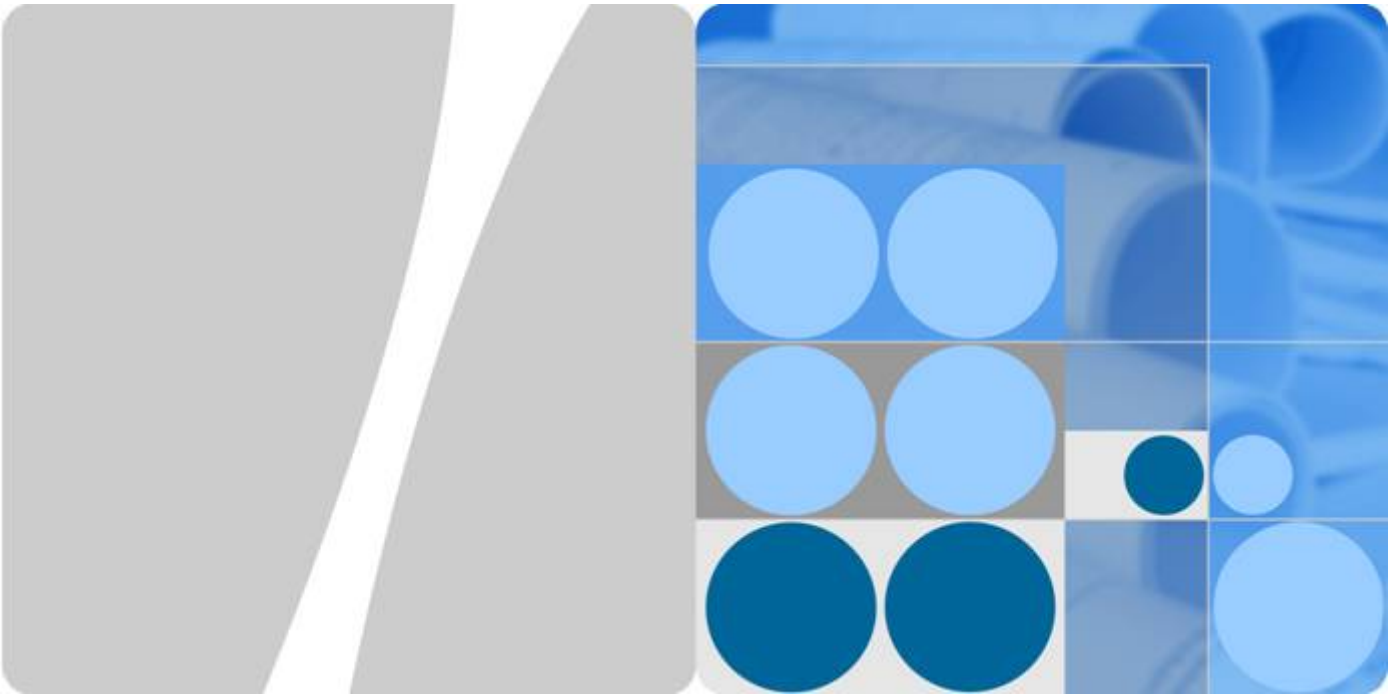


Huawei AR1200 系列企业路由器

V200R002C01

配置指南-IP 业务

文档版本　01

发布日期　2012-04-20

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR1200 中 IP 业务特性的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了 IP 业务特性的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

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 | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-04-20)

第一次正式发布。

目 录

1 ARP 配置

关于本章

ARP 协议用于将 IP 地址映射到 MAC 地址，实现以太网数据帧的传送。

1.1 ARP 概述
ARP 协议是任何以太网设备都必须支持的协议。实现三层 IP 地址与二层 MAC 地址之间的动态映射。

1.2 AR1200 支持的 ARP 特性
介绍 ARP 特性在 AR1200 中的支持情况。

1.3 配置静态 ARP
静态 ARP 是指 IP 地址和 MAC 地址之间有固定的映射关系。静态 ARP 需要网络管理员手动配置。

1.4 配置动态 ARP 表项的优化
动态 ARP 是指系统自动进行 IP 地址到以太网 MAC 地址的解析。动态 ARP 表项是由 ARP 协议动态维护的，不需要手工配置，但是可以通过调整动态 ARP 表项的参数例如老化时间、老化探测次数等来优化设备转发性能。

1.5 配置路由式 Proxy ARP
路由式 Proxy ARP 可以实现在同一网段却不在同一物理网络上的设备能够相互通信的一种功能。

1.6 配置 VLAN 内 Proxy ARP
介绍 VLAN 内 Proxy ARP 的配置，实现同一 VLAN 内二层隔离的主机之间的互通。

1.7 配置 VLAN 间 Proxy ARP
介绍 VLAN 间 Proxy ARP 的配置，实现同一 Super VLAN 内不同的 Sub VLAN 中的主机之间的互通。

1.8 配置 ARP-Ping IP
ARP-Ping IP 是利用 ARP 报文在局域网内探测 IP 地址是否被其它设备使用的一种方法。

1.9 配置 ARP-Ping MAC
ARP-Ping MAC 是利用 ICMP 报文在局域网范围内探测 MAC 地址是否被其他设备使用的一种方法。

1.10 维护 ARP
维护 ARP 包括清除 ARP 统计信息、监控 ARP 运行状况。

1.1 ARP 概述

ARP 协议是任何以太网设备都必须支持的协议。实现三层 IP 地址与二层 MAC 地址之间的动态映射。

在局域网中，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 数据报文必须封装成帧才能通过物理网络发送，因此发送端还必须有接收端的物理地址，所以需要一个从 IP 地址到物理地址的映射。APR 就是实现这个功能的协议。

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

1.2 AR1200 支持的 ARP 特性

介绍 ARP 特性在 AR1200 中的支持情况。

AR1200 支持动态 ARP、静态 ARP、Proxy ARP 和 ARPing。

ARP

ARP 可以分为动态和静态两种。

- 静态 ARP 是指用户手工配置的 IP 地址和 MAC 地址的映射关系。
- 动态 ARP 是指 ARP 协议动态维护的 ARP 映射表项。

Proxy ARP

AR1200 支持的 Proxy ARP 包括三种：

- 路由式 Proxy ARP

  路由式 Proxy ARP 功能可以实现在同一网段却不在同一物理网络上的设备能够相互通信。

  在实际应用中，如果连接路由器的当前主机上没有配置缺省网关地址（即不知道如何到达本网络的中介系统），此时将无法进行数据转发。

  路由式 Proxy ARP 可以解决这个问题，主机发送一个 ARP 请求（请求目的主机的 MAC 地址），使能 Proxy ARP 功能的路由器收到这样的请求后，会使用自己的 MAC 地址作为该 ARP 请求的回应，以此来欺骗主机进行数据转发。

  使能 Proxy ARP 功能的路由器还可隐藏物理网络的细节，使得处于不同物理网络但网段相同的 Ethernet A 和 Ethernet B 的内部主机之间可以正常的相互通信。

- VLAN 内 Proxy ARP

  如果两个用户属于相同的 VLAN，但 VLAN 内配置了用户隔离。用户间要互通，需要在关联了 VLAN 的接口上启动 VLAN 内 Proxy ARP 功能。

  若路由器的接口使能了 VLAN 内 Proxy ARP 功能，接口在接收到目的地址不是自己的 ARP 请求报文后，路由器并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果使能了代理功能，则将路由器的 MAC 地址发送给 ARP 请求方。

  VLAN 内 Proxy ARP 主要用于配置了用户隔离的 VLAN 内的用户间互通。

- VLAN 间 Proxy ARP

如果两个用户属于不同的 VLAN，用户间要进行三层互通，需要在关联了 VLAN 的接口上启动 VLAN 间 Proxy ARP 功能。

若路由器的接口使能了 VLAN 间 Proxy ARP 功能，接口在接收到目的地址不是自己的 ARP 请求报文后，路由器并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果使能了代理功能，则将路由器的 MAC 地址发送给 ARP 请求方。

VLAN 间 Proxy ARP 主要用于：

- 处于不同 VLAN 的用户进行三层通信。
- 可在 Super VLAN 对应的 VLANIF 接口上启动 VLAN 间 Proxy ARP 功能，实现 Sub VLAN 间用户互通。

ARPing

ARPing 包括 ARP-Ping IP 和 ARP-Ping MAC，这两者统称为 ARPing，用于部署二层特性时方便维护。

ARP-Ping IP 是利用 ARP 报文在局域网内探测 IP 地址是否被其他的设备使用的一种方法。

ARP-Ping MAC 是利用 ICMP 报文在局域网范围内探测 MAC 地址是否被其他的设备使用的一种方法。

1.3 配置静态 ARP

静态 ARP 是指 IP 地址和 MAC 地址之间有固定的映射关系。静态 ARP 需要网络管理员手动配置。

1.3.1 建立配置任务

在配置静态 ARP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

配置静态 ARP 表项增加通信的安全性。配置静态 ARP 表项可以限制与指定 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。

在设备上同时配置静态 ARP 和 VRRP 时，不能将 Dot1q 终结子接口、QinQ 终结子接口或 VLANIF 接口下所配置的 VRRP 备份组的虚拟 IP 地址作为该静态 ARP 表项中的 IP 地址，否则会生成错误的主机路由，影响正常转发。

前置任务

在配置静态 ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up
- 配置接口的网络层协议参数，使接口的路由协议状态为 Up

数据准备

在配置静态 ARP 之前，需准备以下数据。

序号	数据
1	静态 ARP 表项的 IP 地址和 MAC 地址
2	静态 ARP 表项的所在的 VPN 实例名和 VLAN ID
3	ARP 报文的出接口

1.3.2 配置普通静态 ARP 表项

静态 ARP 表项在 AR1200 正常工作时一直有效。

背景信息

说明

如果需要为带有两层 tag 的用户报文配置静态 ARP，请使用 **arp static cevid** 命令。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp static** *ip-address mac-address*，配置普通静态 ARP 表项。

----结束

1.3.3 配置 VLAN 内的静态 ARP 表项

介绍 VLAN 内静态 ARP 表项配置过程。

背景信息

说明

如果需要为带有两层 tag 的用户报文配置静态 ARP，请使用 **arp static cevid** 命令。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp static** *ip-address mac-address* [**vid** *vlan-id* **interface** *interface-type interface-number*]。

说明

配置 VLAN 内的静态 ARP 表项时，如果不确定 VLAN 的物理出接口，可以只配置 IP 地址和对应的 MAC 地址，而不需要指定物理出接口。

----结束

1.3.4 配置 VPN 实例内的静态 ARP 表项

当需要实现 VPN 实例内的设备通过二层互相访问时，可以配置 VPN 实例内的静态 ARP。

背景信息

说明

如果需要为带有两层 tag 的用户报文配置静态 ARP，请使用 **arp static cevid** 命令。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name*，配置 VPN 实例内的静态 ARP 表项。

----结束

1.3.5 检查配置结果

操作步骤

- 执行命令 **display arp** [**all**]，查看所有 ARP 映射表，包括静态 ARP 表项和动态 ARP 表项。
- 执行命令 **display arp network** *net-number net-mask* [**dynamic** | **static**]，查看指定网段的 ARP 映射表。
- 执行命令 **display arp static**，查看静态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

显示所有的静态 ARP 表项。

```
<Huawei> display arp static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
1.1.1.1         0efc-0505-86e3            S--
                                            10/-
129.102.0.1     0e00-fc01-0000            S--
11.0.0.1        aa00-fcc0-1200            S--
                                             3/-
--------------------------------------------------------------------------------
Total:3         Dynamic:0       Static:3    Interface:0
```

显示所有的 ARP 表项。

```
<Huawei> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
129.102.0.1     00e0-fc01-0000            S--
118.118.118.1   0018-2000-0083            I -         Vlanif11        vpna
10.1.1.1        0018-2000-0083            I -         Vlanif10
100.1.1.116     0018-2000-0083            I -         Eth0/0/0
```

```
100.1.1.118     0001-0c01-3401  14        D-0         Eth0/0/0
100.1.1.4       0016-ecb7-a879  18        D-0         Eth0/0/0
--------------------------------------------------------------------------------
Total:6         Dynamic:2       Static:1    Interface:3
```

1.4 配置动态 ARP 表项的优化

动态 ARP 是指系统自动进行 IP 地址到以太网 MAC 地址的解析。动态 ARP 表项是由 ARP 协议动态维护的，不需要手工配置，但是可以通过调整动态 ARP 表项的参数例如老化时间、老化探测次数等来优化设备转发性能。

1.4.1 建立配置任务

在配置优化动态 ARP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

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。当到达老化时间或者接口 down 时会删除相应的动态 ARP 表项。

建立动态 ARP 是 AR1200 本身就具有的功能。不需要使用命令启动此功能，可以通过调整动态 ARP 的参数来优化设备转发性能。

前置任务

在配置动态 ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 配置接口的网络层协议。

数据准备

配置动态 ARP 之前，需准备以下数据。

序号	数据
1	动态 ARP 表项所在的接口编号
2	动态 ARP 表项的老化探测次数
3	动态 ARP 表项的老化超时时间

1.4.2 调整动态 ARP 的老化参数

当设备需要频繁更新 ARP 表项时，可以将 ARP 表项的老化超时时间调整小、将 ARP 表项的老化探测次调整大、将 ARP 表项的老化探测时间间隔调整小。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 调整动态 ARP 的老化参数功能支持的接口为 Ethernet 接口、GE 接口、Eth-Trunk 接口、VLANIF 接口和 VE 接口。

步骤 3 执行命令 **arp expire-time** *expire-time*，设置动态 ARP 表项的老化超时时间。

缺省情况下，老化超时时间为 1200 秒，即 20 分钟。

步骤 4 执行命令 **arp detect-times** *detect-times*，设置动态 ARP 表项的老化探测次数。

缺省情况下，动态 ARP 表项的老化探测次数为 3。某动态 ARP 表项到达老化时间以后，设备定时发送 ARP 老化探测报文进行探测，如果超过设置的探测次数后仍没有收到对端设备的应答，该 ARP 表项将被老化。

步骤 5 （可选）执行命令 **arp detect-mode unicast**，设置接口以单播方式发送 ARP 老化探测报文。

缺省情况下，接口以广播方式发送 ARP 老化探测报文。

----结束

1.4.3 使能 ARP 抑制功能

系统在同一时间内接收到大量源 IP 地址相同的 ARP 报文时，需要对 ARP 表项进行重复更新。为了维护系统性能，可以启动 ARP 抑制功能，系统将对 ARP 报文只应答，不更新。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp-suppress enable**，使能当前设备上的 ARP 抑制功能。

缺省情况下，ARP 抑制功能为关闭，只对 VLANIF 接口进行抑制。

使能当前设备上的 ARP 抑制功能后，只对 Eth-Trunk 和 VLANIF 接口生效。

----结束

1.4.4 使能二层拓扑探测功能

使能二层拓扑探测功能后，当二层接口状态由 Down 变为 Up 时，系统更新所有该二层口所属 VLAN 对应的 ARP 表项。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **l2-topology detect enable**，使能二层拓扑探测功能。

缺省情况下，系统不使能二层拓扑探测功能。

----结束

1.4.5 检查配置结果

可以查看动态 ARP 的配置信息。

操作步骤

- 执行命令 **display arp** [**all**]，查看所有 ARP 映射表，包括静态 ARP 表项和动态 ARP 表项。
- 执行命令 **display arp interface** *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]，查看指定接口的 ARP 映射表。
- 执行命令 **display arp network** *net-number net-mask* [**dynamic** | **static**]，查看指定网段的 ARP 映射表。
- 执行命令 **display arp dynamic** ，查看动态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

查看接口 GE1/0/0 的 ARP 表项。

```
<Huawei> display arp interface gigabitethernet 1/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         GE1/0/0        r1
192.168.1.1     0000-0a41-0200  15        D-6         GE1/0/0        r1
-------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

显示所有的动态 ARP 表项。

```
<Huawei> display arp dynamic
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
10.137.217.210  00e0-fc01-0203            I -         GE1/0/0
10.137.216.1    0025-9e38-a09e  20        D-0         GE1/0/0
10.137.217.208  00e0-fc01-0205  16        D-0         GE1/0/0
10.2.2.1        00e0-fc99-9999            I -         Eth-Trunk0
10.6.3.34       00e0-fc01-0204            I -         GE2/0/0.1
192.168.20.1    00e0-fc99-9999            I -         Vlanif100
10.0.0.1        00e0-fc99-9999            I -         Vlanif200
-------------------------------------------------------------------------------
Total:7         Dynamic:2      Static:0    Interface:5
```

1.5 配置路由式 Proxy ARP

路由式 Proxy ARP 可以实现在同一网段却不在同一物理网络上的设备能够相互通信的一种功能。

1.5.1 建立配置任务

在配置路由式 Proxy ARP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

当两台主机属于不同的物理网络但属于同一网段，并且没有配置网关时，可以在连接两台主机的路由设备上使能路由式 Proxy ARP 功能，通过路由式 Proxy ARP 实现两台主机之间的 IP 地址解析。

前置任务

在配置路由式 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。

数据准备

在配置路由式 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动路由式 Proxy ARP 的接口编号
2	启动路由式 Proxy ARP 的接口 IP 地址

1.5.2 配置接口的 IP 地址

在启动路由式 Proxy ARP 的接口上配置的 IP 地址应该与该接口所连接的局域网中主机的 IP 地址处于同一网段。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。

支持路由式 Proxy ARP 的接口有：Ethernet 接口、Ethernet 子接口、GE 接口、GE 子接口、Virtual-Ethernet 接口、Eth-Trunk 接口、Eth-Trunk 子接口和 VLANIF 接口，其中接口为三层接口或三层接口的子接口。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口 IP 地址。

在启动路由式 Proxy ARP 的接口上配置的 IP 地址应该与该接口所连接的局域网中主机的 IP 地址处于同一网段。

----结束

1.5.3 配置路由式 Proxy ARP 功能

实现同一 IP 网络内不同子网的互通，需配置路由式 Proxy ARP 功能。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

支持路由式 Proxy ARP 的接口有：Ethernet 接口、Ethernet 子接口、GE 接口、GE 子接口、Virtual-Ethernet 接口、Eth-Trunk 接口、Eth-Trunk 子接口和 VLANIF 接口，其中接口为三层接口或三层接口的子接口。

步骤 3 执行命令 **arp-proxy enable**，使能接口的路由式 Proxy ARP 功能。

缺省情况下，关闭接口的路由式 Proxy ARP 功能。

----结束

1.5.4 检查配置结果

可以查看路由式 Proxy ARP 的配置信息。

操作步骤

- 执行命令 **display arp interface** *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]，查看指定接口的 ARP 映射表。
- 执行命令 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**],查看指定的 VPN 实例的 ARP 映射表。
- 执行命令 **display arp dynamic**，查看动态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

查看接口 GE1/0/0 的 ARP 表项。

```
<Huawei> display arp interface gigabitethernet 1/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         GE1/0/0       r1
192.168.1.1     0000-0a41-0200  15        D-6         GE1/0/0       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

显示 VPN r1 的所有 ARP 表项。

```
<Huawei> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.10.20.9      0018-2000-0083            I -         Vlanif888
10.10.10.6      0018-2000-0083            I -         Vlanif833
--------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0    Interface:2
```

查看 ARP 表项的统计信息。

```
<Huawei> display arp statistics all
Dynamic:1       Static:0
```

1.6 配置 VLAN 内 Proxy ARP

介绍 VLAN 内 Proxy ARP 的配置，实现同一 VLAN 内二层隔离的主机之间的互通。

1.6.1 建立配置任务

在配置 VLAN 内 Proxy ARP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

如果两个用户属于相同的 VLAN，但它们分别连接到被二层隔离的两个端口上，通过在设备上启动 VLAN 内 Proxy ARP 功能，可以实现这两个用户的三层互通。

前置任务

在配置 VLAN 内 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置 VLAN
- 配置 VLAN 内用户隔离

数据准备

在配置 VLAN 内 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动 VLAN 内 Proxy ARP 的接口编号
2	启动 VLAN 内 Proxy ARP 的接口 IP 地址
3	启动 VLAN 内 Proxy ARP 的接口关联的 VLAN ID

1.6.2 配置接口的 IP 地址

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图；或执行 **interface vlanif** *vlan-id* 命令，进入 VLANIF 接口视图。

支持 VLAN 内 Proxy ARP 的接口有：VLANIF 接口、Ethernet 子接口、GE 子接口和 Eth-Trunk 子接口。

步骤 3 执行 **ip address** *ip-address* { *mask* | *mask-length* }命令，配置接口的 IP 地址。

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

----结束

1.6.3 （可选）配置子接口关联的 VLAN

请在使用子接口实现 VLAN 内互通的设备上进行以下配置。

背景信息

说明

在 Ethernet 子接口、GE 子接口或 Eth-Trunk 子接口上启用 VLAN 内 Proxy ARP 需要执行本步骤的操作。在 VLANIF 接口上启用 VLAN 内 Proxy ARP 不需要执行本步骤，直接进行下一步操作。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图。

步骤 3 执行 **dot1q termination vid** *vid* 命令，配置子接口 dot1q 封装的单层 VLAN ID。

----结束

1.6.4 使能 VLAN 内 Proxy ARP

需要在关联了 VLAN 的接口上启动 VLAN 内 Proxy ARP 功能，实现相同 VLAN 内被隔离的用户间三层互通。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图；或执行 **interface vlanif** *vlan-id* 命令，进入 VLANIF 接口视图。

步骤 3 执行 **arp-proxy inner-sub-vlan-proxy enable** 命令，使能 VLAN 内 Proxy ARP。

缺省情况下，不使能 VLAN 内 Proxy ARP 功能。

----结束

1.6.5 检查配置结果

可以查看 VLAN 内 Proxy ARP 的配置信息。

操作步骤

- 执行命令 **display arp interface** *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]，查看指定接口的 ARP 映射表。

- 执行命令 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**],查看指定的 VPN 实例的 ARP 映射表。
- 执行命令 **display arp dynamic**，查看动态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

查看接口 GE1/0/0 的 ARP 表项。

```
<Huawei> display arp interface gigabitethernet 1/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         GE1/0/0       r1
192.168.1.1     0000-0a41-0200  15        D-6         GE1/0/0       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

显示 VPN r1 的所有 ARP 表项。

```
<Huawei> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.10.20.9      0018-2000-0083            I -         Vlanif888
10.10.10.6      0018-2000-0083            I -         Vlanif833
--------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0    Interface:2
```

查看 ARP 表项的统计信息。

```
<Huawei> display arp statistics all
Dynamic:1       Static:0
```

1.7 配置 VLAN 间 Proxy ARP

介绍 VLAN 间 Proxy ARP 的配置，实现同一 Super VLAN 内不同的 Sub VLAN 中的主机之间的互通。

1.7.1 建立配置任务

在配置 VLAN 间 Proxy ARP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

VLAN 聚合就是在一个物理网络内，用多个 VLAN 隔离广播域，使不同的 VLAN 属于同一个子网。它引入 Super-VLAN 和 Sub-VLAN 的概念，一个 Super-VLAN 可以包含一个或多个保持着不同广播域的 Sub-VLAN。Sub-VLAN 不再占用一个独立的子网网段，在同一个 Super-VLAN 中，无论主机属于哪一个 Sub-VLAN，它的 IP 地址都在 Super-VLAN 对应的子网网段内。

Sub-VLAN 共用 Super-VLAN 的三层接口与外部进行三层通信，既减少了一部分子网号、子网缺省网关地址的消耗，又实现了不同广播域使用同一子网网段地址的目的。这样消除了子网差异，增加了编址的灵活性，减少了闲置地址浪费。

但是，同一 Super VLAN 内的不同 Sub VLAN 下的主机之间是不能互通的。这时为了实现不同 Sub VLAN 下主机之间的互通，可以在 Super VLAN 对应的子接口或 VLANIF 接口上启动 VLAN 间 Proxy ARP 功能。

前置任务

在配置 VLAN 间 Proxy ARP 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置 VLAN 聚合

数据准备

在配置 VLAN 间 Proxy ARP 之前，需准备以下数据。

序号	数据
1	启动 VLAN 间 Proxy ARP 的接口编号
2	启动 VLAN 间 Proxy ARP 的接口 IP 地址
3	启动 VLAN 间 Proxy ARP 的接口关联的 VLAN ID

1.7.2 配置接口的 IP 地址

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图；或执行 **interface vlanif** *vlan-id* 命令，进入 VLANIF 接口视图。

支持 VLAN 间 Proxy ARP 的接口有：VLANIF 接口、Ethernet 子接口、GE 子接口和 Eth-Trunk 子接口。

步骤 3 执行 **ip address** *ip-address* { *mask* | *mask-length* }命令，配置接口的 IP 地址。

接口上配置的 IP 地址应该与该接口所关联的 VLAN 的用户 IP 地址在同一网段。

----结束

1.7.3 （可选）配置子接口关联的 VLAN

请在使用子接口实现 VLAN 间互通的设备上进行以下配置。

背景信息

说明

在 Ethernet 子接口、GE 子接口或 Eth-Trunk 子接口上启用 VLAN 间 Proxy ARP 需要执行本步骤的操作。在 VLANIF 接口上启用 VLAN 间 Proxy ARP 不需要执行本步骤，直接进行下一步操作。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图。

步骤 3 执行 **dot1q termination vid** *vid* 命令，配置子接口 dot1q 封装的单层 VLAN ID。

----结束

1.7.4 使能 VLAN 间 Proxy ARP

需要在关联了 VLAN 的子接口上启动 VLAN 间 Proxy ARP 功能，实现属于不同 VLAN 的用户间的互通。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface** { **ethernet** | **gigabitethernet** | **eth-trunk** } *interface-number.sub-interface-number* 命令，进入子接口视图；或执行 **interface vlanif** *vlan-id* 命令，进入 VLANIF 接口视图。

步骤 3 执行 **arp-proxy inter-sub-vlan-proxy enable** 命令，使能 VLAN 间 Proxy ARP。

缺省情况下，不使能 VLAN 间 Proxy ARP 功能。

----结束

1.7.5 检查配置结果

可以查看 VLAN 间 Proxy ARP 的配置信息。

操作步骤

- 执行命令 **display arp interface** *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]，查看指定接口的 ARP 映射表。
- 执行命令 **display arp vpn-instance** *vpn-instance-name* [**dynamic** | **static**],查看指定的 VPN 实例的 ARP 映射表。
- 执行命令 **display arp dynamic**，查看动态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

查看接口 GE1/0/0 的 ARP 表项。

```
<Huawei> display arp interface gigabitethernet 1/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         GE1/0/0       rl
192.168.1.1     0000-0a41-0200  15        D-6         GE1/0/0       rl
-------------------------------------------------------------------------------
```

```
Total:2         Dynamic:1       Static:0    Interface:1
```

显示 VPN r1 的所有 ARP 表项。

```
<Huawei> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.10.20.9      0018-2000-0083            I -         Vlanif888
10.10.10.6      0018-2000-0083            I -         Vlanif833
--------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0    Interface:2
```

查看 ARP 表项的统计信息。

```
<Huawei> display arp statistics all
Dynamic:1       Static:0
```

1.8 配置 ARP-Ping IP

ARP-Ping IP 是利用 ARP 报文在局域网内探测 IP 地址是否被其它设备使用的一种方法。

1.8.1 建立配置任务

在配置 ARP-Ping IP 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

ARP-Ping IP 是利用 ARP 报文在局域网内探测 IP 地址是否被其他的设备使用的一种方法。

用户对设备配置 IP 地址前，需要确认该 IP 地址有没有被网络上的其他设备使用，可以通过发送 ARP 报文，确认该 IP 的使用情况，以便做出相应调整。

前置任务

在配置 ARP-Ping IP 之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up。

数据准备

在配置 ARP-Ping IP 之前，需准备以下数据。

序号	数据
1	需要确认的 IP 地址。

1.8.2 使用 ARP-Ping IP 检测 IP 地址

ARP-Ping IP 检测是通过发送 ARP 请求报文实现的。

背景信息

ARP-Ping IP 是利用 ARP 报文在局域网内探测 IP 地址是否被其他设备使用的一种方法。通过 **ping** 命令也可以探测该 IP 地址是否被网络上的其他设备使用。由于 **ping** 命令发送的 ICMP Echo Request 报文是三层报文，如果带有防火墙功能的目的主机和路由设备设置了对 ICMP Echo Request 报文不进行回复的功能时，就不会回复 ICMP Reply 报文，造成该 IP 没有被使用的假象。由于 ARP Request 报文是二层协议，大多数情况下可以透过设置了对 ICMP Echo Request 报文不进行回复的防火墙，从而避免了此类情况的发生。

操作步骤

步骤 1 执行命令 **arp-ping ip** *ip-address* [**interface** *interface-type interface-number* [**vlan-id** *vlan-id*]]，在局域网范围内查询 IP 地址是否被其他设备使用的情况。

----结束

任务示例

命令执行结果如下：

- 如果 IP 地址没有被使用

```
[Huawei] arp-ping ip 110.1.1.2
 ARP-Pinging 110.1.1.2:

Error: Request timed out.
Error: Request timed out.
Error: Request timed out.
Info: The IP address is not used by anyone!
```

- 如果 IP 地址已被使用

```
[Huawei] arp-ping ip 128.1.1.1
 ARP-Pinging 128.1.1.1:

128.1.1.1 is used by 00e0-517d-f202
```

1.9 配置 ARP-Ping MAC

ARP-Ping MAC 是利用 ICMP 报文在局域网范围内探测 MAC 地址是否被其他设备使用的一种方法。

1.9.1 建立配置任务

在配置 ARP-Ping MAC 前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

当只知道该网段一个特定的 MAC 地址而不知道其对应的 IP 地址时，可以配置 ARP-Ping MAC 功能发送广播的 ICMP 报文（三层），得到该 MAC 所对应的 IP 地址。通过这种方法，可以查询到该网段内特定 MAC 所对应的 IP 地址。

前置任务

在配置 ARP-Ping MAC 之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up。

数据准备

在配置 ARP-Ping MAC 之前，需准备以下数据。

序号	数据
1	需要确认的 MAC 地址。

1.9.2 使用 ARP-Ping MAC 检测 MAC 地址

ARP-Ping MAC 检测是通过发送 ICMP 报文实现的。

操作步骤

步骤 1 执行命令 **arp-ping mac** *mac-address* { *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* }，查询 MAC 地址是否被其他的设备使用。

----结束

任务示例

命令执行结果如下：

- 如果 MAC 地址没有被使用

```
<Huawei> arp-ping mac 0013-46e7-2ef5 interface Eth-Trunk 0
  OutInterface: Eth-Trunk0 MAC[00-13-46-E7-2E-F5], press CTRL_C to break
Error: Request timed out
Error: Request timed out
Error: Request timed out

    ----- ARP-Ping MAC statistics -----
    3 packet(s) transmitted
    0 packet(s) received
    MAC[00-13-46-E7-2E-F5]  not be used
```

- 如果 MAC 地址被使用

```
<Huawei> arp-ping mac 00e0-fc03-0201 interface Vlanif 5
  OutInterface: Vlanif5 MAC[00-E0-FC-03-02-01], press CTRL_C to break

    ----- ARP-Ping MAC statistics -----
    1 packet(s) transmitted
    1 packet(s) received

    IP ADDRESS               MAC ADDRESS
    50.1.1.2                 00-E0-FC-03-02-01
```

1.10 维护 ARP

维护 ARP 包括清除 ARP 统计信息、监控 ARP 运行状况。

1.10.1 清除 ARP 表项

介绍了使用 reset 命令清除 ARP 统计信息。

背景信息

注意

- 清除 ARP 表项后，将取消 IP 地址和 MAC 地址的映射关系，可能导致无法访问某些节点。清除前请务必仔细确认。
- 清除静态 ARP 表项后，静态 ARP 表项将无法恢复，清除前请务必仔细确认。

操作步骤

步骤 1 在确认需要清除 ARP 映射表中的 ARP 项后，请在用户视图下执行 **reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **packet statistics** | **static** }命令。

----结束

1.10.2 监控 ARP 运行状况

介绍了使用 display 命令监控 ARP 运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 ARP 的运行情况。

操作步骤

- 执行命令 **display arp** [**all**]，查看所有 ARP 映射表，包括静态 ARP 表项和动态 ARP 表项。
- 执行命令 **display arp interface** *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]，查看指定接口的 ARP 映射表。
- 执行命令 **display arp network** *net-number net-mask* [**dynamic** | **static**]，查看指定网段的 ARP 映射表。
- 执行命令 **display arp static**，查看静态 ARP 映射表。
- 执行命令 **display arp dynamic**，查看动态 ARP 映射表。
- 执行命令 **display arp statistics** { **all** | **interface** *interface-type interface-number* }，查看整机或指定接口的 ARP 表项的统计信息。

----结束

任务示例

查看接口 GE1/0/0 的 ARP 表项。

```
<Huawei> display arp interface gigabitethernet 1/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
```

```
192.168.1.11    0000-0a41-0201            I -         GE1/0/0       r1
192.168.1.1     0000-0a41-0200  15        D-6         GE1/0/0       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

显示所有的动态 ARP 表项。

```
<Huawei> display arp dynamic
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.137.217.210  00e0-fc01-0203            I -         GE1/0/0
10.137.216.1    0025-9e38-a09e  20        D-0         GE1/0/0
10.137.217.208  00e0-fc01-0205  16        D-0         GE1/0/0
10.2.2.1        00e0-fc99-9999            I -         Eth-Trunk0
10.6.3.34       00e0-fc01-0204            I -         GE2/0/0.1
192.168.20.1    00e0-fc99-9999            I -         Vlanif100
10.0.0.1        00e0-fc99-9999            I -         Vlanif200
--------------------------------------------------------------------------------
Total:7         Dynamic:2       Static:0    Interface:5
```

