务器

AAA（Authentication, Authorization and Accounting，认证、授权和计费）服务器，用于对用户进行认证和计费管理。

1.1.2 ADVPN的基本原理

ADVPN 采用 Client/Server 模式，工作在 TCP/IP 协议栈的应用层。ADVPN 支持 UDP 和 GRE 两种隧道封装模式。按照工作方式的不同，可将一个 ADVPN 域中的设备划分为一个 Server 和多个 Client，Server 的公网地址为静态地址，Client 的公网地址既可以静态配置也可以动态获取，而 Client 的私网地址则需要按照规划静态分配。在同一个 ADVPN 域内，同一个 Hub 组内的节点的私网地址应该在同一个网段内。

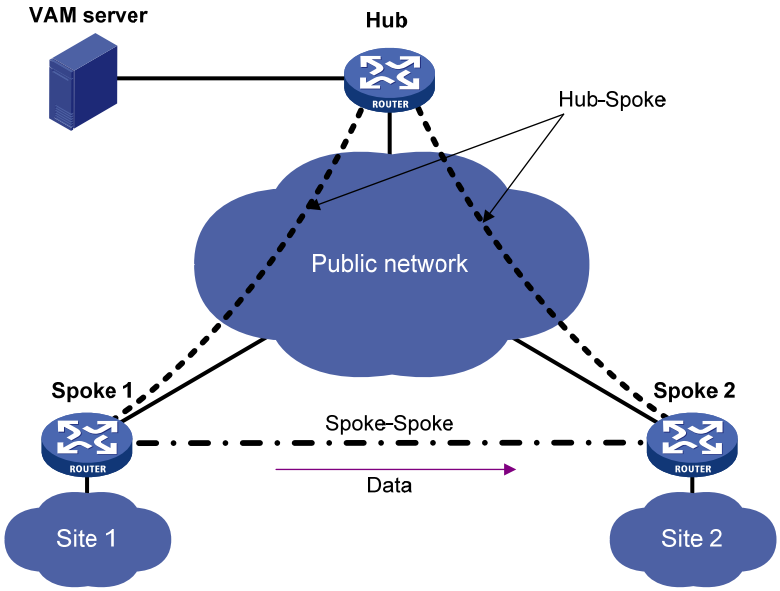
每一个 Client 向 Server 注册自己的公网地址和私网地址的对应关系。Client 向 Server 注册成功之后，其他 Client 可以从 Server 查询到该 Client 的公网地址，以便在 Client 之间建立 ADVPN 隧道。Server 与 Client 间通过 VAM 协议进行消息传递，Client 之间通过 ADVPN 隧道协议进行隧道的建立、维护和删除。任何节点退出或加入 ADVPN 都能自动通知 Server。

1.1.3 ADVPN的组网结构

1. Full-Mesh（全互联）网络

- 如 图 1-1 所示，所有的ADVPN节点在同一个Hub组内，Spoke之间可以建立隧道直接通信，Hub主要作为路由信息交换的中心。作为Spoke的Client节点在向VAM Server注册后获得该ADVPN域中Hub的信息，并与Hub建立永久的隧道连接；任意的两个Spoke之间也可以直接建立隧道，但该隧道是动态的，当在一段规定时间（Spoke-Spoke隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。

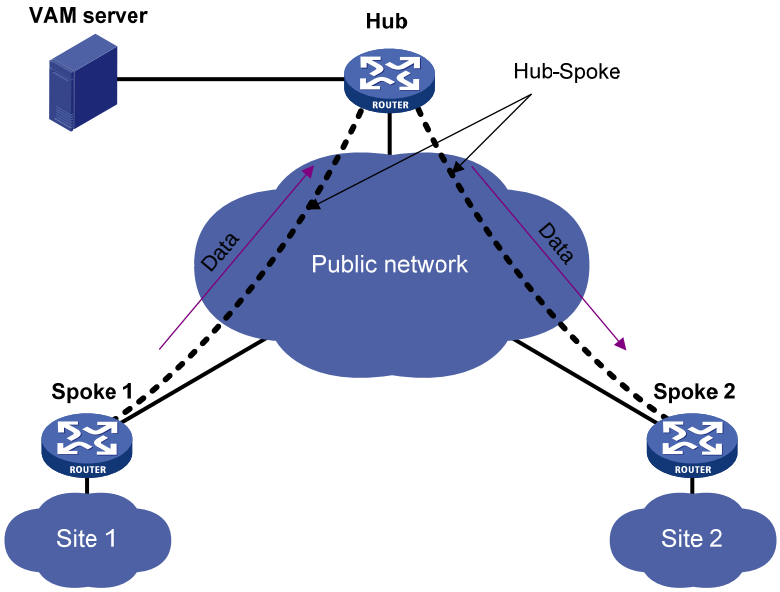
图1-1 Full-Mesh 组网示意图



2. Hub-Spoke网络

如 图 1-2 所示，所有的ADVPN节点在同一个Hub组内，Spoke之间不能建立隧道直接通信，只能通过Hub转发数据，Hub既作为路由信息交换的中心，又作为数据转发的中心。Spoke与Hub建立永久的隧道连接，Spoke之间的数据通过Hub转发。

图1-2 Hub-Spoke 组网示意图



3. 大规模Full-Mesh网络

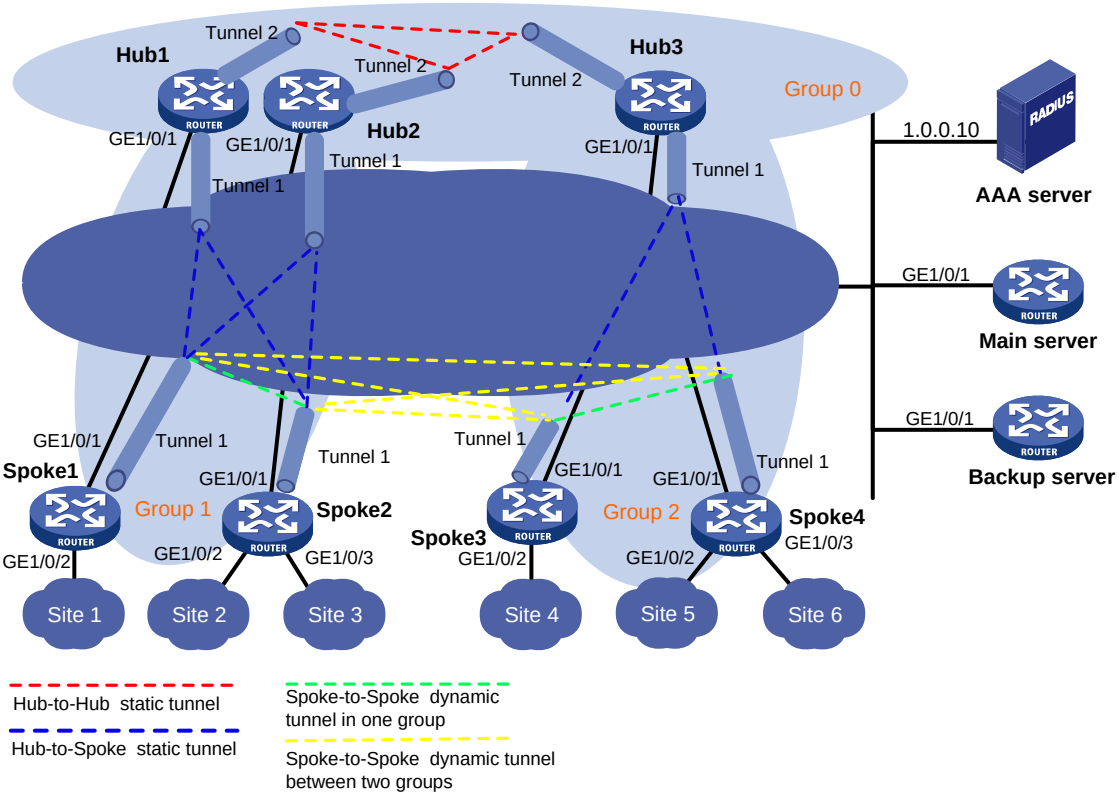
如 图 1-3 所示，当一个ADVPN网络中有大量ADVPN节点时，由于某些原因（如动态路由协议邻居数限制等），一个Hub组内无法部署全部的ADVPN节点。此时，需要将ADVPN网络划分为多个Hub组，并选择其中一个Hub组作为骨干区域。将ADVPN节点部署到除骨干区域外其他Hub组中。

每个 Hub 组内至少有 1 个 Hub，并且这些 Hub 需要同时部署到骨干区域中。骨干区域采用 Full-Mesh 组网，其它 Hub 组可以使用 Full-Mesh 组网也可以使用 Hub-Spoke 组网。

同一个 Hub 组内，隧道建立方式和数据转发方式由其组网方式决定。不同 Hub 组间，数据需要通过本组的 Hub 转发到目的组的 Hub，再由目的组 Hub 转发到对应的 Spoke。

为了减少 Hub 跨组转发数据时的压力，可以允许不同组的 Spoke 直接建立隧道，但该隧道是动态的，当在一段规定时间（Spoke-Spoke 隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。

图1-3 大规模 Full-Mesh 组网示意图



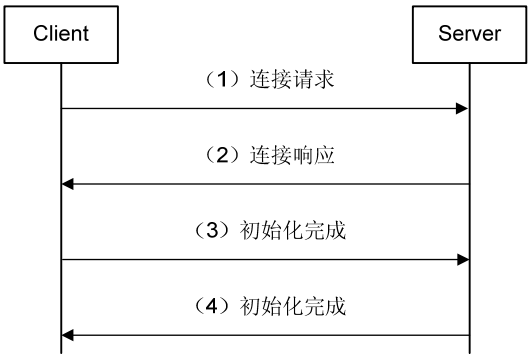
1.1.4 ADVPN的工作过程

ADVPN 的工作过程分为连接初始化、注册和隧道建立三个阶段，下面对这三个阶段做简单说明。

1. 连接初始化阶段

Client 在第一次与 Server 连接时，首先进行连接的初始化，双方协商决定是否需要对 VAM 协议报文进行保护。如果需要保护，则协商出报文加密和完整性验证算法及生成加密密钥和完整性验证密钥，并对协商出的结果作出确认。只有连接初始化完成后，才能进入注册阶段。

图1-4 连接初始化流程图



如 图 1-4 所示，连接初始化的过程为：

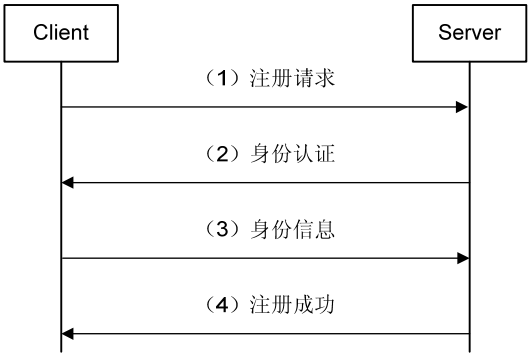
(1) Client 通过连接请求报文将自己支持的完整性验证算法、加密算法等发送给 Server。

(2) Server 按照优先级从高到低的顺序从自己支持的算法列表中依次选择算法，与 Client 发送的算法列表进行匹配。如果匹配成功，则使用该算法，Server 通过连接响应报文将算法协商结果发送给 Client，同时，Server 和 Client 生成加密密钥和完整性验证密钥。

(3) Client 和 Server 分别利用初始化完成报文来验证各种算法和密钥的协商是否成功。

2. 注册阶段

图1-5 注册流程图



如 图 1-5 所示，注册阶段的具体过程为：

(1) Client 向 Server 发送注册请求报文，注册请求报文中包括 ADVPN 节点的信息。

(2) Server 收到注册请求报文后，根据配置决定是否对该 Client 进行身份认证。如果配置为不认证，则直接注册 Client 信息并向 Client 发送注册成功响应，身份认证步骤省略；如果配置为认证，Server 向 Client 回应身份认证请求，并指明需要的认证方法（CHAP 认证时还返回一个随机数）。

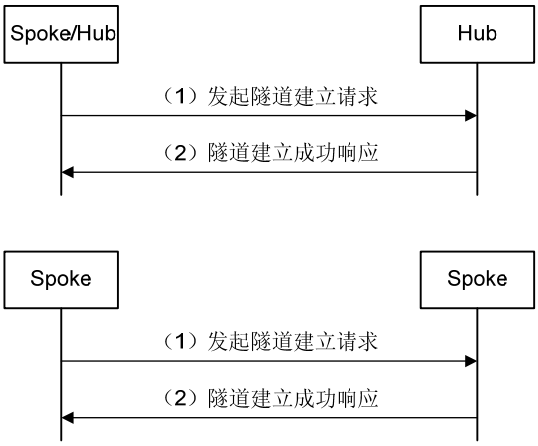
(3) Client 向 Server 提交自己的身份信息。

(4) Server 收到 Client 的身份认证信息后向 AAA 服务器发起认证，收到 AAA 认证成功的响应后再发送计费请求，当 Server 收到计费成功响应后，向 Client 发送注册成功响应报文，注册成功报文会携带下发给 Client 的 Hub 信息。

3. 隧道建立阶段

当Spoke注册成功后，要和Hub建立永久隧道，一个Spoke可以和任意多个Hub建立永久隧道。如果在一个ADVPN域中有两个Hub，则Hub之间需要建立永久隧道。具体隧道建立流程如 图 1-6 所示。

图1-6 隧道建立流程图



(1) 发起隧道建立请求

- Hub-Spoke：Spoke 注册成功后，要与所在 ADVPN 中的 Hub 建立永久隧道。Spoke 只要收到 Server 下发的 Hub 信息，就会检查与这些 Hub 地址之间是否有对应的隧道存在。如果隧道不存在则向 Hub 发送隧道建立报文；如果隧道存在则不建立隧道。
- Hub-Hub 隧道：Hub 注册成功后，Server 会将所在 ADVPN 中已注册成功的 Hub 地址添加到注册响应报文中下发给 Hub。Hub 检查这些地址与其之间是否有对应的隧道存在。如果隧道不存在则向其发送隧道建立报文；如果隧道存在则不建立隧道。
- Spoke-Spoke 隧道：在 Full-Mesh 组网中，Spoke 收到某个数据报文后，若没有查到相应的能够转发该报文的隧道，则会向 Server 发送地址解析请求，根据得到的地址解析响应向对端 Spoke 发起建立隧道的请求。

(2) 隧道接收方收到建立隧道的请求后，保存相应的隧道连接信息，并向发起方发送建立隧道响应报文。如果隧道发起方收到隧道建立成功的响应报文，表示隧道建立成功，否则表示隧道建立失败。

1.1.5 设备支持的ADVPN特性

1. UDP封装的ADVPN报文对NAT网关自然穿越

当隧道发起方在 NAT 网关后侧时，则可以建立穿越 NAT 的 Spoke-Spoke 隧道；如果隧道接收方在 NAT 网关后侧，则数据包要由 Hub 转发，直到接收方发起隧道建立请求。如果双方都在 NAT 网关后侧，则它们都无法与对方建立隧道，所有的数据包都只能从 Hub 转发。

如果 NAT 网关采用 Endpoint-Independent Mapping（不关心对端地址和端口转换模式），隧道接收方在 NAT 网关后侧时，也可以建立穿越 NAT 的 Spoke-Spoke 隧道。

2. VAM Client对动态IP地址的支持

隧道两端的 Tunnel 接口不需要配置隧道目的地址，VAM Client 在 VAM Server 上注册自己的公/私网地址，当需要建立隧道时，可以从 VAM Server 获取对端 Client 的公网地址，从而动态的建立隧

道。当 VAM Client 的 IP 地址改变时，会向 VAM Server 重新注册，从而实现了对动态 IP 地址的支持。

3. VAM Server对VAM Client的AAA身份认证

初始化过程完成之后，VAM Client 要向 VAM Server 注册，注册过程中可以要求对 VAM Client 进行身份认证，VAM 支持 PAP 和 CHAP 两种认证方式。VAM Server 通过 AAA 对加入到 ADVPN 域的客户端进行身份认证，认证通过后 VAM Client 才能接入到 ADVPN 网络。

4. 利用预共享密钥验证VAM Client和VAM Server的身份

VAM Client 和 VAM Server 必须配置统一的预共享密钥，用于生成加密/完整性验证的密钥。VAM Client/VAM Server 通过报文解密、完整性验证是否成功，判断二者的预共享密钥是否相同，从而实现对 VAM Server/VAM Client 的身份认证。

5. VAM协议报文的加密保护

可以选择对 VAM 协议报文进行加密，加密算法支持 AES-128、AES-256、DES 和 3DES 算法。

6. 数据报文的IPsec加密保护

ADVPN 隧道的数据报文可以由 IPsec 安全框架保护，采用安全协议 ESP、AH 或 AH-ESP（先采用 ESP 协议，再采用 AH 协议），通过 IKE 协商安全策略。

7. 策略的统一管理

VAM Server 对整个 ADVPN 域的策略进行统一的管理。

8. 支持多个ADVPN域

VAM Server 上可以配置多个 ADVPN 域。

1.2 ADVPN配置任务简介

ADVPN 的配置涉及到 VAM、AAA、Tunnel、IPsec 安全框架和路由配置。组网时一般先配置好 ADVPN 服务器端，然后是 ADVPN 客户端的 Hub 设备，最后是 Spoke 设备。

表1-1 ADVPN 配置任务简介

配置任务		说明	详细配置
配置ADVPN服务器端	配置AAA	可选	1.3
	配置VAM Server	必选	1.4
配置ADVPN客户端	配置VAM Client	必选	1.5
	配置ADVPN隧道	必选	1.6
	配置路由	必选	1.7
	配置IPsec保护ADVPN隧道报文	可选	1.8

1.3 配置AAA

ADVPN 服务器端可以根据需要使用 AAA 对接入到 ADVPN 域的 Client 进行身份认证，只有通过身份认证的 Client 才可以接入到 ADVPN 域。

ADVPN 服务器端 AAA 的具体配置请参见“安全配置指导”中的“AAA”。

1.4 配置VAM Server

该配置主要对 ADVPN 服务器端的参数进行设置，并制定相关的策略，即是否对 VAM 的协议报文进行保护，Server 对 Client 的认证方式等等。

1.4.1 VAM Server配置任务简介

表1-2 VAM Server 配置任务简介

配置任务	说明	详细配置
创建ADVPN域	必选	1.4.2
启动VAM Server功能	必选	1.4.3
配置VAM Server的预共享密钥	必选	1.4.4
配置Hub组	必选	1.4.5
配置VAM Server的监听端口号	可选	1.4.6
配置VAM协议报文的安全参数	可选	1.4.7
配置对VAM Client的身份认证方式	可选	1.4.8
配置Keepalive报文参数	可选	1.4.9
配置请求报文重传参数	可选	1.4.10

1.4.2 创建ADVPN域

创建 ADVPN 域时必须指定一个唯一的 ID。进入已经创建的 ADVPN 域时，不需要指定 ID。

表1-3 创建 ADVPN 域

操作	命令	说明
进入系统视图	**system-view**	-
创建ADVPN域，并进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	缺省情况下，没有配置ADVPN域

1.4.3 启动VAM Server功能

该配置用来启动服务器端 ADVPN 域的 VAM Server 功能。

表1-4 启动 VAM Server 功能

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
启动VAM Server功能	启动所有或指定ADVPN域的VAM Server功能	**vam server enable** { **all** | **advpn-domain** *domain-name* }	二者选其一 缺省情况下，VAM Server功能处于关闭状态
	启动指定ADVPN域的VAM Server功能	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	
		server enable	

1.4.4 配置VAM Server的预共享密钥

预共享密钥是 VAM Server 用来和 VAM Client 建立安全通道的公共密钥材料。在连接初始化阶段预共享密钥用来生成验证和加密连接请求、连接响应报文的初始密钥；如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥。

同一个 ADVPN 域内的 VAM Server 和 VAM Client 上配置的预共享密钥必须一致。

表1-5 配置 VAM Server 的预共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server的预共享密钥	**pre-shared-key** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，未配置VAM Server的预共享密钥

1.4.5 配置Hub组

在大规模组网情况下，将 ADVPN 域划分为多个 Hub 组可以方便管理。创建 Hub 组后，可以按照 Spoke 的私网地址网段或地址范围，将 Spoke 划分到不同的 Hub 组中，并为每个 Hub 组指定一个或多个 Hub。

当 VAM Client 向 VAM Server 注册时，根据 VAM Client 的私网地址将 VAM Client 划分到对应的 ADVPN 域 Hub 组中：

(1) 根据 Hub 组名称字典序依次匹配各 Hub 组内配置的 Hub 地址。

(2) 如果匹配上，则 VAM Client 为 Hub，并被划分到该 Hub 组；如果 VAM Client 不是 Hub，再根据 Hub 组名称字典序依次匹配各 Hub 组内配置的 Spoke 私网地址范围。

(3) 如果匹配上，则 VAM Client 为 Spoke，并被划分到该 Hub 组；否则，VAM Client 既不是 Hub 也不是 Spoke，注册失败。

VAM Server 只向 VAM Client 下发其所属的 Hub 组内的 Hub 信息。VAM Client 只与本 Hub 组内的 Hub 建立永久 ADVPN 隧道会话。

1. 创建Hub组

表1-6 创建 Hub 组

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
创建Hub组，并进入Hub组视图	**hub-group** *group-name*	缺省情况下，不存在Hub组

2. 配置Hub组内的Hub私网地址

每个 Hub 组必须至少配置一个 Hub 私网地址。

表1-7 配置 Hub

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置Hub的私网地址	**hub private-address** *private-ip-address* [**public-address** { *public-ip-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]	二者选其一 缺省情况下，Hub组内没有配置Hub私网地址
	hub ipv6 private-address *private-ipv6-address* [**public-address** { *public-ip-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]	

3. 配置Hub组内的Spoke私网地址范围

每个 Hub 组可以配置多个 Spoke 的 IPv6 私网地址范围，将按照地址从小到大的顺序排列。

表1-8 配置 Spoke 的地址范围

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置Spoke的私网地址范围	**spoke private-address** { **range** *start-address end-address* | **network** *ip-address* { *mask-length* | *mask* } }	二者选其一 缺省情况下，Hub组内没有配置Spoke的私网地址范围
	spoke ipv6 private-address { **range** *start-ipv6-address end-ipv6-address* | **network** *prefix/prefix-length* }	

4. 配置跨Hub组建立Spoke-Spoke直连隧道的规则

配置了跨 Hub 组建立 Spoke-Spoke 直连隧道的规则，在 Hub 上线后，VAM Server 通过数据流信息报文将指定的规则下发到 Hub。在 Hub 转发私网数据报文的同时，会将数据报文与收到的规则进行匹配。如果匹配成功，Hub 向发送该数据报文的 Spoke 发送重定向报文。Spoke 收到重定向报文后，向 VAM Server 查询被重定向的数据报文目的地址的直连路由，以及直连路由下一跳所对应的 Spoke 的公网地址，并与该 Spoke 建立直连隧道。

跨 Hub 组 Spoke-Spoke 直连隧道建立前，数据报文仍由 Hub 进行转发。直连隧道建立后，数据报文将直接发送到直连路由下一跳所对应的 Spoke，而不再经过 Hub 中转。

表1-9 配置跨 Hub 组建立 Spoke-Spoke 直连隧道的规则

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置跨Hub组建立Spoke-Spoke直连隧道的规则	**shortcut interest** { **all** | **acl** { *acl-number* | **name** *acl-name* } }	二者选其一 缺省情况下，没有配置跨Hub组建立Spoke-Spoke直连隧道的规则，不允许跨Hub组建立Spoke-Spoke直连隧道
	shortcut ipv6 interest { **all** | **acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* } }	

1.4.6 配置VAM Server的监听端口号

VAM Server 的监听端口号与 VAM Client 上指定的 VAM Server 的端口号必须一致。

表1-10 配置监听端口号

操作	命令	说明
进入系统视图	**system-view**	-
配置VAM Server的监听端口号	**vam server listen-port** *port-number*	缺省情况下，VAM Server的监听端口号为18000

1.4.7 配置VAM协议报文的安全参数

该配置用来设置 VAM 协议报文的验证、加密算法。VAM Server 根据配置的报文完整性验证、加密算法以及优先级与 VAM Client 发送的算法列表进行协商，协商后的算法分别作为两端协议报文的完整性验证算法和加密算法。

需要注意的是：

- VAM Server 与 VAM Client 之间的连接初始化请求和响应报文固定使用 SHA-1 验证算法和 AES-CBC-128 加密算法，其他 VAM 协议报文根据二者的协商结果选择验证/加密算法。
- 验证/加密算法在配置中的出现顺序决定其使用优先级。VAM Server 在与 VAM Client 协商时，从 VAM Client 支持的验证/加密算法列表中选择配置最靠前的算法作为协商结果。

- 修改验证/加密算法对已经注册的 VAM Client 没有影响，新注册的 VAM Client 将采用修改后的算法进行协商。

表1-11 配置 VAM 协议报文的安全参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM协议报文的验证算法	**authentication-algorithm** { **aes-xcbc-mac** | **md5** | **none** | **sha-1** | **sha-256** } *	缺省情况下，VAM协议报文的验证算法为SHA-1
配置VAM协议报文的加密算法	**encryption-algorithm** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **des-cbc** | **none** } *	缺省情况下，按照优先级由高到低依次使用AES-CBC-256、AES-CBC-192、AES-CBC-128、AES-CTR-256、AES-CTR-192、AES-CTR-128、3DES-CBC、DES-CBC算法

1.4.8 配置对VAM Client的身份认证方式

该配置用来设置 VAM Server 对 VAM Client 的认证方式。对于 VAM Server 启用 AAA 对 VAM Client 进行认证的情况，目前只支持 PAP 和 CHAP 两种身份验证方式。