1.11 配置举例

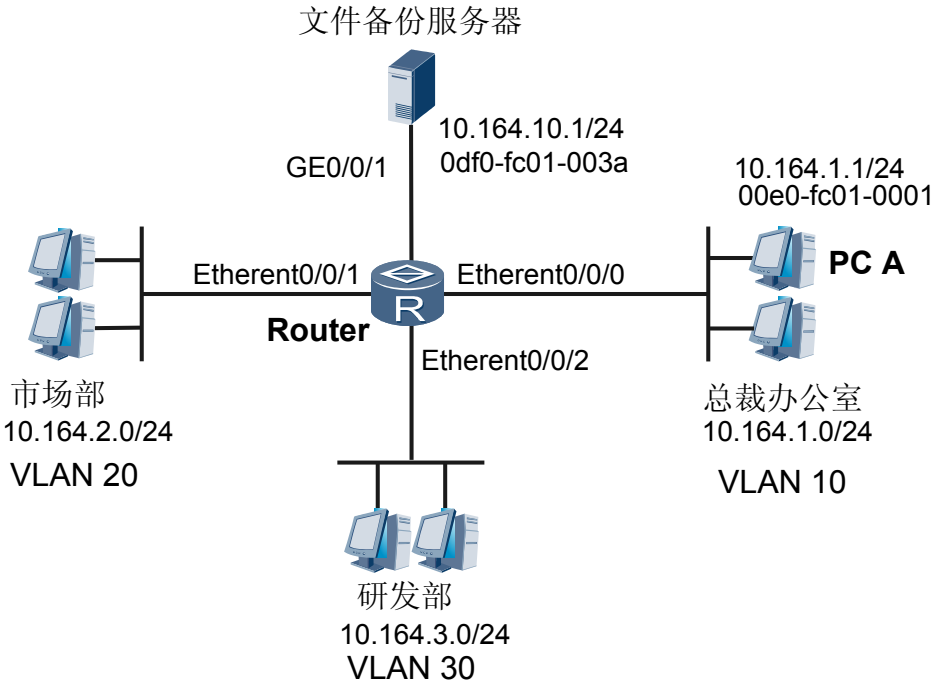
1.11.1 配置静态 ARP 示例

本组网以企业部门为例，通过合理配置静态 ARP，保证通信的安全性。

组网需求

如图 1-1 所示，企业通过 Router 实现各个部门之间的互连，且各个部门加入不同的 VLAN，其中，总裁办公室和文件备份服务器采取手工方式分配到固定 IP 地址，其他部门通过 DHCP 方式分配到动态 IP 地址。由于市场部拥有访问外网的权利，主机经常会感染 ARP 病毒的，攻击 Router 并修改 Router 上的动态 ARP 表项，造成总裁办公室与外界的通信中断以及各个部门不能正常访问文件备份服务器。公司希望在 Router 进行配置，以保证总裁办公室与外界的通信安全，并保证各个部门能正常访问文件备份服务器。

图 1-1 配置静态 ARP 组网图



配置思路

静态 ARP 的配置思路如下：

1. 在 Router 上为总裁办公室主机配置静态 ARP 表项，防止总裁办公室主机的 ARP 表项被 ARP 攻击报文修改，造成总裁办公室与外界的通信中断。
2. 在 Router 上为文件备份服务器配置静态 ARP 表项，防止文件备份服务器的 ARP 表项被 ARP 攻击报文修改，造成各个部门不能正常访问文件备份服务器。

数据准备

为完成此配置示例，需准备如下的数据：

- Router 连接总裁办公室的接口：Ethernet0/0/0。
- Ethernet0/0/0 加入的 VLAN 的 ID：10。
- VLANIF10 的 IP 地址：10.164.1.20/24。
- 总裁办公室主机的 IP 地址网段为 10.164.1.0/24。选取 IP 地址为 10.164.1.1 的主机 PC A 为例，对应的 MAC 地址为 00e0-fc01-0001。
- Router 连接文件备份服务器的接口：Ethernet2/0/0。
- Ethernet2/0/0 的 IP 地址：10.164.10.10/24。
- 文件备份服务器的 IP 地址为 10.164.10.1/24，对应的 MAC 地址为 0df0-fc01-003a。

操作步骤

步骤 1 在 Router 上为总裁办公室主机配置静态 ARP 表项。

创建 VLAN10。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 10
[Router-vlan10] quit
```

将接口 Ethernet0/0/0 加入 VLAN10。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port hybrid tagged vlan 10
```

配置接口 VLANIF10 的 IP 地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.164.1.20 255.255.255.0
[Router-Vlanif10] quit
```

配置总裁办公室主机的静态 ARP 表项。以 PC A 为例，IP 地址为 10.164.1.1，对应的 MAC 地址为 00e0-fc01-0001，VLAN 编号为 10，出接口为 Ethernet0/0/0。

```
[Router] arp static 10.164.1.1 00e0-fc01-0001 vid 10 interface ethernet 0/0/0
```

配置总裁办公室其他主机的静态 ARP 表项，配置方法同 PC A。

步骤 2 在 Router 上为文件备份服务器配置静态 ARP 表项。

配置 Ethernet2/0/0 的 IP 地址。

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 10.164.10.10 255.255.255.0
[Router-Ethernet2/0/0] quit
```

配置文件备份服务器的静态 ARP 表项，IP 地址为 10.164.10.1/24，对应的 MAC 地址为 0df0-fc01-003a。

```
[Router] arp static 10.164.10.1 0df0-fc01-003a
```

步骤 3 检查配置结果。

执行命令 **display current-configuration**，查看已配置的静态 ARP 表项。

```
<Router> display current-configuration | include arp
 arp static 10.164.1.1 00e0-fc01-0001 vid 10 interface ethernet 0/0/0
 arp static 10.164.1.2 00e0-fc01-0002 vid 10 interface ethernet 0/0/0
 arp static 10.164.1.3 00e0-fc01-0003 vid 10 interface ethernet 0/0/0
 arp static 10.164.10.1 0df0-fc01-003a
```

----结束

配置文件

以下给出 Router 的配置文件。

```
#
 sysname Router
#
vlan batch 10 20 30
#
interface Ethernet 0/0/0
 port hybrid tagged vlan 10
#
interface Ethernet 0/0/1
 port hybrid tagged vlan 20
#
interface Ethernet 0/0/2
```

```
 port hybrid tagged vlan 30
##
interface Vlanif 10
 ip address 10.2.2.2 255.255.255.0
#
interface Ethernet 2/0/0
 ip address 10.164.10.10 255.255.255.0
#
 arp static 10.164.1.1 00e0-fc01-0001 vid 10 interface ethernet 0/0/0
 arp static 10.164.1.2 00e0-fc01-0002 vid 10 interface ethernet 0/0/0
 arp static 10.164.1.3 00e0-fc01-0003 vid 10 interface ethernet 0/0/0
 arp static 10.164.10.1 0df0-fc01-003a
#
return
```

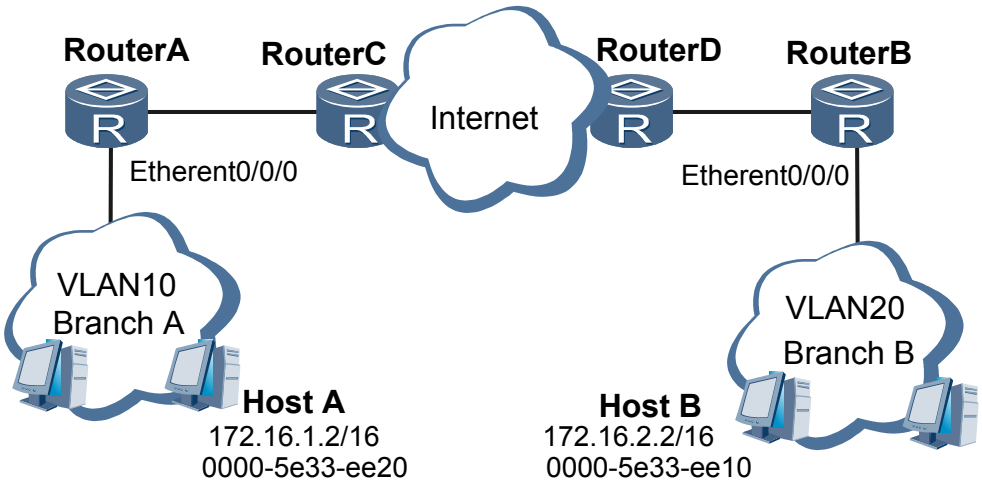
1.11.2 配置路由式 Proxy ARP 示例

该组网使用路由式 Proxy ARP 功能，实现属于同一网段但位于不同物理网络的两个子公司之间互相通信。

组网需求

如图 1-2 所示，某企业的子公司 A 和子公司 B 位于不同城市，子公司之间存在多个路由设备且路由可达，且所使用的 IP 地址属于同一个网段（172.16.0.0/16）。由于两个子公司之间被路由器间隔，属于不同的广播域，因此无法在同一个局域网内实现互通；子公司的主机没有配置默认网关，无法实现跨网段互通。现在公司需要在不改变主机配置的情况下，实现两个子公司之间的通信。

图 1-2 配置路由式 Proxy ARP 组网图



配置思路

采用如下的配置思路实现子公司 A 和子公司 B 之间互通：

1. 在 RouterA 上将连接子公司 A 的接口划分到 VLAN10，在 RouterB 上将连接子公司 B 的接口划分到 VLAN20。
2. 在子公司 A 和子公司 B 的 VLANIF 接口上使能路由式 Proxy ARP 功能，实现子公司 A 和子公司 B 互通。

数据准备

为完成此配置举例，需要准备如下数据：

- RouterA 连接子公司 A 的接口：Etherent0/0/0。
- RouterB 连接子公司 B 的接口：Etherent0/0/0。
- VLANIF10 的 IP 地址：172.16.1.1/24。
- VLANIF10 的 MAC 地址：00e0－fc39－80aa。
- VLANIF20 的 IP 地址：172.16.2.1/24。
- VLANIF20 的 MAC 地址：00e0－fc39－80bb。

操作步骤

步骤 1 配置 RouterA

创建 VLAN10。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan 10
[RouterA-vlan10] quit
```

将接口 Etherent0/0/0 加入 VLAN10。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type access
[RouterA-Ethernet0/0/0] port default vlan 10
[RouterA-Ethernet0/0/0] quit
```

配置接口 VLANIF10 的 IP 地址。

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 172.16.1.1 255.255.255.0
```

在接口 VLANIF10 上使能路由式 Proxy ARP 功能。

```
[RouterA-Vlanif10] arp-proxy enable
[RouterA-Vlanif10] quit
```

步骤 2 配置 RouterB

RouterB 的配置过程参照 RouterA。

步骤 3 验证配置结果

在子公司 A 选取一台主机 HostA（IP 地址：172.16.1.2/16），在子公司 B 选取一台主机 HostB（IP 地址：172.16.2.2/16）。在 HostA 上对 HostB 的 IP 地址执行 **ping** 命令。

```
C:\Documents and Settings\Administrator>ping 172.16.2.2
 PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/10/10 ms
```

查看 HostA 的 ARP 表，可以看到 HostB 所对应的 MAC 地址是接口 VLANIF10 的 MAC 地址。

```
C:\Documents and Settings\Administrator>arp -a
Interface: 172.16.1.2 --- 0x2
  Internet Address      Physical Address      Type
  172.16.2.2            00e0-fc39-80aa        dynamic
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
vlan batch 10
#
interface Vlanif 10
 ip address 172.16.1.1 255.255.255.0
 arp-proxy enable
#
interface ethernet 0/0/0
 port link-type access
 port default vlan 10
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
vlan batch 20
#
interface Vlanif 20
 ip address 172.16.2.1 255.255.255.0
 arp-proxy enable
#
interface ethernet 0/0/0
 port link-type access
 port default vlan 20
#
return
```

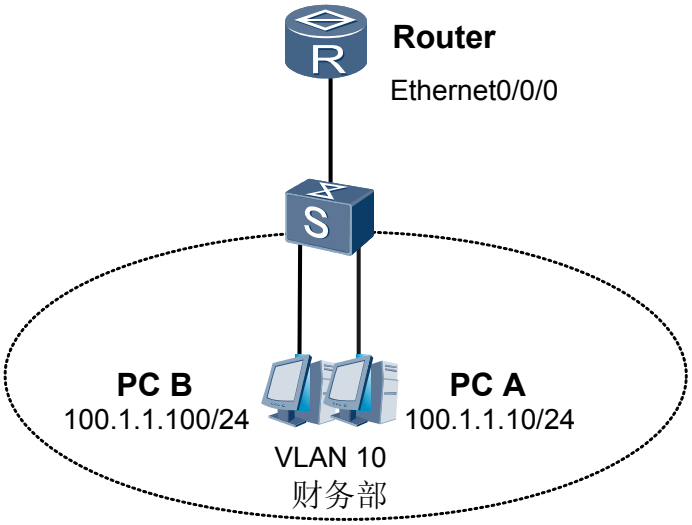
1.11.3 配置 VLAN 内 Proxy ARP 示例

该组网以位于同一个 VLAN 的企业部门为例，介绍为了隔绝广播风暴而采用 VLAN 内 Proxy ARP 进行三层通信的配置思路与配置过程。

组网需求

如图 1-3 所示，企业财务部的主机位于同一个 VLAN 内。部门主机访问外网时经常遭到病毒攻击，感染病毒的主机发送大量广播报文，在 VLAN 内产生广播风暴，严重时使部门主机不能正常通信。公司希望采取方法可以有效地隔离部门内的广播风暴，保证部门员工的正常通信以及信息安全。

图 1-3 配置 VLAN 内 Proxy ARP 组网图



配置思路

VLAN 内 Proxy ARP 的配置思路如下：

1. 在交换机的下行接口上配置接口隔离，禁止部门的主机之间进行二层通信，消除 VLAN 内的广播风暴的影响。
2. 在 VLANIF 接口上使能 VLAN 内的 Proxy ARP，在避免广播风暴的同时实现部门主机间的三层通信。

数据准备

为完成此配置举例，需要准备如下数据：

- Router 连接财务部的接口：Etherent0/0/0。
- 接口 Etherent0/0/0 所加入 VLAN 的 ID：10。
- 接口 VLANIF10 的 IP 地址:100.1.1.12/24。

操作步骤

步骤 1 配置接口 Etherent0/0/0 加入 VLAN10

创建 VLAN10。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 10
[Router-vlan10] quit
```

将接口 Etherent0/0/0 加入 VLAN10。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port hybrid tagged vlan 10
```

配置接口 VLANIF10 的 IP 地址。

```
[Router] interface vlanif 10
```

```
[Router-Vlanif10] ip address 100.1.1.12 255.255.255.0
[Router-Vlanif10] quit
```

步骤 2 配置交换机设备。

在交换机设备上创建 VLAN10，并将所有接口加入 VLAN10。配置连接用户的下行接口彼此隔离。（配置过程略）

步骤 3 配置 PC 的 IP 地址

分别为各 PC 配置 IP 地址，并使它们和接口 VLANIF10 的地址处于同一网段。

配置成功后，各 PC 与 Router 之间可以相互 Ping 通，但 PC 之间不能相互 Ping 通。

步骤 4 配置在接口 VLANIF10 上启动 VLAN 内 Proxy ARP

```
[Router] interface vlanif 10
[Router-Vlanif10] arp-proxy inner-sub-vlan-proxy enable
[Router-Vlanif10] quit
```

步骤 5 验证配置结果

选取部门内的两台主机 PC A 与 PC B，互相可以 Ping 通。

```
[Router] ping 100.1.1.100
 PING 100.1.1.100: 56  data bytes, press CTRL_C to break
    Reply from 100.1.1.100: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 100.1.1.100: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 100.1.1.100: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 100.1.1.100: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 100.1.1.100: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 100.1.1.100 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/10/10 ms
```

----结束

配置文件

Router 的配置文件

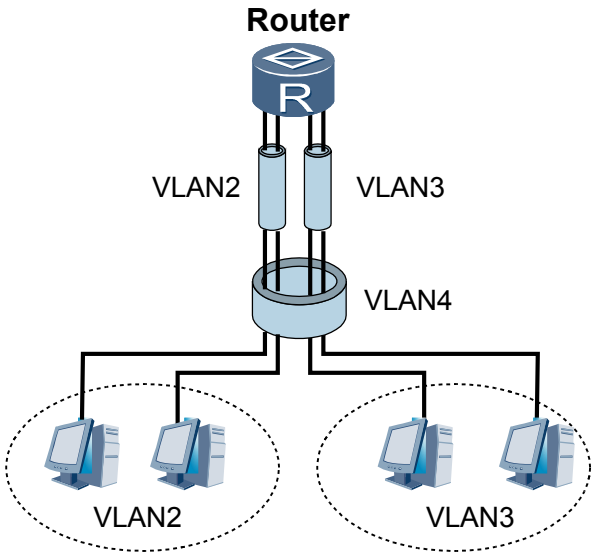
```
#
 sysname Router
#
vlan batch 10
#
interface Vlanif 10
 ip address 100.1.1.12 255.255.255.0
 arp-proxy inner-sub-vlan-proxy enable
#
interface ethernet 0/0/0
 port hybrid tagged vlan 10
#
return
```

1.11.4 配置 VLAN 间 Proxy ARP 示例

组网需求

如图 1-4 所示，VLAN2 和 VLAN3 组成 super-VLAN4，作为 sub-VLAN 的 VLAN2 和 VLAN3 内的主机之间不能互相 Ping 通。在配置 VLAN 间 Proxy ARP 后，VLAN2 和 VLAN3 内的主机之间可以互相 Ping 通。

图 1-4 配置 VLAN 间 Proxy ARP 组网图



配置思路

VLAN 间 Proxy ARP 的配置思路如下：

1. 配置 super-VLAN 和 sub-VLAN。
2. 将接口加入到从 sub-VLAN 中。
3. 创建 super-VLAN 的 VLANIF 接口并配置其 IP 地址。
4. 启动 VLAN 间 Proxy ARP。

数据准备

为完成此配置示例，需准备如下的数据：

- super-VLAN 和 sub-VLAN 的 VLANID。
- 接口 Ethernet0/0/0 和 Ethernet0/0/1 属于 sub-VLAN2。
- 接口 Ethernet0/0/2 和 Ethernet0/0/3 属于 sub-VLAN3。
- super-VLAN 的接口 VLANIF4 的 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0。

操作步骤

步骤 1 配置 super-VLAN 和 sub-VLAN。

配置 sub-VLAN2。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 2
[Router-vlan2] quit
```

将 Ethernet0/0/0 和 Ethernet0/0/1 加入到 sub-VLAN2 中。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port link-type access
[Router-Ethernet0/0/0] port default vlan 2
[Router-Ethernet0/0/0] quit
```

```
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type access
[Router-Ethernet0/0/1] port default vlan 2
[Router-Ethernet0/0/1] quit
```

配置 sub-VLAN3。

```
[Router] vlan 3
[Router-vlan3] quit
```

将 Ethernet0/0/2 和 Ethernet0/0/3 加入到 sub-VLAN3 中。

```
[Router] interface ethernet 0/0/2
[Router-Ethernet0/0/2] port link-type access
[Router-Ethernet0/0/2] port default vlan 3
[Router-Ethernet0/0/2] quit
[Router] interface ethernet 0/0/3
[Router-Ethernet0/0/3] port link-type access
[Router-Ethernet0/0/3] port default vlan 3
[Router-Ethernet0/0/3] quit
```

配置 super-VLAN4，并将 sub-VLAN2 和 sub-VLAN3 加入到 super-VLAN 中。

```
[Router] vlan 4
[Router-vlan4] aggregate-vlan
[Router-vlan4] access-vlan 2
[Router-vlan4] access-vlan 3
[Router-vlan4] quit
```

步骤 2 创建和配置接口 VLANIF4。

创建接口 VLANIF4。

```
[Router] interface vlanif 4
```

配置接口 VLANIF4 的 IP 地址

```
[Router-Vlanif4] ip address 10.10.10.1 24
```

步骤 3 在接口 VLANIF4 启动 VLAN 间 Proxy ARP。

```
[Router-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
[Router-Vlanif4] quit
```

步骤 4 检查配置结果。

执行命令 **display current-configuration**，查看 super-VLAN、sub-VLAN 以及 VLANIF 接口的相关配置。查询结果请见下面给出的配置文件。

执行命令 **display arp**，查看所有 ARP 表项。

```
<Router> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN
------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif4
10.10.10.2      00e0-fc00-0002  19        D-0         Ethernet0/0/0
                                          2/-
10.10.10.3      00e0-fc00-0003  19        D-0         Ethernet0/0/1
                                          2/-
10.10.10.4      00e0-fc00-0004  19        D-0         Ethernet0/0/2
                                          3/-
10.10.10.5      00e0-fc00-0005  19        D-0         Ethernet0/0/3
                                          3/-
------------------------------------------------------------------------------
Total:5         Dynamic:4       Static:0    Interface:1
```

----结束

配置文件

以下仅给出 Router 的配置文件。

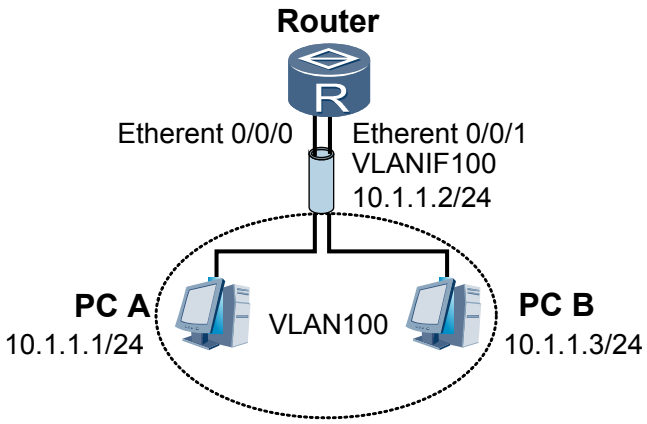
```
#
 sysname Router
#
 vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
 #
interface Vlanif4
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface ethernet 0/0/0
 port link-type access
 port default vlan 2
#
interface ethernet 0/0/1
 port link-type access
 port default vlan 2
#
interface ethernet 0/0/2
 port link-type access
 port default vlan 3
#
interface ethernet 0/0/3
 port link-type access
 port default vlan 3
#
return
```

1.11.5 配置 ARP 二层拓扑探测示例

组网需求

如图 1-5 所示，两个 Ethernet 接口以 default 方式加入 VLAN100，在设备上配置 ARP 二层拓扑探测功能，查看 ARP 表项的变化。

图 1-5 配置 ARP 二层拓扑探测组网图



配置思路

采用如下的思路配置二层拓扑探测：

1. 配置两个 Ethernet 接口以 default 方式加入 VLAN 100。
2. 使能二层拓扑探测功能，查看 ARP 表项的变化。

数据准备

完成此配置，需准备如下的数据：

- 要加入 VLAN 的接口类型和接口编号
- VLANIF 接口和 PC 的 IP 地址

操作步骤

步骤 1 创建 VLAN100，并配置 Router 的两个 Ethernet 接口以 default 方式加入 VLAN。

创建 VLAN100，配置 VLANIF 接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] interface vlanif 100
[Router-vlanif100] ip address 10.1.1.2 24
[Router-vlanif100] quit
```

配置 Ethernet 接口以 default 方式加入 VLAN100。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port link-type access
[Router-Ethernet0/0/0] port default vlan 100
[Router-Ethernet0/0/0] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type access
[Router-Ethernet0/0/1] port default vlan 100
[Router-Ethernet0/0/1] quit
```

步骤 2 使能二层拓扑探测功能。

```
[Router] l2-topology detect enable
```

步骤 3 重启接口 Ethernet0/0/0，并查看 ARP 表项及老化时间的变化。

查看 Router 的 ARP 表项，可以看到 Router 已经学习到了 PC 的 MAC 地址。

```
[Router] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M)  TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900              I -           Vlanif100
10.1.1.1        00e0-c01a-4901  20          D-0           Ethernet0/0/0
10.1.1.3        00e0-de24-bf04  20          D-0           Ethernet0/0/1
--------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0    Interface:1
```

依次 **shutdown**、**undo shutdown** 接口 Ethernet0/0/0，并查看 ARP 表项的老化时间。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] shutdown
[Router-Ethernet0/0/0] undo shutdown
[Router-Ethernet0/0/0] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
```

```
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900            I -           Vlanif100
10.1.1.3        00e0-de24-bf04  0         D-0           Ethernet0/0/1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

说明

由输出信息可以看到，Ethernet0/0/0 被 shutdown 之后，从 Ethernet0/0/0 学习到的 ARP 表项被删除。Ethernet0/0/0 被 undo shutdown，接口状态重新变为 Up 后，Ethernet0/0/1 学习到的 ARP 表项的老化时间变为 0。

当老化时间变为 0 时，设备会发送 ARP 老化探测报文，更新 ARP 表项。

```
[Router-Ethernet0/0/0] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900            I -           Vlanif100
10.1.1.3        00e0-de24-bf04  20        D-0           Ethernet0/0/1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

说明

表项更新后，老化时间重新变为默认值 20（分钟）。

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
l2-topolgy detect enable
#
 vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Ethernet 0/0/0
 port link-type access
 port default vlan 100
#
interface Ethernet 0/0/1
 port link-type access
 port default vlan 100
#
return
```

2 IP 地址配置

关于本章

通过为网络设备配置 IP 地址，可以实现网络设备之间数据的通信。

2.1 IP 地址概述
介绍 IP 地址的概念。

2.2 AR1200 支持的 IP 地址特性
介绍 AR1200 支持的 IP 地址配置方法。

2.3 配置接口的 IP 地址
介绍接口配置 IP 地址的方法。

2.4 配置接口借用 IP 地址
介绍接口借用其他接口 IP 地址的方法。

2.5 配置举例
举例说明 IP 地址的配置。

2.1 IP 地址概述

介绍 IP 地址的概念。

在 IP 网络中通信，每个主机都需要拥有一个 IP 地址。

IP 地址是在 Internet 上使用的 32 比特地址，由网络号和主机号两部分组成。

IP 地址的网络号字段用来标识一个网络，主机号字段用来标识网络中的具体某台网络设备。对这些设备而言，无论实际所处的物理位置如何，只要它们的网络号相同，它们就处在同一个网络中。

2.2 AR1200 支持的 IP 地址特性

介绍 AR1200 支持的 IP 地址配置方法。

说明

本手册中，IP 地址是指 IPv4 地址。

AR1200 支持以下几种 IP 地址的配置方法：

- 静态手工配置接口的 IP 地址。
- 接口借用其他接口的 IP 地址。
- 利用 PPP 协议的地址协商功能为客户端接口分配 IP 地址。

为节约 IP 地址空间，AR1200 支持将 P2P 接口的 IP 地址掩码长度配置为 31 位。配置 31 位掩码后，同一个网段下将只有两个 IP 地址，即网段地址和该网段广播地址，均被解释为主机地址。

AR1200 支持将 Loopback 接口的 IP 地址掩码长度配置为 32 位。

2.3 配置接口的 IP 地址

介绍接口配置 IP 地址的方法。

2.3.1 建立配置任务

在配置接口的 IP 地址前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

为了运行 IP 业务，需要为接口配置 IP 地址。AR1200 的每个接口可以配置多个 IP 地址，其中一个主 IP 地址，其余为从 IP 地址。

一般情况下，一个接口只需要配置一个主 IP 地址，但在有些特殊情况下需要配置从 IP 地址。例如，一台 AR1200 通过一个接口连接了一个物理网络，但该物理网络的设备分别属于两个不同的网络，为了使 AR1200 与物理网络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。

说明

AR1200 不支持在二层接口上配置 IP 地址。

前置任务

在配置接口的 IP 地址之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理状态为 Up。
- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up。

数据准备

在配置接口的 IP 地址之前，需要准备如下数据。

序号	数据
1	接口的编号。
2	接口的主 IP 地址和子网掩码。
3	（可选）接口的从 IP 地址和子网掩码。

2.3.2 配置接口的主 IP 地址

接口上的主 IP 地址只能为一个。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的主 IP 地址。

一个接口只能有一个主 IP 地址，当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。

----结束

2.3.3 (可选)配置接口的从 IP 地址

当接口需要与不同网段的主机进行通信时，需要为该接口配置从 IP 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } **sub**，配置接口的从 IP 地址。

如果用户需要为接口配置多个从 IP 地址，可以反复执行此步骤。每个接口最多可以配置 31 个从 IP 地址。

----结束

2.3.4 检查配置结果

操作步骤

- 使用 **display ip interface** [*interface-type interface-number*]命令，查看接口上的 IP 地址的相关配置信息。
- 使用 **display ip interface brief** [*interface-type* [*interface-number*]]命令，查看接口上 IP 地址的简要信息。

----结束

任务示例

查看 GigabitEthernet1/0/0 接口的 IP 地址的相关配置信息。

```
<Huawei> display ip interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 11022, bytes : 660443, multicasts : 0
output packets : 9634, bytes : 533292, multicasts : 0
Directed-broadcast packets:
 received packets:         1796, sent packets:              0
 forwarded packets:           0, dropped packets:           0
ARP packet input number:       52872
  Request packet:              52852
  Reply packet:                   20
  Unknown packet:                  0
Internet Address is 10.137.217.210/23
Broadcast address : 10.137.217.255
TTL being 1 packet number:         0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

查看 GigabitEthernet1/0/0 接口的 IP 地址的简要信息。

```
<Huawei> display ip interface brief gigabitethernet 1/0/0
*down: administratively down
(l): loopback
(s): spoofing
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet1/0/0              10.137.217.210/23    up         up
```

2.4 配置接口借用 IP 地址

介绍接口借用其他接口 IP 地址的方法。

2.4.1 建立配置任务

在配置 IP 地址借用前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

在有些应用环境下，为了节约 IP 地址资源，需要配置某个接口借用其他接口的 IP 地址。有时某个接口只是偶尔使用，这种情况也可配置该接口借用其他接口的 IP 地址，而不必让其一直占用一个单独的 IP 地址。

前置任务

在配置接口借用 IP 地址之前，需完成以下任务：

- 配置借用接口和被借用接口的物理特性。
- 配置借用接口和被借用接口的链路层协议。

数据准备

在配置接口借用 IP 地址之前，需要准备如下数据。

序号	数据
1	被借用接口的编号及其 IP 地址和掩码。
2	借用接口的编号。

说明

这里的配置过程仅包含配置接口借用 IP 地址的过程，不包括配置到对端网段的静态路由的过程。

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，所以必须手工配置一条到对端网段的静态路由，才能实现设备路由间的连通。

2.4.2 配置被借用接口的主 IP 地址

背景信息

说明

这里的配置过程仅包含配置接口借用 IP 地址的过程，不包括配置到对端网段的静态路由的过程。

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，所以必须手工配置一条到对端网段的静态路由，才能实现设备路由间的连通。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入被借用接口的接口视图。

被借用接口可以是以太网接口、Loopback 接口、Eth-trunk 接口、VLANIF 接口等接口。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置被借用接口的主 IP 地址。

一个接口只能有一个主 IP 地址，当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。

----结束

2.4.3 配置接口借用 IP 地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入借用接口的接口视图。

封装了 PPP、HDLC 的接口以及 ATM 接口、Tunnel 接口等接口可借用其他接口的 IP 地址。

封装了 FR 的 P2P 子接口可借用其他接口的 IP 地址。

以太接口可以借用 Loopback 接口的 IP 地址。

步骤 3 执行命令 **ip address unnumbered interface** *interface-type interface-number*，配置接口借用指定接口的 IP 地址。

----结束

2.4.4 检查配置结果

操作步骤

- 执行 **display ip interface** [*interface-type interface-number*]命令，查看接口上的 IP 地址的相关配置信息。
- 执行 **display ip interface brief** [*interface-type* [*interface-number*]]命令，查看接口上 IP 地址的简要信息。

----结束

任务示例

查看 GE2/0/0 借用 LoopBack0 的 IP 地址的配置情况。

```
<Huawei> display ip interface gigabitethernet 2/0/0

GigabitEthernet2/0/0 is standby,
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
```

```
Directed-broadcast packets:
 received packets:            0, sent packets:              0
 forwarded packets:           0, dropped packets:           0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
  Internet Address is unnumbered, using address of LoopBack0(202.117.23.45/24)
Broadcast address : 202.117.23.255
TTL being 1 packet number:         0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

2.5 配置举例

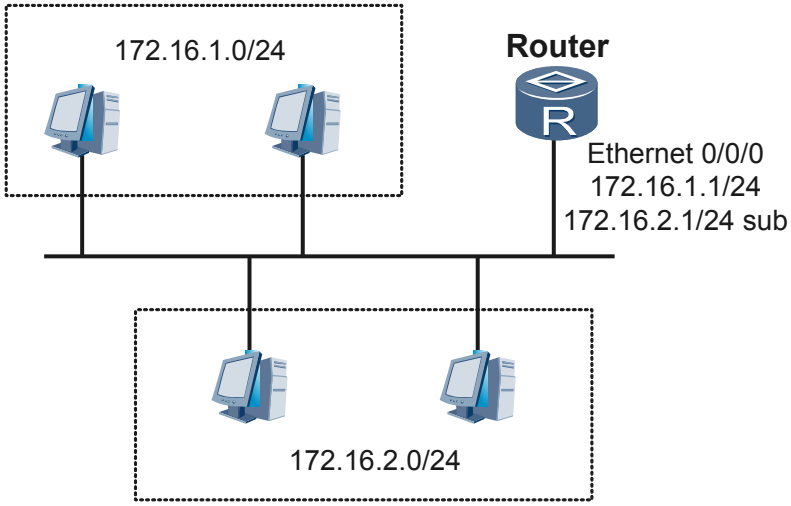
举例说明 IP 地址的配置。

2.5.1 配置接口的主从 IP 地址示例

组网需求

如图 2-1 所示，Router 上只有一个空闲以太网接口 Ethernet0/0/0，但该局域网中的计算机分别属于 2 个不同的网段 172.16.1.0/24 和 172.16.2.0/24，为使用户不修改当前的主机地址同时又能通过 Router 访问外部网络，此时在以太网接口 Ethernet0/0/0 上配置主 IP 地址 172.16.1.1/24 和从 IP 地址 172.16.2.1/24，用来接入两个不同的网段。

图 2-1 配置 IP 地址示例



配置思路

配置主从 IP 地址的思路如下：

1. 分析接口所连接的网段地址。
2. 配置接口的主从 IP 地址。

数据准备

为完成此配置举例，需要准备如下的数据：

- 接口的主 IP 地址和子网掩码。
- 接口的从 IP 地址和子网掩码。

操作步骤

步骤 1 配置 Router 的接口 Ethernet0/0/0 的主从 IP 地址

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] ip address 172.16.1.1 24
[Router-Ethernet0/0/0] ip address 172.16.2.1 24 sub
```

步骤 2 验证配置结果

从 Router 上 Ping 网段 172.16.1.0 内的主机，可通。

```
<Router> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=128 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

从 Router 上 Ping 网段 172.16.2.0 内的主机，可通。

```
<Router> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

----结束

配置文件

Router 的配置文件。

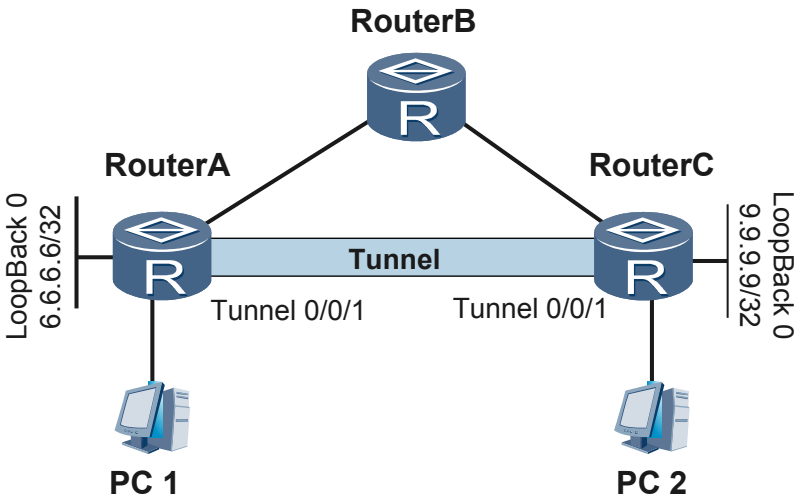
```
#
 sysname Router
#
interface 0/0/0
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
return
```

2.5.2 配置接口借用 IP 地址示例

背景信息

如图 2-2 所示，RouterA 的 Tunnel0/0/1 接口与 RouterC 通过隧道相连。RouterA 和 RouterC 的 Tunnel0/0/1 接口不常用，为了节省 IP 地址，配置 RouterA 的 Tunnel0/0/1 接口借用 RouterA 的 Loopback0 接口的 IP 地址，并配置 RouterC 的 Tunnel0/0/1 接口借用 RouterC 的 Loopback0 接口的 IP 地址。

图 2-2 配置 Tunnel 接口借用 Loopback 接口组网图



配置思路

配置思路如下：

- 配置 RouterA 及 RouterC 的 Loopback0 接口的 IP 地址。
- 配置 OSPF。
- 配置 RouterA 的 Tunnel0/0/1 信息，包括该接口借用 Loopback0 接口的 IP 地址。
- 配置 RouterC 的 Tunnel0/0/1 信息，包括该接口借用 Loopback0 接口的 IP 地址。

数据准备

为完成此配置举例，需要准备如下数据：

- RouterA 的 Loopback0 接口的 IP 地址。

- RouterC 的 Loopback0 接口的 IP 地址。

说明

本例的操作步骤和配置文件只列出与接口借用 IP 地址配置相关的信息。

操作步骤

步骤 1 配置 RouterA。

配置 RouterA 的 Loopback0 接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 6.6.6.6 32
[RouterA-LoopBack0] quit
```

配置 OSPF。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Tunnel0/0/1 接口借用 Loopback0 接口的 IP 地址。

```
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] ip address unnumbered interface loopback 0
[RouterA-Tunnel0/0/1] quit
```

步骤 2 RouterC 的配置步骤参见 RouterA 的配置。

步骤 3 检查配置结果。

在 RouterA 上检查 Tunnel0/0/1 的配置结果。

```
<RouterA> display ip interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:           0
Internet Address is unnumbered, using address of LoopBack0(6.6.6.6/32)
Broadcast address : 6.6.6.6
TTL being 1 packet number:         0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
```

```
Netmask reply:                0
Unknown type:                 0
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface LoopBack0
 ip address 6.6.6.6 255.255.225.255
#
interface Tunnel 0/0/1
 ip address unnumbered interface LoopBack0
#
ospf 1
 area 0.0.0.0
  network 6.6.6.6 0.0.0.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface LoopBack0
 ip address 9.9.9.9 255.255.225.255
#
interface Tunnel 0/0/1
 ip address unnumbered interface LoopBack0
#
ospf 1
 area 0.0.0.0
  network 9.9.9.9 0.0.0.0
#
return
```

3 IPv6 基础配置

关于本章

IPv6 协议栈是 IPv6 网络中路由协议和应用协议的支撑。

3.1 IPv6 概述
IPv6 是 IPv4 的升级版本，解决了目前 IPv4 存在的许多不足之处。

3.2 AR1200 支持的 IPv6 特性
IPv6 协议栈实现的基本功能包括 IPv6 地址配置、IPv6 邻居发现、路由器通告、ICMPv6 报文控制、PMTU。IPv6 协议栈是路由协议和应用协议的支撑。

3.3 配置接口的 IPv6 地址
手工为网络设备配置 IPv6 地址，使该设备可以与网络上其他设备进行通信。

3.4 配置 IPv6 邻居发现
IPv6 邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议代替了 IPv4 中的 ARP 协议（Address Resolution Protocol）、ICMP 设备发现消息（Router Discovery）和 ICMP 重定向消息（Redirect）。新增了邻居可达性检测功能。

3.5 配置 IPv4/IPv6 双协议栈
为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界路由器上启动 IPv4/IPv6 双协议栈。

3.6 配置 PMTU
通过配置 PMTU，在网络中使用一个合适的 MTU 值来发送报文，使得报文在整个传输过程中不需要分片，减轻中间路由器的工作压力，以便有效地利用网络资源并得到最佳的吞吐量。

3.7 配置 TCP6
通过对 TCP6 报文的相关设置，可以提高网络的性能。

3.8 维护 IPv6
维护 IPv6 包括清除 IPv6 运行信息、监控 IPv6 运行状况。

3.9 配置举例
配置示例中包括组网需求、配置注意事项、配置思路等。举例说明接口 IPv6 地址的配置以及邻居发现协议的配置。

3.1 IPv6 概述

IPv6 是 IPv4 的升级版本，解决了目前 IPv4 存在的许多不足之处。

IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation），它是 Internet 工程任务组（IETF）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别就是 IP 地址的长度从 32 位升为 128 位。

3.2 AR1200 支持的 IPv6 特性

IPv6 协议栈实现的基本功能包括 IPv6 地址配置、IPv6 邻居发现、路由器通告、ICMPv6 报文控制、PMTU。IPv6 协议栈是路由协议和应用协议的支撑。

AR1200 支持 IPv6 协议族以及 TCP6 协议族。

AR1200 支持在下列接口配置 IPv6 功能：

- Ethernet 接口及子接口
- Gigabit-Ethernet 接口及子接口
- Serial 接口（只有 link-protocol 为 PPP 或 HDLC 的 Serial 接口支持 IPv6 功能）
- POS 接口（只有 link-protocol 为 PPP 或 HDLC 的 POS 接口支持 IPv6 功能）
- Tunnel 接口
- Loopback 接口
- Eth-Trunk 接口、Eth-Trunk 子接口、IP-Trunk 接口
- VLANIF 接口

IPv6 地址

IPv6 的 128 位 IP 地址有以下两种表示形式。

- X:X:X:X:X:X:X:X

  在这种形式中，128 位的 IP 地址被分为 8 组，每组的 16 位用 4 个十六进制字符（0 ～ 9，A ～ F）来表示，组和组之间用冒号（:）隔开。其中每个“X”代表一组十六进制数值。
- X:X:X:X:X:X:d.d.d.d

  分为如下两种类型：

  - IPv4 兼容 IPv6 地址
  - IPv4 映射 IPv6 地址

  在这种形式中，“X”代表高阶的六组数字，用十六进制数来表示每组的 16 比特。“d”代表低阶的四组数字，用十进制数表示每组的 8 比特。后边的部分（d.d.d.d）其实就是一个标准的 IPv4 地址。

一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID。
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID。

源/目的地址选择

当网络管理者需要指定和预知系统发送报文的源/目的地址时，可以定义一组地址选择规则，这些规则构成地址选择策略表。该表类似于路由表，使用最长匹配原则查找规则。地址选择的结果是由源地址和目的地址共同决定的。

IPv6 邻居发现

IPv6 邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议代替了 IPv4 中的 ARP 协议（Address Resolution Protocol）和 ICMP 路由器发现消息（Router Discovery），并提供了其他功能。

IPv6 的 PMTU

网络中不同网络的 MTU 值不同的问题可以通过以下两种方法来解决：

- 路由器根据需要对报文进行分片。这对于源端主机来说很容易，但是需要中间路由器来完成分片和重组的工作。
- 源端主机使用一个合适的 MTU 值来发送报文，使报文在中间路由器不需要分片，减轻中间路由器的工作压力。由于 IPv6 中间路由器不支持对 IPv6 报文进行分片，所以 IPv6 报文的分片只能采用这种方法。

PMTU 发现（Path MTU Discovery）机制的目的就是要找到一个从源端到目的端的路径上的最小 MTU 值。

IPv6 的 FIB 特性

为了连接不同的网络拓扑需要运行不同的路由协议，这样就产生了 RIB（Routing Information base）。RIB 是创建 FIB 的基础，路由器会根据路由管理策略，从 RIB 中提取出最小转发信息并放入 FIB。用户还可通过路由管理向 FIB 中增加静态路由。

FIB（Forwarding Information Base）中包含了路由器在转发报文时所必需的一组最小信息。一个 FIB 条目中一般包括目的地址、前缀长度、传输端口、下一跳地址、标明路由特征的标志以及时间戳。路由器使用 FIB 的各项来转发报文。

FIB 的操作包括两个单独的部分，用于控制平面的是 FibAgent，用于转发平面的是 FibContainer。控制平面（FibAgent）负责跟 RM 模块交互，将 FIB 下载到转发引擎，对于分布式系统，还需要将 FIB 下载到 I/O 板。

FIB 包含的元素有：

- Destination address：报文发送的目的网络地址或主机地址。
- Prefix length：目的地址前缀长度，可确定目的地址是否对应网络或主机。
- Nexthop：为了将报文发送到目的地址所要经过的紧邻的下一跳地址。
- Flag(s)：标明路由特征。
- Interface：报文的出接口。
- Timestamp：FIB 项生成的时间。
- Tunnel ID：Tunnel 隧道 ID。

说明

IPv6 功能需要使用 License 授权。缺省情况下，设备所有的 IPv6 功能受限无法使用。如果需要使用 IPv6 功能，请联系华为办事处申请并购买如下 License:

- AR1200 数据业务增值包

3.3 配置接口的 IPv6 地址

手工为网络设备配置 IPv6 地址，使该设备可以与网络上其他设备进行通信。

3.3.1 建立配置任务

介绍配置接口的 IPv6 地址的应用环境、前置任务、数据准备和配置过程。

应用环境

在路由器与 IPv6 设备通信时，需要为接口配置 IPv6 地址。

AR1200 支持在下列接口配置 IPv6 地址：

- Ethernet 接口及子接口
- GigabitEthernet 接口及子接口
- Tunnel 接口
- Loopback 接口
- Eth-Trunk 接口、Eth-Trunk 子接口（只有转换为三层模式后支持 IPv6 功能）
- VLANIF 接口
- VT 接口
- VE 接口

每个接口最多可配置 10 个地址，包括链路本地地址和全球单播地址。

链路本地地址用于邻居发现协议和无状态自动配置进程中链路本地节点之间的通信。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。

链路本地地址可以通过自动生成或手动配置两种方式获得：使能系统自动配置链路本地地址的命令后，系统将为接口自动生成一个链路本地地址；手动配置的链路本地地址必须是一个有效的链路本地地址（FE80::/10）。

因为链路本地地址只能用于链路本地节点之间的通信，通常用于满足协议的通信需求，与用户间的通信没有直接关系，所以推荐使用链路本地地址的自动生成方式。

全球单播地址等同于 IPv4 公网地址，用于公网上的数据转发，是用户通信所必需的地址。

EUI-64 地址与全球单播地址作用相同，区别是前者只需指定网络位，其主机位由接口的 MAC 地址转化而来，而后者需要指定整个 128bit 的完整地址。需要注意的是，EUI-64 地址指定的网络位前缀长度（prefix-length）不能大于 64。

EUI-64 地址和全球单播地址可以同时配置，也可以任选其一，都可以完成正常通信；但是同一接口下配置的多个地址不能属于同一网段。

前置任务

在配置接口的 IPv6 地址之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up

数据准备

在配置接口的 IPv6 地址之前，需准备以下数据。

序号	数据
1	接口的编号
2	手动配置的链路本地地址
3	全球单播地址和前缀长度

3.3.2 启动 IPv6 报文转发功能

在接口视图下使能了 IPv6 功能，才能在接口下进行其他 IPv6 相关的配置。如果希望接口可以转发 IPv6 报文，还必须在系统视图下使能 IPv6 功能。

背景信息

如果要使能接口对 IPv6 报文进行转发的功能，必须同时使能系统视图下和接口视图下的 IPv6 功能。因为：

- 在系统视图下执行命令 **ipv6**，只是使能了路由器对 IPv6 报文的转发功能，并没有使能接口的 IPv6 功能，也不能进行 IPv6 的相关配置。
- 在接口视图下执行命令 **ipv6 enable**，只是使能了接口的 IPv6 功能，路由器不能对 IPv6 报文进行转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6**，使能路由器 IPv6 报文转发能力。

缺省情况下，路由器不使能对 IPv6 报文的转发能力。

如果要对 IPv6 报文进行转发，必须先在系统视图下使能路由器的 IPv6 报文转发能力。否则即使在接口上使能了 IPv6 功能，路由器也无法转发 IPv6 的报文。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入需要使能 IPv6 功能的接口视图。

步骤 4 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

如果要在接口视图下进行 IPv6 的相关配置，必须先在接口视图下使能 IPv6 功能。

缺省情况下，接口下不使能 IPv6 功能。

----结束

3.3.3 配置接口的链路本地 IPv6 地址

链路本地地址用于邻居发现协议和无状态自动配置进程中链路本地上节点之间的通信。链路本地地址只在本地链路有效。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 请根据不同情况进行以下配置。

- 如果配置接口的自动链路本地地址，请执行命令 **ipv6 address auto link-local**。
- 如果手动配置接口的链路本地地址，请执行命令 **ipv6 address** *ipv6-address* **link-local**。

如果不使用命令配置接口的链路本地地址，当**配置接口的全球单播 IPv6 地址**后，会自动生成一个链路本地地址。

----结束

3.3.4 配置接口的全球单播 IPv6 地址

全球单播地址等同于 IPv4 公网地址，可用于路由前缀可以聚合的链路，降低路由表项的数量。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } 或 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**，配置接口的全球单播地址。

----结束

3.3.5 配置接口的 IPv6 任播地址

任播地址用来标识一组接口。

背景信息

任播地址（Anycast）共享单播地址资源。它用来标识一组接口，通常这组接口属于不同的节点。

- 与组播地址一样，多个节点都监听这个地址，因此任播地址只能作为目的地址使用。
- 与组播地址不同，发送到任播地址的数据包被传输给此地址所标识的一组接口中距离源节点最近的一个接口（最“近”的一个，是指根据路由协议的距离度量）。

在 AR1200 实现中，当需要使用 6to4 隧道实现 6to4 网络与本地（Native）IPv6 网络通信时，可以在 6to4 中继路由设备的 Tunnel 接口上配置前缀为 **2002:c058:6301/48** 的任播地址。

也可以通过在 6to4 中继路由设备的 Tunnel 接口上配置 6to4 地址实现以上功能，但是当网络中存在多个 6to4 中继路由设备时，两者的区别在于：

- 如果使用 6to4 地址，需要在每个设备的 Tunnel 接口上分别配置不同的地址。
- 如果使用任播地址，只需在每个设备的 Tunnel 接口上配置同一个地址，减少了地址个数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**，配置接口的任播 IPv6 地址。

----结束

3.3.6 检查配置结果

完成接口的 IPv6 地址配置后，可以查看接口的 IPv6 地址的配置信息。

前提条件

已经完成 IPv6 地址的所有配置。

操作步骤

- 使用 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令查看接口 IPv6 信息。
- 使用 **display ipv6 statistics** 命令查看 IPv6 报文统计信息。

----结束

任务示例

执行命令 **display ipv6 interface**，能够查看接口配置的 IPv6 地址。

```
<Huawei> display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00 [TENTATIVE]
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF04:5D00
    FF02::2
    FF02::1
  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
```

执行命令 **display ipv6 interface brief**，能够查看接口配置的 IPv6 地址以及接口状态。

```
<Huawei> display ipv6 interface brief
*down: administratively down
(l): loopback
```

```
(s): spoofing
Interface                   Physical            Protocol
GigabitEthernet2/0/0        up                  up
[IPv6 Address] 2030::101:101
GigabitEthernet2/0/1        up                  up
[IPv6 Address] 2001::1
LoopBack0                   up                  up(s)
[IPv6 Address] Unassigned
```

执行命令 **display ipv6 statistics**，能够查看 IPv6 报文统计信息。

```
<Huawei> display ipv6 statistics
IPv6 Protocol:

  Sent packets:
    Total              : 3630
    Local sent out     : 3630       Forwarded          : 0
    Raw packets        : 0          Discarded          : 0
    Fragmented         : 0          Fragments          : 0
    Fragments failed   : 0          Multicast          : 0

  Received packets:
    Total              : 3630       Local host         : 3630
    Hop count exceeded : 0          Header error       : 0
    Too big            : 0          Routing failed     : 0
    Address error      : 0          Protocol error     : 0
    Truncated          : 0          Option error       : 0
    Fragments          : 0          Reassembled        : 0
    Reassembly timeout : 0          Multicast          : 0
```

3.4 配置 IPv6 邻居发现

IPv6 邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议代替了 IPv4 中的 ARP 协议（Address Resolution Protocol）、ICMP 设备发现消息（Router Discovery）和 ICMP 重定向消息（Redirect）。新增了邻居可达性检测功能。

3.4.1 建立配置任务

介绍配置 IPv6 邻居发现的应用环境、前置任务、数据准备和配置过程。

应用环境

对于一个节点而言，当其配置一个 IPv6 地址之后，首先会确定此地址是否可用、不冲突。当一个节点是主机时，路由器需要通知主机向特定目的地址转发报文的理想下一跳地址；当一个节点是路由器时，需要发布自己的地址、地址前缀和其他配置参数以指导主机进行参数配置。在 IPv6 报文转发过程中，节点需要确定邻居节点的链路层地址和其可达性。可以通过邻居发现功能来实现这些要求。

大部分的 ND 配置是基于接口来实现的。

目前支持在以下接口配置 IPv6 ND：

- Ethernet 接口及子接口
- GigabitEthernet 接口及子接口
- Tunnel 接口
- Eth-Trunk 接口、Eth-Trunk 子接口

- VLANIF 接口

前置任务

在配置 IPv6 ND 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数
- 配置接口的 IPv6 地址

数据准备

在配置 IPv6 ND 之前，需准备以下数据。

序号	数据
1	需要配置 IPv6 ND 的接口的编号
2	静态邻居的 IPv6 地址和 MAC 地址
3	RA 消息的发布间隔时间、前缀和存活时间
4	自动配置的标志位
5	ND 的跳数限制
6	DAD 发送次数
7	NS 消息重传时间间隔
8	NUD 可达时间
9	接口 MTU

3.4.2 配置静态邻居

通过手工配置静态邻居，可以获得邻居的 IPv6 地址和 MAC 地址的映射关系。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 根据不同类型的接口，执行以下命令：

- 配置普通三层接口的静态邻居表项时，执行 **ipv6 neighbor** *ipv6-address mac-address* 命令。
- 配置 VLANIF 接口的静态邻居表项时，执行 **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number* 命令。
- 配置 QinQ 终结子接口或 Dot1q 终结子接口的静态邻居表项时，执行 **ipv6 neighbor** *ipv6-address mac-address* **vid** *vid* [**cevid** *cevid*]命令。

说明

如果接口配置了动态 QinQ，则不允许配置静态邻居表项。

可以在接口或其子接口上配置静态邻居，每个接口最多可配置 300 项。

----结束

3.4.3 打开 RA 消息的发布开关

打开路由器通告的开关，设备可以发布 RA 报文，为主机提供前缀等信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 （可选）执行命令 **undo ipv6 nd ra halt**，使能 RA 消息的发布功能。

----结束

3.4.4 配置 RA 消息的发布周期

路由器周期性的发布 RA 报文，其中包括前缀和一些标志位的信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ipv6 nd ra** { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }，配置 RA 消息发布间隔时间。

缺省情况下，最大时间间隔是 600 秒，最小时间间隔是 200 秒。

最大时间间隔不能小于最小时间间隔。

当 RA 报文的最大发布间隔设置为小于 9 秒时，将最小发布间隔时间调整为与最大发布间隔时间相同。

----结束

3.4.5 配置需要发布的地址前缀信息

本地链路上的节点可以使用这些前缀完成地址自动配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ipv6 nd ra prefix** { *ipv6-address ipv6-prefix-length* | *ipv6-prefix*/*ipv6-prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]，配置 RA 消息中的前缀。

----结束

3.4.6 配置需要发布的其他信息

RA 报文中携带路由器发布报文的跳数限制、前缀选项、邻居可达时间、RA 报文的存活时间。

背景信息

重复地址检测 DAD（Duplicate Address Detect）是 IPv6 进行地址自动配置时的一个过程，可以配置连续发送的 DAD 消息的数量。

设置路由器发送邻居请求 NS（Neighbor Solicitation）消息的时间间隔。缺省情况下，NS 重传间隔时间是 1000 毫秒。

NUD（Neighbor Unreachability Detection）表示邻居不可达性检测。缺省情况下，NUD 可达时间为 30000 毫秒。

接口的最大传输单元 MTU 确定了接口上的 IP 报文是否需要分片。接口 MTU 的缺省值根据接口类型的不同而不同，GigabitEthernet 的 MTU 为 1500 字节。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 nd hop-limit** *limit*，配置跳数限制。

参数 *limit* 的取值范围是 1 ～ 255。缺省情况下，跳数限制为 64 跳。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **ipv6 nd ra hop-limit** *limit*，配置跳数限制。

limit 的取值范围是 0 ～ 255。缺省情况下，跳数限制为 64 跳。

说明

- 如果接口下配置了 **ipv6 nd ra hop-limit** 命令，则发送的 RA 报文中的跳数限制以接口的配置为准。
- 如果接口下没有配置 **ipv6 nd ra hop-limit** 命令，则发送的 RA 报文中的跳数限制以全局配置的为准，即以 **ipv6 nd hop-limit** 命令配置的为准。

步骤 5 执行命令 **ipv6 nd ra router-lifetime** *ra-lifetime*，配置 RA 消息的存活时间。

说明

- 在执行 **ipv6 nd ra** 命令设置 RA 消息的发布间隔时间时，发布间隔时间应该小于或等于 IPv6 RA 消息的存活时间。
- 缺省情况下，RA 消息的发布最大间隔时间为 600 秒，最小间隔时间为 200 秒。
- 缺省情况下，RA 消息的存活时间为 1800 秒。如果配置了 RA 消息的前缀信息，存活时间仍为 1800 秒。

步骤 6 执行命令 **ipv6 nd dad attempts** *value*，配置 DAD 发送次数。

步骤 7 执行命令 **ipv6 nd ns retrans-timer** *interval*，配置 NS 消息重传时间间隔。

步骤 8 执行命令 **ipv6 nd nud reachable-time** *value*，配置 NUD 可达时间。

步骤 9 执行命令 **ipv6 mtu** *mtu*，配置接口 MTU。

----结束

后续处理

修改了 IPv6 的 MTU 值之后，需要在该接口视图下依次执行 **shutdown** 和 **undo shutdown** 命令，配置才会生效。

3.4.7 配置默认路由器优先级和路由信息

通过在本链路内发布携带默认路由器优先级和路由信息的 RA 报文，帮助主机在发送报文时选择合适的转发路由器。

背景信息

当主机所在的链路中存在多个路由器时，主机需要根据报文的目的地址选择转发路由器。在这种情况下，路由器通过发布默认路由器优先级和特定路由信息给主机，提高主机根据不同的目的地选择合适的转发路由器的能力。

主机收到包含路由信息的 RA 报文后，会更新自己的路由表。当主机向其他设备发送报文时，通过查询该列表的路由信息，选择合适的路由发送报文。

主机收到包含默认路由器优先级信息的 RA 报文后，会更新自己的默认路由器列表。当主机向其他设备发送报文时，如果没有路由可选，则首先查询该列表，然后选择本链路内优先级最高的路由器发送报文；如果该路由器故障，主机根据优先级从高到低的顺序，依次选择其他路由器。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ipv6 nd ra preference** { **high** | **medium** | **low** }，配置 RA 报文中的默认路由器优先级信息。

步骤 4 执行命令 **ipv6 nd ra route-information** *ipv6-address prefix-length* **lifetime** *route-lifetime* [**preference** { **high** | **medium** | **low** }]，配置 RA 报文中的路由选项信息。

----结束

3.4.8 检查配置结果

可以查看 IPv6 邻居发现的配置信息。

前提条件

已经完成 IPv6 邻居发现的所有配置。

操作步骤

- 使用 **display ipv6 neighbors** [*ipv6-address* | [**vid** *vlan-id*] *interface-type interface-number* | **vpn-instance** *vpn-instance-name*]、**display ipv6 neighbors** *interface-type interface-number*| [**vid** *vid*] | [**cevid** *cevid*]命令查看邻居缓存的内容。
- 使用 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令查看接口 IPv6 信息。

----结束

任务示例

执行命令 **display ipv6 neighbors**，可以看到邻居缓存中有 IPv6 地址和所属接口等信息。

```
<Huawei> display ipv6 neighbors gigabitethernet 1/0/0
------------------------------------------------------------
IPv6 Address : 3003::2
Link-layer   : 00e0-fc89-fe6e            State : STALE
Interface    : GE1/0/0                   Age   : 7
VLAN         : 10                         CEVLAN: -
VPN name     : vpn1                      Is Router: TRUE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FE89:FE6E
Link-layer   : 00e0-fc89-fe6e            State : STALE
Interface    : GE1/0/0                   Age   : 7
VLAN         : 10                         CEVLAN: -
Is Router: TRUE
Secure FLAG  : UN-SECURE
------------------------------------------------------------
Total: 2       Dynamic: 2       Static: 0
```

执行命令 **display ipv6 interface**，能够查看接口配置的 IPv6 地址。

```
<Huawei> display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::1
  Global unicast address(es):
    2001::1, subnet is 2001::/64
    5000::A19:A6FF:FECE:7D4B, subnet is 5000::/63
  Joined group address(es):
    FF02::1:FFCE:7D4B
    FF02::2
    FF02::1
    FF02::1:FF00:1
  MTU is 1280 bytes
  ND DAD is disabled
  ND reachable time is 10000 milliseconds
  ND retransmit interval is 10000 milliseconds
  Hosts use DHCP to obtain routable addresses.
```

执行命令 **display ipv6 interface brief**，能够查看接口配置的 IPv6 地址以及接口状态。当接口状态为 UP 时表示配置成功。

```
<Huawei> display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical             Protocol
GigabitEthernet2/0/2       up                   up
[IPv6 Address] 2030::101:101
GigabitEthernet2/0/3       up                   up
[IPv6 Address] 2001::1
LoopBack0                  up                   up(s)
[IPv6 Address] Unassigned
```

3.5 配置 IPv4/IPv6 双协议栈

为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界路由器上启动 IPv4/IPv6 双协议栈。

3.5.1 建立配置任务

介绍配置 IPv4/IPv6 双协议栈的应用环境、前置任务、数据准备和配置过程。

应用环境

如果路由器既有 IPv4 连接，又有 IPv6 连接，就需要启动 IPv4/IPv6 双协议栈。

AR1200 中启用 IPv4/IPv6 双协议栈的操作非常简单，只要在系统视图下使能 IPv6 报文转发能力，并在相应的接口上配置有 IPv4 地址或 IPv6 地址。此时，路由器就可在相应的接口上进行 IPv4 和 IPv6 的报文转发。

前置任务

在配置 IPv4/IPv6 双协议栈之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数

数据准备

在配置 IPv4/IPv6 双协议栈之前，需准备以下数据。

序号	数据
1	IPv4 网络侧接口的类型及编号
2	IPv4 网络侧接口的 IPv4 地址及掩码
3	IPv6 网络侧接口的类型及编号
4	IPv6 网络侧接口的 IPv6 地址及前缀

3.5.2 使能 IPv6 报文转发能力

使能 IPv6 报文转发能力即在系统视图下和接口视图下分别使能 IPv6 功能。

背景信息

如果要使能接口对 IPv6 报文进行转发的功能，必须同时使能系统视图下和接口视图下的 IPv6 功能。因为：

- 在系统视图下执行命令 **ipv6**，只是使能了路由器对 IPv6 报文的转发功能，并没有使能接口的 IPv6 功能，也不能进行 IPv6 的相关配置。
- 在接口视图下执行命令 **ipv6 enable**，只是使能了接口的 IPv6 功能，路由器不能对 IPv6 报文进行转发。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6**，使能 IPv6 报文转发能力。

缺省情况下，路由器不使能对 IPv6 报文的转发能力。

如果要对 IPv6 报文进行转发，必须先在系统视图下使能路由器的 IPv6 报文转发能力。否则即使在接口上配置有 IPv6 地址，路由器无法转发 IPv6 的报文。

步骤 3 执行命令 **interface** *interface-type interface-number*，进行需要使能 IPv6 功能的接口视图。

步骤 4 执行命令 **ipv6 enable**，使能接口的 IPv6 功能。

如果要在接口视图下进行 IPv6 的相关配置，必须先在接口视图下使能 IPv6 功能。

缺省情况下，接口下不使能 IPv6 功能。

----结束

3.5.3 配置接口的 IPv4 和 IPv6 地址

在 IPv4 网络侧和 IPv6 网络侧分别配置 IPv4 地址和 IPv6 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 IPv4 网络侧的接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IPv4 地址。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **interface** *interface-type interface-number*，进入 IPv6 网络侧的接口视图。

步骤 6 请根据不同情况进行一下配置。

- 配置接口的自动链路本地地址，请执行命令 **ipv6 address auto link-local**。
- 配置接口的自定义链路本地地址，请执行命令 **ipv6 address** *ipv6-address* **link-local**。
- 配置接口的全球单播地址，请执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }。
- 配置接口的 IPv6 EUI-64 格式地址，请执行命令 **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**。

----结束

3.5.4 检查配置结果

可以查看 IPv4/IPv6 双协议栈的配置信息。

前提条件

已经完成 IPv4/IPv6 双协议栈的所有配置。

操作步骤

- 在接口视图下使用 **display this** 命令，显示接口的 IPv4/IPv6 双协议栈信息。

----结束

任务示例

GE1/0/0 在接口视图下执行命令 **display this**，可以看到接口的 IPv4/Ipv6 的相关信息。

```
[Huawei-GigabitEthernet1/0/0] display this
[V200R002C00]
#
```

```
interface GigabitEthernet0/0/1
 ipv6 enable
 ip address 20.1.1.1 255.255.255.0
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
#
return
```

3.6 配置 PMTU

通过配置 PMTU，在网络中使用一个合适的 MTU 值来发送报文，使得报文在整个传输过程中不需要分片，减轻中间路由器的工作压力，以便有效地利用网络资源并得到最佳的吞吐量。

3.6.1 建立配置任务

介绍配置 PMTU 的应用环境、前置任务、数据准备和配置过程。

应用环境

通过配置 PMTU，在网络中使用一个合适的 MTU 值来发送报文，使得报文在整个传输过程中不需要分片，减轻中间路由器的工作压力，以便有效地利用网络资源并得到最佳的吞吐量。

前置任务

在配置 PMTU 之前，需完成以下任务。

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数

数据准备

在配置 PMTU 之前，需准备以下数据。

序号	数据
1	需要配置的 IPv6 地址和 PMTU 值
2	PMTU 的老化时间

3.6.2 建立静态 PMTU 表项

可以根据发送报文所经过的路径的最小 MTU 值，手工配置静态 PMTU，使报文的传输更加快速。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 pathmtu** *ipv6-address* [*path-mtu*]，对指定的 IPv6 地址配置 PMTU 值。

缺省情况下，IPv6 地址的 PMTU 值是 1500 字节。

- 静态 PMTU 表项个数上限为 300。
- 公网中 PMTU 表项个数（包括动态、静态）AR200 和 AR1200 的上限是 512,AR2200 和 AR3200 的上限是 1024。

----结束

3.6.3 配置动态 PMTU 表项的老化时间

PMTU 老化时间用来更改动态 PMTU 项在缓存中的存活时间，静态 PMTU 项不会被老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ipv6 pathmtu age** *age-time*，配置 PMTU 老化时间。

缺省情况下，动态 PMTU 项的老化时间是 10 分钟。

静态 PMTU 存在的情况下，动态 PMTU 不生效。

----结束

3.6.4 检查配置结果

可以查看 PMTU 的配置信息。

前提条件

已经完成 PMTU 的所有配置。

操作步骤

- 使用 **display ipv6 pathmtu** { *ipv6-address* | **all** | **dynamic** | **static** }命令查看所有 PMTU 项。
- 使用 **display ipv6 interface** [*interface-type interface-number* | **brief**]命令查看接口当前的 MTU 值。

----结束

任务示例

执行命令 **display ipv6 pathmtu**，可以看到目的 IPv6 地址、PMTU 值、老化时间和类型。

```
<Huawei> display ipv6 pathmtu all
IPv6 Destination Address   ZoneID     PathMTU   LifeTime(M)  Type
fe80::12                   0          1300      40           Dynamic
2222::3                    0          1280      --           Static
------------------------------------------------------------------------------
Total: 2      Dynamic: 1     Static: 1
```

执行命令 **display ipv6 interface**，能够查看接口当前的 MTU 值。

```
<Huawei> display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
```

```
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF04:5D00
    FF02::2
    FF02::1
  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
```

3.7 配置 TCP6

通过对 TCP6 报文的相关设置，可以提高网络的性能。

3.7.1 建立配置任务

介绍配置 TCP6 的应用环境、前置任务、数据准备和配置过程。

应用环境

有时为了优化网络性能，需要调整 TCP6 的参数。

前置任务

在配置 TCP6 之前，需完成以下任务。

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up

数据准备

在配置 TCP6 之前，需准备以下数据。

序号	数据
1	TCP6 的 FIN-WAIT 定时器的值
2	TCP6 的 SYN-WAIT 定时器的值
3	TCP6 滑动窗口的大小

3.7.2 配置 TCP6 定时器

通过设置两个 TCP6 定时器，可以控制 TCP6 的连接时间。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp ipv6 timer syn-timeout** *timer-value*，配置 TCP 的 SYN-WAIT 定时器。

缺省情况下，SYN-WAIT 定时器的值为 75 秒。

步骤 3 执行命令 **tcp ipv6 timer fin-timeout** *timer-value*，配置 TCP6 的 FIN-WAIT 定时器。

缺省情况下，FIN-WAIT 定时器的值为 600 秒。

----结束

3.7.3 配置 TCP6 的滑动窗口大小

通过配置 TCP6 的滑动窗口的大小，设置 TCP6 的 Socket 接收和发送缓冲区的大小，提高网络的性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp ipv6 window** *window-size*，配置 TCP6 的缓冲区大小。

TCP6 缓冲区的大小的取值范围是 1KB ～ 32KB。缺省情况下，TCP6 的收发缓冲区的大小为 8KB（千字节）。

----结束

3.7.4 检查配置结果

可以查看 TCP6 的配置信息。

前提条件

已经完成基于 IPv6 的 TCP 的所有配置。

操作步骤

- 使用 **display tcp ipv6 statistics** 命令查看相关的 TCP6 统计信息。
- 使用 **display tcp ipv6 status** 命令查看 TCP6 的连接状态。
- 使用 **display udp ipv6 statistics** 命令查看 UDP6 相关统计信息。
- 使用 **display ipv6 socket** [**socketype** *socket-type* | **task-id** *task-id* **socket-id** *socket-id*]命令查看指定套接字相关信息。

----结束

任务示例

执行命令 **display tcp ipv6 statistics**、**display tcp ipv6 status** 和 **display udp ipv6 statistics**，可以看到 TCP6 和 UDP6 的连接状态和统计信息。