需要注意的是：

- 如果配置时指定的认证 ISP 域不存在，则 VAM Server 对 VAM Client 的身份认证会失败。
- 修改认证方式对已经注册的 VAM Client 没有影响，新注册的 VAM Client 将按照修改后的认证方式进行身份认证。

表1-12 配置对客户端的认证方式

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server对VAM Client的身份认证方式	**authentication-method** { **none** | { **chap** | **pap** } [**domain** *isp-name*] }	缺省情况下，VAM Server使用CHAP方式，对VAM Client进行身份认证，认证使用的ISP域为用户配置的系统默认域

1.4.9 配置Keepalive报文参数

VAM Client 和 VAM Server 之间通过 Keepalive 报文保持联系。该配置用来设置 VAM Client 发送 Keepalive 报文的时间间隔和重发次数。当 VAM Client 注册成功后，VAM Server 会将配置的参数在注册响应中下发给 VAM Client，同一个 ADVPN 域中所有 VAM Client 的 Keepalive 报文参数都是相同的。

VAM Client 按照 VAM Server 指定的时间间隔向 VAM Server 发送 Keepalive 报文，VAM Server 收到 Keepalive 报文后回复响应报文。当 Keepalive 报文的重发次数达到指定的值仍没有收到 VAM Server 的响应时，VAM Client 认为与 VAM Server 的连接中断，不再发送 Keepalive 报文。当 VAM Server 时间间隔×重发次数的时间内没有收到 VAM Client 的 Keepalive，则认为与 VAM Client 的连接中断，会删除该 VAM Client 的信息并将其下线。

需要注意的是，如果 VAM Server 改变 Keepalive 报文参数，则修改后的参数只对新注册的 VAM Client 生效，已经注册的 VAM Client 不受影响。

表1-13 配置 Keepalive 报文参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Client向VAM Server发送Keepalive报文的时间间隔和重试次数	**keepalive interval** *time-interval* **retry** *retry-times*	缺省情况下，VAM Client发送Keepalive报文的时间间隔为180秒，重试次数是3次

1.4.10 配置请求报文重传参数

VAM Server 向 VAM Client 发送请求报文后，如果在指定的时间间隔内没有收到响应报文，VAM Server 将重新发送该请求报文，直到收到响应报文或者 VAM Client Keepalive 超时为止。

表1-14 配置报文重传参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server重发请求报文的时间间隔	**retry interval** *time-interval*	缺省情况下，VAMServer重发请求报文的时间间隔为5秒

1.5 配置VAM Client

通过 VAM Client 端的配置，可以指定 VAM Client 所在 ADVPN 域、VAM Client 注册的主/备 VAM Server 地址和端口号，以及 VAM Client 的本地用户信息等，为 VAM Client 向 VAM Server 发起初始化连接请求，并最终成功注册到 VAM Server 上做了必要准备。

1.5.1 VAM Client配置任务简介

表1-15 VAM Client 配置任务简介

配置任务	说明	详细配置
创建VAM Client	必选	1.5.2

配置任务	说明	详细配置
启动VAM Client功能	必选	1.5.3
配置VAM Server的地址	必选	1.5.4
配置VAM Client所属的ADVPN域	必选	1.5.5
配置VAM Client的预共享密钥	必选	1.5.6
配置请求报文重传参数	可选	1.5.7
配置VAM Client连接超时的静默时间	可选	1.5.8
配置认证用户名和密码	可选	1.5.9

1.5.2 创建VAM Client

表1-16 创建 VAM Client

操作	命令	说明
进入系统视图	**system-view**	-
创建VAM Client，并进入VAM Client视图	**vam client name** *client-name*	缺省情况下，没有配置VAM Client

1.5.3 启动VAM Client功能

表1-17 启动 VAM Client 功能

操作		命令	说明
进入系统视图		**system-view**	-
启动VAM Client功能	启动所有或指定VAM Client的VAM Client功能	**vam client enable { all | name** *client-name* **}**	二者选其一 缺省情况下，VAM Client的VAM Client功能处于关闭状态
	启动指定VAM Client的VAM Client功能	**vam client name** *client-name*	
		client enable	

1.5.4 配置VAM Server的地址

可以为一个 VAM Client 配置两个 VAM Server，一个主 VAM Server，一个备 VAM Server。VAM Client 会同时向主 VAM Server 和备 VAM Server 进行注册，如果都注册成功，VAM Client 会优先使用先注册成功的 VAM Server 向其下发的信息。当该 VAM Server 故障时，VAM Client 再使用另外一个 VAM Server 下发的信息。

需要注意的是：

- 如果主 VAM Server 和备 VAM Server 的地址相同（配置了相同的地址或通过域名解析到相同的地址），则只有主 VAM Server 有效。

- 如果要指定 VAM Server 的端口号，则必须和 VAM Server 上配置的监听端口号一致。

1. 配置主VAM Server的地址

表1-18 配置主 VAM Server 的地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置主VAM Server的地址	**server primary** { **name** *host-name* | **ip-address** *ip-address* | **ipv6-address** *ipv6-address* } [**port** *port-number*]	缺省情况下，没有配置主VAM Server的地址

2. 配置备VAM Server的地址

表1-19 配置备 VAM Server 的地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置备VAM Server的地址	**server secondary** { **name** *host-name* | **ip-address** *ip-address* | **ipv6-address** *ipv6-address* } [**port** *port-number*]	缺省情况下，没有配置备VAM Server的地址

1.5.5 配置VAM Client所属的ADVPN域

表1-20 配置 VAM Client 所属的 ADVPN 域

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client所属的ADVPN域	**advpn-domain** *domain-name*	缺省情况下，VAM Client不属于任何ADVPN域

1.5.6 配置VAM Client的预共享密钥

预共享密钥是 VAM Client 用来和 VAM Server 建立安全通道的公共密钥材料。在连接初始化阶段预共享密钥用来生成验证和加密连接请求、连接响应报文的初始密钥；如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥。

同一个 ADVPN 域内的 VAM Client 和 VAM Server 上配置的预共享密钥必须一致。

表1-21 配置 VAM Client 的预共享密钥

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client的预共享密钥	**pre-shared-key** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，无预共享密钥

1.5.7 配置请求报文重传参数

VAM Client 向 VAM Server 发送请求报文后，如果在指定的时间间隔内没有收到响应报文，VAM Client 将重新发送请求报文。如果重新发送请求报文的次数超过指定的重发次数，则 VAM Client 认为 VAM Server 不可达。

需要注意的是：

- 私网注册请求报文和节点信息更新请求报文不受重发次数的限制，将会按照指定的时间间隔一直发送，直至 VAM Client 下线。
- VAM Client 发送 Keepalive 报文的时间间隔和重发次数由 VAM Server 的配置决定。

表1-22 配置 VAM 协议报文重传参数

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM协议报文重传参数	**retry interval** *time-interval* ***count*** *retry-times*	缺省情况下，VAM协议报文重发间隔时间为5秒，重传次数为3次

1.5.8 配置VAM Client连接超时的静默时间

VAM Client 在与 VAM Server 连接超时后，会进入静默状态，此时 VAM Client 不处理任何报文。当静默时间到达后，VAM Client 将重新上线。

表1-23 配置 VAM Client 连接超时的静默时间

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client连接超时的静默时间	**dumb-time** *time-interval*	缺省情况下，VAM Client连接超时的静默时间为120秒

1.5.9 配置认证用户名和密码

配置 VAM Client 的用户名和密码，用于向 VAM Server 进行身份认证。

表1-24 配置认证用户和密码

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置认证用户名和密码	**user** *username* **password** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，没有配置认证用户名和密码

1.6 配置ADVPN隧道

通过 ADVPN 隧道的配置，可以配置 ADVPN 隧道接口的私网地址、隧道两端接口所绑定的 VAM Client、隧道的空闲超时时间以及隧道建立失败的静默时间等，为建立 ADVPN 隧道做了必要准备。

关于 Tunnel 接口的详细介绍，关于 **interface tunnel**、**source** 和 **tunnel dfbit enable** 命令以及 Tunnel 接口下更多配置命令的详细介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。

表1-25 配置 ADVPN 隧道

操作	命令	说明
进入系统视图	**system-view**	-
创建ADVPN隧道类型的Tunnel接口，并进入Tunnel接口视图	**interface tunnel** *number* [**mode advpn** { **gre** | **udp** } [**ipv6**]]	缺省情况下，设备上不存在任何Tunnel接口 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败
配置Tunnel接口的私网地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**] **ipv6 address** *ipv6-address prefix-length*	二者至少选其一 缺省情况下，Tunnel接口上没有配置私网地址 在同一个Hub组中，所有Tunnel接口的地址应该配置为同一个网段
配置ADVPN隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有配置ADVPN隧道的源端地址和源接口 如果设置的是源端地址，则该地址将作为封装后隧道报文的源地址；如果设置的是源接口，则该接口的地址将作为封装后隧道报文的源地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
（可选）配置ADVPN报文绑定的源端口号	**advpn source-port** *port-number*	缺省情况下，ADVPN报文绑定的源端口号为18001 本命令只有在UDP封装模式的ADVPN隧道类型的Tunnel接口下才能配置 如果Tunnel接口下配置了**compatible**参数，则该Tunnel接口绑定的源端口号必须和其他Tunnel接口不同

操作	命令	说明
配置Tunnel接口绑定的VAM Client	**vam client** *client-name* [**compatible advpn0**]	缺省情况下，Tunnel隧道接口没有绑定任何VAM Client 一个VAM Client只能与一个IPv4 ADVPN类型的Tunnel接口绑定 一个VAM Client只能与一个IPv6 ADVPN隧道类型的Tunnel接口绑定
	vam ipv6 client *client-name*	
（可选）配置ADVPN隧道的私网信息	**advpn network** *ip-address* { *mask-length* | *mask* } [**preference** *preference-value*]	缺省情况下，没有配置ADVPN隧道的私网信息 私网路由的优先级建议高于其他动态路由协议，低于静态路由
	advpn ipv6 network *prefix/prefix-length* [**preference** *preference-value*]	
（可选）配置ADVPN隧道会话的Keepalive报文发送周期及最大发送次数	**keepalive interval** *time-interval* **retry** *retry-times*	缺省情况下，ADVPN隧道会话的Keepalive报文发送周期为180秒，最大发送次数为3次 在同一个ADVPN域中，所有Tunnel接口的Keepalive报文发送周期及最大发送次数必须一致
（可选）配置Spoke-Spoke类型ADVPN隧道的空闲超时时间	**advpn session idle-time** *time-interval*	缺省情况下，Spoke-Spoke类型ADVPN隧道的空闲超时时间为600秒 修改此参数，已经建立的Spoke-Spoke类型ADVPN隧道会使用修改后的参数值重新开始计时
（可选）配置ADVPN隧道连接失败的静默时间	**advpn session dumb-time** *time-interval*	缺省情况下，ADVPN隧道连接失败的静默时间为120秒 修改此参数对已经建立的ADPVN隧道没有影响，之后建立的ADPVN隧道会使用修改后的参数值

说明

如果设备上配置了多个使用 GRE 封装的 ADVPN 隧道接口，且隧道的源端地址或源接口相同时，不同 GRE 封装的 ADVPN 隧道接口的 GRE Key 必须不同。关于 GRE Key 的详细介绍请参见“三层技术-IP 业务配置指导”中的“GRE”。

1.7 配置路由

ADVPN 本身是一个私有网络，因此设备上必须配置路由。ADVPN 隧道建立以后，路由协议通过隧道进行邻居发现、路由更新，并建立路由表。路由协议只在 Hub 和 Spoke 以及各 Hub 之间进行交互，在 Spoke 与 Spoke 之间不直接交换路由信息。

ADVPN 客户端 IPv4 私网支持的路由协议为 OSPF、RIP 和 BGP：

- 采用 OSPF 路由协议时，如果是 Full-Mesh 网络，OSPF 接口的网络类型需要配置为 **broadcast**；如果是 Hub-Spoke 网络，OSPF 接口的网络类型需要配置为 **p2mp**。OSPF 的具体配置请参见“三层技术-IP 路由配置指导”中的“OSPF”。
- 采用 RIP 路由协议时，如果是 Full-Mesh 网络，可以使用 RIP-1 或 RIP-2 广播方式；如果是 Hub-Spoke 网络，需要使用 RIP-2 组播方式，并且关闭水平分割功能。RIP 的具体配置请参见“三层技术-IP 路由配置指导”中的“RIP”。
- 采用 BGP 路由协议时，如果是 Full-Mesh 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端 Spoke 的路由下一跳为对端 Spoke 的地址；如果是 Hub-Spoke 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端 Spoke 的路由下一跳为 Hub 的地址。BGP 和路由策略的具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”和“路由策略”。