```
<Huawei> display tcp ipv6 statistics
Received packets:
     total: 0
     total(64bit high-capacity counter): 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0
     window update packets: 0
     checksum error: 0
```

```
     offset error: 0
     short error: 0
     duplicate packets: 0 (0 bytes)
     partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets with data after window: 0 (0 bytes)
     packets after close: 0
     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0
     too much ACK packets: 0
     packets dropped due to MD5 authentication failure: 0
     packets dropped due to absence of MSO: 0
     packets dropped due to presence of MSO: 0
     packets received with MD5 Signature Option: 0

Sent packets:
     total: 0
     urgent packets: 0
     total(64bit high-capacity counter): 0
     control packets: 0 (including 0 RST)
     window probe packets: 0
     window update packets: 0
     data packets: 0 (0 bytes)
     data packets retransmitted: 0 (0 bytes)
     ACK only packets: 0 (0 delayed)
     packets sent with MD5 Signature Option: 0

Other Statistics:
     retransmitted timeout: 0
     connections dropped in retransmitted timeout: 0
     keepalive timeout: 0
     keepalive probe: 0
     keepalive timeout, so connections disconnected: 0
     initiated connections: 0
     accepted connections: 0
     established connections: 0
     closed connections: 0 (dropped: 0, initiated dropped: 0)

<Huawei> display tcp ipv6 status
* - MD5 Authentication is enabled.
TCP6CB   TID/SoID  Local Address        Foreign Address      State        VPNID
19df05d0 9/3       ::->23               ::->0                Listening    0
<Huawei> display udp ipv6 statistics
Received packets:
     total: 0
     total(64bit high-capacity counter): 0
     checksum error: 0
     shorter than header: 0
     invalid message length: 0
     no socket on port: 0
     no multicast port: 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
     packets sent for external pre processing: 1

Sent packets:
     total: 0
     total(64bit high-capacity counter): 0
```

执行命令 **display ipv6 socket**，能够查看套接字的相关信息。

```
<Huawei> display ipv6 socket
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
```

```
Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

SOCK_RAW:
```

3.8 维护 IPv6

维护 IPv6 包括清除 IPv6 运行信息、监控 IPv6 运行状况。

3.8.1 清除 IPv6 运行信息

介绍了使用 reset 命令清除 IPv6 运行信息。

背景信息

注意

清除 IPv6 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除数据包的 IPv6 报文处理的统计信息后，请在用户视图下执行 **reset ipv6 statistics** 命令。
- 在确认需要清除缓存中的 PMTU 项后，请在用户视图下执行 **reset ipv6 pathmtu** { **all** | **dynamic** | **static** }命令。
- 在确认需要清除 IPv6 邻居缓存项后，请在用户视图下执行 **reset ipv6 neighbors** { **all** | **dynamic** | **static** | **vid** *vlan-id* [*interface-type interface-number*] | *interface-type interface-number* [**dynamic** | **static**] }命令。
- 在确认需要清除地址选择策略表项信息后，请在用户视图下执行 **reset ipv6 address-policy** 命令。
- 在确认需要清除所有 TCP6 统计信息后，请在用户视图下执行 **reset tcp ipv6 statistics** 命令。
- 在确认需要清除所有 UDP6 统计信息后，请在用户视图下执行 **reset udp ipv6 statistics** 命令。
- 在确认需要清除所有重叠分片攻击源的记录信息后，请在用户视图下执行 **reset ipv6 attack-source overlapping-fragment** 命令。

----结束

3.9 配置举例

配置示例中包括组网需求、配置注意事项、配置思路等。举例说明接口 IPv6 地址的配置以及邻居发现协议的配置。

3.9.1 配置接口的 IPv6 地址示例

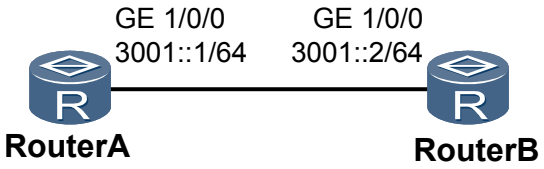
本举例介绍接口的 IPv6 地址的配置过程。

组网需求

如图 3-1 所示，两台路由器通过 Eth 接口相连，给接口配置 IPv6 全球单播地址，验证它们之间的互通性。

需要配置的全球单播地址为 3001::1/64 和 3001::2/64。

图 3-1 配置接口的 IPv6 地址组网图



配置思路

配置接口的 IPv6 地址思路如下：

1. 使能路由器的 IPv6 转发能力
2. 配置接口的 IPv6 全球单播地址

数据准备

为完成此配置例，需准备如下的数据：

- 接口的全球单播地址

操作步骤

步骤 1 使能路由器的 IPv6 转发能力

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ipv6
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] ipv6
```

步骤 2 配置接口的全球单播地址

配置 RouterA。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address 3001::1/64
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address 3001::2/64
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 3 验证配置结果

如果配置成功，可以查看配置的全球单播地址，以及接口状态为 Up，IPv6 协议状态为 Up。

显示 RouterA 的接口信息。

```
[RouterA] display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE01:E3
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::2
    FF02::1
    FF02::1:FF01:E3
  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
```

显示 RouterB 的接口信息。

```
[RouterB] display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::A19:A6FF:FE9B:6D3B
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:2
    FF02::2
    FF02::1
    FF02::1:FF9B:6D3B
  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
```

从 RouterA 上 PingRouterB 的全球单播 IPv6 地址。

```
[RouterA] ping ipv6 3001::2
  PING 3001::2 : 56  data bytes, press CTRL_C to break
    Reply from 3001::2
    bytes=56 Sequence=1 hop limit=64  time = 2 ms
    Reply from 3001::2
    bytes=56 Sequence=2 hop limit=64  time = 2 ms
    Reply from 3001::2
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
    Reply from 3001::2
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 3001::2
    bytes=56 Sequence=5 hop limit=64  time = 2 ms

  --- 3001::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
round-trip min/avg/max = 2/2/2 ms
```

----结束

配置文件

- RouterA 配置文件

```
#
 sysname RouterA
#
ipv6
#
interface gigabitethernet1/0/0
ipv6 enable
ipv6 address 3001::1/64
#
return
```

- RouterB 配置文件

```
#
 sysname RouterB
#
ipv6
#
interface gigabitethernet1/0/0
ipv6 enable
ipv6 address 3001::2/64
#
return
```

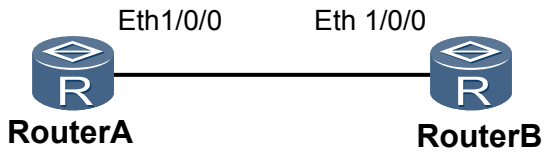
3.9.2 配置 IPv6 邻居发现示例

本举例介绍 IPv6 邻居发现的配置过程。

组网需求

如图 3-2 所示，两台路由器通过 Eth 接口相连，给接口配置 IPv6 链路本地地址，使能路由器通告报文 RA 的发布功能，验证 IPv6 邻居发现。

图 3-2 配置 IPv6 邻居发现示例



配置思路

采用如下的思路配置 IPv6 邻居发现：

1. 使能路由器的 IPv6 转发能力。
2. 在接口 GigabitEthernet1/0/0 上配置链路本地单播地址。
3. 在接口 GigabitEthernet1/0/0 上使能路由器通告报文 RA 的发布。

数据准备

完成此配置，需准备如下的数据：

- 配置接口的 IPv6 链路本地地址

操作步骤

步骤 1 使能路由器的 IPv6 转发能力

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ipv6
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] ipv6
```

步骤 2 配置接口的链路本地单播地址

配置 RouterA。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address auto link-local
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address auto link-local
```

步骤 3 使能 RA 报文发布功能

使能 RouterA 的 RA 报文发布功能。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo ipv6 nd ra halt
```

使能 RouterB 的 RA 报文发布功能。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo ipv6 nd ra halt
```

步骤 4 验证配置结果

如果配置成功，可以查看配置的链路本地单播地址，以及接口状态为 Up，IPv6 协议状态为 Up。

显示 RouterA 的接口 GigabitEthernet1/0/0 的信息。

```
[RouterA-GigabitEthernet1/0/0] display this ipv6 interface
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE01:E3
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF01:E3
    FF02::2
    FF02::1
  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 advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

显示 RouterB 的接口信息。

```
[RouterB-GigabitEthernet1/0/0] display this ipv6 interface
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::A19:A6FF:FE9B:6D3B
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF9B:6D3B
    FF02::2
    FF02::1
  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 advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

显示 RouterA 的邻居表项。

```
[RouterA] display ipv6 neighbors
------------------------------------------------------------------------------
IPv6 Address : FE80::A19:A6FF:FE9B:6D3B
Link-layer   : 0819-a69b-6d3b                    State : STALE
Interface    : Eth1/0/0                          Age   : 27
VLAN         : -                                 CEVLAN: -
Is Router    : TRUE
Secure FLAG  : UN-SECURE

------------------------------------------------------------------------------
Total: 1       Dynamic: 1       Static: 0
```

显示 RouterB 的邻居表项。

```
[RouterB] display ipv6 neighbors
------------------------------------------------------------------------------
IPv6 Address : FE80::2E0:FCFF:FE01:E3
Link-layer   : 00e0-fc01-00e3                    State : STALE
Interface    : Eth1/0/0                          Age   : 39
VLAN         : -                                 CEVLAN: -
Is Router    : TRUE
Secure FLAG  : UN-SECURE

------------------------------------------------------------------------------
Total: 1       Dynamic: 1       Static: 0
```

----结束

配置文件

- RouterA 配置文件

```
#
 sysname RouterA
```

```
#
ipv6
#
interface Ethernet1/0/0
 ipv6 enable
 ipv6 address auto link-local
 undo ipv6 nd ra halt
#
return
```

- RouterB 配置文件

```
#
 sysname RouterB
#
ipv6
#
interface Ethernet1/0/0
 ipv6 enable
 ipv6 address auto link-local
 undo ipv6 nd ra halt
#
return
```

4 DNS 配置

关于本章

介绍了 AR1200 上 DNS 的基本原理、基本功能、配置过程和配置举例。

4.1 DNS 概述
介绍 DNS 的基本概念。

4.2 AR1200 支持的 DNS 特性
介绍 DNS 特性在 AR1200 中的支持情况。

4.3 配置 DNS 客户端
配置 DNS 客户端使用域名与其他设备通信。

4.4 配置 DNS Proxy/Relay
简要介绍 DNS proxy/relay 的配置。DNS proxy/relay 是指在路由器上启动 DNS 代理功能。

4.5 配置 DDNS 客户端
DDNS 可以动态更新域名和 IP 地址的对应关系，当域名所对应的 IP 地址发生变化，DDNS 可以得到域名所对应的最新的 IP 地址，从而保证用户使用域名成功访问网络中的站点。

4.6 维护 DNS
介绍维护 DNS 的配置。

4.7 配置举例
介绍 DNS 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

4.1 DNS 概述

介绍 DNS 的基本概念。

TCP/IP 提供了通过 IP 地址来确定设备的功能，但对用户来讲，记住某台设备的 IP 地址是相当困难的，因此专门设计了一种字符串形式的主机命名机制，这些主机名与 IP 地址一一对应。在 IP 地址与主机名之间需要有一种转换和查询机制，提供这种机制的系统就是域名系统 DNS（Domain Name System）。

域名系统 DNS 使用一种有层次的命名方式，为网上的设备指定一个有意义的名字，并且在网络上设置域名解析服务器，建立域名与 IP 地址的对应关系。这样用户就可以使用便于记忆的、有意义的域名，而不必去记忆复杂的 IP 地址。

4.2 AR1200 支持的 DNS 特性

介绍 DNS 特性在 AR1200 中的支持情况。

AR1200 作为 DNS 客户端

AR1200 作为 DNS 客户端支持静态域名解析和动态域名解析。

- 静态域名解析。静态域名解析即手动建立域名和 IP 地址之间的对应关系。当 DNS 客户端需要域名所对应的 IP 地址，即到静态域名解析表中去查找指定的域名，然后获得所对应的 IP 地址。
- 动态域名解析。动态域名解析有专用的 DNS 服务器，负责接受 DNS 客户端提出的域名解析请求。DNS 服务器首先在本机数据库内部解析，如果判断不属于本域范围之内，就将请求交给上一级的 DNS 服务器，直到完成解析，解析的结果或者为 IP 地址，或者域名不存在，并将解析的结果反馈给 DNS 客户端。

AR1200 作为 DNS Proxy/Relay

AR1200 支持 DNS proxy/relay 功能。当局域网内部没有 DNS 服务器时，局域网内的 DNS 客户端可以通过已使能 DNS proxy/relay 功能的 AR1200 连接到外部 DNS 服务器，DNS 服务器进行正确的 DNS 解析后，DNS 客户端可以访问 Internet。

DNS relay 和 DNS proxy 功能相同，区别在于 DNS proxy 接收到 DNS 客户端的 DNS 查询报文后会查找本地 cache，而 DNS relay 不会查询本地 cache，而是直接转发给 DNS 服务器进行解析，从而节省了 DNS relay 上的 DNS cache 开销。

AR1200 作为 DDNS 客户端

AR1200 支持 DDNS 客户端功能。指定 AR1200 的三层接口或者 VLANIF 接口作为 DDNS 客户端后，当这些接口的 IP 地址发生变化，AR1200 将此接口新的 IP 地址通知 DDNS 服务器，DDNS 服务器将动态更新 DNS 服务器上域名和 IP 地址的对应关系，保证通过域名解析到正确的 IP 地址。

4.3 配置 DNS 客户端

配置 DNS 客户端使用域名与其他设备通信。

4.3.1 建立配置任务

在配置 DNS 客户端前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

由于 Internet 协议（IP）地址结构不便于记忆（比如点分式表示的 202.112.131.109），所以大多数组织采用缩写词或有意义的名字（称为域名，如 www.sina.com.cn）来表示地址，而不是使用 IP 地址。但是，如何让非 IP 标识的域名映射为 IP 地址呢？IP 地址与其域名之间的映射是依靠解析器及 DNS 服务器来完成的。

DNS 客户端主要完成解析器的功能，它的主要功能是完成 IP 地址和主机的域名之间的转换。

如果用户使用域名访问其他设备的次数很少，或者没有可用的 DNS 服务器时，需要配置静态 DNS。配置静态 DNS 需要网络管理员知道域名与 IP 地址的对应关系，且在域名与 IP 地址的对应关系变化时，需要手动修改 DNS 表项。

如果用户需要使用域名访问很多的设备，且有可用的 DNS 服务器，此时可配置动态 DNS。动态 DNS 需要有 DNS 服务器的支持。

前置任务

在配置 DNS 客户端之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 配置 DNS 服务器。
- 配置本路由设备与 DNS 服务器之间的路由。

数据准备

在配置 DNS 客户端之前，需要准备以下数据。

序号	数据
1	静态 DNS 表项的域名和对应的 IP 地址
2	（可选）DNS 服务器的 IP 地址
3	（可选）本端路由设备的 IP 地址
4	（可选）动态 DNS 的域名后缀的列表

4.3.2 配置静态 DNS

介绍静态 DNS 表项的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip host** *host-name ip-address*，配置静态 DNS 表项。

每个主机名只能对应一个 IP 地址，当对同一主机名进行多次配置时，最后配置的 IP 地址有效。如果有多个主机名需要解析，则需要重复步骤 2。

----结束

4.3.3 配置动态 DNS

介绍动态 DNS 的配置。

背景信息

配置动态 DNS 包括使能动态域名解析功能、配置域名服务器、配置本端设备的 IP 地址和配置域名后缀等步骤。如果设备使用 DHCP 服务器来分配 IP 地址，且 DHCP 服务器下发给设备的信息中包括了 DNS 服务器的地址和域名后缀列表，那么步骤中只需要使能动态域名解析功能即可。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能动态域名解析功能。

步骤 3 （可选）执行命令 **dns server** *ip-address*，配置 DNS 客户端访问的 DNS 服务器的 IP 地址。

步骤 4 （可选）执行命令 **dns server source-ip** *ip-address*，指定本端路由设备作为 DNS 客户端进行 DNS 通信时的源 IP 地址。

指定本端设备的 IP 地址，以指定的 IP 地址与 DNS 服务器端通信，从而保证通信的安全。

步骤 5 （可选）执行命令 **dns domain** *domain-name*，配置域名后缀。

----结束

后续处理

系统最多支持 6 个域名服务器、1 个指定的源地址、10 个域名后缀。如果要配置多个域名服务器，则需重复步骤 3。如果要配置多个域名后缀，则需重复步骤 5。

4.3.4 检查配置结果

查看 DNS 客户端的相关配置信息。

操作步骤

- 执行命令 **display ip host**，查看静态 DNS 表项。
- 执行命令 **display dns server**，查看 DNS 服务器的配置信息。
- 执行命令 **display dns domain**，查看域名后缀的配置信息。

- 执行命令 **display dns dynamic-host**，查看动态 DNS 表项信息。

----结束

任务示例

查看静态 DNS 表项。

```
<Huawei> display ip host
Host                 Age        Flags  Address
www.3322.org         0          static 10.138.90.34
members.3322.org     0          static 10.138.90.51
checkip.dyndns.com   0          static 10.138.90.51
members.dyndns.org   0          static 10.138.90.51
```

查看 DNS 服务器的配置信息。

```
<Huawei> display dns server
Type:
D:Dynamic     S:Static

DNS Server    Type    IP Address
    1          S      10.10.1.1
    2          S      10.10.1.2
```

查看域名后缀的配置信息。

```
<Huawei> display dns domain
No                   Domain-name
1                    com
2                    net
```

查看 IP 域名缓存区中的动态 DNS 表项信息。

```
<Huawei> display dns dynamic-host
Host                                TTL   Type   Address(es)
sipx.autosrv.com                    114   IP     192.168.2.18
sip.autosrv.com                     237   IP     192.168.2.61
sip.autonaptr.com                   117   IP     192.168.2.19
_sip._tcp.autosrv.com               55    SRV    0 0 0 sipx.autosrv.com
                                                 0 0 0 sip.autosrv.com
autonaptr.com                       0     NAPTR  101 10 A SIP+D2T  sip.autona
```

4.4 配置 DNS Proxy/Relay

简要介绍 DNS proxy/relay 的配置。DNS proxy/relay 是指在路由器上启动 DNS 代理功能。

4.4.1 建立配置任务

在配置 DNS proxy/relay 前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

DNS proxy/relay 是指在 AR1200 上启动 DNS 代理功能，这样在局域网内部没有 DNS 服务器时，局域网内部的 DNS 客户端可以通过已使能 DNS proxy/relay 功能的 AR1200 连接到外部 DNS 服务器，DNS 服务器进行正确的 DNS 解析后，DNS 客户端可以访问 Internet。

使用 DNS proxy/relay 可以减少网络管理成本，当 DNS 服务器的 IP 地址发生变更，只需要更改 DNS proxy/relay 的配置，而不需要更改所有 DNS 客户端上的配置。

前置任务

在配置 DNS proxy/relay 之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 配置 DNS 服务器。
- 配置本路由设备与 DNS 客户端和 DNS 服务器之间的路由。

数据准备

序号	数据
1	DNS 服务器的 IP 地址
2	（可选）DNS spoofing 功能应答的 IP 地址
3	（可选）DNS 转发表项老化时间

4.4.2 配置 DNS 服务器

介绍 DNS proxy/relay 访问的 DNS 服务器的配置过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能动态域名解析功能。

步骤 3 执行命令 **dns server** *ip-address*，配置 DNS proxy/relay 访问的 DNS 服务器。

----结束

4.4.3 （可选）配置 DNS Spoofing 功能

介绍 DNS spoofing 功能的配置过程。

背景信息

当 AR1200 使能 DNS proxy/relay 功能后，如果设备上没有配置 DNS 服务器地址或不存在到达 DNS 服务器的路由，则设备不会转发 DNS 服务器的域名解析请求，也不会应答该请求。如果此时设备上同时使能了 DNS spoofing 功能，则会利用配置的 IP 地址作为域名解析结果，欺骗性地应答域名解析请求。

为了 DNS spoofing 生效除了需要使能 DNS proxy 或者 DNS relay 外，需要满足如下条件之一：

- 没有配置 DNS 服务器；
- 配置 DNS 服务器，但是没有使能 DNS 动态解析；

- 没有到达 DNS 服务器的路由；
- 通往 DNS 服务器的出接口上没有可用的源 IP 地址。

当满足以上某一个条件时，DNS proxy 或者 DNS relay 接收到一个 A 类查询时，使用 DNS spoofing 配置的 IP 地址进行应答。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns proxy enable**，使能 DNS proxy 功能；或执行命令 **dns relay enable**，使能 DNS relay 功能。

DNS relay 和 DNS proxy 功能相同，区别在于 DNS proxy 接收到 DNS 客户端的 DNS 查询报文后会查找本地 cache，而 DNS relay 不会查询本地 cache，而是直接转发给 DNS 服务器进行解析，从而节省了 DNS relay 上的 DNS cache 开销。

步骤 3 执行命令 **dns spoofing** *ip-address*，使能 DNS spoofing 功能，并指定应答的 IP 地址。

----结束

4.4.4 （可选）配置转发表项老化时间

介绍转发表项老化时间的配置过程。

背景信息

当 DNS proxy/relay 受到攻击时，DNS proxy/relay 的转发映射表会被占满，无法进行新的 DNS 查询，导致 DNS 客户端通过 DNS proxy/relay 无法进行域名解析，根据以上场景提供转发表项老化时间机制，当设备收到攻击转发映射表被占满时，通过清除转发表项使设备恢复功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns proxy enable**，使能 DNS proxy 功能；或执行命令 **dns relay enable**，使能 DNS relay 功能。

DNS relay 和 DNS proxy 功能大致相同，区别在于 DNS proxy 接收到 DNS 客户端的 DNS 查询报文后会查找本地 cache，而 DNS relay 不会查询本地 cache，而是直接转发给 DNS 服务器进行解析，从而节省了 DNS relay 上的 DNS cache 开销。

步骤 3 （可选）执行命令 **dns forward expire-time** *time*，配置 DNS proxy/relay 转发表项的老化时间。

缺省情况下，DNS 转发表项的老化时间默认为 60 秒。

----结束

4.4.5 检查配置结果

查询 DNS 转发的映射关系表。

操作步骤

- 执行命令 **display dns forward table** [**source-ip** *ip-address*]，查询 DNS 转发的映射关系表。

----结束

任务示例

显示 DNS proxy/relay 映射关系表

```
<Huawei> display dns forward table
Domain name            : ma.huawei.com
Source IP              : 1.1.1.3
Source port            : 33025
Source packet id       : 42564
Forward packet id      : 1
Retry count            : 2
Query type             : 1
```

4.5 配置 DDNS 客户端

DDNS 可以动态更新域名和 IP 地址的对应关系，当域名所对应的 IP 地址发生变化，DDNS 可以得到域名所对应的最新的 IP 地址，从而保证用户使用域名成功访问网络中的站点。

4.5.1 建立配置任务

在配置 DDNS 客户端前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

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。

AR1200 作为 DDNS 客户端，当提供 Web 服务的接口的 IP 地址发生变化，将此接口新的 IP 地址通知 DDNS 服务器，DDNS 服务器将动态更新 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。

前置任务

在配置 DNS 客户端之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 在 DDNS 服务器网站上进行用户注册。
- 配置本路由设备与 DDNS 服务器之间的路由。

数据准备

序号	数据
1	DDNS 服务器 URL 地址
2	（可选）DDNS 更新启动后，定时发起更新请求的时间间隔
3	应用 DDNS 策略的接口编号

4.5.2 创建 DDNS 策略

使用 DDNS 功能时，首先在系统视图创建 DDNS 策略。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ddns policy** *policy-name*，创建 DDNS 策略，并进入 DDNS 策略视图。

----结束

4.5.3 配置 DDNS 策略

介绍 DDNS 策略的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ddns policy** *policy-name*，创建 DDNS 策略，并进入 DDNS 策略视图。

步骤 3 执行命令 **url** *request-url*，指定 DDNS 更新请求的 URL 地址。

使能 DDNS 策略后，需填写 URL 地址，说明此策略与哪个 DDNS 服务提供商相连。AR1200 向不同 DDNS 服务器请求更新的过程各不相同，因此，DDNS 服务器 URL 地址的配置方式也存在差异：

- 设备基于 HTTP 与 www.3322.org 通信时，DDNS 更新请求的 URL 地址格式为：

  http://username:password@members.3322.org/dyndns/update'system=dyndns&hostname=<h>&ip=<a>

- 设备基于 TCP 与 www.oray.cn 通信时，DDNS 更新请求的 URL 地址格式为：

  oray://username:password@phddnsdev.oray.net

步骤 4 （可选）执行命令 **interval** *interval-time*，指定 DDNS 更新启动后，定时发起更新请求的时间间隔。

使能 DDNS 策略后，通过设置定时刷新时间间隔来触发定时刷新。缺省情况下，定时发起更新请求的时间间隔为 3600 秒。

----结束

4.5.4 绑定 DDNS 策略

通过在接口上应用指定的 DDNS 策略来更新指定的 FQDN（Fully Qualified Domain Name，合格域名）与 IP 地址的对应关系，并启动 DDNS 更新。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ddns apply policy** *policy-name* **fqdn** *domain-name*，在接口上绑定 DDNS 策略。

AR1200 支持在三层接口和 VLANIF 接口上绑定 DDNS 策略。

----结束

4.5.5 检查配置结果

介绍检查 DDNS 的配置结果。

操作步骤

- 执行命令 **display ddns policy** *policy-name*，查看 DDNS 策略的信息。
- 执行命令 **display ddns interface** *interface-type interface-number*，查看接口下 DDNS 策略的信息。

----结束

任务示例

显示名称为 JackPolicy 的 DDNS 策略的信息。

```
<Huawei> display ddns policy JackPolicy
Policy name          : JackPolicy
Policy interval time : 3600
Policy URL           : oray://Jack:Jack2010@phddnsdev.oray.net
Policy bind count    : 1

=====  interface GigabitEthernet1/0/0 ======
  Statuses: START
  Refresh: enable
```

显示 VlANIF100 的接口下的 DDNS 策略的信息。

```
<Huawei> display ddns interface Vlanif 100
=====  Policy JackPolicy =======
  URL: oray://Jack:Jack2010@phddnsdev.oray.net
  Statuses: START
  Refresh: enable
```

4.6 维护 DNS

介绍维护 DNS 的配置。

4.6.1 清除 DNS 客户端的动态 DNS 表项

介绍清除 DNS 客户端的动态 DNS 表项的配置。

操作步骤

步骤 1 执行命令 **reset dns dynamic-host**，清除 DNS 客户端的动态 DNS 表项。

清除 DNS 客户端的动态 DNS 表项后，将无法恢复，清除之前务必仔细确认。

----结束

4.6.2 清除 DNS Proxy/Relay 的转发表项

若 DNS proxy 或 DNS relay 受到恶意攻击，导致 DNS 转发的映射关系表满时，可通过 reset dns forward table 命令清空映射关系表。

操作步骤

步骤 1 执行命令 **reset dns forward table** [*ip-address*]，清除 DNS 转发的映射关系表。

----结束

4.6.3 手动刷新 DDNS 策略

介绍手动刷新 DDNS 策略的配置

操作步骤

步骤 1 执行命令 **reset ddns policy** *policy-name* [*interface-type interface-num*]，手动刷新 DDNS 策略，更新应用此策略的所有 IP 地址和域名间的绑定关系。

----结束

4.7 配置举例

介绍 DNS 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

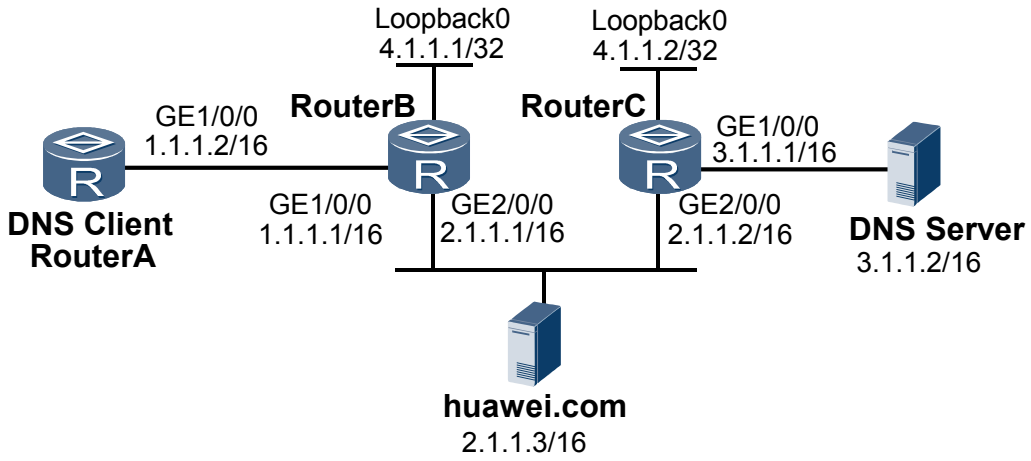
4.7.1 配置 DNS 客户端示例

组网需求

如图 4-1 所示，设备 RouterA 作为 DNS 客户端和 DNS 服务器配合，使得设备 RouterA 通过域名（huawei.com）能够访问 IP 地址为 2.1.1.3/16 的主机，配置域名后缀为 com 和 net。

在设备 RouterA 上配置 RouterB 和 RouterC 的静态 DNS 表项，使得 RouterA 能够使用域名对设备 RouterB 和 RouterC 进行管理。

图 4-1 配置 DNS 客户端组网图



配置思路

DNS 的配置思路如下：

1. 配置静态 DNS 表项。
2. 使能 DNS 域名解析功能。
3. 配置 DNS 服务器的 IP 地址。
4. 配置域名后缀。
5. 配置 OSPF。

数据准备

为完成此配置举例，需要准备如下数据：

- RouterA 的连接 RouterB 的接口编号以及接口的 IP 地址。
- 设备 RouterB 和 RouterC 的域名名称为 DeviceB 和 DeviceC。
- DNS 服务器的 IP 地址。
- 域名后缀。

操作步骤

步骤 1 配置设备 RouterA

配置 GE1/0/0 接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.2 255.255.0.0
[RouterA-GigabitEthernet1/0/0] quit
```

配置 OSPF。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.0.0 0.0.255.255
```

```
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置静态 DNS 表项。

```
[RouterA] ip host DeviceB 4.1.1.1
[RouterA] ip host DeviceC 4.1.1.2
```

使能 DNS 域名解析功能。

```
[RouterA] dns resolve
```

配置 DNS 服务器的 IP 地址。

```
[RouterA] dns server 3.1.1.2
```

配置域名后缀 net。

```
[RouterA] dns domain net
```

配置域名后缀 com。

```
[RouterA] dns domain com
```

说明

若要完成对域名的解析，还需要在 RouterB 和 RouterC 上配置 ospf，以便配置 RouterA 至 DNS 服务器的路由。RouterB 和 RouterC 的 ospf 具体配置参看配置文件。

步骤 2 验证配置结果

在设备 RouterA 上执行 **ping huawei.com** 命令，可以 ping 通，且对应的目的地址为 2.1.1.3。

```
<RouterA> ping huawei.com
Trying DNS server (3.1.1.2)
  PING huawei.com (2.1.1.3): 56  data bytes, press CTRL_C to break
    Reply from 2.1.1.3: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2.1.1.3: bytes=56 Sequence=2 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=3 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=4 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=5 ttl=126 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

在 RouterA 用 **display ip host** 命令可以查看到静态 DNS 表项中主机名和 IP 地址的对应关系。

```
<RouterA> display ip host
Host                 Age        Flags  Address
DeviceB              0          static 4.1.1.1
DeviceC              0          static 4.1.1.2
```

在 RouterA 用 **display dns dynamic-host** 命令可以查看到动态缓存区中的动态 DNS 表项信息。

```
<RouterA> display dns dynamic-host
Host                                    TTL   Type   Address(es)
huawei.com                              114   IP     2.1.1.3
```

说明

显示信息中的 TTL 表示该表项存在的时间，单位是秒。

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
 ip host DeviceB 4.1.1.1
 ip host DeviceC 4.1.1.2
#
 dns resolve
 dns server 3.1.1.2
 dns domain net
 dns domain com
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.2 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
interface LoopBack0
 ip address 4.1.1.1 255.255.255.255
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.1 255.255.0.0
#
interface GigabitEthernet 2/0/0
 ip address 2.1.1.1 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
  network 2.1.0.0 0.0.255.255
  network 4.1.1.1 0.0.0.0
#
return
```

RouterC 的配置文件

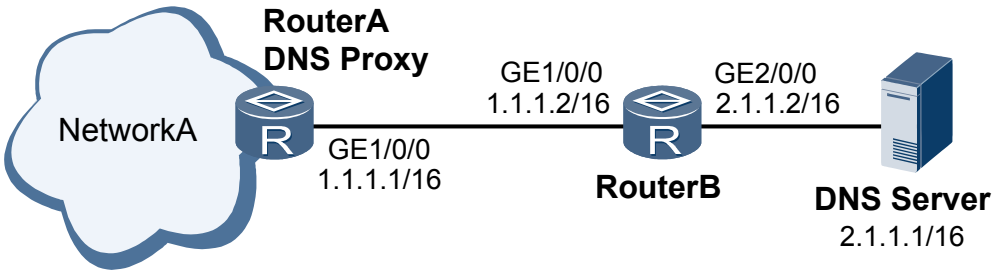
```
#
 sysname RouterC
#
interface LoopBack0
 ip address 4.1.1.2 255.255.255.255
#
interface GigabitEthernet 1/0/0
 ip address 3.1.1.1 255.255.0.0
#
interface GigabitEthernet 2/0/0
 ip address 2.1.1.2 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 2.1.0.0 0.0.255.255
  network 3.1.0.0 0.0.255.255
  network 4.1.1.2 0.0.0.0
#
return
```

4.7.2 配置 DNS proxy 示例

组网需求

如图 4-2 所示，局域网 NetworkA 中没有 DNS 服务器，NetworkA 中的用户通过作为 DNS proxy 的 RouterA 访问外部网络的 DNS 服务器来解析域名。如果 RouterA 通往 DNS 服务器的路由不可达，则使用 DNS spoofing 功能配置的 IP 地址进行应答。

图 4-2 配置 DNS proxy 组网图



配置思路

DNS proxy 的配置思路如下：

1. 配置 DNS 服务器。
2. 配置 DNS spoofing 功能。

数据准备

为完成此配置举例，需要准备如下数据：

- DNS 服务器的 IP 地址。
- 配置 DNS proxy 转发表项的老化时间。
- DNS spoofing 功能应答的 IP 地址。

操作步骤

步骤 1 配置 GE1/0/0 接口的 IP 地址

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 255.255.0.0
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 2 配置 DNS 服务器

使能动态域名解析功能。

```
[RouterA] dns resolve
```

配置 DNS proxy/Relay 访问的 DNS 服务器。

```
[RouterA] dns server 2.1.1.1
```

使能 DNS proxy 功能。

```
[RouterA] dns proxy enable
```

配置 DNS proxy/relay 转发表项的老化时间为 150 秒。

```
[RouterA] dns forward expire-time 150
```

步骤 3 配置 DNS spoofing 功能，并指定应答的 IP 地址为 10.1.1.3

```
[RouterA] dns spoofing 10.1.1.3
```

步骤 4 配置 OSPF

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.0.0 0.0.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

说明

若要完成 DNS proxy 功能，还需要在 RouterB 上配置 ospf，以便配置 RouterA 至 DNS 服务器的路由。RouterB 的 ospf 具体配置参看配置文件。

步骤 5 验证配置结果

在 RouterA 上使用 **display current-configuration** 命令查看 DNS proxy 的相关配置。

```
<RouterA> display current-configuration | include dns
 dns resolve
 dns server 2.1.1.1
 dns proxy enable
 dns spoofing 10.1.1.3
 dns forward expire-time 150
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.1 255.255.0.0
#
 dns resolve
 dns server 2.1.1.1
 dns proxy enable
 dns forward expire-time 150
#
 dns spoofing 10.1.1.3
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.2 255.255.0.0
```

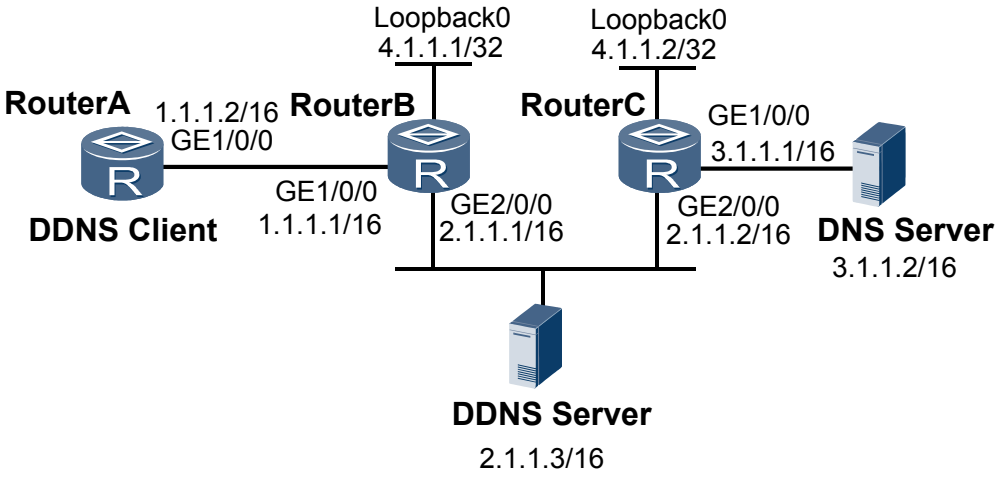
```
#
interface GigabitEthernet 2/0/0
 ip address 2.1.1.2 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
  network 2.1.0.0 0.0.255.255
#
return
```

4.7.3 配置 DDNS 客户端示例

组网需求

如图 4-3 所示，设备 RouterA 的域名为 www.abc.com，通过 DHCP 服务器获取 IP 地址，因此 IP 地址可能会发生变更，所以需要使用 DDNS 客户端功能保持其域名能够对应最新的 IP 地址。使用 www.oray.cn 作为 DDNS 服务器，当 RouterA 的 IP 地址发生变更，则应用 DDNS 客户端功能请求 DDNS 服务器，此时 DDNS 服务器将通知 DNS 服务器重新配置域名和 IP 地址的对应关系。

图 4-3 配置 DDNS 客户端组网图



配置思路

DDNS 客户端的配置思路如下：

1. 创建 DDNS 策略。
2. 配置 DDNS 服务器 URL。
3. 配置定时发起请求的时间间隔。
4. 绑定 DDNS 策略。

数据准备

为完成此配置举例，需要准备如下数据：

- 设备 RouterA 的域名。

- DDNS 服务器 URL。
- DDNS 客户端登陆 DDNS 服务器的用户名和密码。
- 定时发起请求的时间间隔。

操作步骤

步骤 1 配置设备 RouterA

创建 DDNS 策略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ddns policy mypolicy
```

配置 DDNS 服务器 URL。

```
[RouterA-ddns-policy-mypolicy] url oray://steven:nevets@phddnsdev.oray.net
```

配置定时发起请求的时间间隔。

```
[RouterA-ddns-policy-mypolicy] interval 3600
[RouterA-ddns-policy-mypolicy] quit
```

使能 DNS 域名解析功能。

```
[RouterA] dns resolve
```

配置 DNS 服务器的 IP 地址。

```
[RouterA] dns server 3.1.1.2
```

在接口 GE1/0/0 绑定上 DDNS 策略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.2 255.255.0.0
[RouterA-GigabitEthernet1/0/0] ddns apply policy mypolicy fqdn www.abc.com
[RouterA-GigabitEthernet1/0/0] quit
```

配置完成后，当接口 GE1/0/0 的 IP 地址变化时，RouterA 将通过 DDNS 服务器通知 DNS 服务器建立域名 www.abc.com 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 www.abc.com 解析到最新的 IP 地址。

配置 OSPF。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.0.0 0.0.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

说明

若要实现 DDNS 客户端、DDNS 服务器和 DNS 服务器之间的路由互通，还需要在 RouterB 和 RouterC 上配置 ospf 功能。RouterB 和 RouterC 的 ospf 功能的具体配置参看配置文件。

步骤 2 验证配置结果

在 RouterA 上用 **display ddns policy mypolicy** 命令可以查看名称为 mypolicy 的 DDNS 策略的信息。

```
<RouterA> display ddns policy mypolicy
Policy name          : mypolicy
Policy interval time : 3600
Policy URL           : oray://steven:nevets@phddnsdev.oray.net
Policy bind count    : 1
```

```
=====  interface GigabitEthernet1/0/0 ======
  Statuses: ESTABLISH
  Refresh: enable
```

在 RouterA 上用 **display ddns interface gigabitethernet 1/0/0** 命令可以显示 GE1/0/0 的接口下的 DDNS 策略的信息。

```
<RouterA> display ddns interface gigabitethernet 1/0/0
=====  Policy mypolicy =======
  URL: oray://steven:nevets@phddnsdev.oray.net
  Statuses: ESTABLISH
  Refresh: enable
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
ddns policy mypolicy
 url oray://steven:nevets@phddnsdev.oray.net
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.2 255.255.0.0
 ddns apply policy mypolicy fqdn www.abc.com
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
interface LoopBack0
 ip address 4.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.0.0
#
interface GigabitEthernet2/0/0
 ip address 2.1.1.1 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 1.1.0.0 0.0.255.255
  network 2.1.0.0 0.0.255.255
  network 4.1.1.1 0.0.0.0
#
return
```

RouterC 的配置文件

```
#
 sysname RouterC
#
interface LoopBack0
 ip address 4.1.1.2 255.255.255.255
#
```

```
interface GigabitEthernet1/0/0
 ip address 3.1.1.1 255.255.0.0
#
interface GigabitEthernet2/0/0
 ip address 2.1.1.2 255.255.0.0
#
ospf 1
 area 0.0.0.0
  network 2.1.0.0 0.0.255.255
  network 3.1.0.0 0.0.255.255
  network 4.1.1.2 0.0.0.0
#
return
```

5 NAT 配置

关于本章

通过 NAT 配置，实现了私网和公网地址的互相转换，解决 IPv4 地址短缺的问题，同时能够隐藏私网内部拓扑，提升网络的安全性。

5.1 NAT 概述
NAT（Network Address Translation）又称为网络地址转换，用于实现私有网络和公有网络之间的互访。

5.2 AR1200 支持的 NAT 特性
AR1200 支持的 NAT 特性包括：静态 NAT、PAT、内部服务器、NAT ALG 功能、NAT 过滤、NAT 映射、Easy IP、两次 NAT 及 NAT 多实例。

5.3 配置 NAT
配置 NAT 实现私有网络和公有网络之间的互访，单个用户可以采用 Easy IP 方式，多个用户可以采用地址池方式。

5.4 配置示例
介绍使用 NAT 提高网络安全性的各种示例。

5.1 NAT 概述

NAT（Network Address Translation）又称为网络地址转换，用于实现私有网络和公有网络之间的互访。

私有网络地址和公有网络地址

私有网络地址（以下简称私网地址）是指内部网络或主机的 IP 地址，公有网络地址（以下简称公网地址）是指在互联网上全球唯一的 IP 地址。IANA（Internet Assigned Number Authority）规定将下列的 IP 地址保留用作私网地址，不在 Internet 上被分配，可在一个单位或公司内部使用。

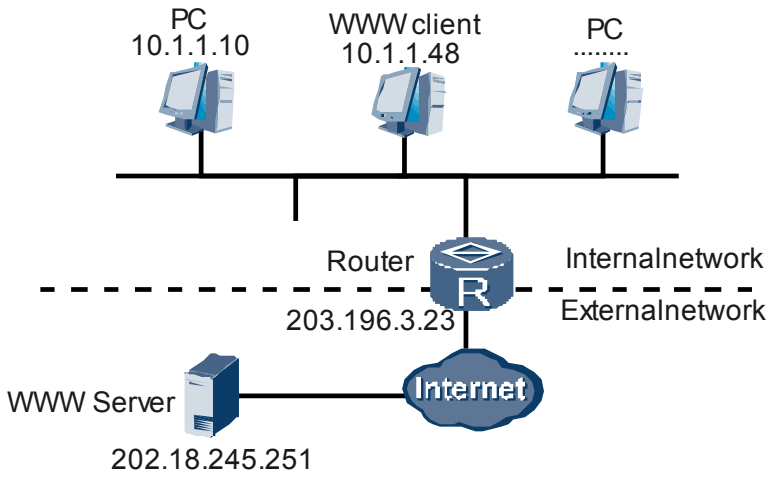
- A 类私有地址：10.0.0.0 ～ 10.255.255.255
- B 类私有地址：172.16.0.0 ～ 172.31.255.255
- C 类私有地址：192.168.0.0 ～ 192.168.255.255

各企业在预见未来内部主机和网络的数量后，选择合适的内部网络地址。不同企业的内部网络地址可以相同。如果一个公司选择上述三个范围之外的其它网段作为内部网络地址，则当与其他网络互通时有可能会造成混乱。

NAT 基本原理

如图 5-1 所示，当内部网络的主机访问互联网或与公有网络的主机通信时，需要进行网络地址转换。

图 5-1 NAT 示意图



内部网络的地址是 10.0.0.0 网段，而对外的公有网络 IP 地址是 203.196.3.23。内部的主机 10.1.1.48 以 WWW 方式访问外部网络的服务器 202.18.245.251。

主机 10.1.1.48 发出一个数据报文，选择一个源端口 6084，目的端口为 80。在通过 NAT 后，该报文的源地址和端口可能改为 203.196.3.23:32814，目的地址与端口不做改变。在 AR1200 中维护着一张地址和端口对应表。

当外部网络的 WWW 服务器返回结果时，AR1200 会将结果数据报文中目的 IP 地址及端口转化为 10.1.1.48:6084。这样内部主机 10.1.1.48 就可以访问外部服务器了。

5.2 AR1200 支持的 NAT 特性

AR1200 支持的 NAT 特性包括：静态 NAT、PAT、内部服务器、NAT ALG 功能、NAT 过滤、NAT 映射、Easy IP、两次 NAT 及 NAT 多实例。

静态 NAT

静态 NAT 实现私网地址和公网地址的一对一转换。有多少个私网地址就需要配置多少个公网地址。静态 NAT 不能节约公网地址，但可以起到隐藏内部网络的作用。

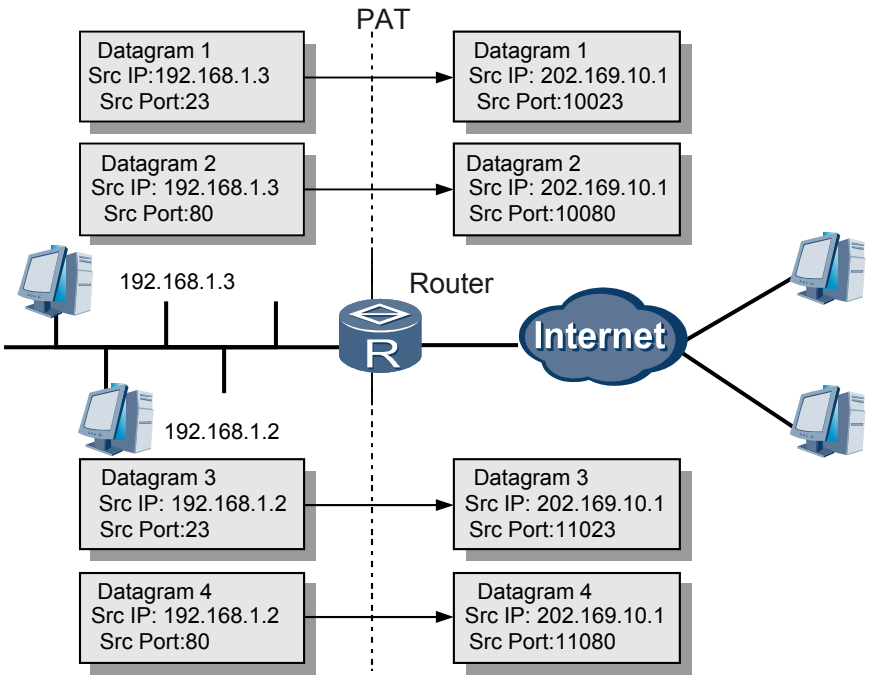
内部网络向外部网络发送报文时，静态 NAT 将报文的源 IP 地址替换为对应的公网地址；外部网络向内部网络发送响应报文时，静态 NAT 将报文的目的地址替换为相应的私网地址。

PAT

PAT 又称为 NAPT（Network Address Port Translation），它实现一个公网地址和多个私网地址之间的映射，因此可以节约公网地址。PAT 的基本原理是将不同私网地址的报文的源 IP 地址转换为同一公网地址，但他们被转换为该地址的不同端口号，因而仍然能够共享同一地址。

PAT 需要维护一张私网地址和端口的映射表。当不同的私网地址向外发送报文时，PAT 将报文的源 IP 地址替换为相同公网地址，但源端口号被替换为不同的端口号；当外部网络向内部网络发送响应报文时，PAT 根据报文的目的端口号，将报文的目的 IP 地址替换为不同的私网地址，如图 5-2 所示。

图 5-2 PAT 示意图



内部服务器

地址转换具有“屏蔽”内部主机的作用，但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一个 WWW 服务器，或是一台 FTP 服务器。

使用 NAT 可以灵活地添加内部服务器，例如可以使用 202.110.10.10 作为 Web 服务器的外部地址，使用 202.110.10.11 作为 FTP 服务器的外部地址，甚至还可以使用 202.110.10.12:8080 这样的地址作为 Web 的外部地址。还可为外部用户提供多台同样的服务器，如提供多台 Web 服务器。

通过配置内部服务器，可将相应的外部地址、端口等映射到内部的服务器上，提供了外部网络主机访问内部服务器的功能。

NAT 映射

由于 IPv4 地址的短缺，以及出于安全考虑等因素，在因特网中广泛采用了 NAT 技术。由于不同厂商实现的 NAT 功能不同，可能会导致使用 STUN、TURN、ICE 技术的应用软件无法穿越 NAT，这些技术广泛应用于 SIP 代理等软件，因此有必要实现符合这些软件能够进行 NAT 穿越的 NAT 映射类型，以便允许多种应用能够一致性的工作。

NAT 过滤

NAT 过滤是指 NAT 设备对外网发到内网的流量进行过滤，即当私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过 NAT 设备时会进行过滤。

Easy IP

Easy IP 的概念很简单，当进行地址转换时，直接使用接口的公有 IP 地址作为转换后的源地址。同样它也利用访问控制列表控制哪些内部地址可以进行地址转换。

地址转换应用层网关

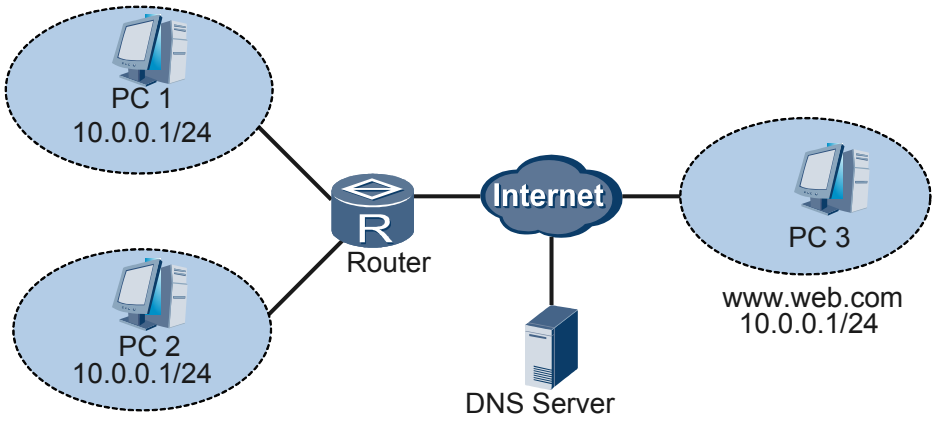
地址转换会导致许多对 NAT 敏感的应用协议无法正常工作，必须针对该协议进行特殊的处理。所谓对 NAT 敏感的协议是指该协议的某些报文的有效载荷中携带 IP 地址和（或）端口号，如果不进行特殊处理，将会影响后继的协议交互。

地址转换应用层网关 NAT ALG（NAT Application Level Gateway）是解决特殊协议穿越 NAT 的一种常用方式，该方法按照地址转换规则，对载荷中的 IP 地址和端口号进行替换，从而实现对该协议的透明中继。目前 AR1200 的 NAT ALG 支持 DNS、FTP 协议、RTSP（Real-Time Streaming Protocol ）和 SIP（Session Initiation Protocol ）。

两次 NAT

常规地址转换技术只转换报文的源地址或目的地址，而两次 NAT（Twice NAT）技术可以将报文的源地址和目的地址同时转换，该技术应用于内部网络主机地址与公网上主机地址重叠的情况。如**图 5-3** 所示：内部网络主机 PC1 和公网上主机 PC3 的地址重叠。这种情况下，内部网络主机 PC2 访问主机 PC3 的报文不会到达目的主机，而会被错误的转发到主机 PC1 上。两次 NAT 技术通过在 AR1200 上配置重叠地址池到临时地址的映射关系（在实现常规 NAT 的基础上），将重叠地址转换为唯一的临时地址，来保证报文的正确转发。

图 5-3 两次 NAT 示意图



例如，在 AR1200 上配置两次 NAT：

第一步：配置常规 NAT（多对多地址转换）。配置 NAT 地址池 200.0.0.1 ～ 200.0.0.100，并应用到广域网接口。

第二步：配置一组重叠地址到临时地址的映射。10.0.0.0<－－>3.0.0.0。

此映射表示，重叠地址池与临时地址池一一对应，转换规则为：

临时地址 = 临时地址池首地址 +（重叠地址 － 重叠地址池首地址）

重叠地址 = 重叠地址池首地址 +（临时地址 － 临时地址池首地址）

当内部主机 PC2 直接用域名访问公网上的主机 PC3 时，报文的处理流程如下：

1. PC2 发送解析域名为 www.web.com 的 Web 服务器的 DNS 请求，经公网 DNS 服务器解析后，AR1200 收到 DNS 服务器的响应报文。AR1200 检查 DNS 响应报文载荷中的解析回来的地址 10.0.0.1，经检查该地址为重叠地址（与重叠地址池匹配），将地址 10.0.0.1 转换为对应的临时地址 3.0.0.1。之后再对 DNS 响应报文进行目的地址转换（常规 NAT 处理），发送给 PC2。
2. PC2 用 www.web.com 对应的临时地址 3.0.0.1 发起访问，当报文到达 AR1200 时，先转换报文的源地址（常规 NAT 处理），再将报文的目的地址即临时地址，转换为对应的重叠地址 10.0.0.1。
3. 将报文送到广域网出接口，并经广域网逐跳转发至主机 PC3。
4. 当 PC3 给 PC2 返回的报文到达 AR1200 时，先检查报文的源地址 10.0.0.1，该地址为重叠地址（与重叠地址池匹配），则将源地址转换为对应的临时地址 3.0.0.1。之后再对返回报文的目的地址进行常规 NAT 转换，并发送给 PC2。

VPN 关联的源 NAT

AR1200 的 NAT 不仅可以使内部网络的用户访问外部网络，还允许分属于不同 VPN（Virtual Private Network）的用户通过同一个出口访问外部网络，能够解决内部网络中 IP 地址重叠的 VPN 同时访问外网主机的问题。

VPN 关联的 NAT Server

AR1200 的 NAT 支持 VPN 关联的 NAT server，提供给外部网络访问 VPN 内主机的机会，能够支持内网多个 VPN 地址重叠的场景。

5.3 配置 NAT

配置 NAT 实现私有网络和公有网络之间的互访，单个用户可以采用 Easy IP 方式，多个用户可以采用地址池方式。

5.3.1 建立配置任务

在配置 NAT 转换之前，了解 NAT 的应用环境，以及配置 NAT 需要提前完成的任务和准备的数据。

应用环境

在私有网络和公有网络的连接处需要配置 NAT。通过 NAT，可以实现私网地址和公网地址的转换。

前置任务

在配置源 NAT 之前，需要完成以下任务。

- 创建基本 ACL 或高级 ACL 并配置规则。

数据准备

在配置 NAT 之前，需要准备以下数据。

序号	数据
1	公网地址池的编号、起始 IP 地址和结束 IP 地址
2	基本 ACL 或高级 ACL 编号
3	内部服务器的信息：协议类型、外部地址、外部端口号、内部地址（可含 VPN 实例）、内部端口号（可选）
4	静态 NAT 的信息：协议类型、外部地址、外部端口号、内部地址（可含 VPN 实例）、内部端口号（可选）、子网掩码
5	重叠地址池和临时地址池索引、起始 IP 地址、地址池长度，内网 VPN 实例（可选）
6	域名、外部地址、外部端口号

5.3.2 配置地址池

NAT 采用地址池满足内部多个用户同时访问外部网络时进行地址转换的需求。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat address-group** *group-index start-address end-address*，配置公网地址池。

公网地址池是一组公网地址的集合，当内部数据报文通过 NAT 时，AR1200 将会选择地址池中的某个地址作为转换后的源地址。

公网地址池使用数字编号，最多可配置 8 个。

缺省情况下，AR1200 中未配置公网地址池。

----结束

5.3.3 配置 ACL 和地址池关联

ACL 可以限制内网的部分用户通过 NAT 转换访问公网，实现管理员对内部网络用户的精细管理。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **nat outbound** *acl-number* [**address-group** *group-index* [**no-pat**] | **interface loopback** *interface-number*]，配置 ACL 和地址池关联。

通过配置 ACL 和地址池的关联，将符合 ACL 中的数据报文的源地址进行地址转换，选用地址池中的某个地址进行转换。可以在同一个接口上配置不同的地址转换关联。

no-pat 表示使用一对一的地址转换，只转换数据包的地址而不转换端口信息。

----结束

5.3.4 配置 Easy IP

对符合 ACL 中的数据报文的源地址，直接使用接口的 IP 地址作为转换后的地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **nat outbound** *acl-number* [**address-group** *group-index* [**no-pat**] | **interface loopback** *interface-number*]，配置 Easy IP。

----结束

5.3.5 配置内部服务器

服务器放到私网中可以提高服务器的安全性，避免公网大量用户的攻击。同时可以满足正常用户访问服务器的需求。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行如下命令配置 NAT 内部服务器：

- **nat server protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** } *global-port* **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]
- **nat server protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]
- **nat server** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** *global-address* **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

配置内部服务器可以使外部网络主动访问私网中的服务器。当外部网络向内部服务器的外部地址（global-address）发起连接请求时，NAT 将该请求的目的地址替换为私网地址（host-address）后，转发给私网内的服务器。

说明

配置 NAT 内部服务器时，其中的 global-address 和 host-address 必须保证和设备现有地址没有重复，包括设备接口地址，用户地址池地址等，以避免冲突。

----结束

5.3.6 配置静态 NAT

静态 NAT 实现私网地址和公网地址的一对一转换。静态 NAT 不能节约公网地址，但可以起到隐藏内部网络的作用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行如下命令配置静态 NAT：

- **nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** } *global-port* **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]
- **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [**vpn-instance** *vpn-instance-name*]**inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]
- **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** *global-address* **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]

说明

配置静态 NAT 时，其中的 global-address 和 host-address 必须保证和设备现有地址没有重复，包括设备接口地址，用户地址池地址等，以避免冲突。

----结束

5.3.7 使能 NAT ALG 功能

对于封装在 IP 数据报文中的协议报文，正常的 NAT 转换会导致错误，NAT 应用级网关可以实现对这些特殊协议的正常转换。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat alg** { **all** | **dns** | **ftp** | **rtsp** | **sip** } **enable**，使能 NAT ALG 功能。

在使能某应用协议的 NAT ALG 功能后，该应用协议可以正常穿越 NAT，否则该应用协议不能正常工作。

all 表示同时支持 DNS、FTP、SIP 及 RTSP 协议的 NAT 穿越。

----结束

5.3.8 配置 NAT 过滤

NAT 过滤是指 NAT 设备对外网发到内网的流量进行过滤，即当私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过 NAT 设备时会进行过滤。

背景信息

NAT 过滤包括三种类型：

- 与外部地址和端口无关的 NAT 过滤行为。
- 与外部地址相关端口无关的 NAT 过滤行为。
- 与外部地址和端口都相关的 NAT 过滤行为。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat filter-mode** { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }，配置 NAT 过滤方式。

NAT 过滤技术应用在外网访问内网做目的 NAT 时，缺省采用 **endpoint-and-port-dependent** 方式，表示查询 NAT 反向映射表时，以“源 IP+源端口＋目的 IP+目的端口+协议号”作索引进行匹配。

----结束

5.3.9 配置 NAT 映射

配置 NAT 映射可以满足使用 STUN、TURN、ICE 等 NAT 穿越技术的终端软件能够穿越 NAT。

背景信息

由于 IPv4 地址的短缺，以及出于安全考虑等因素，在因特网中广泛采用了 NAT 技术，NAT 映射包含如下三种类型：

- 外部地址和端口无关的映射：对相同的内部 IP 和端口重用相同的地址端口映射。
- 外部地址相关端口无关的映射：对相同的内部 IP 地址和端口访问相同的外部 IP 地址时重用相同的端口映射。
- 外部地址和端口相关的映射：对相同的内部 IP 地址和端口号访问相同的外部 IP 地址和端口号重用相同的端口映射（如果此映射条目还处在活动状态）。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat mapping-mode endpoint-independent** [**tcp** | **udp**] [**dest-port** *port-number*]，配置 NAT 映射模式。

NAT 映射技术应用在内网访问外网做源 NAT 时，查询 NAT 映射表，缺省采用外部地址和端口相关的映射。

----结束

5.3.10 配置 DNS Mapping

当内部网络无 DNS 服务器，但存在类型不同的多台内部服务器（如 FTP、WWW 等），且内部主机希望通过不同域名区分并访问其对应的内部服务器时配置 DNS-Mapping。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat dns-map** *domain-name global-address global-port* { **tcp** | **udp** }，配置域名到外部 IP 地址、端口号、协议类型的映射。

AR1200 最多支持配置 32 条映射。

步骤 3 执行命令 **nat alg** { **all** | **dns** | **ftp** | **rtsp** | **sip** } **enable**，使能 DNS 的 NAT ALG 功能。

注意

在使能 DNS 的 NAT ALG 功能后，DNS 报文才可以正常穿越 NAT，否则内部主机无法使用外网 DNS 服务器的解析结果访问内部服务器。

----结束

5.3.11 配置两次 NAT

两次 NAT 指源 IP 地址和目的 IP 地址同时转换，应用于内部网络主机地址与外部网络上主机地址重叠的情况。

背景信息

当内部网络主机地址与公网上主机地址重叠时，需要配置重叠地址池到临时地址池的映射关系。用户通过配置重叠地址池到临时地址池的映射关系，将从外网到内网的重叠地址转换为唯一的临时地址，来保证报文的正确转发，同时用户还需要配置常规的 NAT Outbound，实现双向 NAT 的功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nat overlap-address** *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]，配置两次 NAT。

重叠地址池和临时地址池是一些连续的 IP 地址集合，两个地址池长度相等，每个地址池中地址个数最大为 255。

全局允许配置 8 个重叠地址池到临时地址池的映射关系。

当配置中的 VPN 实例删除时，两次 NAT 的配置也同步删除。

----结束

5.3.12 检查配置结果

配置 NAT 之后，可以查看 NAT 的相关信息。

操作步骤

- 执行 **display nat alg** 查看地址转换应用层网关 NAT ALG 是否使能。
- 执行 **display nat address-group** [*group-index*] [**verbose**]查看 NAT 地址池的配置信息。
- 执行 **display nat dns-map** [*domain-name*]查看 DNS Mapping 信息。
- 执行 **display nat outbound** [**acl** *acl-number* | **address-group** *group-index* | **interface** { **EthernetGigabitEthernet** } *interface-number.subnumber*]查看 NAT Outbound 信息。
- 执行 **display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }命令查看 NAT 双向地址转换的相关信息。
- 执行 **display nat server** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number.subnumber*]命令查看 NAT Server 的配置信息。
- 执行 **display nat static** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-name*]命令查看 NAT Static 的配置信息。
- 执行 **display nat mapping table** { **all** | **number** }命令查看 NAT 映射表信息或个数。

----结束

5.4 配置示例

介绍使用 NAT 提高网络安全性的各种示例。

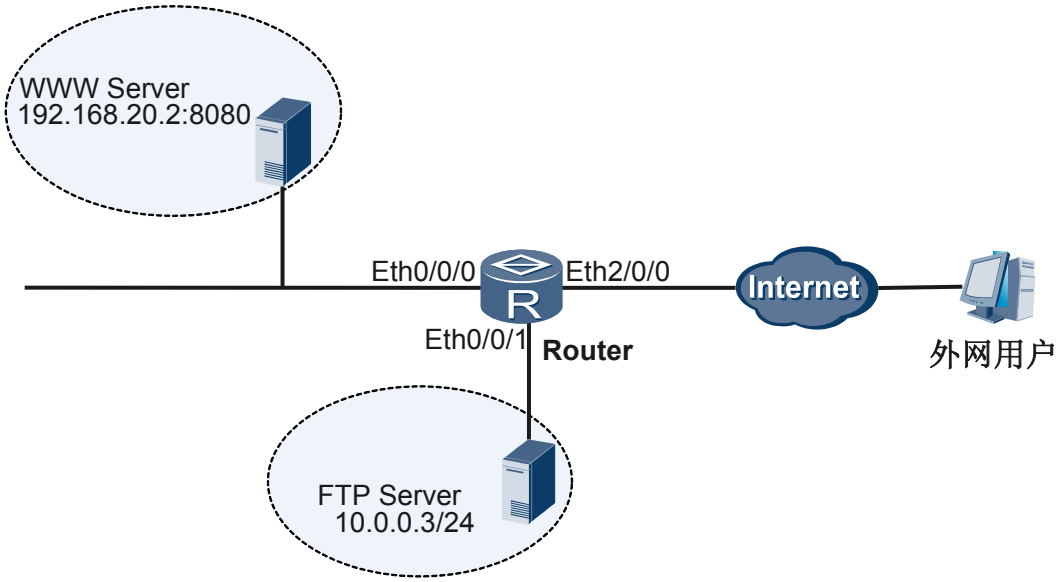
5.4.1 配置 NAT Server 示例

组网需求

如图 5-4 所示，某公司的网络通过 AR1200 的地址转换功能连接到广域网。该公司提供 WWW Server 和 FTP Server 供外部网络用户访问。其中 WWW Server 的内部 IP 地址为

192.168.20.2:8080，对外公布的地址为 202.169.10.5/24。FTP Server 的内部 IP 地址为 10.0.0.3/24，对外公布的地址为 202.169.10.33/24,对端运营商侧地址为 202.169.10.2/24。

图 5-4 配置 NAT Server 组网图



配置思路

采用如下思路配置 NAT Server：

1. 配置接口 IP 地址，并在 WAN 侧接口下配置 NAT Server，实现外部网络用户访问内网服务器功能。
2. 配置缺省路由。
3. 配置内网网关。
4. 使能 FTP 的 NAT ALG 功能，实现外部用户的 FTP 访问能正常穿越 NAT。

操作步骤

步骤 1 在 AR1200 上配置接口 IP 地址和 NAT Server。

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.20.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] vlan 200
[Huawei-vlan200] quit
[Huawei] interface vlanif 200
[Huawei-Vlanif200] ip address 10.0.0.1 24
[Huawei-Vlanif200] quit
[Huawei] interface Ethernet 0/0/1
[Huawei-Ethernet0/0/1] port link-type access
[Huawei-Ethernet0/0/1] port default vlan 200
```

```
[Huawei-Ethernet0/0/1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-ethernet 2/0/0] ip address 202.169.10.1 24
[Huawei-ethernet 2/0/0] nat server protocol tcp global 202.169.10.5 www inside 192.168.20.2
8080
[Huawei-ethernet 2/0/0] nat server protocol tcp global 202.169.10.33 ftp inside 10.0.0.3 ftp
[Huawei-ethernet 2/0/0] quit
```

步骤 2 在 AR1200 上配置缺省路由，下一跳地址为 202.169.10.2。

```
[Huawei] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

步骤 3 在 AR1200 上使能 FTP 的 NAT ALG 功能。

```
[Huawei] nat alg ftp enable
```

步骤 4 检查配置结果。

在 AR1200 上执行 **display nat server** 操作，结果如下。

```
[Huawei] display nat server
   Nat Server Information:
  Interface  : ethernet 2/0/0
    Global IP/Port     : 202.169.10.5/80(www)
    Inside IP/Port     : 192.168.20.2/8080
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----

    Global IP/Port     : 202.169.10.33/21(ftp)
    Inside IP/Port     : 10.0.0.3/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----

  Total :    2
```

在 AR1200 上执行 **display nat alg** 操作，结果如下。

```
[Huawei] display nat alg
NAT Application Level Gateway Information:
----------------------------------
  Application            Status
----------------------------------
  dns                    Disabled
  ftp                    Enabled
  rtsp                   Disabled
  sip                    Disabled
----------------------------------
```

验证外网用户是否能正常访问公司的 WWW Server 和 FTP Server。

----结束

配置文件

```
#
 vlan batch 100 200
#
 nat alg ftp enable
#
interface Vlanif100
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif200
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
```