ADVPN 客户端 IPv6 私网支持的路由协议为 OSPFv3、RIPng 和 IPv6 BGP：

- 采用 OSPFv3 路由协议时，如果是 Full-Mesh 网络，OSPF 接口的网络类型需要配置为 **broadcast**；如果是 Hub-Spoke 网络，OSPFv3 接口的网络类型需要配置为 **p2mp**。OSPFv3 的具体配置请参见“三层技术-IP 路由配置指导”中的“OSPFv3”
- 采用 RIPng 路由协议时，只支持 Hub-Spoke 网络，并且需要关闭水平分割功能。RIPng 的具体配置请参见“三层技术-IP 路由配置指导”中的“RIPng”
- 采用 IPv6 BGP 路由协议时，如果是 Full-Mesh 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端 Spoke 的路由下一跳为对端 Spoke 的地址；如果是 Hub-Spoke 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端 Spoke 的路由下一跳为 Hub 的地址。IPv6 BGP 和路由策略的具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”和“路由策略”。

1.8 配置IPsec保护ADVPN隧道报文

设备支持用 IPsec 安全框架来保护 ADVPN 隧道数据报文和控制报文的传递，其基本配置思路如下：

(1) 配置 IPsec 安全提议：指定安全协议、认证算法和加密算法、封装模式等。

(2) 配置 IKE 协商方式的 IPsec 安全框架。

(3) 在 ADVPN 隧道接口上应用 IKE 协商方式的 IPsec 安全框架。

详细配置请参见“安全配置指导”中的“IPsec”。

1.9 ADVPN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 ADVPN 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** 命令可以清除相应的统计信息。

表1-26 ADVPN 显示和维护

操作	命令
显示注册到 VAM Server 上的 VAM Client 的 IPv4 私网地址映射信息	**display vam server address-map** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]] [**verbose**]

操作	命令
显示注册到 VAM Server 上的 VAM Client 的 IPv6 私网地址映射信息	**display vam server ipv6 address-map** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]] [**verbose**]
显示注册到 VAM Server 上的 VAM Client 的 IPv4 私网信息。	**display vam server private-network** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]
显示注册到 VAM Server 上的 VAM Client 的 IPv6 私网信息。	**display vam server ipv6 private-network** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]
显示VAM Server上ADVPN域的统计信息	**display vam server statistics** [**advpn-domain** *domain-name*]
显示 VAM Client 的状态机信息	**display vam client fsm** [**name** *client-name*]
显示 VAM Client 的统计信息	**display vam client statistics** [**name** *client-name*]
显示 VAM Client 收到的 VAM Server 下发的跨 Hub 组建立 IPv4 Spoke-Spoke 直连隧道的规则	**display vam client shortcut interest** [**name** *client-name*]
显示 VAM Client 收到的 VAM Server 下发的跨 Hub 组建立 IPv6 Spoke-Spoke 直连隧道的规则	**display vam client shortcut ipv6 interest** [**name** *client-name*]
显示IPv4 ADVPN隧道的信息	**display advpn session** [**interface tunnel** *number* [**private-address** *private-ip-address*]] [**verbose**]
显示IPv6 ADVPNr隧道的信息	**display advpn ipv6 session** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]] [**verbose**]
清除注册到VAM Server上的IPv4私网地址映射信息	**reset vam server address-map** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]
清除注册到VAM Server上的IPv6私网地址映射信息	**reset vam server ipv6 address-map** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]
清除VAM Server上ADVPN域的统计信息	**reset vam server statistics** [**advpn-domain** *domain-name*]
重置VAM Client的状态机	**reset vam client fsm** [**name** *client-name*]
清除VAM Client的统计信息	**reset vam client statistics** [**name** *client-name*]
删除IPv4 ADVPN隧道	**reset advpn session statistics** [**interface tunnel** *number* [**private-address** *private-ip-address*]]
删除IPv6 ADVPN隧道	**reset advpn ipv6 session statistics** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]
清除IPv4 ADVPN隧道的统计信息	**reset advpn session statistics** [**interface tunnel** *number* [**private-address** *private-ip-address*]]
清除IPv6 ADVPN隧道的统计信息	**reset advpn ipv6 session statistics** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]

1.10 ADVPN典型配置举例

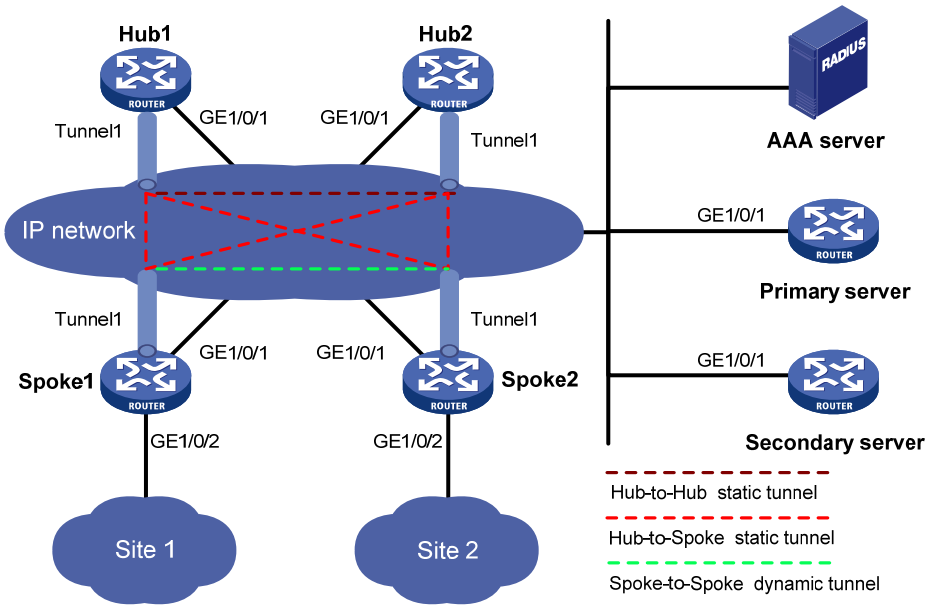
1.10.1 IPv4 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在 IPv4 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立隧道连接。

2. 组网图

图1-7 IPv4 Full-Mesh 类型 ADVPN 组网图



Hub 1	GE1/0/1	1.0.0.1/24	Spoke 1	GE1/0/1	1.0.0.3/24
	Tunnel1	192.168.0.1/24		GE1/0/2	192.168.1.1/24
Hub 2	GE1/0/1	1.0.0.2/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE1/0/1	1.0.0.4/24
AAA server		1.0.0.10/24		GE1/0/2	192.168.2.1/24
Primary server	GE1/0/1	1.0.0.11/24		Tunnel1	192.168.0.4/24
Secondary server	GE1/0/1	1.0.0.12/24			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
```

```
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥为 123456。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 Hub2，密码为 Hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2
```

```
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 0
```

```
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
```

```
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address              Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                    Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                    Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                    Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                    Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address              Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                    Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                    Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                    Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                    Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.0.2      1.0.0.2                     --    H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                     --    H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.4                     --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                     --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                     --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                     --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                     --    S-H   Success    0H 46M  8S
192.168.0.4      1.0.0.4                     --    S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。

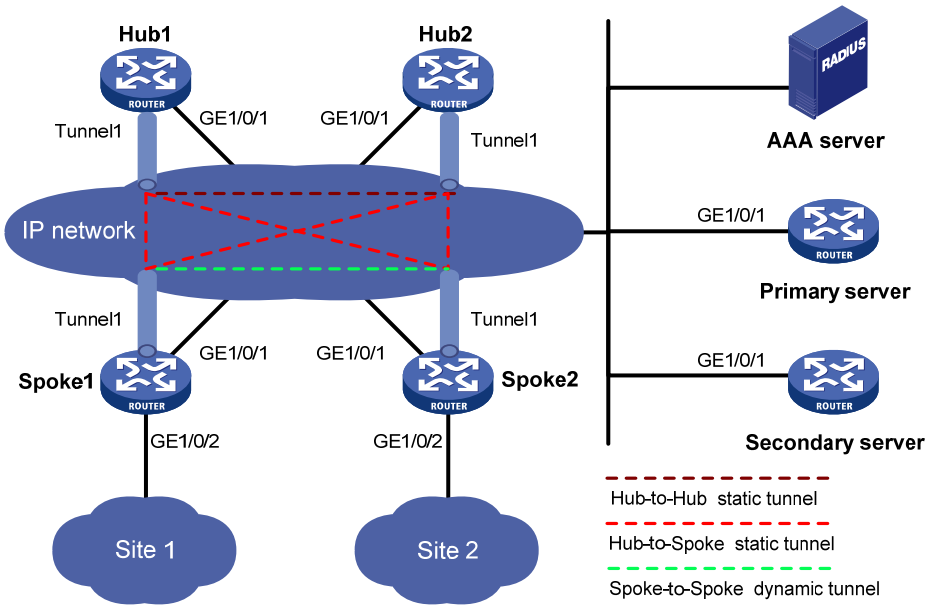
1.10.2 IPv6 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在 IPv6 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立隧道连接。

2. 组网图

图1-8 IPv6 Full-Mesh 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE1/0/1	1::1/64	Spoke 1	GE1/0/1	1::3/64
	Tunnel1	192:168::1/64		GE1/0/2	192:168:1::1/64
Hub 2	GE1/0/1	1::2/64		Tunnel1	192:168::3/64
	Tunnel1	192:168::2/64	Spoke 2	GE1/0/1	1::4/64
AAA server		1::10/64		GE1/0/2	192:168:2::1/64
Primary server	GE1/0/1	1::11/64		Tunnel1	192:168::4/64
Secondary server	GE1/0/1	1::12/64			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
```

```
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke ipv6 private-address network
192:168::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置主、被 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
[Hub1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装模式的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre ipv6
[Hub1-Tunnel1] ipv6 address 192:168::1 64
[Hub1-Tunnel1] ipv6 address fe80::1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1
[Hub1-Tunnel1] ospfv3 1 area 0
[Hub1-Tunnel1] ospfv3 network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）

- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre ipv6
[Hub2-Tunnel1] ipv6 address 192:168::2 64
```

```
[Hub1-Tunnel1] ipv6 address fe80::2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2
[Hub2-Tunnel1] ospfv3 1 area 0
[Hub2-Tunnel1] ospfv3 network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.3
[Spoke1-ospfv3-1] area 0
[Spoke1-ospfv3-1-area-0.0.0.0] quit
[Spoke1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre ipv6
[Spoke1-Tunnel1] ipv6 address 192:168::3 64
[Hub1-Tunnel1] ipv6 address fe80::3 link-local
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 0
[Spoke1-Tunnel1] ospfv3 network-type broadcast
[Spoke1-Tunnel1] ospfv3 dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.4
[Spoke2-ospfv3-1] area 0
[Spoke2-ospfv3-1-area-0.0.0.0] quit
[Spoke2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre ipv6
[Spoke2-Tunnel1] ipv6 address 192:168::4 64
[Hub1-Tunnel1] ipv6 address fe80::4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 0
[Spoke2-Tunnel1] ospfv3 network-type broadcast
[Spoke2-Tunnel1] ospfv3 dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
```

```
0          192:168::2           1::2                 Hub    No   0H 47M 31S
0          192:168::3           1::3                 Spoke  No   0H 28M 25S
0          192:168::4           1::4                 Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  --    H-H   Success    0H 46M  8S
192:168::3            1::3                  --    H-S   Success    0H 27M 27S
192:168::4            1::4                  --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192:168::4。

```
[Spoke2] ping ipv6 192:168::4
Ping6(56 data bytes) 192:168::4 --> 192:168::4, press CTRL_C to break
56 bytes from 192:168::4, icmp_seq=0 hlim=64 time=3.000 ms
56 bytes from 192:168::4, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 192:168::4, icmp_seq=2 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=4 hlim=64 time=1.000 ms

--- Ping6 statistics for 192:168::4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.200/3.000/0.980 ms
```

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
192.168::4            1::4                  --    S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。

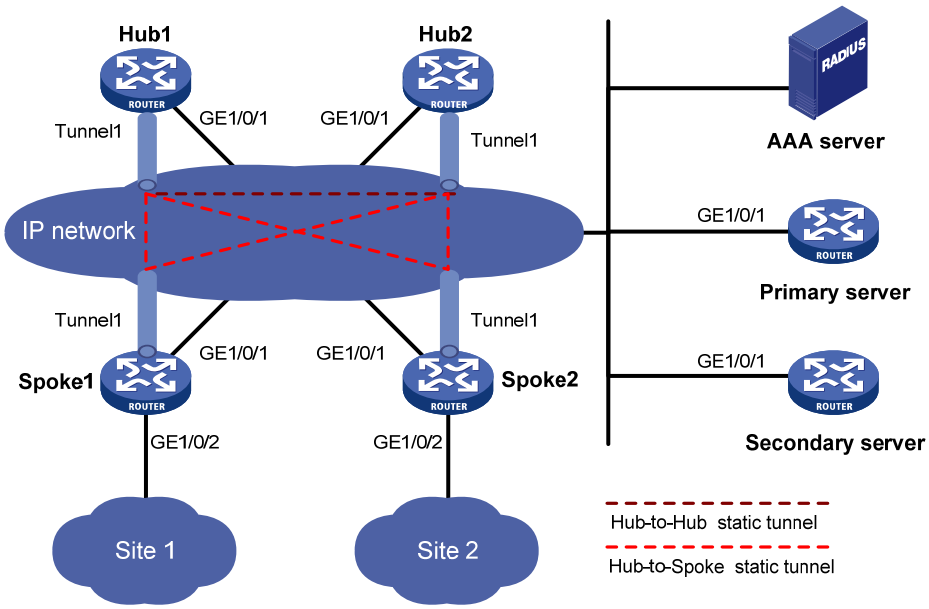
1.10.3 IPv4 Hub-Spoke类型ADVPN典型配置举例

1. 组网需求

- 在 IPv4 Hub-Spoke 的组网方式下，数据通过 Hub-Spoke 隧道进行转发。主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。

2. 组网图

图1-9 IPv4 Hub-Spoke 类型 ADVPN 组网图



Hub 1	GE1/0/1	1.0.0.1/24	Spoke 1	GE1/0/1	1.0.0.3/24
	Tunnel1	192.168.0.1/24		GE1/0/2	192.168.1.1/24
Hub 2	GE1/0/1	1.0.0.2/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE1/0/1	1.0.0.4/24
AAA server		1.0.0.10/24		GE1/0/2	192.168.2.1/24
Primary server	GE1/0/1	1.0.0.11/24		Tunnel1	192.168.0.4/24
Secondary server	GE1/0/1	1.0.0.12/24			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
```

```
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```
配置 ISP 域的 AAA 方案。
```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```
- 配置 VAM Server

创建 ADVPN 域 abc。
```
[PrimaryServer] vam server advpn-domain abc id 1
```
创建 Hub 组 0。
```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```
指定 Hub 组内 Hub 的 IPv4 私网地址。
```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
```
指定 Hub 组内 Spoke 的 IPv4 私网地址范围。
```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```
配置 VAM Server 的预共享密钥为 123456。
```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```
配置对 VAM Client 进行 CHAP 认证。
```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```
启动该 ADVPN 域的 VAM Server 功能。
```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```
(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。
```
<Hub1> system-view
[Hub1] vam client name Hub1
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub1-vam-client-Hub1] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub1，密码为 hub1。
```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```
配置 VAM Server 的 IP 地址。
```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.11
```

```
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type p2mp
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 Hub2，密码为 Hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2
[Hub2-Tunnel1] ospf network-type p2mp
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
```

```
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 0
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
```

```
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type p2mp
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
```

```
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type p2mp
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                   Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
```

```
Private address  Public address              Port  Type  State      Holding time
192.168.0.2      1.0.0.2                    --    H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                    --    H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.4                    --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                    --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                    --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

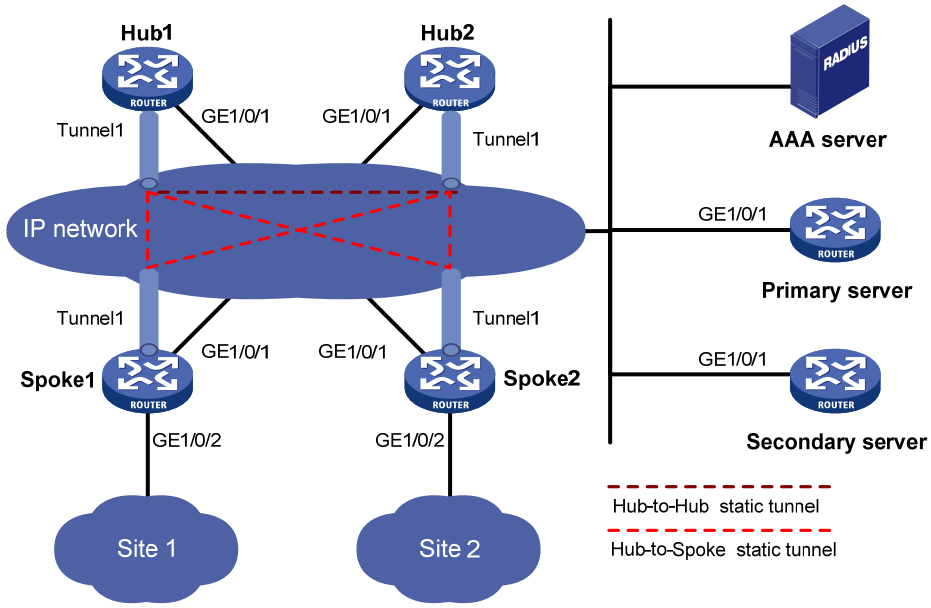
1.10.4 IPv6 Hub-Spoke类型ADVPN典型配置举例

1. 组网需求

- 在 IPv6 Hub-Spoke 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。

2. 组网图

图1-10 IPv6 Hub-Spoke 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE1/0/1	1::1/64	Spoke 1	GE1/0/1	1::3/64
	Tunnel1	192:168::1/64		GE1/0/2	192:168:1::1/64
Hub 2	GE1/0/1	1::2/64		Tunnel1	192:168::3/64
	Tunnel1	192:168::2/64	Spoke 2	GE1/0/1	1::4/64
AAA server		1::10/64		GE1/0/2	192:168:2::1/64
Primary server	GE1/0/1	1::11/64		Tunnel1	192:168::4/64
Secondary server	GE1/0/1	1::12/64			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
```

```
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke ipv6 private-address network
192:168::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
```

```
[Hub1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre ipv6
[Hub1-Tunnel1] ipv6 address 192:168::1 64
[Hub1-Tunnel1] ipv6 address fe80::1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1
[Hub1-Tunnel1] ospfv3 1 area 0
[Hub1-Tunnel1] ospfv3 network-type p2mp
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre ipv6
[Hub2-Tunnel1] ipv6 address 192:168::2 64
[Hub1-Tunnel1] ipv6 address fe80::2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2
[Hub2-Tunnel1] ospfv3 1 area 0
[Hub2-Tunnel1] ospfv3 network-type p2mp
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.3
[Spoke1-ospfv3-1] area 0
[Spoke1-ospfv3-1-area-0.0.0.0] quit
[Spoke1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre ipv6
[Spoke1-Tunnel1] ipv6 address 192:168::3 64
[Hub1-Tunnel1] ipv6 address fe80::3 link-local
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 0
[Spoke1-Tunnel1] ospfv3 network-type p2mp
[Spoke1-Tunnel1] ospfv3 dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 的功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
```

```
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.4
[Spoke2-ospfv3-1] area 0
[Spoke2-ospfv3-1-area-0.0.0.0] quit
[Spoke2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre ipv6
[Spoke2-Tunnel1] ipv6 address 192:168::4 64
[Hub1-Tunnel1] ipv6 address fe80::4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 0
[Spoke2-Tunnel1] ospfv3 network-type p2mp
[Spoke2-Tunnel1] ospfv3 dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
```

```
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  --    H-H   Success    0H 46M  8S
192:168::3            1::3                  --    H-S   Success    0H 27M 27S
192:168::4            1::4                  --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192:168::4。

```
[Spoke2] ping ipv6 192:168::4
Ping6(56 data bytes) 192:168::4 --> 192:168::4, press CTRL_C to break
56 bytes from 192:168::4, icmp_seq=0 hlim=64 time=3.000 ms
56 bytes from 192:168::4, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 192:168::4, icmp_seq=2 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=4 hlim=64 time=1.000 ms

--- Ping6 statistics for 192:168::4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.200/3.000/0.980 ms
```

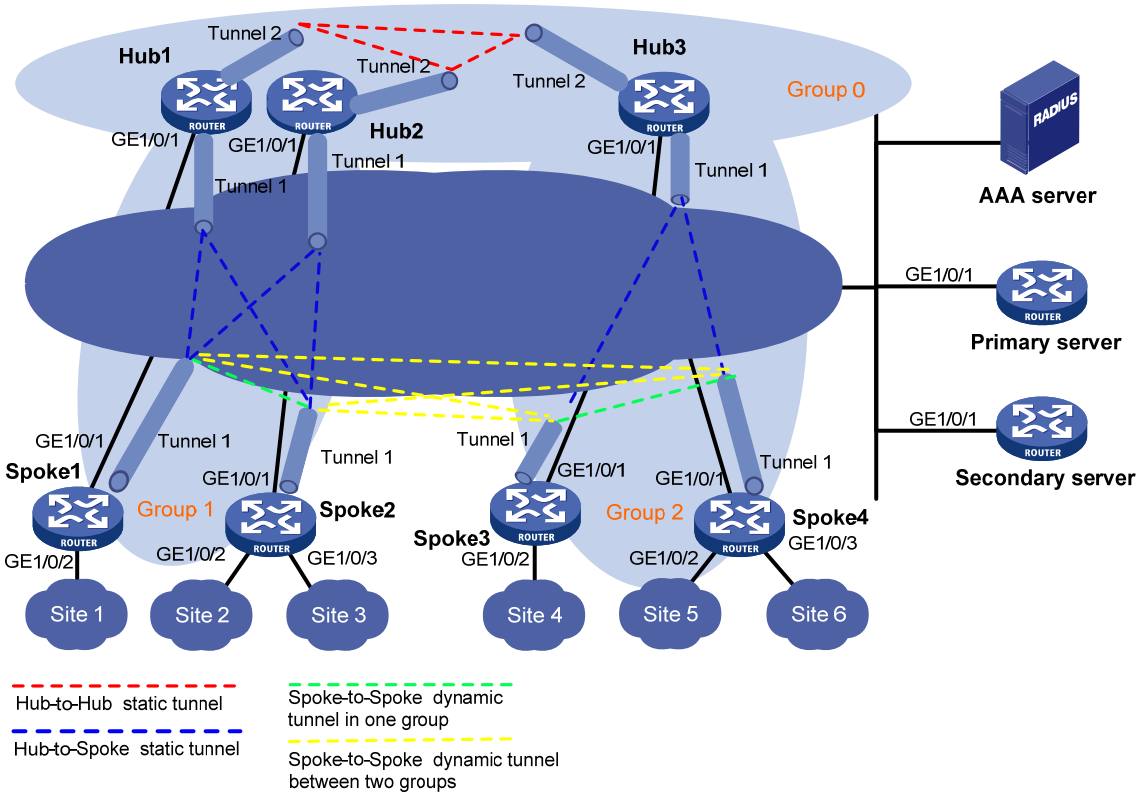
1.10.5 大规模IPv4 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在大规模 IPv4 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立隧道连接。

2. 组网图

图1-11 大规模 IPv4 Full-Mesh 类型 ADVPN 组网图



Hub 1	GE1/0/1	1.0.0.1/24	Spoke 1	GE1/0/1	1.0.0.4/24
	Tunnel1	192.168.1.1/24		GE1/0/2	192.168.10.1/24
	Tunnel2	192.168.0.1/24		Tunnel1	192.168.1.3/24
Hub 2	GE1/0/1	1.0.0.2/24	Spoke 2	GE1/0/1	1.0.0.5/24
	Tunnel1	192.168.1.2/24		GE1/0/2	192.168.20.1/24
	Tunnel2	192.168.0.2/24		GE1/0/3	192.168.30.1/24
Hub 3	GE1/0/1	1.0.0.3/24		Tunnel1	192.168.1.4/24
	Tunnel1	192.168.2.1/24	Spoke 3	GE1/0/1	1.0.0.6/24
	Tunnel2	192.168.0.3/24		GE1/0/2	192.168.40.1/24
AAA server		1.0.0.10/24		Tunnel1	192.168.2.2/24
Primary server	GE1/0/1	1.0.0.11/24	Spoke 4	GE1/0/1	1.0.0.7/24
Secondary server	GE1/0/1	1.0.0.12/24		GE1/0/2	192.168.50.1/24
				GE1/0/3	192.168.60.1/24
				Tunnel1	192.168.2.3/24

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
[PrimaryServer-radius-abc] key authentication simple 123
```

```
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.3
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

创建 Hub 组 1。

```
[PrimaryServer-vam-server-domain-abc] hub-group 1
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub private-address 192.168.1.1
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub private-address 192.168.1.2
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] spoke private-address network
192.168.1.0 255.255.255.0
```

允许建立跨组 Spoke-Spoke 直连隧道。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut interest all
[PrimaryServer-vam-server-domain-abc-hub-group-1] quit
```

创建 Hub 组 2。

```
[PrimaryServer-vam-server-domain-abc] hub-group 2
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] hub private-address 192.168.2.1
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] spoke private-address network
192.168.2.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut interest all
[PrimaryServer-vam-server-domain-abc-hub-group-2] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1Group0。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1Group0] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1Group0] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1Group0] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1Group0] client enable
[Hub1-vam-client-Hub1Group0] quit
```

创建 VAM Client Hub1Group1。

```
[Hub1] vam client name Hub1Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1Group1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1Group1] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1Group1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1Group1] client enable
[Hub1-vam-client-Hub1Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
```

```
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] area 1
[Hub1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.1] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ip address 192.168.1.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1Group1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1Group0
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2Group0。

```
<Hub2> system-view
[Hub2] vam client name Hub2Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group0] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group0] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2Group0] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group0] client enable
[Hub2-vam-client-Hub2Group0] quit
```

创建 VAM Client Hub2Group1。