```
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 200
#
interface Ethernet 2/0/0
 ip address 202.169.10.1 255.255.255.0
 nat server protocol tcp global 202.169.10.5 www inside 192.168.20.2 8080
 nat server protocol tcp global 202.169.10.33 ftp inside 10.0.0.3 ftp
#
ip route-static 0.0.0.0 0.0.0.0 Ethernet 2/0/0
#
return
```

5.4.2 配置 NAT Outbound 示例

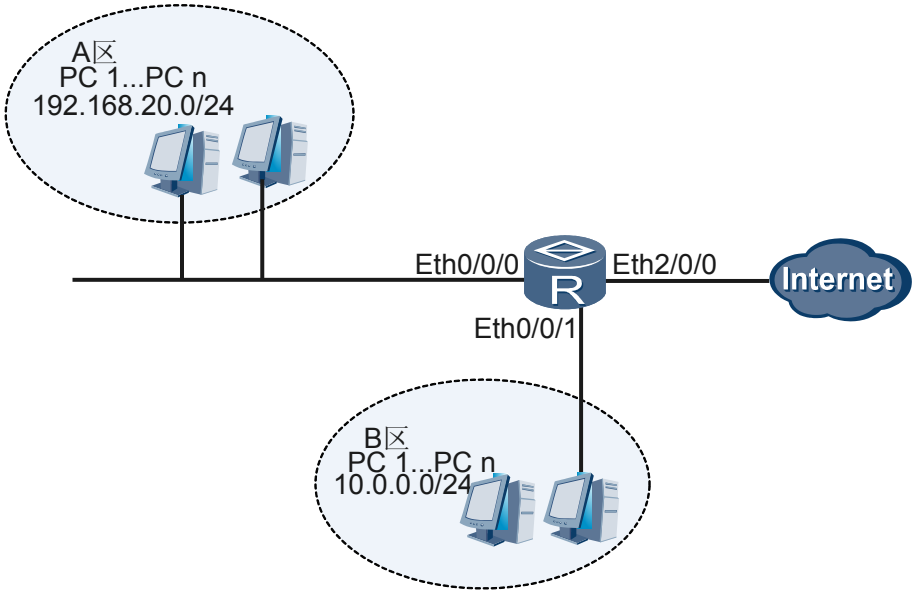
组网需求

如图 5-5 所示，某公司 A 区的网络通过 AR1200 的地址转换功能访问广域网。使用公网地址池中的地址（202.169.10.100 ～ 202.169.10.200）采用一对一的方式替换 A 区内部的主机地址（网段为 192.168.20.0/24），访问广域网。

B 区的网络通过 AR1200 的地址转换功能访问广域网。结合 B 区的公网 IP 地址比较少的情况，使用公网地址池（202.169.10.80 ～ 202.169.10.83）采用 IP 地址和端口的替换方式替换 B 区内部的主机地址（网段为 10.0.0.0/24），访问广域网。

其中 AR1200 上接口 Ethernet2/0/0 的公网地址为 202.169.10.1/24,对端运营商侧地址为 202.169.10.2/24。

图 5-5 配置 NAT Outbound 组网图



配置思路

采用如下思路配置 NAT Outbound：

1. 配置接口 IP 地址。
2. 配置缺省路由。
3. 在 WAN 侧接口下配置 NAT Outbound，实现内部主机访问外网服务功能。

操作步骤

步骤 1 在 AR1200 上配置接口 IP 地址。

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.20.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] vlan 200
[Huawei-vlan200] quit
[Huawei] interface vlanif 200
[Huawei-Vlanif200] ip address 10.0.0.1 24
[Huawei-Vlanif200] quit
[Huawei] interface Ethernet 0/0/1
[Huawei-Ethernet0/0/1] port link-type access
[Huawei-Ethernet0/0/1] port default vlan 200
[Huawei-Ethernet0/0/1] quit
[Huawei] interface Ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 202.169.10.1 24
[Huawei-Ethernet2/0/0] quit
```

步骤 2 在 AR1200 上配置缺省路由，指定下一跳地址为 202.169.10.2。

```
[Huawei] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

步骤 3 在 AR1200 上配置 NAT Outbound。

```
[Huawei] nat address-group 1 202.169.10.100 202.169.10.200
[Huawei] nat address-group 2 202.169.10.80 202.169.10.83
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule 5 permit source 192.168.20.0 0.0.0.255
[Huawei-acl-basic-2000] quit
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 10.0.0.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] interface Ethernet 2/0/0
[Huawei-Ethernet2/0/0] nat outbound 2000 address-group 1 no-pat
[Huawei-Ethernet2/0/0] nat outbound 2001 address-group 2
[Huawei-Ethernet2/0/0] quit
```

步骤 4 检查配置结果。

在 AR1200 上执行 **display nat outbound** 操作，结果如下。

```
[Huawei] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface                       Acl      Address-group/IP/Interface      Type
 ----------------------------------------------------------------------
 Ethernet2/0/0           2000                     1    no-pat
 Ethernet2/0/0           2001                     2       pat
 ----------------------------------------------------------------------
  Total : 2
```

在 AR1200 上执行如下操作：

```
<Huawei> ping -a 192.168.20.1 202.169.10.2
  PING 202.169.10.2: 56 data bytes, press CTRL_C to break
```

```
    Reply from 202.169.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms
<Huawei> ping -a 10.0.0.1 202.169.10.2
  PING 202.169.10.2: 56 data bytes, press CTRL_C to break
    Reply from 202.169.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms
```

----结束

配置文件

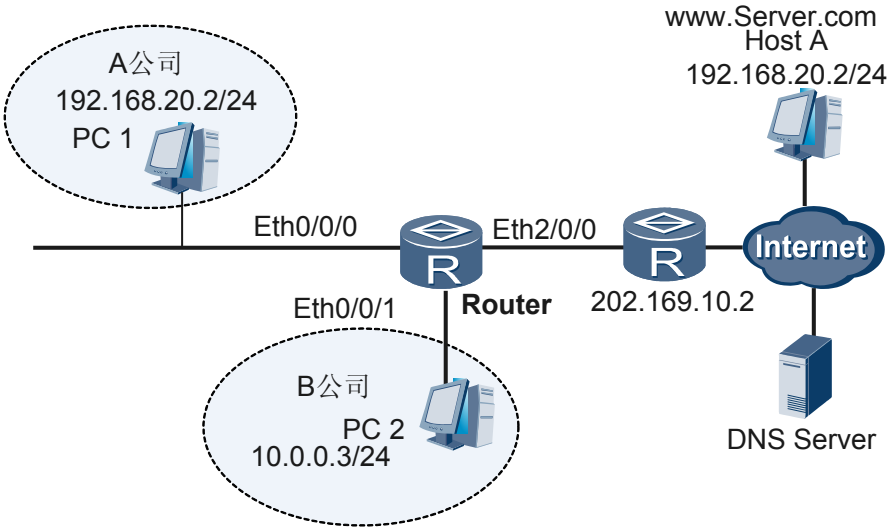
```
#
 vlan batch 100 200
 #
acl number 2000
 rule 5 permit source 192.168.20.0 0.0.0.255
#
acl number 2001
 rule 5 permit source 10.0.0.0
0.0.0.255
#
interface Vlanif100
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif200
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/1
 port link-type access
 port default vlan
200
#
interface Ethernet2/0/0
 ip address 202.169.10.1 255.255.255.0
 nat outbound 2000 address-group 1 no-pat
 nat outbound 2001 address-group 2
#
 nat address-group 1 202.169.10.100 202.169.10.200
 nat address-group 2 202.169.10.80 202.169.10.83
#
ip route-static 0.0.0.0 0.0.0.0 Ethernet 2/0/0
#
return
```

5.4.3 配置两次 NAT 示例

组网需求

如图 5-6 所示，内部网络主机 PC1 和公网上主机 Host A 的地址重叠。这种情况下，内部网络主机 PC2 访问主机 Host A 的报文不会到达目的主机，而有可能会被错误的转发到主机 PC1 上。两次 NAT 技术通过在 AR1200 上配置重叠地址池到临时地址池的映射关系（在实现常规 NAT 的基础上），将重叠地址转换为唯一的临时地址，来保证报文的正确转发。

图 5-6 配置两次 NAT 组网图



配置思路

采用如下思路配置两次 NAT：

1. 配置接口 IP 地址。
2. 配置 DNS-Mapping，实现通过域名访问服务器功能。
3. 配置重叠地址池到临时地址池的映射关系，将重叠地址转换为唯一的临时地址。
4. 配置常规 NAT Outbound，实现内网用户访问外网服务功能。

操作步骤

步骤 1 在 AR1200 上配置接口 IP 地址。

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.20.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] vlan 200
[Huawei-vlan200] quit
[Huawei] interface vlanif 200
[Huawei-Vlanif200] ip address 10.0.0.1 24
[Huawei-Vlanif200] quit
[Huawei] interface Ethernet 0/0/1
[Huawei-Ethernet0/0/1] port link-type access
[Huawei-Ethernet0/0/1] port default vlan 200
[Huawei-Ethernet0/0/1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 202.169.10.2 24
[Huawei-Ethernet2/0/0] quit
```

步骤 2 在 AR1200 上配置 DNS-Mapping。

```
[Huawei] nat alg dns enable
[Huawei] nat dns-map www.Server.com 192.168.20.2 80 tcp
```

步骤 3 在 AR1200 上配置重叠地址池到临时地址池的映射关系。

```
[Huawei] nat overlap-address 0 192.168.20.2 202.169.100.2 pool-length 254
```

步骤 4 在 AR1200 上配置临时地址池到出接口 Ethernet2/0/0 的静态路由。

```
[Huawei] ip route-static 202.169.100.2 32 ethernet 2/0/0  202.169.10.2
```

步骤 5 在 AR1200 的出接口 Ethernet2/0/0 上配置 NAT Outbound。

1. 配置 ACL，并配置允许 Host A 通过的 rule。

```
[Huawei] acl 3180
[Huawei-acl-adv-3180] rule permit ip source 192.168.20.0 0.0.0.255
[Huawei-acl-adv-3180] quit
```

2. 配置常规 NAT Outbound 要使用的 NAT 地址池。

```
[Huawei] nat address-group 1 160.160.0.2 160.160.0.254
```

3. 在出接口 Ethernet2/0/0 上配置常规 NAT Outbound。

```
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] nat outbound 3180 address-group 1
[Huawei-Ethernet2/0/0] quit
```

步骤 6 检查配置结果。

在 AR1200 上执行 **display nat overlap-address all** 命令查看地址池映射关系。

```
[Huawei] display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 ------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address    Pool-Length       Inside-VPN-Instance-Name
 ------------------------------------------------------------------------------
 0   192.168.20.2     202.169.100.2   254
 ------------------------------------------------------------------------------
  Total : 1
```

在 AR1200 上执行 **display nat outbound** 命令查看 NAT Outbound 信息。

```
[Huawei] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface                       Acl      Address-group/IP/Interface      Type
 ----------------------------------------------------------------------
 Ethernet2/0/0                   3180                     1               pat
 ----------------------------------------------------------------------
  Total : 1
```

----结束

配置文件

```
#
 vlan batch 100 200
#
acl number 3180
 rule 5 permit ip source 192.168.20.0
0.0.0.255
#
 nat alg dns enable
#
 nat address-group 1 160.160.0.2 160.160.0.254
#
 nat dns-map www.server.com 192.168.20.2 80 tcp
#
 nat overlap-address 0 192.168.20.2 202.169.100.2 pool-length 254
#
ip route-static 202.169.100.2 255.255.255.255 Ethernet2/0/0 202.169.10.2
```

```
#
interface Vlanif100
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif200
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 200
#
interface Ethernet2/0/0
 ip address 202.169.10.1 255.255.255.0
 nat outbound 3180 address-group 1
#
return
```

6 DHCP 配置

关于本章

DHCP（Dynamic Host Configuration Protocol）技术实现用户地址和配置信息的动态分配和集中管理，可以快速、动态地为用户分配和管理 IP 地址，保证 IP 地址的合理分配，提高 IP 地址使用效率。

6.1 DHCP 概述
DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户进行动态管理和配置的技术。

6.2 AR1200 支持的 DHCP 特性
介绍 DHCP 特性在 AR1200 中的支持情况。

6.3 配置基于全局地址池的 DHCP 服务器
配置基于全局地址池的 DHCP 服务器，从所有接口上线的用户都可以选择该地址池中的地址。

6.4 配置基于接口地址池的 DHCP 服务器
配置基于接口地址池的 DHCP 服务器，从这个接口上线的用户都从该接口地址池中获取 IP 地址等配置信息。

6.5 配置 DHCP 中继
DHCP 客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，获取 IP 地址等配置信息。

6.6 配置 DHCP/BOOTP 客户端
指定 AR1200 的三层接口作为 DHCP/BOOTP 客户端时，可以使用 DHCP/BOOTP 协议从 DHCP 服务器动态获得 IP 地址及其他配置信息。

6.7 配置 DHCP 报文限速
用户可以在全局、VLAN 或接口下配置限制 DHCP 报文上送速率，如果在全局、VLAN 或接口下同时配置，有效的顺序为接口优先，VLAN 其次，最后为全局。

6.8 维护 DHCP
完成 DHCP 配置后，介绍如何清除 DHCP 统计信息以及如何监控 DHCP 运行状况。

6.9 配置举例
DHCP 的配置举例包括组网需求、组网图、配置注意事项、配置思路和配置步骤。

6.1 DHCP 概述

DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户进行动态管理和配置的技术。

随着网络规模的不断扩大和网络复杂度的提高，计算机的数量经常超过可供分配的 IP 地址数量。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回 IP 地址等相应配置信息给客户端，以实现 IP 地址等信息的动态配置。

早期的 DHCP 协议只适用于 DHCP 客户端和服务器处于同一个子网内的情况，不可以跨网段工作，这样就需要为每一个子网配置一个 DHCP 服务器，浪费资源。DHCP 中继的引入解决了这一问题。

6.2 AR1200 支持的 DHCP 特性

介绍 DHCP 特性在 AR1200 中的支持情况。

AR1200 作为 DHCP 服务器

AR1200 可以作为 DHCP 服务器为上线用户分配 IP 地址。客户端向服务器发送配置申请报文（包括 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回携带相应配置信息的报文，请求报文和回应报文都采用 UDP 进行封装。

当 AR1200 作为 DHCP 服务器时，需要在 AR1200 上创建地址池，为 DHCP 客户端分配 IP 地址。地址池包括两种类型：全局地址池和接口地址池。

- 配置基于全局地址池的 DHCP 服务器，从所有接口上线的用户都可以选择该地址池中的地址。
- 配置基于接口地址池的 DHCP 服务器，只有从指定接口上线的用户才可以从该地址池中分配地址。

当 AR1200 作为 DHCP 服务器时，支持两种分配地址模式：通过 DHCP 全局地址池向客户端分配 IP 地址和通过 DHCP 接口地址池向客户端分配 IP 地址。

AR1200 作为 DHCP 中继

AR1200 支持 DHCP 中继功能。当 AR1200 作为 DHCP 中继时，客户端可以通过 AR1200 与其他网段的 DHCP 服务器通信，从 DHCP 服务器的全局地址池中获取 IP 地址及其他配置信息。这样，多个网段的 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。

AR1200 作为 DHCP/BOOTP 客户端

AR1200 支持 DHCP/BOOTP 客户端功能。指定 AR1200 的三层接口作为 DHCP/BOOTP 客户端时，可以使用 DHCP/BOOTP 协议从 DHCP 服务器动态获得 IP 地址及其他配置信息，方便用户配置，也便于集中管理。

AR1200 支持 DHCP 报文限速功能

AR1200 支持 DHCP 报文限速功能，防止网络中的攻击者发送大量的 DHCP 报文对 AR1200 的 DHCP 协议栈造成影响。

6.3 配置基于全局地址池的 DHCP 服务器

配置基于全局地址池的 DHCP 服务器，从所有接口上线的用户都可以选择该地址池中的地址。

6.3.1 建立配置任务

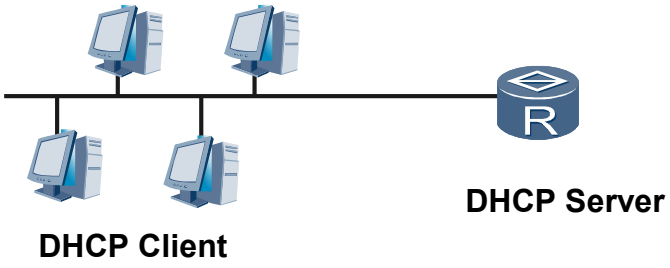
在配置基于全局地址池的 DHCP 服务器前了解此功能的应用环境、前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AR1200 作为 DHCP 服务器，可以在 AR1200 上配置全局地址池，此时 AR1200 通过 DHCP 全局地址池向客户端分配 IP 地址及其他配置信息。全局地址池模式应用于以下两种场景：

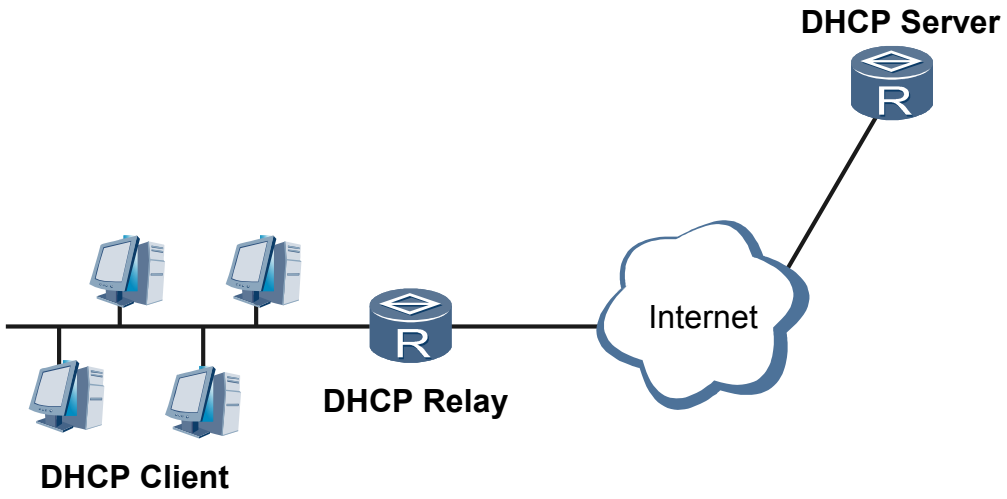
当 DHCP 客户端和作为 DHCP 服务器的 AR1200 在同一个网段时，DHCP 客户端可以从全局地址池中获取 IP 地址及其他配置信息。如图 6-1 所示。

图 6-1 全局地址池模式的第一种应用场景



当 DHCP 客户端和作为 DHCP 服务器的 AR1200 不在同一个网段时，DHCP 客户端可以通过 DHCP 中继从全局地址池中获取 IP 地址及其他配置信息。如图 6-2 所示。

图 6-2 全局地址池模式的第二种应用场景



前置任务

在配置基于全局地址池的 DHCP 服务器之前，需完成以下任务：

- 保证 DHCP 客户端的和 AR1200 之间链路正常，能够通信
- 配置客户端的 DNS 服务（根据实际需要，可选择配置）
- 配置客户端的 NetBIOS 服务（根据实际需要，可选择配置）
- 配置 AR1200 到 DNS 服务器和 NetBIOS 服务器的路由（如果没有配置这两种服务器，则无需配置路由）
- 配置 DHCP 自定义选项（根据实际需要，可选择配置）

数据准备

在配置基于全局地址池的 DHCP 服务器之前，需准备以下数据。

序号	数据
1	地址池的名字、IP 地址范围、租期、（可选）地址池中不参与自动分配的 IP 地址的范围、（可选）需要静态绑定的 IP 地址和 MAC 地址表项
2	DHCP 客户端的出口网关
3	（可选）DNS 服务器的 IP 地址以及 DHCP 客户端的域名
4	（可选）NetBIOS 服务器的 IP 地址以及 DHCP 客户端的 NetBIOS 节点类型
5	（可选）DHCP 自定义选项的编码以及对应的 ASCII 字符串、十六进制数字或 IP 地址

6.3.2 配置接口工作在全局地址池模式

配置接口工作在全局地址池模式，从该接口上线的用户可以从全局地址池中获取 IP 地址等配置信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在全局地址池模式的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 4 执行命令 **ip address** *ip address* { *mask* | *mask-length* }，配置接口的 IP 地址。

配置了接口的 IP 地址后，此接口下的用户申请 IP 地址时。

- 如果 DHCP 客户端和作为 DHCP 服务器的 AR1200 处于同一个网段，中间没有中继设备时，AR1200 会选择与此接口的 IP 地址在同一个网段的地址池来分配 IP 地址。如果接口未配置 IP 地址，或者没有和接口地址在相同网段的地址池，用户无法上线。
- 如果 DHCP 客户端和作为 DHCP 服务器的 AR1200 处于不同网段，中间存在中继设备时，AR1200 需解析收到的 DHCP 请求报文中 giaddr 字段指定的 IP 地址，如果该 IP 地址匹配不到相应的地址池，则用户上线失败。

步骤 5 执行命令 **dhcp select global**，配置接口工作在全局地址池模式，从该接口上线的用户可以从全局地址池中获取 IP 地址等配置信息。

----结束

6.3.3 配置全局地址池的相关属性

配置全局地址池的相关属性，包括地址范围、地址租期、不参与自动分配的 IP 地址以及静态绑定的 IP 地址。根据客户端的实际需要，可以选择采用动态地址分配方式或静态地址绑定方式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入全局地址池视图。

缺省情况下，AR1200 上没有创建任何全局地址池。

步骤 3 执行命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的 IP 地址范围。

配置地址池网段时，同一地址池中只能配置一个地址段，通过掩码设定地址范围的大小。

说明

配置全局地址池可动态分配的 IP 地址范围时，请尽量保证该地址范围与 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。

步骤 4 （可选）执行命令 **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }，配置 IP 地址租期。

缺省情况下，IP 地址的租期为 1 天。

对于不同的地址池，DHCP 服务器可以指定不同的地址租用期限，但同一地址池中的地址都具有相同的期限。

步骤 5 （可选）执行命令 **excluded-ip-address** *start-ip-address* [*end-ip-address*]，配置地址池中不参与自动分配的 IP 地址。

有些地址分配给其他的服务，如分配给 DNS 服务器就不能再分配给客户端使用。可以执行 **excluded-ip-address** 命令配置地址池中不参与自动分配的 IP 地址。多次执行该命令，可以配置多个不参与自动分配的 IP 地址。

步骤 6 执行命令 **gateway-list** *ip-address* &<1-8>，配置 DHCP 客户端的出口网关地址。

说明

DHCP 客户端访问本网段以外的服务器或主机时，数据必须通过出口网关进行收发。

为了对流量进行负载分担和提高网络的可靠性，可以配置多个出口网关，每个地址池最多可以配置 8 个网关地址。网关地址不能是子网广播地址。

步骤 7 （可选）执行命令 **static-bind ip-address** *ip-address* **mac-address** *mac-address*，采用静态地址绑定方式将全局地址池中的 IP 地址与 MAC 地址绑定。

当一个用户需要固定的 IP 地址时，可以将地址池中没有在使用的 IP 地址与用户的 MAC 地址绑定。

说明

采用静态地址绑定方式将全局地址池中的 IP 地址与 MAC 地址绑定时，该 IP 地址必须在全局地址池可动态分配的 IP 地址范围之内。

步骤 8 （可选）执行命令 **recycle** *start-ip-address* [*end-ip-address*]，配置回收地址池中无法释放的地址。

----结束

6.3.4 （可选）动态配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务

AR1200 作为 DHCP 服务器时，配置动态配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务的功能，可以自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端。

背景信息

为了保证 DHCP 客户端的正常通信，DHCP 服务器在给客户端分配 IP 地址的同时，需指定 DNS 服务器的配置信息和 NetBIOS 的配置信息。用户如果不知道运营商分配的这些配置信息，可以采用动态配置的方式自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端。

说明

当地址池里有静态配置的 DNS，NetBIOS，Domain-name 等信息时，以静态配置优先。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **import all**，动态配置 DHCP 客户端使用的 DNS 配置信息和 NetBIOS 配置信息。

----结束

6.3.5 （可选）静态配置 DHCP 客户端的 DNS 服务

指定客户端在网络上使用的 DNS 域名和 DNS 服务器的 IP 地址。

背景信息

用户主机通过域名访问 Internet 时，需要将域名解析为 IP 地址，这是通过域名系统 DNS（Domain Name System）实现的。因此，为了使 DHCP 客户端成功接入 Internet，DHCP 服务器应在为客户端分配 IP 地址的同时指定 DNS 服务器地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **domain-name** *domain-name*，配置分配给 DHCP 客户端的 DNS 域名。

在 DHCP 服务器上，可以为每个地址池分别指定客户端使用的 DNS 域名。

步骤 4 执行命令 **dns-list** *ip-address* &<1-8>，配置 DHCP 客户端使用的 DNS 服务器的 IP 地址。

为了对流量进行负载分担和提高网络的可靠性，可配置多个 DNS 服务器。每个地址池最多可以配置 8 个 DNS 服务器地址。

----结束

6.3.6 （可选）静态配置 DHCP 客户端的 NetBIOS 服务

对于使用 Windows Microsoft 操作系统的客户端，由 NetBIOS 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。

背景信息

说明

NetBIOS：Network Basic Input Output System，网络基本输入/输出系统的简称。

DHCP 客户端使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种。

- b 类节点（b-node）：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。
- 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。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **nbns-list** *ip-address* &<1-8>，配置 DHCP 客户端的 NetBIOS 服务器地址。

每个地址池最多可以配置 8 个 NetBIOS 服务器地址。

步骤 4 执行命令 **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }，配置 DHCP 客户端的 NetBIOS 节点类型。

缺省情况下，不指定客户端的 NetBIOS 节点类型。

----结束

6.3.7 （可选）配置全局地址池 DHCP 自定义选项

随着 DHCP 的不断发展，新的可选配置项会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将新选项添加到 DHCP 服务器的属性列表中。

背景信息

如果用户在 DHCP 服务器端配置了 Option，DHCP 客户端在申请 IP 地址的时候，会通过服务器端回应的 DHCP 报文获得 Option 字段中的配置信息。

说明

常用的功能，如客户端的 DNS 服务、NetBIOS 服务、租期等，可以通过 Option 命令进行配置，但是以相关命令的配置为优先。如果相关命令没有配置，而配置了对应的 Option 选项，那么会取用 Option 命令配置的值。

相关命令如下：

- DNS 服务：**domain-name**、**dns-list**
- NetBIOS 服务：**nbns-list**、**netbios-type**
- 租期：**lease**

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip pool** *ip-pool-name*，进入 IP 地址池视图。

步骤 3 执行命令 **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* &<1-8> }，配置 DHCP 自定义选项。

option 命令用于将指定选项内容通过服务器端回应的 DHCP 报文携带给客户端。使用该命令前，需要明确选项功能。DHCP 的知名选项，请参考 RFC2132。

----结束

6.3.8 （可选）配置防止 IP 地址重复分配功能

为防止 IP 地址重复分配导致地址冲突，AR1200 应用为 DHCP 服务器时为客户端分配地址前，需要先对该地址进行探测。

背景信息

地址探测是通过 **dhcp server ping** 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果在最长等待 Ping 响应的时间内没有得到应答，则继续发送 Ping 报文，直到发送 Ping 包数量达到最大值，如果仍然没有收到应答，则认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址是唯一的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server ping packet** *number*，配置 AR1200 发送 Ping 包的最大数量。

缺省情况下，AR1200 发送 Ping 包的最大数量为 0，即不进行 ping 操作。

步骤 3 执行命令 **dhcp server ping timeout** *milliseconds*，配置 AR1200 发送 Ping 包的最长等待响应时间。

缺省情况下，AR1200 等待 Ping 响应的最长时间为 500 毫秒。

----结束

6.3.9 检查配置结果

查看基于全局地址池的 DHCP 服务器的配置信息。

前提条件

已经完成基于全局地址池的 DHCP 服务器的所有配置。

操作步骤

- 执行命令 **display dhcp server statistics**，查看 DHCP 服务器的统计信息。
- 执行命令 **display ip pool name** *ip-pool-name* [*low-ip-address high-ip-address* | **all** | **expired** | **conflict** | **used**]，查看已经配置的全局地址池信息。

----结束

任务示例

执行命令 **display dhcp server statistics**，查看 DHCP 服务器的统计信息。

```
<Huawei> display dhcp server statistics
 DHCP Server Statistics:

 Client Request:            6
  Dhcp Discover:            1
  Dhcp Request:             4
  Dhcp Decline:             0
  Dhcp Release:             1
  Dhcp Inform:              0
 Server Reply:              4
  Dhcp Offer:               1
  Dhcp Ack:                 3
  Dhcp Nak:                 0
 Bad Messages:              0
```

执行命令 **display ip pool name** *ip-pool-name*，查看名称为“pool1”的 IP 地址池信息。

```
<Huawei> display ip pool name pool1

Pool-Name      : pool1
  Pool-No        : 2
  Lease          : 3 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-Server0    : 10.10.10.5
  DNS-Server1    : 10.10.10.6
  NBNS-Server0   : 20.20.20.5
  Netbios-type   : -
  Position       : Local           Status          : Unlocked
  Gateway-0      : 10.10.10.10
  Mask           : 255.255.255.0
  Vpn instance   : --
  ------------------------------------------------------------------------------
            Start             End  Total   Used   Idle(Expired)   Conflict Disable
  ------------------------------------------------------------------------------
       10.10.10.1      10.10.10.254    253      0     253           0        0
  ------------------------------------------------------------------------------
```

6.4 配置基于接口地址池的 DHCP 服务器

配置基于接口地址池的 DHCP 服务器，从这个接口上线的用户都从该接口地址池中获取 IP 地址等配置信息。

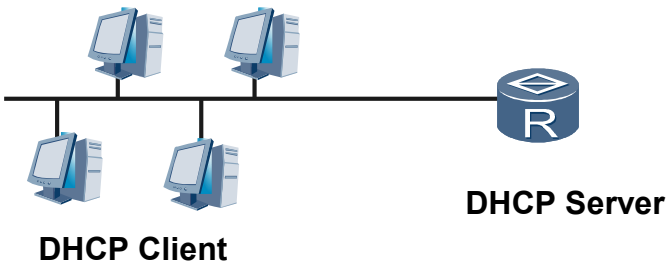
6.4.1 建立配置任务

在配置接口地址池的 DHCP 服务器前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

AR1200 作为 DHCP 服务器，可以在 AR1200 上配置接口地址池。接口地址池模式只适用于 DHCP 客户端和 DHCP 服务器在同一个网段的情况。如图 6-3 所示。

图 6-3 接口地址池模式的应用场景



前置任务

在配置基于接口地址池的 DHCP 服务器之前，需完成以下任务：

- 保证 DHCP 客户端和 AR1200 之间链路正常，能够通信
- 配置 DNS 服务器（根据实际需要，可选择配置）
- 配置 NetBIOS 服务器（根据实际需要，可选择配置）

- 配置 AR1200 到 DNS 服务器和 NetBIOS 服务器的路由（如果没有配置这两种服务器，则无需配置路由）

数据准备

在配置基于接口地址池的 DHCP 服务器之前，需准备以下数据。

序号	数据
1	使能地址池功能的接口编号、IP 地址范围、租期、（可选）地址池中不参与自动分配的 IP 地址的范围、（可选）需要静态绑定的 IP 地址和 MAC 地址表项
2	（可选）DNS 服务器的 IP 地址以及 DHCP 客户端的域名
3	（可选）NetBIOS 服务器的 IP 地址以及 DHCP 客户端的 NetBIOS 节点类型
4	（可选）DHCP 自定义选项的编码以及对应的 ASCII 字符串、十六进制数字或 IP 地址

6.4.2 配置接口地址池的相关属性

配置接口地址池的相关属性，包括地址租期、不参与自动分配的 IP 地址以及静态绑定的 IP 地址。根据客户端的实际需要，可以选择采用动态地址分配方式或静态地址绑定方式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 服务。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在接口地址池模式的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

步骤 5 执行命令 **dhcp select interface**，配置 AR1200 采用接口地址池的 DHCP 服务器模式。

接口地址池可动态分配的 IP 地址范围就是接口的 IP 地址所在的网段，且只在此接口下有效。

步骤 6 （可选）执行命令 **dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }，配置 IP 地址租期。

缺省情况下，IP 地址的租期为 1 天。

步骤 7 （可选）执行命令 **dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*]，配置地址池中不参与自动分配的 IP 地址。

有些地址分配给其他的服务，如分配给 DNS 服务器就不能再分配给客户端使用。可以执行该命令配置地址池中不参与自动分配的 IP 地址。多次执行该命令，可以配置多个不参与自动分配的 IP 地址。

步骤 8 （可选）执行命令 **dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address*，采用静态地址绑定方式将接口地址池中的 IP 地址与 MAC 地址绑定。

当一个用户需要固定的 IP 地址时，可以将地址池中没有在使用的 IP 地址与用户的 MAC 地址绑定。

说明

采用静态地址绑定方式将接口地址池中的 IP 地址与 MAC 地址绑定时，该 IP 地址必须在接口地址池可动态分配的 IP 地址范围之内。

----结束

6.4.3 （可选）动态配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务

AR1200 作为 DHCP 服务器时，配置动态配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务的功能，可以自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端。

背景信息

为了保证 DHCP 客户端的正常通信，DHCP 服务器在给客户端分配 IP 地址的同时，需指定 DNS 服务器的配置信息和 NetBIOS 的配置信息。用户如果不知道运营商分配的这些配置信息，可以采用动态配置的方式自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端。

说明

当地址池里有静态配置的 DNS，NetBIOS，Domain-name 等信息时，以静态配置优先。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在接口地址池模式的接口有 GE 接口及其子接口、Ethernet 接口及其子接口、Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp select interface**，使能接口的 DHCP 服务功能。

步骤 4 执行命令 **dhcp server import all**，动态配置 DHCP 客户端使用的 DNS 配置信息和 NetBIOS 配置信息。

----结束

6.4.4 （可选）静态配置 DHCP 客户端的 DNS 服务

指定客户端在网络上使用的 DNS 域名和 DNS 服务器的 IP 地址。

背景信息

用户主机通过域名访问 Internet 时，需要将域名解析为 IP 地址，这是通过域名系统 DNS（Domain Name System）实现的。因此，为了使 DHCP 客户端成功接入 Internet，DHCP 服务器应在为客户端分配 IP 地址的同时指定 DNS 服务器地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在接口地址池模式的接口有 GE 接口及其子接口、Ethernet 接口及其子接口、Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp server domain-name** *domain-name*，配置分配给 DHCP 客户端的 DNS 域名。

步骤 4 执行命令 **dhcp server dns-list** *ip-address* &<1-8>，为 DHCP 客户端指定 DNS 服务器的 IP 地址。

为了对流量进行负载分担和提高网络的可靠性，可配置多个 DNS 服务器。每个地址池最多可以配置 8 个 DNS 服务器地址。

----结束

6.4.5 （可选）静态配置接口地址池的 NetBIOS 服务

对于使用 Windows Microsoft 操作系统的客户端，由 NetBIOS 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。

背景信息

DHCP 客户端使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种。

- b 类节点（b-node）：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。
- 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。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在接口地址池模式的接口有 GE 接口及其子接口、Ethernet 接口及其子接口、Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp server nbns-list** *ip-address* &<1-8>，为 DHCP 客户端指定 NetBIOS 服务器的 IP 地址。

每个地址池最多可以配置 8 个 NetBIOS 服务器地址。

步骤 4 执行命令 **dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }，为 DHCP 客户端指定 NetBIOS 节点类型。

缺省情况下，不指定客户端的 NetBIOS 节点类型。

----结束

6.4.6 （可选）配置接口地址池 DHCP 自定义选项

随着 DHCP 的不断发展，新的可选配置项会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将新选项添加到 DHCP 服务器的属性列表中。

背景信息

如果用户在 DHCP 服务器端配置了 Option，DHCP 客户端在申请 IP 地址的时候，会通过服务器端回应的 DHCP 报文获得 Option 字段中的配置信息。

说明

常用的功能，如客户端的 DNS 服务、NetBIOS 服务、租期等，可以通过 Option 命令进行配置，但是以相关命令的配置为优先。如果相关命令没有配置，而配置了对应的 Option 选项，那么会取用 Option 命令配置的值。

相关命令如下：

- DNS 服务：**dhcp server domain-name**、**dhcp server dns-list**
- NetBIOS 服务：**dhcp server nbns-list**、**dhcp server netbios-type**
- 租期：**dhcp server lease**

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在接口地址池模式的接口有 GE 接口及其子接口、Ethernet 接口及其子接口、Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp server option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* &<1-8> }，配置 DHCP 自定义选项。

dhcp server option 命令用于将指定选项内容通过服务器端回应的 DHCP 报文携带给客户端。使用该命令前，需要明确选项功能。DHCP 的知名选项，请参考 RFC2132。

----结束

6.4.7 （可选）配置防止 IP 地址重复分配功能

为防止 IP 地址重复分配导致地址冲突，AR1200 应用为 DHCP 服务器时为客户端分配地址前，需要先对该地址进行探测。

背景信息

地址探测是通过 **dhcp server ping** 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果在最长等待 Ping 响应的时间内没有得到应答，则继续发送 Ping 报文，直到发送 Ping 包数量达到最大值，如果仍然没有收到应答，则认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址是唯一的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server ping packet** *number*，配置 AR1200 发送 Ping 包的最大数量。

缺省情况下，AR1200 发送 Ping 包的最大数量为 0，即不进行 ping 操作。

步骤 3 执行命令 **dhcp server ping timeout** *milliseconds*，配置 AR1200 发送 Ping 包的最长等待响应时间。

缺省情况下，AR1200 等待 Ping 响应的最长时间为 500 毫秒。

----结束

6.4.8 检查配置结果

查看基于接口地址池的 DHCP 服务器的配置信息。

背景信息

已经完成基于接口地址池的 DHCP 服务器的所有配置。

操作步骤

- 执行命令 **display dhcp server statistics**，查看 DHCP 服务器的统计信息。
- 执行命令 **display ip pool interface** *interface-name* [*low-ip-address high-ip-address* | **all** | **expired** | **conflict** | **used**]，查看已经配置的接口地址池信息。

----结束

任务示例

执行命令 **display dhcp server statistics**，查看 DHCP 服务器的统计信息。

```
<Huawei> display dhcp server statistics

 DHCP Server Statistics:

 Client Request:            6
  Dhcp Discover:            1
  Dhcp Request:             4
  Dhcp Decline:             0
  Dhcp Release:             1
  Dhcp Inform:              0
 Server Reply:              4
  Dhcp Offer:               1
  Dhcp Ack:                 3
  Dhcp Nak:                 0
 Bad Messages:              0
```

执行命令 **display ip pool interface** *ip-pool-name*，查看“VLANIF10”的接口地址池信息。

```
<Huawei> display ip pool interface VLANIF10

Pool-name      : vlanif10
  Pool-No        : 2
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
```

```
NBNS-server0    : -
Netbios-type    : -
Position        : Interface        Status           : Unlocked
Gateway-0       : 192.168.10.2
Mask            : 255.255.255.0
VPN instance    : --
-------------------------------------------------------------------------------
        Start           End     Total  Used  Idle(Expired)  Conflict  Disable
-------------------------------------------------------------------------------
  192.168.10.1  192.168.10.254   253     0    253       0         0         0
-------------------------------------------------------------------------------
```

6.5 配置 DHCP 中继

DHCP 客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，获取 IP 地址等配置信息。

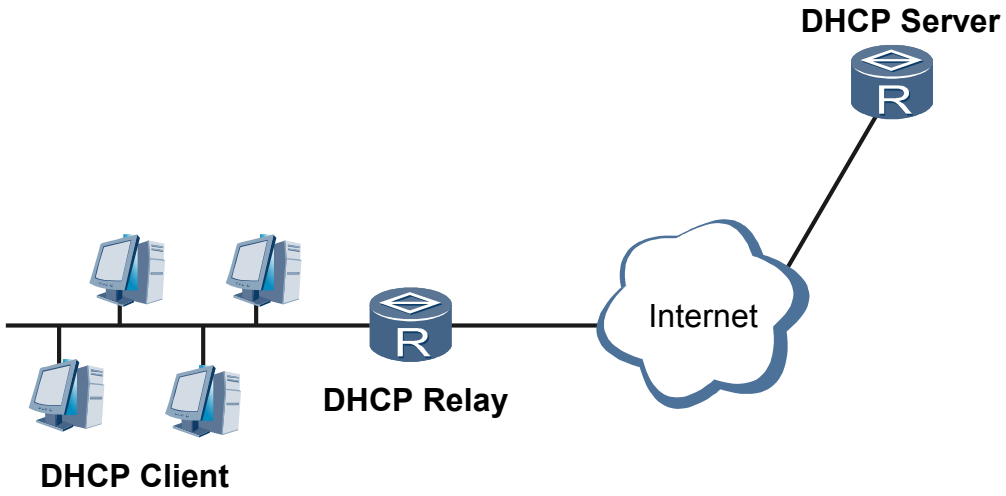
6.5.1 建立配置任务

在配置 DHCP 中继前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当 AR1200 作为 DHCP 中继时，DHCP 客户端可以通过作为 DHCP 中继的 AR1200 与其他网段的 DHCP 服务器通信，从 DHCP 服务器的全局地址池中获取 IP 地址等配置信息。这样，多个网段的 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。如图 6-4 所示。

图 6-4 DHCP 中继的应用场景



说明

AR1200 除了以太类型的接口，其他 WAN 侧接口不支持 DHCP 中继。

前置任务

在配置 DHCP 中继之前，需完成以下任务：

- 配置 DHCP 服务器
- 配置 AR1200 到 DHCP 服务器的路由

数据准备

在配置 DHCP 中继之前，需准备以下数据。

序号	数据
1	DHCP 服务器组的名称
2	DHCP 服务器组中的 DHCP 服务器 IP 地址
3	启动 DHCP 中继功能的接口编号及接口的 IP 地址

6.5.2 配置指定接口工作在 DHCP 中继模式

当客户端与 DHCP 服务器不在同一网段时，通过 DHCP 中继转发客户端到 DHCP 服务器的请求。

背景信息

说明

DHCP 服务器和 DHCP 客户端之间的 DHCP 报文中继次数不能超过 16 次，否则 DHCP 报文将被丢弃。

一个 Super-Vlan 下使能了 DHCP 中继功能后，则该 Super-Vlan 下不能使能 DHCP Snooping 功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在 DHCP 中继模式的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

说明

配置服务器上 IP 地址池的出口网关时，出口网关的 IP 地址和 DHCP 中继的 IP 地址必须完全一致。

步骤 5 执行命令 **dhcp select relay**，启动接口的 DHCP 中继功能。

----结束

后续处理

AR1200 应用为 DHCP 中继时，客户端发送的 DHCP 请求报文可以通过 DHCP 中继转发到 DHCP 服务器。使能接口的中继功能后，还需要在接口下配置 DHCP 服务器的 IP 地址。AR1200 支持以下两种方法配置 DHCP 服务器的 IP 地址：

- **6.5.3 配置 DHCP 中继转发的目的服务器组**并**6.5.4 配置 DHCP 中继接口绑定 DHCP 服务器组**。
- 直接在接口视图下执行命令 **dhcp relay server-ip** *ip-address*，配置 DHCP 中继所代理的 DHCP 服务器地址。

6.5.3 配置 DHCP 中继转发的目的服务器组

配置 DHCP 服务器组并向服务器组中添加服务器地址信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp server group** *group-name*，创建 DHCP 服务器组并进入 DHCP 服务器组视图。

全局最多可以配置 64 个 DHCP 服务器组。

步骤 3 执行命令 **dhcp-server** *ip-address* [*ip-address-index*]，向 DHCP 服务器组中添加 DHCP 服务器。

每个 DHCP 服务器组下最多可以配置 8 个 DHCP 服务器。不指定索引时，系统将自动分配一个空闲的索引。

----结束

6.5.4 配置 DHCP 中继接口绑定 DHCP 服务器组

使能接口的中继功能后，可以在接口上绑定 DHCP 服务器组，从而为 DHCP 客户端指定可以访问的 DHCP 服务器。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在 DHCP 中继模式的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp relay server-select** *group-name*，指定接口对应的 DHCP 服务器组。

----结束

6.5.5 （可选）配置 DHCP 中继请求 DHCP 服务器释放客户端的 IP 地址

在某些情况下，比如强制某用户下线等，可能需要通过 DHCP 中继向 DHCP 服务器发出请求，释放客户端申请到的 IP 地址。

背景信息

配置 DHCP 中继请求 DHCP 服务器释放客户端的 IP 地址功能后，DHCP 中继会主动向指定的 DHCP 服务器发送 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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 支持工作在 DHCP 中继模式的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口。

步骤 3 执行命令 **dhcp relay release** *client-ip-address mac-address server-ip-address*，向指定的 DHCP 服务器申请释放 DHCP 客户端已经获取到的 IP 地址。

----结束

6.5.6 检查配置结果

DHCP 中继配置成功后，通过命令查看 DHCP 中继的配置信息。

前提条件

已经完成 DHCP 中继功能的所有配置。

操作步骤

- 执行 **display dhcp relay** { **all** | **interface** *interface-type interface-number* }命令，查看接口配置的中继 DHCP 服务器组和服务器组对应的服务器。
- 执行 **display dhcp relay statistics** 命令，查看 DHCP 中继统计信息。
- 执行 **display dhcp server group** *group-name* 命令，查看 DHCP 服务器组的配置信息。

----结束

任务示例

执行 **display dhcp relay interface** *interface-type interface-number* 命令，查看指定接口 VLANIF100 配置的 DHCP 服务器组及其包含的 DHCP 服务器信息。

```
<Huawei> display dhcp relay interface vlanif 100

**  Vlanif100 DHCP Relay Configuration  **
 DHCP server group name : group1
   DHCP server IP [0] :10.10.10.10
   DHCP server IP [1] :10.10.10.11
   DHCP server IP [2] :10.10.10.12
```

执行 **display dhcp relay statistics** 命令，查看 DHCP 中继统计信息。

```
<Huawei> display dhcp relay statistics
The statistics of DHCP RELAY:
    DHCP packets received from clients    : 0
        DHCP DISCOVER packets received    : 0
        DHCP REQUEST packets received     : 0
        DHCP RELEASE packets received     : 0
        DHCP INFORM packets received      : 0
        DHCP DECLINE packets received     : 0
    DHCP packets sent to clients          : 0
        Unicast packets sent to clients   : 0
        Broadcast packets sent to clients : 0
    DHCP packets received from servers    : 0
        DHCP OFFER packets received       : 0
```

```
    DHCP ACK packets received        : 0
    DHCP NAK packets received        : 0
  DHCP packets sent to servers       : 0
  DHCP Bad packets received          : 0
```

执行 **display dhcp server group** *group-name* 命令，查看 DHCP 服务器组 group1 的配置信息。

```
<Huawei> display dhcp server group group1
  Group-name          : group1
  Group-type          : --
    (0)  Server-IP    : 100.10.10.1
    (1)  Server-IP    : 100.10.10.2
    Gateway           : --
    VPN instance      : --
    1 DHCP server group(s) in total
```

6.6 配置 DHCP/BOOTP 客户端

指定 AR1200 的三层接口作为 DHCP/BOOTP 客户端时，可以使用 DHCP/BOOTP 协议从 DHCP 服务器动态获得 IP 地址及其他配置信息。

6.6.1 建立配置任务

在配置 DHCP/BOOTP 客户端前了解此功能的应用环境、配置此功能的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

指定 AR1200 的三层接口作为 DHCP/BOOTP 客户端时，可以使用 DHCP/BOOTP 协议从 DHCP 服务器动态获得 IP 地址及其他配置信息，方便用户配置，也便于集中管理。

说明

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。

前置任务

在配置 DHCP/BOOTP 客户端之前，需完成以下任务：

- 配置 DHCP 服务器
- 配置 DHCP 中继（据实际需要，可选择配置）
- 配置 AR1200 到 DHCP 中继或 DHCP 服务器的路由

数据准备

在配置 DHCP/BOOTP 客户端之前，需准备以下数据。

序号	数据
1	DHCP 服务器组的名称
2	DHCP 服务器组中的 DHCP 服务器 IP 地址
3	启动 DHCP 中继功能的接口编号及接口的 IP 地址

6.6.2 （可选）配置 DHCP/BOOTP 客户端属性

通过配置 DHCP/BOOTP 客户端属性，有助于 DHCP/BOOTP 客户端和 DHCP 服务器之间的通信。

操作步骤

- 配置 DHCP 客户端属性。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 服务。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持工作在 DHCP 客户端的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VE 接口。
  4. 执行命令 **ip address dhcp client hostname** *hostname*，配置 DHCP 客户端的主机名。
  5. 执行命令 **ip address dhcp client option61** *client-name*，配置 DHCP 客户端的标识。
  6. 执行命令 **ip address dhcp client request-option** { **dhcp-file-name** | **dns-domain** | **ftp-user-ip** | **ftp-user-name** | **ftp-user-password** | **route** | **tftp-server-ip** | **tftp-server-name** }*，配置 DHCP 客户端的参数请求的选项列表。
- 配置 BOOTP 客户端属性。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 服务。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持工作在 BOOTP 客户端的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VE 接口。
  4. 执行命令 **ip address bootp client hostname** *hostname*，配置 BOOTP 客户端的主机名。

----结束

6.6.3 使能 DHCP/BOOTP 客户端

在接口上使能 DHCP/BOOTP 客户端功能，可以使接口通过 DHCP 服务器获取 IP 地址等配置信息。

操作步骤

- 使能 DHCP 客户端。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 服务。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持工作在 DHCP 客户端的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VE 接口。

4. 执行命令 **ip address dhcp-alloc**，使能 AR1200 的 DHCP 客户端功能。

- 使能 BOOTP 客户端。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 服务。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持工作在 BOOTP 客户端的接口有三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VE 接口。
  4. 执行命令 **ip address bootp-alloc**，使能 AR1200 的 BOOTP 客户端功能。

----结束

6.6.4 检查配置结果

DHCP/BOOTP 客户端配置成功后，通过命令查看 DHCP/BOOTP 客户端的配置信息。

前提条件

已经完成 DHCP/BOOTP 客户端的所有配置。

操作步骤

- 执行命令 **display current-configuration**，查看 DHCP/BOOTP 客户端的配置信息。

----结束

任务示例

执行 **display current-configuration** 命令，查看 DHCP 客户端的配置信息。

```
[Huawei] display current-configuration
...
#
interface GigabitEthernet1/0/0
 ip address dhcp-alloc
#
...
```

当接口成功分配到 IP 地址，执行 **display interface** 命令查看接口的 IP 地址信息。

```
[Huawei] display interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, Huawei Series, GigabitEthernet1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is allocated by DHCP, 22.22.22.222/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc11-000a
Last physical up time   : 2007-12-01 10:48:50
Last physical down time : 2007-12-01 10:52:56
Current system time: 2007-12-01 16:52:01
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi    : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 1928 bits/sec,Record time: 2007-11-30 14:57:22
Output peak rate 7384 bits/sec,Record time: 2007-11-30 10:13:15

Input:  833 packets, 72696 bytes
```

```
Unicast:                59,  Multicast:               757
Broadcast:              17,  Jumbo:                     0
Discard:                 0,  Total Error:               0
```

6.7 配置 DHCP 报文限速

用户可以在全局、VLAN 或接口下配置限制 DHCP 报文上送速率，如果在全局、VLAN 或接口下同时配置，有效的顺序为接口优先，VLAN 其次，最后为全局。

应用环境

如果网络中有攻击者不断地发送 DHCP 报文，会对 AR1200 的 DHCP 协议栈造成影响。

为了避免受到攻击者发送大量 DHCP 报文攻击，可以在 AR1200 上配置 DHCP 报文限速功能，检查 DHCP 报文，并限制报文的上送速率，在一定的时间内只允许规定数目的报文上送协议栈，多余的报文将被丢弃。

操作步骤

- 系统视图下配置 DHCP 报文限速
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 功能。
  3. 执行命令 **dhcp check dhcp-rate enable**，使能 DHCP 报文速率检查功能。

     缺省情况下，不使能 DHCP 报文速率检查功能。
  4. 执行命令 **dhcp check dhcp-rate** *rate*，配置 DHCP 报文上送到 DHCP 协议栈的检查速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps 以内。超过此速率限制的 DHCP 报文会被丢弃。
  5. （可选）执行命令 **dhcp check dhcp-rate alarm enable**，使能 DHCP 报文速率检查告警功能。

     缺省情况下，不使能 DHCP 报文速率检查告警功能。
  6. （可选）执行命令 **dhcp check dhcp-rate alarm threshold** *threshold*，配置 DHCP 报文的速率检查告警阈值。

     缺省情况下，DHCP 报文速率检查告警阈值为 100。当 DHCP 报文超过速率限制被丢弃的数目超过此阈值时，发出告警信息。
- VLAN 视图下配置 DHCP 报文限速
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp enable**，使能 DHCP 功能。
  3. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  4. 执行命令 **dhcp check dhcp-rate enable**，使能 DHCP 报文速率检查功能。

     缺省情况下，不使能 DHCP 报文速率检查功能。
  5. 执行命令 **dhcp check dhcp-rate** *rate*，配置 DHCP 报文上送到 DHCP 协议栈的检查速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps 以内。超过此速率限制的 DHCP 报文会被丢弃。

- 接口视图下配置限制 DHCP 报文上送速率
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dhcp check dhcp-rate enable**，使能 DHCP 报文速率检查功能。

     缺省情况下，接口视图下没有使能 DHCP 报文速率检查功能。
  4. 执行命令 **dhcp check dhcp-rate** *rate*，配置 DHCP 报文上送到 DHCP 协议栈的检查速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps 以内。超过此速率限制的 DHCP 报文会被丢弃。
  5. （可选）执行命令 **dhcp alarm dhcp-rate enable**，使能 DHCP 报文速率检查告警功能。

     缺省情况下，不使能 DHCP 报文速率检查告警功能。
  6. （可选）执行命令 **dhcp alarm dhcp-rate threshold** *threshold*，配置 DHCP 报文速率检查告警阈值。

     缺省情况下，DHCP 报文速率检查告警阈值为 100。当 DHCP 报文超过速率限制被丢弃的数目超过此阈值时，发出告警信息。

----结束

检查配置结果

执行 **display current-configuration | include dhcp** 命令，查看全局视图下 DHCP 报文限速配置信息。

```
<Huawei> display current-configuration | include dhcp
  It will take a long time if the content you search is too much or the string you
input is too long, you can press CTRL_C to break
 dhcp enable
 dhcp check dhcp-rate enable
 dhcp check dhcp-rate 90
 dhcp check dhcp-rate alarm enable
 dhcp check dhcp-rate alarm threshold 80
```

6.8 维护 DHCP

完成 DHCP 配置后，介绍如何清除 DHCP 统计信息以及如何监控 DHCP 运行状况。

6.8.1 清除 DHCP 的统计信息

在日常维护工作中，用户可以使用 reset 命令清除指定 DHCP Server 组的统计信息。

背景信息

注意

清除 DHCP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除 DHCP 服务器的统计信息后，请在用户视图下执行 **reset dhcp server statistics** 命令。
- 在确认需要清除 DHCP 中继的统计信息后，请在用户视图下执行 **reset dhcp relay statistics** 命令。

----结束

6.8.2 监控 DHCP 运行状况

在日常维护工作中，用户可以在任意视图下选择执行以下命令，了解 DHCP 的运行情况。

操作步骤

- 执行 **display dhcp relay** { **all** | **interface** *interface-type interface-number* }命令，查看在接口下配置的中继 DHCP 服务器组和服务器组对应的服务器。
- 执行 **display dhcp relay statistics** 命令，查看 DHCP Relay 统计信息。
- 执行 **display dhcp server group** [*group-name*]命令，查看 DHCP 服务器组成员的配置信息。

----结束

6.9 配置举例

DHCP 的配置举例包括组网需求、组网图、配置注意事项、配置思路和配置步骤。

6.9.1 同网段内配置基于全局地址池的 DHCP 服务器示例

DHCP 客户端和 DHCP 服务器在同一网段，配置基于全局地址池的 DHCP 服务器给客户端分配 IP 地址的过程。

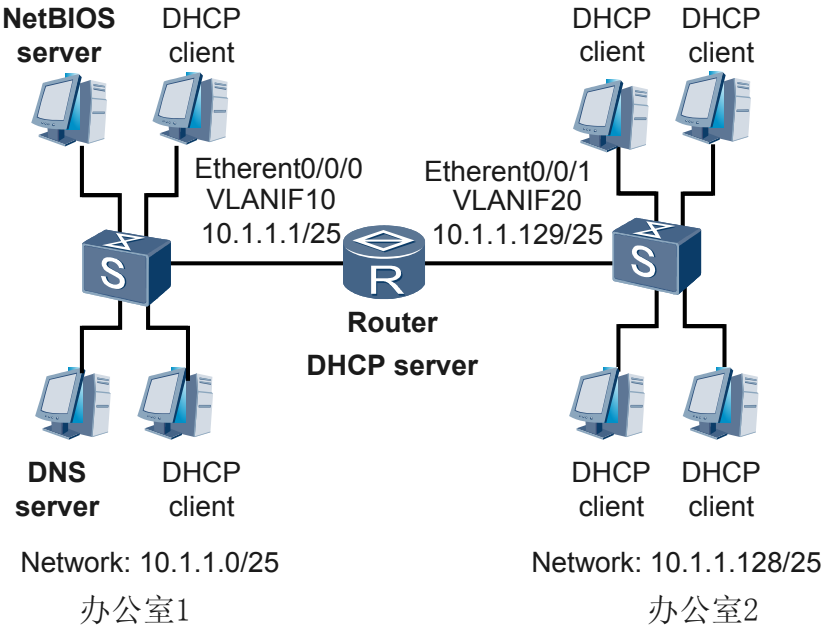
组网需求

如图 6-5 所示，某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 Router 作为 DHCP 服务器统一分配 IP 地址。

已知办公室 1 所属的网段为 10.1.1.0/25，主机都加入 VLAN10，办公室 1 的主机只使用 DNS 服务，不使用 NetBIOS 服务；办公室 2 所属的网段为 10.1.1.128/25，主机都加入 VLAN20，办公室 2 的主机使用 DNS 服务和 NetBIOS 服务。

企业需要在 RouterA 上配置全局地址池，并采取动态地址分配方式为两个办公室的主机分配 IP 地址。

图 6-5 配置基于全局地址池的 DHCP 服务器组网图



配置思路

DHCP 服务器的配置思路如下：

1. 在 Router 上使能 DHCP 功能。
2. 为办公室 1 和办公室 2 各创建一个全局地址池并配置地址池的相关属性，如地址池范围、出口网关、NetBIOS 地址、地址租用期限等。
3. 配置 VLANIF 接口下本地 DHCP 服务器的地址分配方式，即 DHCP 服务器从全局地址池中给客户端分配 IP 地址。

数据准备

要完成此配置举例，需要准备以下数据：

1. 为办公室 1 和办公室 2 创建的全局地址池名称：pool1 和 pool2。
2. pool1 和 pool2 的地址池范围：10.1.1.0/25 和 10.1.1.128/25。
3. 办公室 1 和办公室 2 的出口网关地址：10.1.1.1 和 10.1.1.129。
4. 办公室 1 的 IP 地址租期：10 天；办公室 2 的 IP 地址租期：2 天。
5. DNS 服务器地址：10.1.1.2。
6. NetBIOS 服务器地址：10.1.1.4。
7. VLANIF10 和 VLANIF20 的 IP 地址：10.1.1.1 和 10.1.1.129。

操作步骤

步骤 1 使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname Router
```

```
[Router] dhcp enable
```

步骤 2 创建地址池并配置相关属性。

配置 IP 地址池 1 的属性（地址池范围、DNS 地址、出口网关和地址池租期）。

```
[Router] ip pool pool1
[Router-ip-pool-pool1] network 10.1.1.0 mask 255.255.255.128
[Router-ip-pool-pool1] dns-list 10.1.1.2
[Router-ip-pool-pool1] gateway-list 10.1.1.1
[Router-ip-pool-pool1] excluded-ip-address 10.1.1.2
[Router-ip-pool-pool1] excluded-ip-address 10.1.1.4
[Router-ip-pool-pool1] lease day 10
[Router-ip-pool-pool1] quit
```

配置 IP 地址池 2 的属性（地址池范围、DNS 地址、出口网关、NetBOIS 地址和地址池租期）

```
[Router] ip pool pool2
[Router-ip-pool-pool2] network 10.1.1.128 mask 255.255.255.128
[Router-ip-pool-pool2] dns-list 10.1.1.2
[Router-ip-pool-pool2] nbns-list 10.1.1.4
[Router-ip-pool-pool2] gateway-list 10.1.1.129
[Router-ip-pool-pool2] lease day 2
[Router-ip-pool-pool2] quit
```

步骤 3 配置 VLANIF 接口下地址分配方式。

配置接口 Ethernet0/0/0 和 Ethernet0/0/1 分别加入相应的 VLAN。

```
[Router] vlan batch 10 20
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port hybrid pvid vlan 10
[Router-Ethernet0/0/0] port hybrid untagged vlan 10
[Router-Ethernet0/0/0] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port hybrid pvid vlan 20
[Router-Ethernet0/0/1] port hybrid untagged vlan 20
[Router-Ethernet0/0/1] quit
```

配置 VLANIF10 接口下的客户端从全局地址池中获取 IP 地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 255.255.255.128
[Router-Vlanif10] dhcp select global
[Router-Vlanif10] quit
```

配置 VLANIF20 接口下的客户端从全局地址池中获取 IP 地址。

```
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.1.129 255.255.255.128
[Router-Vlanif20] dhcp select global
[Router-Vlanif20] quit
```

步骤 4 验证配置结果。

在 Router 上使用 **display ip pool** 命令用来查看 IP 地址池配置情况。

```
[Router] display ip pool
  ------------------------------------------------------------------------
  Pool-name      : pool1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.128
  Vpn instance   : --

  ------------------------------------------------------------------------
  Pool-name      : pool2
```

```
  Pool-No         : 1
  Position        : Local          Status          : Unlocked
  Gateway-0       : 10.1.1.129
  Mask            : 255.255.255.128
  Vpn instance    : --


  IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
 vlan batch 10 20
#
dhcp enable
#
 ip pool pool1
 ip pool pool2
#
ip pool pool1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.128
 excluded-ip-address 10.1.1.2
 excluded-ip-address 10.1.1.4
 dns-list 10.1.1.2
 lease day 10 hour 0 minute 0
#
ip pool pool2
 gateway-list 10.1.1.254
 network 10.1.1.128 mask 255.255.255.128
 dns-list 10.1.1.2
 nbns-list 10.1.1.4
 lease day 2 hour 0 minute 0
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.128
 dhcp select global
#
interface Vlanif20
 ip address 10.1.1.129 255.255.255.128
 dhcp select global
#
interface Ethernet 0/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet 0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

6.9.2 同网段内配置基于接口地址池的 DHCP 服务器示例

配置基于接口地址池的 DHCP 服务器解决在同一网络内的客户端从服务器获取 IP 地址的过程。

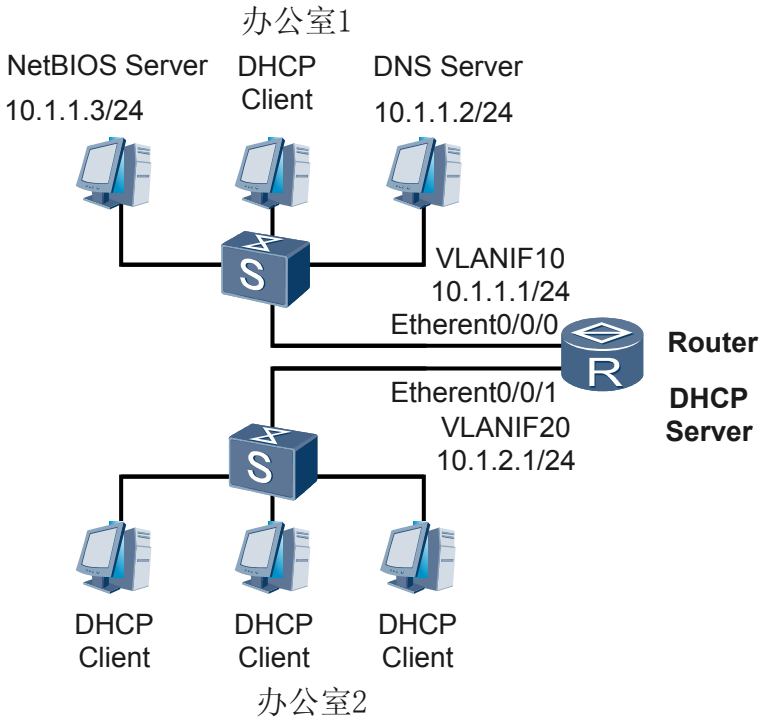
组网需求

如图 6-6 所示，某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 Router 作为 DHCP 服务器统一分配 IP 地址。

已知办公室 1 所属的网段为 10.1.1.0/24，主机都加入 VLAN10，办公室 1 使用 DNS 服务和 NetBIOS 服务；办公室 2 所属的网段为 10.1.2.0/24，主机都加入 VLAN20，办公室 2 不使用 DNS 服务和 NetBIOS 服务。

企业需要在 RouterA 上配置接口地址池，并采取动态地址分配方式为两个办公室的主机分配 IP 地址。

图 6-6 配置基于接口地址池的 DHCP 服务器组网图



配置思路

基于接口地址池的 DHCP 服务器的配置思路如下：

1. 在 Router 上使能 DHCP 功能。
2. 创建 VLANIF 接口，并配置 VLANIF 接口的 IP 地址，以确定接口地址池的 IP 地址网段。
3. 使能接口地址池，DHCP 服务器从接口地址池中给机房内的 PC 机分配 IP 地址。
4. 配置地址池相关属性，包括 DNS 服务器地址、NetBOIS 服务器地址、地址租期等，准备提供给客户端。

数据准备

要完成此配置举例，需要准备以下数据：

1. VLANIF10 和 VLANIF20 的 IP 地址：10.1.1.1 和 10.1.2.1。
2. 办公室 1 的 IP 地址租期：30 天；办公室 2 的 IP 地址租期：20 天。
3. DNS 服务器地址：10.1.1.2。
4. NetBIOS 服务器地址：10.1.1.3。

操作步骤

步骤 1 使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
```

步骤 2 配置 VLANIF 接口下地址分配方式。

配置接口 Ethernet0/0/0 和 Ethernet0/0/1 分别加入相应的 VLAN。

```
[Router] vlan batch 10 20
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port hybrid pvid vlan 10
[Router-Ethernet0/0/0] port hybrid untagged vlan 10
[Router-Ethernet0/0/0] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port hybrid pvid vlan 20
[Router-Ethernet0/0/1] port hybrid untagged vlan 20
[Router-Ethernet0/0/1] quit
```

配置 VLANIF10 接口下的客户端从接口地址池中获取 IP 地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 255.255.255.0
[Router-Vlanif10] dhcp select interface
[Router-Vlanif10] quit
```

配置 VLANIF20 接口下的客户端从接口地址池中获取 IP 地址。

```
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.2.1 255.255.255.0
[Router-Vlanif20] dhcp select interface
[Router-Vlanif20] quit
```

步骤 3 配置接口地址池的 DNS 服务和 NetBOIS 服务。

配置 VLANIF10 接口地址池下的 DNS 服务和 NetBOIS 服务。

```
[Router] interface vlanif 10
[Router-Vlanif10] dhcp server domain-name huawei.com
[Router-Vlanif10] dhcp server dns-list 10.1.1.2
[Router-Vlanif10] dhcp server nbns-list 10.1.1.3
[Router-Vlanif10] dhcp server excluded-ip-address 10.1.1.2
[Router-Vlanif10] dhcp server excluded-ip-address 10.1.1.3
[Router-Vlanif10] dhcp server netbios-type b-node
```

步骤 4 配置接口地址池中地址租用期限。

配置办公室 1 的 IP 地址租用期限为 30 天。

```
[Router] interface vlanif 10
[Router-Vlanif10] dhcp server lease day 30
[Router-Vlanif10] quit
```

配置办公室 2 的 IP 地址租用期限为 20 天。

```
[Router] interface vlanif 20
[Router-Vlanif20] dhcp server lease day 20
[Router-Vlanif20] quit
```

步骤 5 验证配置结果。

在 Router 上使用 **display ip pool interface** 命令用来查看接口地址池配置情况。

```
[Router] display ip pool interface vlanif10
  Pool-name      : vlanif10
  Pool-No        : 0
  Lease          : 30 Days 0 Hours 0 Minutes
  Domain-name    : huawei.com
  DNS-Server0    : 10.1.1.2
  NBNS-Server0   : 10.1.1.3
  Netbios-type   : b-node
  Position       : Interface       Status          : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
     10.1.1.1      10.1.1.254   253     0   251       0         0        2
 ------------------------------------------------------------------------------
[Router] display ip pool interface vlanif20
  Pool-name      : vlanif20
  Pool-No        : 1
  Lease          : 20 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-Server0    : -
  NBNS-Server0   : -
  Netbios-type   : -
  Position       : Interface       Status          : Unlocked
  Gateway-0      : 10.1.2.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
      10.1.2.1     10.1.2.254   253     0   253       0         0        0
 ------------------------------------------------------------------------------
```

----结束

任务示例

Router 的配置文件