```
[Hub2] vam client name Hub2Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group1] user Hub2 password simple Hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group1] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2Group1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group1] client enable
[Hub2-vam-client-Hub2Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] area 1
[Hub2-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.1] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ip address 192.168.1.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2Group1
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2Group0
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Hub3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub3Group0。

```
<Hub3> system-view
[Hub3] vam client name Hub3Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group0] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group0] server primary ip-address 1.0.0.11
[Hub3-vam-client-Hub3Group0] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group0] client enable
[Hub3-vam-client-Hub3Group0] quit
```

创建 VAM Client Hub3Group1。

```
[Hub3] vam client name Hub3Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group1] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group1] server primary ip-address 1.0.0.11
[Hub3-vam-client-Hub3Group1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group1] client enable
[Hub3-vam-client-Hub3Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub3] ike keychain advpn
[Hub3-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub3-ike-keychain-abc] quit
[Hub3] ike profile abc
[Hub3-ike-profile-abc] keychain abc
[Hub3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub3] ipsec transform-set abc
[Hub3-ipsec-transform-set-abc] encapsulation-mode transport
[Hub3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub3-ipsec-transform-set-abc] quit
[Hub3] ipsec profile abc isakmp
[Hub3-ipsec-profile-isakmp-abc] transform-set abc
[Hub3-ipsec-profile-isakmp-abc] ike-profile abc
[Hub3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub3] ospf 1
[Hub3-ospf-1] area 0
[Hub3-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub3-ospf-1-area-0.0.0.0] quit
[Hub3-ospf-1] area 2
[Hub3-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Hub3-ospf-1-area-0.0.0.2] quit
[Hub3-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub3] interface tunnel1 mode advpn udp
[Hub3-Tunnel1] ip address 192.168.2.1 255.255.255.0
[Hub3-Tunnel1] vam client Hub3Group1
[Hub3-Tunnel1] ospf network-type broadcast
[Hub3-Tunnel1] source gigabitethernet 1/0/1
[Hub3-Tunnel1] tunnel protection ipsec profile abc
[Hub3-Tunnel1] undo shutdown
[Hub3-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub3] interface tunnel1 mode advpn udp
[Hub3-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Hub3-Tunnel1] vam client Hub3Group0
[Hub3-Tunnel1] ospf network-type broadcast
[Hub3-Tunnel1] source gigabitethernet 1/0/1
[Hub3-Tunnel1] tunnel protection ipsec profile abc
[Hub3-Tunnel1] undo shutdown
[Hub3-Tunnel1] quit
```

(6) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 1
[Spoke1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.1] network 192.168.10.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.1] quit
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ip address 192.168.1.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] advpn network 192.168.10.0 255.255.255.0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(7) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 1
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.30.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ip address 192.168.1.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] advpn network 192.168.20.0 255.255.255.0
[Spoke2-Tunnel1] advpn network 192.168.30.0 255.255.255.0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(8) 配置 Spoke3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke3。

```
<Spoke3> system-view
[Spoke3] vam client name Spoke3
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke3-vam-client-Spoke3] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke3-vam-client-Spoke3] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke3，密码为 spoke3。

```
[Spoke3-vam-client-Spoke3] user spoke3 password simple spoke3
```

配置 VAM Server 的 IP 地址。

```
[Spoke3-vam-client-Spoke3] server primary ip-address 1.0.0.11
[Spoke3-vam-client-Spoke3] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke3-vam-client-Spoke3] client enable
[Spoke3-vam-client-Spoke3] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke3] ike keychain advpn
[Spoke3-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke3-ike-keychain-abc] quit
[Spoke3] ike profile abc
[Spoke3-ike-profile-abc] keychain abc
[Spoke3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke3] ipsec transform-set abc
[Spoke3-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke3-ipsec-transform-set-abc] quit
[Spoke3] ipsec profile abc isakmp
[Spoke3-ipsec-profile-isakmp-abc] transform-set abc
[Spoke3-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke3] ospf 1
[Spoke3-ospf-1] area 2
[Spoke3-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Spoke3-ospf-1-area-0.0.0.2] network 192.168.40.0 0.0.0.255
[Spoke3-ospf-1-area-0.0.0.2] quit
[Spoke3-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke3] interface tunnel1 mode advpn udp
[Spoke3-Tunnel1] ip address 192.168.2.2 255.255.255.0
```

```
[Spoke3-Tunnel1] vam client Spoke3
[Spoke3-Tunnel1] ospf network-type broadcast
[Spoke3-Tunnel1] ospf dr-priority 0
[Spoke3-Tunnel1] advpn network 192.168.40.0 255.255.255.0
[Spoke3-Tunnel1] source gigabitethernet 1/0/1
[Spoke3-Tunnel1] tunnel protection ipsec profile abc
[Spoke3-Tunnel1] undo shutdown
[Spoke3-Tunnel1] quit
```

(9) 配置 Spoke4

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke4。

```
<Spoke4> system-view
[Spoke4] vam client name Spoke4
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke4-vam-client-Spoke4] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke4-vam-client-Spoke4] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke4，密码为 spoke4。

```
[Spoke4-vam-client-Spoke4] user spoke4 password simple spoke4
```

配置 VAM Server 的 IP 地址。

```
[Spoke4-vam-client-Spoke4] server primary ip-address 1.0.0.11
[Spoke4-vam-client-Spoke4] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke4-vam-client-Spoke4] client enable
[Spoke4-vam-client-Spoke4] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke4] ike keychain advpn
[Spoke4-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke4-ike-keychain-abc] quit
[Spoke4] ike profile abc
[Spoke4-ike-profile-abc] keychain abc
[Spoke4-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke4] ipsec transform-set abc
[Spoke4-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke4-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke4-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke4-ipsec-transform-set-abc] quit
[Spoke4] ipsec profile abc isakmp
[Spoke4-ipsec-profile-isakmp-abc] transform-set abc
[Spoke4-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke4-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke4] ospf 1
[Spoke4-ospf-1] area 2
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.50.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.60.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] quit
[Spoke4-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke4] interface tunnel1 mode advpn udp
[Spoke4-Tunnel1] ip address 192.168.2.3 255.255.255.0
[Spoke4-Tunnel1] vam client Spoke4
[Spoke4-Tunnel1] ospf network-type broadcast
[Spoke4-Tunnel1] ospf dr-priority 0
[Spoke4-Tunnel1] advpn network 192.168.50.0 255.255.255.0
[Spoke4-Tunnel1] advpn network 192.168.60.0 255.255.255.0
[Spoke4-Tunnel1] source gigabitethernet 1/0/1
[Spoke4-Tunnel1] tunnel protection ipsec profile abc
[Spoke4-Tunnel1] undo shutdown
[Spoke4-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Hub    No   0H 28M 25S
1          192.168.1.1      1.0.0.1                   Hub    No   0H 52M  7S
1          192.168.1.2      1.0.0.2                   Hub    No   0H 47M 31S
1          192.168.1.3      1.0.0.4                   Spoke  No   0H 18M 26S
1          192.168.1.4      1.0.0.5                   Spoke  No   0H 28M 25S
2          192.168.2.1      1.0.0.3                   Hub    No   0H 28M 25S
2          192.168.2.2      1.0.0.6                   Spoke  No   0H 25M 40S
2          192.168.2.3      1.0.0.7                   Spoke  No   0H 25M 31S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Hub    No   0H 28M 25S
1          192.168.1.1      1.0.0.1                   Hub    No   0H 52M  7S
1          192.168.1.2      1.0.0.2                   Hub    No   0H 47M 31S
```

```
1          192.168.1.3      1.0.0.4                    Spoke  No   0H 18M 26S
1          192.168.1.4      1.0.0.5                    Spoke  No   0H 28M 25S
2          192.168.2.1      1.0.0.3                    Hub    No   0H 28M 25S
2          192.168.2.2      1.0.0.6                    Spoke  No   0H 25M 40S
2          192.168.2.3      1.0.0.7                    Spoke  No   0H 25M 31S
```

以上显示信息表示 Hub1、Hub2、Hub3、Spoke1、Spoke2、Spoke3 和 Spoke4 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.1.2      1.0.0.2                     18001 H-H   Success    0H 46M  8S
192.168.1.3      1.0.0.3                     18001 H-S   Success    0H 27M 27S
192.168.1.4      1.0.0.4                     18001 H-S   Success    0H 18M 18S

Interface         : Tunnel2
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.0.2      1.0.0.2                     18001 H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                     18001 H-H   Success    0H 27M 27S
```

以上显示信息表示 Hub1 与 Hub2、Hub3、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.1.1      1.0.0.1                     18001 S-H   Success    0H 46M  8S
192.168.1.2      1.0.0.2                     18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

显示 Spoke3 上的 IPv4 ADVPN 隧道信息。

```
[Spoke3] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.2.1      1.0.0.3                     18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke3 与 Hub3 建立了 Hub-Spoke 永久隧道。Spoke4 上的显示信息与 Spoke3 类似。

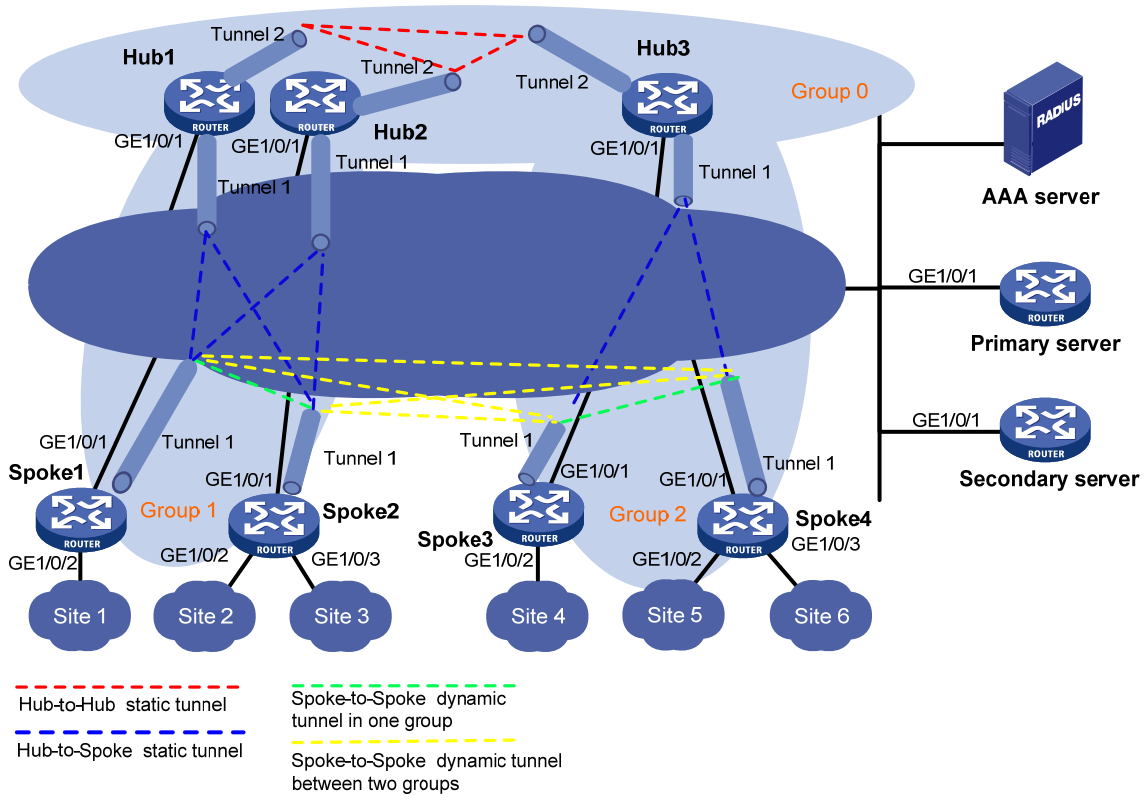
1.10.6 大规模IPv6 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在大规模 IPv6 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立隧道连接。

2. 组网图

图1-12 大规模 IPv6 Full-Mesh 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE1/0/1	1::1/64	Spoke 1	GE1/0/1	1::4/64
	Tunnel1	192:168:1::1/64		GE1/0/2	192:168:10::1/64
	Tunnel2	192:168::1/64		Tunnel1	192:168:1::3/64
Hub 2	GE1/0/1	1::2/64	Spoke 2	GE1/0/1	1::5/64
	Tunnel1	192:168:1::2/64		GE1/0/2	192:168:20::1/64
	Tunnel2	192:168::2/64		GE1/0/3	192:168:30::1/64
Hub 3	GE1/0/1	1::3/64		Tunnel1	192:168:1::4/64
	Tunnel1	192:168:2::1/64	Spoke 3	GE1/0/1	1::6/64
	Tunnel2	192:168::3/64		GE1/0/2	192:168:40::1/64
AAA server		1::10/64		Tunnel1	192:168:2::2/64
Primary server	GE1/0/1	1::11/64	Spoke 4	GE1/0/1	1::7/64
Secondary server	GE1/0/1	1::12/64		GE1/0/2	192:168:50::1/64
				GE1/0/3	192:168:60::1/64
				Tunnel1	192:168:2::3/64

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::3
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

创建 Hub 组 1。

```
[PrimaryServer-vam-server-domain-abc] hub-group 1
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub ipv6 private-address 192:168:1::1
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub ipv6 private-address 192:168:1::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] spoke ipv6 private-address network
192:168:1::0 64
```

允许建立跨组 Spoke-Spoke 直连隧道。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut ipv6 interest all
[PrimaryServer-vam-server-domain-abc-hub-group-1] quit
```

创建 Hub 组 2。

```
[PrimaryServer-vam-server-domain-abc] hub-group 2
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] hub ipv6 private-address 192:168:2::1
```
指定 Hub 组内 Spoke 的 IPv6 私网地址范围。
```
[PrimaryServer-vam-server-domain-abc-hub-group-2] spoke ipv6 private-address network
192:168:2::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut ipv6 interest all
[PrimaryServer-vam-server-domain-abc-hub-group-2] quit
```
配置 VAM Server 的预共享密钥为 123456。
```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```
配置对 VAM Client 进行 CHAP 认证。
```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```
启动该 ADVPN 域的 VAM Server 功能。
```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```
(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1Group0。
```
<Hub1> system-view
[Hub1] vam client name Hub1Group0
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub1-vam-client-Hub1Group0] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub1-vam-client-Hub1Group0] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub1，密码为 hub1。
```
[Hub1-vam-client-Hub1Group0] user hub1 password simple hub1
```
配置 VAM Server 的 IP 地址。
```
[Hub1-vam-client-Hub1Group0] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1Group0] server secondary ipv6-address 1::12
```
开启 VAM Client 功能。
```
[Hub1-vam-client-Hub1Group0] client enable
[Hub1-vam-client-Hub1Group0] quit
```
创建 VAM Client Hub1Group1。
```
[Hub1] vam client name Hub1Group1
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub1-vam-client-Hub1Group1] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub1-vam-client-Hub1Group1] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub1，密码为 hub1。
```
[Hub1-vam-client-Hub1Group1] user hub1 password simple hub1
```
配置 VAM Server 的 IP 地址。
```
[Hub1-vam-client-Hub1Group1] server primary ipv6-address 1::11
```

```
[Hub1-vam-client-Hub1Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1Group1] client enable
[Hub1-vam-client-Hub1Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain advpn
[Hub1-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] area 1
[Hub1-ospfv3-1-area-0.0.0.1] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ipv6 address 192:168:1::1 64
[Hub1-Tunnel1] ipv6 address fe80::1:1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1Group1
[Hub1-Tunnel1] ospfv3 1 area 1
[Hub1-Tunnel1] ospfv3 network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub1] interface tunnel2 mode advpn udp
[Hub1-Tunnel2] ipv6 address 192:168::1 64
```

```
[Hub1-Tunnel2] ipv6 address fe80::1 link-local
[Hub1-Tunnel2] vam ipv6 client Hub1Group0
[Hub1-Tunnel2] ospfv3 1 area 0
[Hub1-Tunnel2] ospf network-type broadcast
[Hub1-Tunnel2] source gigabitethernet 1/0/1
[Hub1-Tunnel2] tunnel protection ipsec profile abc
[Hub1-Tunnel2] undo shutdown
[Hub1-Tunnel2] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2Group0。

```
<Hub2> system-view
[Hub2] vam client name Hub2Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group0] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group0] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2Group0] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group0] client enable
[Hub2-vam-client-Hub2Group0] quit
```

创建 VAM Client Hub2Group1。

```
[Hub2] vam client name Hub2Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group1] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group1] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group1] client enable
[Hub2-vam-client-Hub2Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain advpn
[Hub2-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
```

```
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] area 1
[Hub2-ospfv3-1-area-0.0.0.1] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ipv6 address 192:168:1::2 64
[Hub2-Tunnel1] ipv6 address fe80::1:2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2Group1
[Hub2-Tunnel1] ospfv3 1 area 1
[Hub2-Tunnel1] ospfv3 network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub2] interface tunnel2 mode advpn udp
[Hub2-Tunnel2] ipv6 address 192:168::2 64
[Hub2-Tunnel2] ipv6 address fe80::2 link-local
[Hub2-Tunnel2] vam ipv6 client Hub2Group0
[Hub2-Tunnel2] ospfv3 1 area 0
[Hub2-Tunnel2] ospfv3 network-type broadcast
[Hub2-Tunnel2] source gigabitethernet 1/0/1
[Hub2-Tunnel2] tunnel protection ipsec profile abc
[Hub2-Tunnel2] undo shutdown
[Hub2-Tunnel2] quit
```

(5) 配置 Hub3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub3Group0。

```
<Hub3> system-view
[Hub3] vam client name Hub3Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group0] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group0] server primary ipv6-address 1::11
[Hub3-vam-client-Hub3Group0] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group0] client enable
[Hub3-vam-client-Hub3Group0] quit
```

创建 VAM Client Hub3Group1。

```
[Hub3] vam client name Hub3Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group1] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group1] server primary ipv6-address 1::11
[Hub3-vam-client-Hub3Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group1] client enable
[Hub3-vam-client-Hub3Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub3] ike keychain advpn
[Hub3-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Hub3-ike-keychain-abc] quit
[Hub3] ike profile abc
[Hub3-ike-profile-abc] keychain abc
[Hub3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub3] ipsec transform-set abc
[Hub3-ipsec-transform-set-abc] encapsulation-mode transport
[Hub3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub3-ipsec-transform-set-abc] esp authentication-algorithm sha1
```

```
[Hub3-ipsec-transform-set-abc] quit
[Hub3] ipsec profile abc isakmp
[Hub3-ipsec-profile-isakmp-abc] transform-set abc
[Hub3-ipsec-profile-isakmp-abc] ike-profile abc
[Hub3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Hub3] ospfv3 1
[Hub3-ospfv3-1] router-id 0.0.0.3
[Hub3-ospfv3-1] area 0
[Hub3-ospfv3-1-area-0.0.0.0] quit
[Hub3-ospfv3-1] area 2
[Hub3-ospfv3-1-area-0.0.0.2] quit
[Hub3-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub3] interface tunnel1 mode advpn udp
[Hub3-Tunnel1] ipv6 address 192:168:2::1 64
[Hub3-Tunnel1] ipv6 address fe80::2:1 link-local
[Hub3-Tunnel1] vam ipv6 client Hub3Group1
[Hub3-Tunnel1] ospfv3 1 area 2
[Hub3-Tunnel1] ospfv3 network-type broadcast
[Hub3-Tunnel1] source gigabitethernet 1/0/1
[Hub3-Tunnel1] tunnel protection ipsec profile abc
[Hub3-Tunnel1] undo shutdown
[Hub3-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub3] interface tunnel2 mode advpn udp
[Hub3-Tunnel2] ipv6 address 192:168::3 64
[Hub3-Tunnel2] ipv6 address fe80::3 link-local
[Hub3-Tunnel2] vam ipv6 client Hub3Group0
[Hub3-Tunnel2] ospfv3 1 area 0
[Hub3-Tunnel2] ospfv3 network-type broadcast
[Hub3-Tunnel2] source gigabitethernet 1/0/1
[Hub3-Tunnel2] tunnel protection ipsec profile abc
[Hub3-Tunnel2] undo shutdown
[Hub3-Tunnel2] quit
```

(6) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain advpn
[Spoke1-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.4
[Spoke1-ospfv3-1] area 0
[Spoke1-ospfv3-1-area-0.0.0.0] quit
[Spoke1-ospfv3-1] area 1
[Spoke1-ospfv3-1-area-0.0.0.1] quit
[Spoke1-ospfv3-1] quit
[Spoke1] interface gigabitethernet 1/0/2
[Spoke1-GigabitEthernet1/0/2] ospfv3 1 area 1
[Spoke1-GigabitEthernet1/0/2] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ipv6 address 192:168:1::3 64
[Spoke1-Tunnel1] ipv6 address fe80::1:3 link-local
```

```
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 1
[Spoke1-Tunnel1] ospfv3 network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] advpn ipv6 network 192:168:10::0 64
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(7) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain advpn
[Spoke2-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.5
[Spoke2-ospfv3-1] area 0
[Spoke2-ospfv3-1-area-0.0.0.0] quit
[Spoke2-ospfv3-1] area 1
[Spoke2-ospfv3-1-area-0.0.0.1] quit
[Spoke2-ospfv3-1] quit
[Spoke1] interface gigabitethernet 1/0/2
[Spoke1-GigabitEthernet1/0/2] ospfv3 1 area 1
[Spoke1-GigabitEthernet1/0/2] quit
[Spoke1] interface gigabitethernet 1/0/3
[Spoke1-GigabitEthernet1/0/3] ospfv3 1 area 1
[Spoke1-GigabitEthernet1/0/3] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ipv6 address 192:168:1::4 64
[Spoke2-Tunnel1] ipv6 address fe80::1:4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 1
[Spoke2-Tunnel1] ospfv3 network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] advpn ipv6 network 192:168:20::0 64
[Spoke2-Tunnel1] advpn ipv6 network 192:168:30::0 64
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(8) 配置 Spoke3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke3。

```
<Spoke3> system-view
[Spoke3] vam client name Spoke3
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke3-vam-client-Spoke3] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke3-vam-client-Spoke3] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke3，密码为 spoke3。

```
[Spoke3-vam-client-Spoke3] user spoke3 password simple spoke3
```

配置 VAM Server 的 IP 地址。

```
[Spoke3-vam-client-Spoke3] server primary ipv6-address 1::11
[Spoke3-vam-client-Spoke3] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke3-vam-client-Spoke3] client enable
[Spoke3-vam-client-Spoke3] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke3] ike keychain advpn
[Spoke3-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke3-ike-keychain-abc] quit
[Spoke3] ike profile abc
[Spoke3-ike-profile-abc] keychain abc
[Spoke3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke3] ipsec transform-set abc
[Spoke3-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke3-ipsec-transform-set-abc] quit
[Spoke3] ipsec profile abc isakmp
[Spoke3-ipsec-profile-isakmp-abc] transform-set abc
[Spoke3-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke3] ospfv3 1
[Spoke3-ospfv3-1] router-id 0.0.0.6
[Spoke3-ospfv3-1] area 0
[Spoke3-ospfv3-1-area-0.0.0.0] quit
[Spoke3-ospfv3-1] area 2
[Spoke3-ospfv3-1-area-0.0.0.2] quit
[Spoke3-ospfv3-1] quit
[Spoke3] interface gigabitethernet 1/0/2
[Spoke3-GigabitEthernet1/0/2] ospfv3 1 area 1
[Spoke3-GigabitEthernet1/0/2] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke3] interface tunnel1 mode advpn udp
[Spoke3-Tunnel1] ipv6 address 192:168:2::2 64
[Spoke3-Tunnel1] ipv6 address fe80::2:2 link-local
[Spoke3-Tunnel1] vam ipv6 client Spoke3
[Spoke3-Tunnel1] ospfv3 1 area 2
[Spoke3-Tunnel1] ospfv3 network-type broadcast
[Spoke3-Tunnel1] ospf dr-priority 0
[Spoke3-Tunnel1] advpn ipv6 network 192:168:40::0 64
[Spoke3-Tunnel1] source gigabitethernet 1/0/1
[Spoke3-Tunnel1] tunnel protection ipsec profile abc
[Spoke3-Tunnel1] undo shutdown
```

```
[Spoke3-Tunnel1] quit
```

(9) 配置 Spoke4

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke4。

```
<Spoke4> system-view
[Spoke4] vam client name Spoke4
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke4-vam-client-Spoke4] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke4-vam-client-Spoke4] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke4，密码为 spoke4。

```
[Spoke4-vam-client-Spoke4] user spoke4 password simple spoke4
```

配置 VAM Server 的 IP 地址。

```
[Spoke4-vam-client-Spoke4] server primary ipv6-address 1::11
[Spoke4-vam-client-Spoke4] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke4-vam-client-Spoke4] client enable
[Spoke4-vam-client-Spoke4] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke4] ike keychain advpn
[Spoke4-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke4-ike-keychain-abc] quit
[Spoke4] ike profile abc
[Spoke4-ike-profile-abc] keychain abc
[Spoke4-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke4] ipsec transform-set abc
[Spoke4-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke4-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke4-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke4-ipsec-transform-set-abc] quit
[Spoke4] ipsec profile abc isakmp
[Spoke4-ipsec-profile-isakmp-abc] transform-set abc
[Spoke4-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke4-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

配置私网的路由信息。

```
[Spoke4] ospfv3 1
[Spoke4-ospfv3-1] router-id 0.0.0.7
[Spoke4-ospfv3-1] area 0
[Spoke4-ospfv3-1-area-0.0.0.0] quit
[Spoke4-ospfv3-1] area 2
[Spoke4-ospfv3-1-area-0.0.0.2] quit
```

```
[Spoke4-ospfv3-1] quit
[Spoke4] interface gigabitethernet 1/0/2
[Spoke4-GigabitEthernet1/0/2] ospfv3 1 area 1
[Spoke4-GigabitEthernet1/0/2] quit
[Spoke4] interface gigabitethernet 1/0/3
[Spoke4-GigabitEthernet1/0/3] ospfv3 1 area 1
[Spoke4-GigabitEthernet1/0/3] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke4] interface tunnel1 mode advpn udp
[Spoke4-Tunnel1] ipv6 address 192:168:2::3 64
[Spoke4-Tunnel1] ipv6 address fe80::2:3 link-local
[Spoke4-Tunnel1] vam ipv6 client Spoke4
[Spoke4-Tunnel1] ospfv3 1 area 2
[Spoke4-Tunnel1] ospfv3 network-type broadcast
[Spoke4-Tunnel1] ospf dr-priority 0
[Spoke4-Tunnel1] advpn ipv6 network 192:168:50::0 64
[Spoke4-Tunnel1] advpn ipv6 network 192:168:60::0 64
[Spoke4-Tunnel1] source gigabitethernet 1/0/1
[Spoke4-Tunnel1] tunnel protection ipsec profile abc
[Spoke4-Tunnel1] undo shutdown
[Spoke4-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address       Public address        Type   NAT  Holding time
0          192:168::1            1::1                  Hub    No   0H 52M  7S
0          192:168::2            1::2                  Hub    No   0H 47M 31S
0          192:168::3            1::3                  Hub    No   0H 28M 25S
1          192:168:1::1          1::1                  Hub    No   0H 52M  7S
1          192:168:1::2          1::2                  Hub    No   0H 47M 31S
1          192:168:1::3          1::4                  Spoke  No   0H 18M 26S
1          192:168:1::4          1::5                  Spoke  No   0H 28M 25S
2          192:168:2::1          1::3                  Hub    No   0H 28M 25S
2          192:168:2::2          1::6                  Spoke  No   0H 25M 40S
2          192:168:2::3          1::7                  Spoke  No   0H 25M 31S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address       Public address        Type   NAT  Holding time
0          192:168::1            1::1                  Hub    No   0H 52M  7S
0          192:168::2            1::2                  Hub    No   0H 47M 31S
0          192:168::3            1::3                  Hub    No   0H 28M 25S
1          192:168:1::1          1::1                  Hub    No   0H 52M  7S
```

```
1          192:168:1::2          1::2                  Hub    No   0H 47M 31S
1          192:168:1::3          1::4                  Spoke  No   0H 18M 26S
1          192:168:1::4          1::5                  Spoke  No   0H 28M 25S
2          192:168:2::1          1::3                  Hub    No   0H 28M 25S
2          192:168:2::2          1::6                  Spoke  No   0H 25M 40S
2          192:168:2::3          1::7                  Spoke  No   0H 25M 31S
```

以上显示信息表示 Hub1、Hub2、Hub3、Spoke1、Spoke2、Spoke3 和 Spoke4 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168:1::2          1::2                  18001 H-H   Success    0H 46M  8S
192:168:1::3          1::3                  18001 H-S   Success    0H 27M 27S
192:168:1::4          1::4                  18001 H-S   Success    0H 18M 18S

Interface         : Tunnel2
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  18001 H-H   Success    0H 46M  8S
192:168::3            1::3                  18001 H-H   Success    0H 27M 27S
```

以上显示信息表示 Hub1 与 Hub2、Hub3、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168:1::1          1::1                  18001 S-H   Success    0H 46M  8S
192:168:1::2          1::2                  18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

显示 Spoke3 上的 IPv6 ADVPN 隧道信息。

```
[Spoke3] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168:2::1          1::3                  18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke3 与 Hub3 建立了 Hub-Spoke 永久隧道。Spoke4 上的显示信息与 Spoke3 类似。

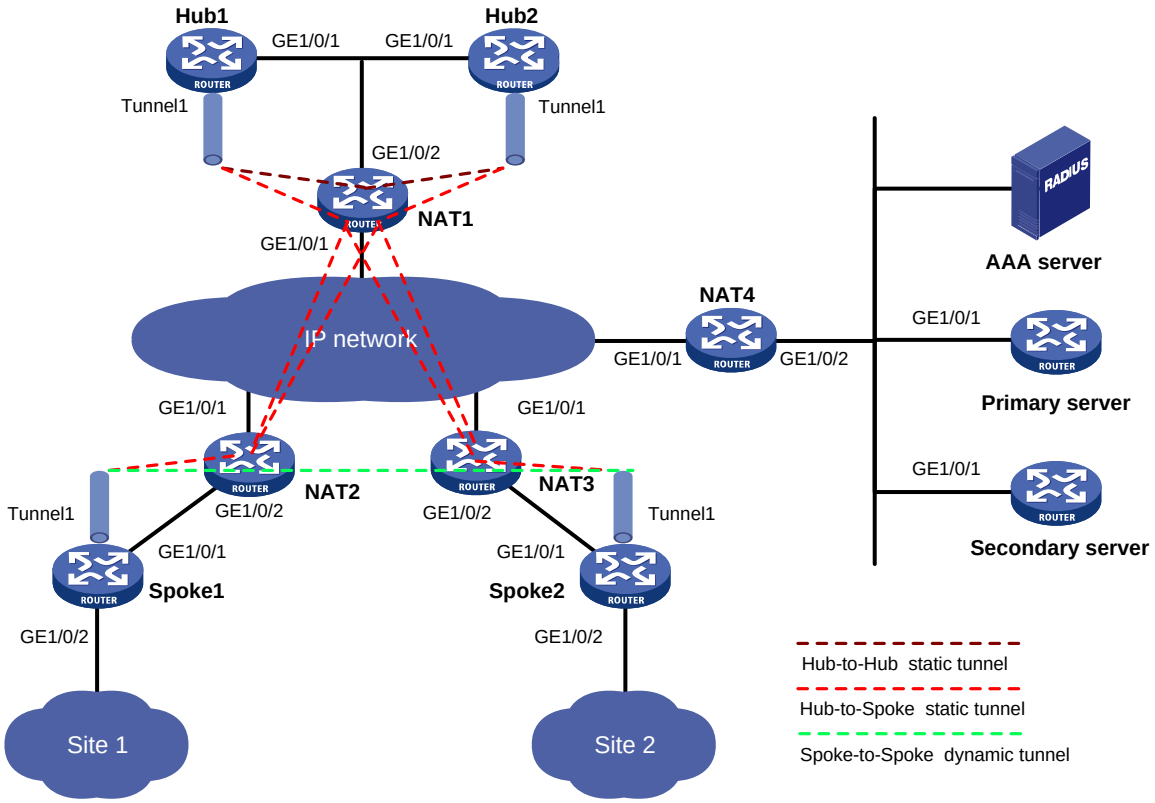
1.10.7 IPv4 Full-Mesh穿越NAT类型ADVPN典型配置举例

1. 组网需求

- 在 IPv4 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久隧道连接。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立隧道连接。
- VAM Server 和各个节点均在 NAT 网关之后。

2. 组网图

图1-13 IPv4 Full-Mesh 穿越 NAT 类型 ADVPN 组网图



Hub 1	GE1/0/1	10.0.0.2/24	Spoke 1	GE1/0/1	10.0.0.2/24
	Tunnel1	192.168.0.1/24		GE1/0/2	192.168.1.1/24
Hub 2	GE1/0/1	10.0.0.3/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE1/0/1	10.0.0.2/24
NAT1	GE1/0/1	1.0.0.1		GE1/0/2	192.168.2.1/24
	GE1/0/2	10.0.0.1		Tunnel1	192.168.0.4/24
NAT2	GE1/0/1	1.0.0.2	NAT4	GE1/0/1	1.0.0.4
	GE1/0/2	10.0.0.1		GE1/0/2	10.0.0.1
NAT3	GE1/0/1	1.0.0.3	AAA server		10.0.0.2/24
	GE1/0/2	10.0.0.1	Primary server	GE1/0/1	10.0.0.3/24
			Secondary server	GE1/0/1	10.0.0.4/24

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 10.0.0.2 1812
[PrimaryServer-radius-abc] primary accounting 10.0.0.2 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
public-address 1.0.0.1 advpn-port 4001
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
public-address 1.0.0.1 advpn-port 4002
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

- 配置默认路由。

```
[PrimaryServer] ip route-static 0.0.0.0 0 10.0.0.1
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.4 port 4001
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.4 port 4002
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

配置默认路由。

```
[Hub1] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 1/0/1
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.4 port 4001
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.4 port 4002
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```

配置默认路由。

```
[Hub2] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 1/0/1
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.4 port 4001
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.4 port 4002
```
开启 VAM Client 功能。
```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```
- 配置 OSPF 路由

配置私网的路由信息。
```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 0
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
[Spoke1-ospf-1] quit
```
配置默认路由。
```
[Spoke1] ip route-static 0.0.0.0 0 10.0.0.1
```
- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。
```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 1/0/1
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```
(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。
```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。
```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```
配置 VAM Server 的 IP 地址。
```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.4 port 4001
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.4 port 4002
```
开启 VAM Client 功能。
```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```
- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

配置默认路由。

```
[Spoke2] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 1/0/1
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(7) 配置 NAT1

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

配置 ACL 2000，允许对内部网络中 10.0.0.0/24 网段的报文进行地址转换。

```
<NAT1> system-view
[NAT1] acl number 2000
[NAT1-acl-basic-2000] rule permit source 10.0.0.0 0.0.0.255
[NAT1-acl-basic-2000] quit
```

在接口 GigabitEthernet1/0/1 上配置 NAT 内部服务器，允许外网 ADVPN 结点使用地址 1.0.0.1 访问内网 Hub1 和 Hub2，同时使得内网 Hub1 和 Hub2 的报文可以进行目的地址转换。

```
[NAT1] interface gigabitethernet 1/0/1
[NAT1-GigabitEthernet1/0/1] nat server protocol udp global current-interface 4001 inside
10.0.0.2 18001
[NAT1-GigabitEthernet1/0/1] nat server protocol udp global current-interface 4002 inside
10.0.0.3 18001
[NAT1-GigabitEthernet1/0/1] nat outbound 2000
[NAT1-GigabitGigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/2 上使能 NAT hairpin 功能。

```
[NAT1] interface gigabitethernet 1/0/2
[NAT1-GigabitEthernet1/0/2] nat hairpin enable
[NAT1-GigabitEthernet1/0/2] quit
```

(8) 配置 NAT2

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

配置 ACL 2000，允许对内部网络中 10.0.0.0/24 网段的报文进行地址转换。

```
<NAT2> system-view
[NAT2] acl number 2000
[NAT2-acl-basic-2000] rule permit source 10.0.0.0 0.0.0.255
```

```
[NAT2-acl-basic-2000] quit
```

创建地址组 1。

```
[NAT2] nat address-group 1
```

添加地址组成员 1.0.0.2。

```
[NAT2-nat-address-group-1] address 1.0.0.2 1.0.0.2
[NAT2-nat-address-group-1] quit
```

在接口 GigabitEthernet1/0/1 上配置内网可以进行目的地址转换。

```
[NAT2] interface gigabitethernet 1/0/1
[NAT2-GigabitEthernet1/0/1] nat outbound 2000 address-group 1
[NAT2-GigabitEthernet1/0/1] quit
```

配置 PAT 方式下的地址转换模式为 EIM，即只要是来自相同源地址和源端口号的且匹配 ACL 2000 的报文，不论其目的地址是否相同，通过 PAT 转换后，其源地址和源端口号都被转换为同一个外部地址和端口号。

```
[NAT2] nat mapping-behavior endpoint-independent acl 2000
```

(9) 配置 NAT3

NAT3 的配置与 NAT2 的配置相似，这里省略。

(10) 配置 NAT4

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

```
<NAT4> system-view
[NAT4] interface gigabitethernet 1/0/1
[NAT4-GigabitEthernet1/0/1] nat server protocol udp global current-interface 4001 inside 10.0.0.3 18000
[NAT4-GigabitEthernet1/0/1] nat server protocol udp global current-interface 4002 inside 10.0.0.4 18000
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    Yes   0H 52M  7S
0          192.168.0.2      1.0.0.1                   Hub    Yes  0H 47M 31S
0          192.168.0.3      1.0.0.2                   Spoke  Yes  0H 28M 25S
0          192.168.0.4      1.0.0.3                   Spoke  Yes  0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    Yes  0H 52M  7S
0          192.168.0.2      1.0.0.1                   Hub    Yes  0H 47M 31S
0          192.168.0.3      1.0.0.2                   Spoke  Yes  0H 28M 25S
0          192.168.0.4      1.0.0.3                   Spoke  Yes  0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address             Port  Type  State      Holding time
192.168.0.2      1.0.0.1                    4002  H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.2                    2001  H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.3                    2001  H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
192.168.0.1      1.0.0.1                    4001  S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.1                    4002  S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address             Port  Type  State      Holding time
192.168.0.1      1.0.0.1                    4001  S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.1                    4002  S-H   Success    0H 46M  8S
192.168.0.4      1.0.0.3                    2001  S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。