```
#
 sysname Router
#
 vlan batch 10 to 20
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 10.1.1.2
 dhcp server netbios-type b-node
 dhcp server nbns-list 10.1.1.3
 dhcp server excluded-ip-address 10.1.1.2 10.1.1.3
 dhcp server lease day 30 hour 0 minute 0
 dhcp server domain-name huawei.com
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 dhcp select interface
 dhcp server lease day 20 hour 0 minute 0
#
interface Ethernet 0/0/0
 port hybrid pvid vlan 10
```

```
 port hybrid untagged vlan 10
#
interface Ethernet 0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

6.9.3 不同网段内配置 DHCP 服务器和 DHCP 中继示例

介绍 DHCP 服务器和客户端不在同一子网中时，DHCP 服务器和 DHCP 中继的配置过程。

组网需求

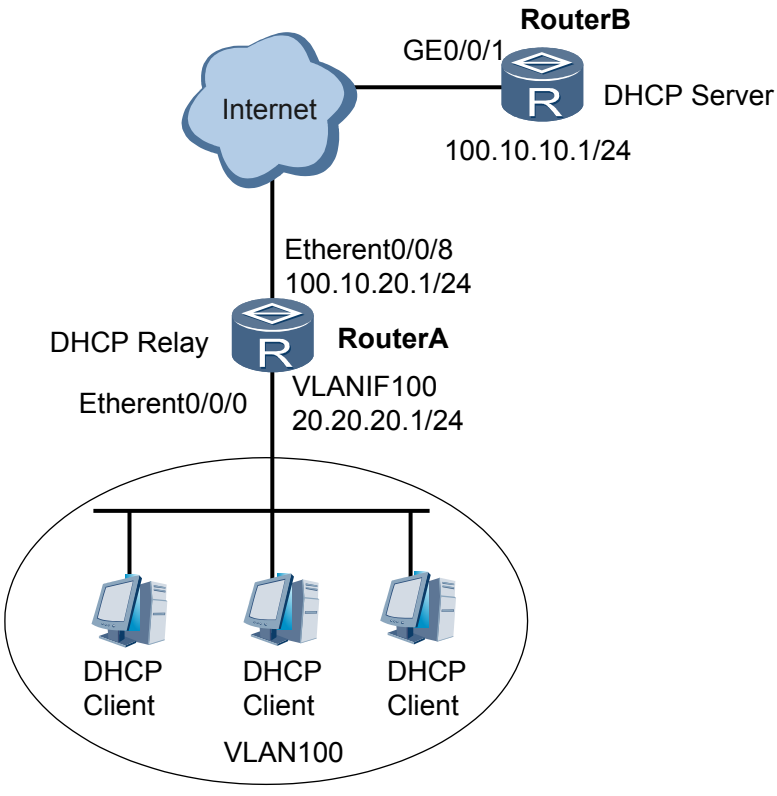
如图 6-7 所示，某公司拥有多个办公地点且位于不同的商务楼宇中，在同一楼宇内办公地点的主机在相同的 VLAN 内，要求在不同办公地点的主机由共同的 DHCP 服务器 RouterB 分配 IP 地址。

已知公司的办公地点 A 的主机所在的网段为 20.20.20.0/24，而 DHCP 服务器所在的网段为 100.10.10.0/24。需要通过带 DHCP 中继功能的 RouterA 转发 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。

其中 RouterA 上接口 Ethernet0/0/8 的公网地址为 100.10.20.1/24,对端运营商侧地址为 100.10.20.2/24。

RouterB 上接口 GE0/0/1 的公网地址为 100.10.10.1/24,对端运营商侧地址为 100.10.10.2/24。

图 6-7 配置 DHCP 中继组网图



办公地点 A

配置思路

DHCP 中继的配置思路如下：

1. 由于公司服务器和办公地点的主机处于不同网段，办公地点 A 的主机通过 RouterA 转发 DHCP 报文，需要在 RouterA 上配置 DHCP 中继功能。
2. 由于公司服务器和办公地点的主机处于不同网段，基于接口的地址池无法给不同网段的主机分配 IP 地址，需要在 RouterB 上配置一个 IP 地址范围为 20.20.20.0/24 的全局地址池。

数据准备

完成此配置举例，需要准备以下数据：

1. DHCP 服务器组的组名：dhcpgroup1。
2. DHCP 服务器的 IP 地址：100.10.10.1。
3. 办公地点 A 的主机所属 VLAN 的 ID：100。
4. 接口 VLANIF100 的 IP 地址：20.20.20.1。
5. 创建的全局地址池名称：pool1。
6. pool1 的地址池范围：20.20.20.0/24。
7. 办公地点 A 的主机的出口网关地址：20.20.20.1。

操作步骤

- 在 RouterA 上配置 DHCP 中继功能。
  1. 创建 DHCP 服务器组并为服务器组添加 DHCP 服务器。

     # 创建 DHCP 服务器组。

     ```
     <Huawei> system-view
     [Huawei] sysname RouterA
     [RouterA] dhcp server group dhcpgroup1
     ```

     # 为 DHCP 服务器组添加 DHCP 服务器。

     ```
     [RouterA-dhcp-server-group-dhcpgroup1] dhcp-server 100.10.10.1
     [RouterA-dhcp-server-group-dhcpgroup1] quit
     ```

  2. 在接口下使能 DHCP 中继功能。

     # 创建 VLAN 并将接口 Etherent0/0/0 加入到 VLAN 中。

     ```
     [RouterA] vlan batch 100
     [RouterA] interface ethernet 0/0/0
     [RouterA-Ethernet0/0/0] port hybrid pvid vlan 100
     [RouterA-Ethernet0/0/0] port hybrid untagged vlan 100
     [RouterA-Ethernet0/0/0] quit
     ```

     # 使能全局 DHCP 功能，并使能接口下 DHCP 中继功能。

     ```
     [RouterA] dhcp enable
     [RouterA] interface vlanif 100
     [RouterA-Vlanif100] dhcp select relay
     [RouterA-Vlanif100] quit
     ```

  3. 配置接口绑定 DHCP 服务器组。

     # 配置接口的 IP 地址。

```
[RouterA] interface vlanif 100
[RouterA-Vlanif100] ip address 20.20.20.1 24
```

配置接口绑定 DHCP 服务器组。

```
[RouterA-Vlanif100] dhcp relay server-select dhcpgroup1
[RouterA-Vlanif100] quit
```

- 在 RouterA 上配置缺省路由。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 100.10.20.2
```

- 在 RouterB 上配置基于全局地址池的 DHCP 服务器功能。

1. 使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dhcp enable
```

2. 配置接口 GE0/0/1 工作在全局地址池模式。

```
[RouterB] interface gigabitethernet 0/0/1
[RouterB-GigabitEthernet0/0/1] ip address 100.10.10.1 24
[RouterB-GigabitEthernet0/0/1] dhcp select global
[RouterB-GigabitEthernet0/0/1] quit
```

3. 创建地址池并配置相关属性。

```
[RouterB] ip pool pool1
[RouterB-ip-pool-pool1] network 20.20.20.0 mask 24
[RouterB-ip-pool-pool1] gateway-list 20.20.20.1
[RouterB-ip-pool-pool1] quit
```

- 在 RouterB 上配置缺省路由。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 100.10.10.2
```

- 验证配置结果。

在 RouterA 上使用 **display dhcp relay** 命令用来查看接口的 DHCP 中继配置情况。

```
[RouterA] display dhcp relay interface vlanif 100
 **  Vlanif100 DHCP Relay Configuration  **
  DHCP server group name : dhcpgroup1
   DHCP server IP [0] :100.10.10.1
```

在 RouterB 上使用 **display ip pool** 命令用来查看 IP 地址池配置情况。

```
[RouterB] display ip pool
  ------------------------------------------------------------------------
  Pool-name      : pool1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.0
  Vpn instance   : --


 IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan 100
#
```

```
 dhcp enable
#
dhcp server group dhcpgroup1
 dhcp-server 100.10.10.1
#
interface Vlanif100
 ip address 20.20.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select dhcpgroup1
#
interface Ethernet 0/0/0
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
 ip route-static 0.0.0.0 0.0.0.0 100.10.20.2
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
 vlan batch 20
#
 dhcp enable
#
ip pool pool1
 network 20.20.20.0 mask 255.255.255.0
 gateway-list 20.20.20.1
#
interface GigabitEthernet0/0/1
 ip address 100.10.10.1 255.255.255.0
 dhcp select global
#
 ip route-static 0.0.0.0 0.0.0.0 100.10.10.2
#
return
```

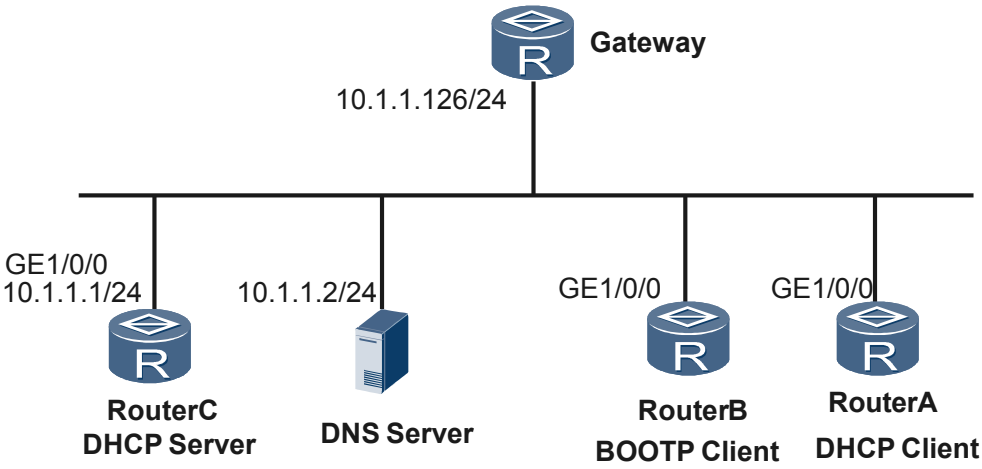
6.9.4 配置 DHCP 和 BOOTP 客户端示例

介绍 DHCP 和 BOOTP 客户端的配置过程。

组网需求

如图 6-8 所示，RouterA 作为 DHCP 客户端，从作为 DHCP 服务器的 RouterC 中获取动态绑定的 IP 地址、DNS 服务器、网关地址等信息；RouterB 作为 BOOTP 客户端，从作为 DHCP 服务器的 RouterC 中获取静态绑定的 IP 地址、DNS 服务器、网关地址等信息。

图 6-8 配置 DHCP 和 BOOTP 客户端组网图



配置思路

DHCP/BOOTP 客户端示例的配置思路如下：

1. 在 RouterA 上使能 DHCP 客户端功能。
2. 在 RouterB 上使能 BOOTP 客户端功能。
3. 在 RouterC 上创建 DHCP 服务器的全局地址池并配置相关属性。

数据准备

完成此配置举例，需要准备以下数据：

1. RouterB 接口 GE1/0/0 的 MAC 地址：a234-e211-a256。
2. RouterC 接口 GE1/0/0 的 IP 地址：10.1.1.1。
3. DHCP 客户端的出口网关地址：10.1.1.126。
4. DHCP 客户端的 DNS 服务器地址：10.1.1.2。

操作步骤

- RouterA 上配置 DHCP 客户端功能。

  # 使能 DHCP 服务。

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

  # 在接口 GE1/0/0 上使能 DHCP 客户端功能。

  ```
  [RouterA] interface gigabitethernet 1/0/0
  [RouterA-GigabitEthernet1/0/0] ip address dhcp-alloc
  ```

- RouterB 上配置 BOOTP 客户端功能。

  # 使能 DHCP 服务。

  ```
  <Huawei> system-view
  ```

```
[Huawei] sysname RouterB
[RouterB] dhcp enable
```

在接口 GE1/0/0 上使能 BOOTP 客户端功能。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address bootp-alloc
```

- 在 RouterC 上创建 DHCP 服务器的全局地址池并配置相关属性。

  1. 使能 DHCP 服务。

     ```
     <Huawei> system-view
     [Huawei] sysname RouterC
     [RouterC] dhcp enable
     ```

  2. 配置接口 GE1/0/0 工作在全局地址池模式。

     ```
     [RouterC] interface GigabitEthernet 1/0/0
     [RouterC-GigabitEthernet1/0/0] ip address 10.1.1.1 24
     [RouterC-GigabitEthernet1/0/0] dhcp select global
     [RouterC-GigabitEthernet1/0/0] quit
     ```

  3. 创建地址池并配置相关属性。

     ```
     [RouterC] ip pool pool1
     [RouterC-ip-pool-pool1] network 10.1.1.0 mask 24
     [RouterC-ip-pool-pool1] gateway-list 10.1.1.126
     [RouterC-ip-pool-pool1] static-bind ip-address 10.1.1.3 mac-address a234-e211-a256
     [RouterC-ip-pool-pool1] dns-list 10.1.1.2
     [RouterC-ip-pool-pool1] quit
     ```

- 验证配置结果。

  # 在 RouterA 上执行 **display current-configuration** 命令，查看 DHCP 客户端功能的配置情况。

  ```
  [RouterA] display current-configuration
  ...
  #
  interface GigabitEthernet1/0/0
   ip address dhcp-alloc
  #
  ...
  ```

  # 当接口成功分配到 IP 地址，在 RouterA 执行 **display interface** 命令查看接口的 IP 地址信息。

  ```
  [RouterA] display interface gigabitethernet 1/0/0
  GigabitEthernet1/0/0 current state : DOWN
  Line protocol current state : DOWN
  Description:HUAWEI, Huawei Series, GigabitEthernet1/0/0 Interface
  Route Port,The Maximum Transmit Unit is 1500
  Internet Address is allocated by DHCP, 10.1.1.11/24
  IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc11-000a
  Last physical up time   : 2007-12-01 10:48:50
  Last physical down time : 2007-12-01 10:52:56
  Current system time: 2007-12-01 16:52:01
  Port Mode: COMMON COPPER
  Speed :  100,  Loopback: NONE
  Duplex: FULL,  Negotiation: ENABLE
  Mdi   : AUTO
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
  Input peak rate 1928 bits/sec,Record time: 2007-11-30 14:57:22
  Output peak rate 7384 bits/sec,Record time: 2007-11-30 10:13:15

  Input:  833 packets, 72696 bytes
    Unicast:                59,  Multicast:                757
    Broadcast:              17,  Jumbo:                      0
    Discard:                 0,  Total Error:                0
  ```

在 RouterB 上执行 **display current-configuration** 命令，查看 BOOTP 客户端功能的配置情况。

```
[RouterB] display current-configuration
...
#
interface GigabitEthernet1/0/0
 ip address bootp-alloc
#
...
```

当接口成功分配到 IP 地址，在 RouterB 执行 **display interface** 命令查看接口的 IP 地址信息。

```
[RouterB] display interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, Huawei Series, GigabitEthernet1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is allocated by DHCP, 10.1.1.22/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc11-000a
Last physical up time   : 2007-12-01 10:48:50
Last physical down time : 2007-12-01 10:52:56
Current system time: 2007-12-01 16:52:01
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 1928 bits/sec,Record time: 2007-11-30 14:57:22
Output peak rate 7384 bits/sec,Record time: 2007-11-30 10:13:15

Input:  833 packets, 72696 bytes
  Unicast:                59,  Multicast:                757
  Broadcast:              17,  Jumbo:                      0
  Discard:                 0,  Total Error:                0
```

在 RouterC 上执行 **display ip pool** 命令，查看 IP 地址池配置情况。

```
[RouterC] display ip pool
  ------------------------------------------------------------------------
  Pool-name      : pool1
  Pool-No        : 0
  Position       : Local          Status          : Unlocked
  Gateway-0      : 10.1.1.126
  Mask           : 255.255.255.0
  Vpn instance   : --


 IP address Statistic
    Total       :250
    Used        :1          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

任务示例

RouterA 的配置文件

```
#
 sysname RouterA
#
 dhcp enable
#
interface GigabitEthernet 1/0/0
 ip address dhcp-alloc
```

```
#
return
```

RouterB 的配置文件

```
#
 sysname RouterB
#
 dhcp enable
#
interface GigabitEthernet 1/0/0
 ip address bootp-alloc
#
return
```

RouterC 的配置文件

```
#
 sysname RouterC
#
 dhcp enable
#
ip pool pool1
 network 10.1.1.0 mask 24
 gateway-list 10.1.1.126
 static-bind ip-address 10.1.1.3 mac-address a234-e211-a256
 dns-list 10.1.1.2
#
interface GigabitEthernet 1/0/0
 ip address 10.1.1.1 24
 dhcp select global
#
return
```

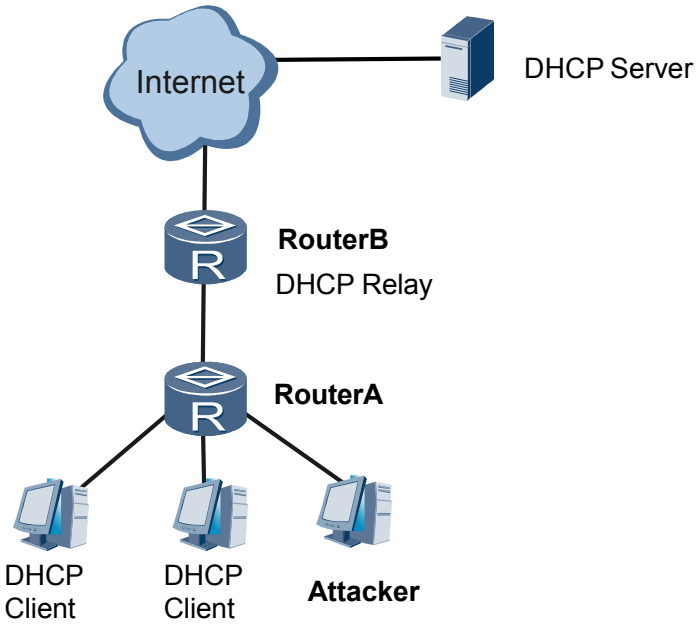
6.9.5 配置 DHCP 报文限速功能示例

介绍限制 DHCP 报文上送速率的基本配置过程，包括配置 DHCP 报文上送协议栈的速率和配置报文限速告警功能。

组网需求

如图 6-9 所示，企业某部门使用 RouterA 作为直接连接用户的设备，该部门主机作为 DHCP 客户端由 DHCP 服务器分配 IP 地址。如果存在攻击者发送大量 DHCP 报文攻击 RouterA，将会造成 RouterA 的 CPU 资源紧张，使合法用户的请求得不到及时处理。为了预防这种情况，网络管理员希望通过在 RouterA 上进行配置，对攻击者发送的 DHCP 报文进行有效防范，使合法用户的请求得到及时处理。

图 6-9 配置 DHCP 报文限速组网图



配置思路

DHCP 报文限速功能的配置思路如下：

- 在 RouterA 上全局配置 DHCP 报文限速功能，将攻击者发送 DHCP 报文的速率限制在正常范围内。

数据准备

1. DHCP 报文的上送速率:90。
2. 告警阈值：80。

操作步骤

步骤 1 使能 DHCP 服务。

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

步骤 2 配置 DHCP 报文上送速率限制。

使能 DHCP 报文速率检查功能。

```
[RouterA] dhcp check dhcp-rate enable
```

配置 DHCP 报文的上送速率。

```
[RouterA] dhcp check dhcp-rate 90
```

步骤 3 配置告警功能。

使能告警功能。

```
[RouterA] dhcp check dhcp-rate alarm enable
```

配置告警阈值。

```
[RouterA] dhcp check dhcp-rate alarm threshold 80
```

步骤 4 验证配置结果。

在 RouterA 上执行 **display current-configuration | include dhcp** 命令，可以看到全局视图下已经使能 DHCP 功能和 DHCP 报文限速功能。

```
[RouterB] display current-configuration | include dhcp
  It will take a long time if the content you search is too much or the string you
input is too long, you can press CTRL_C to break
 dhcp enable
 dhcp check dhcp-rate enable
 dhcp check dhcp-rate 90
 dhcp check dhcp-rate alarm enable
 dhcp check dhcp-rate alarm threshold 80
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
 dhcp enable
 dhcp check dhcp-rate enable
 dhcp check dhcp-rate 90
 dhcp check dhcp-rate alarm enable
 dhcp check dhcp-rate alarm threshold 80
#
 return
```

7 IP 性能配置

关于本章

通过 IP 性能配置，可以提高网络的性能。

7.1 IP 性能概述
在一些特定的网络环境里，需要调整 IP 的参数，以便网络性能达到最佳。这里主要介绍 AR1200 支持的 IP 性能参数。

7.2 AR1200 支持的 IP 性能
介绍 IP 性能特性在 AR1200 中的支持情况。

7.3 配置 IP 性能优化
通过设置 IP 报文的一系列参数以便达到最佳的网络性能。

7.4 配置 IP 报文转发的负载分担方式
通过配置非等价负载分担提高网络转发报文的性能。

7.5 配置 TCP 属性
通过对 TCP 报文的相关设置，可以提高网络的性能。

7.6 维护 IP 性能
维护 IP 性能包括清除 IP 性能统计信息、监控 IP 性能运行状况。

7.7 配置举例
介绍 IP 性能的配置举例。

7.1 IP 性能概述

在一些特定的网络环境里，需要调整 IP 的参数，以便网络性能达到最佳。这里主要介绍 AR1200 支持的 IP 性能参数。

7.2 AR1200 支持的 IP 性能

介绍 IP 性能特性在 AR1200 中的支持情况。

AR1200 支持的与 IP 性能相关的功能主要包括：

- ICMP 重定向报文的发送功能
- TCP FIN-Wait 定时器
- TCP SYN-Wait 定时器
- 面向连接 Socket 的收发缓冲区
- 逐流的等价负载分担功能
- 非等价负载分担功能
- TCP、IP、UDP、Socket Monitor 统计与显示功能
- IP 源地址校验功能
- 广播报文转发功能
- IP 源路由选项报文控制功能
- IP 报文强制分片功能
- PMTU 的老化时间
- 接口的 TCP 最大报文段长度

7.3 配置 IP 性能优化

通过设置 IP 报文的一系列参数以便达到最佳的网络性能。

7.3.1 建立配置任务

在配置 IP 性能优化前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

在一些特定的网络环境里，需要微调 IP 的参数，以便达到最佳的网络性能。优化 IP 性能涉及到设置一系列的参数。

前置任务

在配置 IP 性能优化之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up

- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up
- 配置接口的 IP 地址
- 配置 ACL

数据准备

在配置 IP 性能优化之前，需准备以下数据。

序号	数据
1	需要进行源地址校验的接口编号
2	需要转发广播报文的接口编号以及 ACL 编号
3	需要清除报文的 DF 标志的接口编号
4	需要配置 ICMP 重定向的接口编号

7.3.2 配置 IP 源地址校验

通过配置 IP 源地址校验，可以检验 IP 报文的源地址是否是合法地址，从而提高网络的安全性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip verify source-address**，使能接口对接收报文的 IP 源地址校验功能。

缺省情况下，接口不对接收的报文进行源地址合法性检查。

AR1200 仅支持对从接口转发到 CPU 的报文进行源地址合法性检查。

----结束

7.3.3 配置 IP 源路由选项报文控制功能

配置对 IP 源路由选项报文进行控制，可以防止通过 IP 源路由选项恶意探测网络结构，提高了网络的安全性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **discard srr**，对带 IP 源路由选项的报文不作处理。

----结束

7.3.4 配置广播报文转发

通过对接口转发广播报文进行控制，可以提高网络的性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip forward-broadcast** [**acl** *acl-number*]，配置接口转发广播报文。

缺省情况下，接口不转发广播报文。

----结束

7.3.5 配置出接口 IP 报文强制分片功能

通过该配置任务，可以设置在接口的出方向启用 IP 报文强制分片功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

说明

清除 DF 的功能对从接口发出的报文有效，因此需在发送报文的接口上进行配置。

步骤 3 执行命令 **clear ip df**，配置在接口的出方向启用 IP 报文强制分片功能。

缺省情况下，接口不对出方向的 IP 报文进行强制分片。

----结束

7.3.6 配置 ICMP 属性

通过控制 ICMP 报文发送功能，可以防止针对 ICMP 报文的攻击。

背景信息

缺省情况下，系统 ICMP 重定向报文发送功能是打开的。

注意

如果关闭系统 ICMP 重定向报文发送功能，则路由器在任何情况下都不会再发出 ICMP 重定向报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **icmp redirect send**，打开系统 ICMP 重定向报文发送功能。

----结束

7.3.7 配置本机下发协议报文的发送方式

配置本机下发协议报文的发送方式，可以对本机下发的 IP 单播协议报文进行管理和控制。

背景信息

缺省情况下，本机下发的 IP 单播协议报文优先级高于所有的 IP 报文转发流量，能够得到优先调度，且没有带宽限制，可以抢占完整个带宽。

用户可以根据自己的需求对本机产生的 IP 单播协议报文进行管理配置，修改其优先级，合理分配整个带宽。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip soft-forward enhance enable**，使能设备的 IP 增强转发功能。

步骤 3 执行命令 **set priority**，设置本机下发的 IP 单播协议报文的 DSCP 优先级。

----结束

7.3.8 配置高端 LAN 板路由转发模式

配置高端 LAN 板路由转发模式，可以去使能/使能高端 LAN 板路由转发功能。

背景信息

缺省情况下高端 LAN 板（8FE1GE 和 24GE）使能了路由转发功能，是支持 IP 报文路由转发的。但是在高端 LAN 板（8FE1GE 和 24GE）部署 ACL 操作复杂，且无法部署 ACl 流策略和 URPF 等业务，给用户的使用造成了局限性。去使能高端 LAN 板路由转发功能，可以将高端 LAN 板收到的报文引流至多核辅核 CPU，使报文在多核辅核 CPU 上进行转发，并允许部署 ACL 流策略和 URPF 等业务，以及简化 ACL 的部署。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **set workmode lan-card l3centralize**，去使能高端 LAN 板（8FE1GE 和 24GE）路由转发功能。

注意

- 执行该命令后，接口加入 Voice VLAN 的自动模式不生效，只能使用手动模式。
- 执行该命令后，源 MAC 或目的 MAC 为黑洞 MAC 的协议报文不会被丢弃。

----结束

7.3.9 检查配置结果

可以查看 IP 性能优化的配置信息。

操作步骤

- 执行 **display udp statistics** 命令，查看 UDP 流量统计信息。
- 执行 **display ip interface** [*interface-type interface-number*]命令或 **display ip interface brief** [*interface-type interface-number*]命令，查看 IP 层接口信息。
- 执行 **display ip statistics** 命令，查看 IP 流量统计信息。
- 执行 **display icmp statistics** 命令，查看 ICMP 流量统计信息。
- 执行 **display ip socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type*]命令，查看系统当前所有的套接口信息。

----结束

任务示例

执行命令 **display udp statistics**，可以查看 UDP 流量统计信息。

```
<Huawei> display udp statistics
Received packets:
Total: 13228
Total(64bit high-capacity counter): 13228
checksum error: 0
shorter than header: 0, data length larger than packet: 0
unicast(no socket on port): 0
broadcast/multicast(no socket on port): 954
not delivered, input socket full: 0
input packets missing pcb cache: 0

Sent packets:
Total: 11904
Total(64bit high-capacity counter): 11904
```

执行命令 **display ip interface**，可以查看 IP 层接口信息。

```
<Huawei> display ip interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:           0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
Internet protocol processing : disabled
Broadcast address : 0.0.0.0
TTL being 1 packet number:         0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
```

```
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
```

执行命令 **display ip statistics**，可以查看 IP 流量统计信息。

```
<Huawei> display ip statistics
 Input:     sum            31786      local            31786
            bad protocol       0      bad format           0
            bad checksum       0      bad options
            discard srr        0      TTL exceeded         0
  Output:   forwarding         0      local            41289
            dropped            0      no route             1
  Fragment: input              0      output               0
            dropped            0
            fragmented         0      couldn't fragment    0
  Reassembling:sum             0      timeouts             0
```

执行命令 **display icmp statistics**，可以查看 ICMP 流量统计信息。

```
<Huawei> display icmp statistics
  Input: bad formats            0      bad checksum                    0
         echo                   0      destination unreachable         0
         source quench          0      redirects                       0
         echo reply             0      parameter problem               0
         timestamp              0      information request             0
         mask requests          0      mask replies                    0
         time exceeded          0
         Mping request          0      Mping reply                     0
  Output:echo                   0      destination unreachable       168
         source quench          0      redirects                       0
         echo reply             0      parameter problem               0
         timestamp              0      information reply               0
         mask requests          0      mask replies                    0
         time exceeded          0
         Mping request          0      Mping reply                     0
```

7.4 配置 IP 报文转发的负载分担方式

通过配置非等价负载分担提高网络转发报文的性能。

7.4.1 建立配置任务

介绍配置 IP 报文转发的负载分担的应用环境、前置任务、数据准备和配置过程。

应用环境

AR1200 到达目标地址有多条等价路由，形成等价链路。这些等价链路带宽不同，同时存在高速链路和低速链路。

说明

如果路由表中有多条路由能够到达同一目的地址，且这些条目的优先级、跳数和开销都相等，那么 AR1200 就会把这些路由表条目看作是等价路由。

缺省情况下，AR1200 采用逐流的等价负载分担 ECMP（Equal Cost Multiple Path）方式，即流量在这些等价链路上平均分配，不会考虑链路带宽的差异。这容易造成低速链路流量阻塞以及高速链路的带宽不能得到有效利用的问题。

为了解决上述问题，用户可以在接口上配置非等价负载分担 UCMP（Unequal Cost Multiple Path）功能，这样等价链路可根据带宽不同而分担不同比例的流量，使负载分担更合理。

前置任务

在配置 IP 报文转发的负载分担之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up

数据准备

在配置 IP 报文转发的负载分担之前，需准备以下数据。

序号	数据
1	配置非等价负载分担 UCMP 功能的接口编号。
2	（可选）手动配置带宽的接口编号。
3	（可选）在接口上手动配置的带宽值。

7.4.2 配置非等价负载分担

配置非等价负载分担功能，等价链路可根据带宽不同而分担不同比例的流量，使负载分担更合理。

背景信息

AR1200 不考虑链路带宽的差异，在这些等价链路上平均分配流量，这种情况容易造成低速链路流量阻塞以及高速链路的带宽不能得到有效利用的问题。为了解决这个问题，用户可以在接口上配置非等价负载分担功能，这样等价链路可根据带宽不同而分担不同比例的流量，使负载分担更合理。

配置非等价负载分担功能时，存在以下两种情形，使用户需要在接口上手动配置带宽。

- 用户需要根据实际情况调节等价链路的带宽，使等价链路按照用户配置的带宽值参与流量的非等价负载分担。
- 如果等价链路的出接口是逻辑接口，在逻辑接口上使能 UCMP 功能前，必须先手动配置带宽。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

说明

当进入逻辑接口视图时，步骤 3 为必选。

步骤 3（可选）执行命令 **load-balance bandwidth** *bandwidth*，手动配置当前接口的带宽。

步骤 4 执行命令 **load-balance unequal-cost enable**，使能当前接口非等价负载分担功能。

缺省情况下，不使能当前接口非等价负载分担功能。

步骤 5 执行命令 **shutdown**，关闭当前接口。

步骤 6 执行命令 **undo shutdown**，开启当前接口。

步骤 7 执行命令 **quit**，退出物理接口视图。

如果需要在其他接口下配置非等价负载分担功能，请反复执行步骤 2 ～ 7。

说明

只有当所有等价链路的出接口都使能 UCMP 功能，且触发了 FIB 表项重新下发后，各等价链路才在 AR1200 上进行非等价负载分担。如果其中任一接口没有使能 UCMP 功能，即使触发了 FIB 表项重新下发，各等价链路仍进行等价负载分担。

----结束

7.4.3 检查配置结果

可以查看 IP 报文转发的负载分担的配置信息。

操作步骤

- 执行 **display fib** [*slot-id*]命令，查看接口板的 FIB 表。
- 执行 **display fib acl** *acl-number* [**verbose**]命令，过滤显示 FIB 信息。
- 执行 **display fib** [*slot-id*] *destination-address1* [*desinationt-mask1*] [**longer**] [**verbose**]命令，按照目的地址进行匹配显示 FIB 表项。
- 执行 **display fib** [*slot-id*] *destination-address1 destination-mask1 destination-address2 destination-mask2* [**verbose**]命令，查看目的地址在输入的 *destination-address1 destination-mask1* 到 *destination-address2 destination-mask2* 范围内的 FIB 表项。
- 执行 **display fib ip-prefix** *prefix-name* [**verbose**]命令，根据所输入的 *prefix-name* 名字把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 执行 **display fib interface** *interface-type interface-number* 命令，根据所输入的接口类型和编号把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 执行 **display fib next-hop** *ip-address* 命令，根据所输入的下一跳 IP 地址把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 执行 **display fib** [*slot-id*] **statistics** 命令查看 FIB 表项的总数目。

----结束

任务示例

执行命令 **display fib**，可以查看转发信息表摘要信息。

```
<Huawei> display fib
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
             S - Static Route,  D - Dynamic Route, B - Black Hole Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 4
Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.1/32       127.0.0.1       HU   t[49]         InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[49]         InLoop0         0x0
127.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
255.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
```

7.5 配置 TCP 属性

通过对 TCP 报文的相关设置，可以提高网络的性能。

7.5.1 建立配置任务

在配置 TCP 属性前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

TCP 协议是重要的网络协议之一，在一些特定的网络环境里需要调整 TCP 参数，以便提升网络的性能。

前置任务

在配置 TCP 属性之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路协层议状态为 Up
- 配置接口的网络层协议参数，使接口的路由协议状态为 Up

数据准备

在配置 TCP 属性之前，需准备以下数据。

序号	数据
1	SYN-Wait 定时器、FIN-Wait 定时器、Socket 收发缓冲区的大小

7.5.2 配置 TCP 定时器

通过设置两个 TCP 定时器，可以控制 TCP 的连接时间。

背景信息

TCP 的定时器有：

- SYN-Wait 定时器：当发送 SYN 报文时，TCP 启动 SYN-Wait 定时器，若 SYN-Wait 超时前未收到回应报文，则 TCP 连接将被终止。SYN-Wait 定时器的取值范围是 2 秒～ 600 秒，缺省值是 75 秒。
- FIN-Wait 定时器：当 TCP 的连接状态由 FIN_WAIT_1 变为 FIN_WAIT_2 时启动 FIN-Wait 定时器，若 FIN-Wait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。FIN-Wait 定时器的取值范围是 76 秒～ 3600 秒，缺省值是 675 秒。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp timer syn-timeout** *interval*，配置 TCP 连接建立 SYN-Wait 定时器时间。

步骤 3 执行命令 **tcp timer fin-timeout** *interval*，配置 TCP 的 FIN-WAIT（FIN_WAIT_2）定时器时间。

----结束

7.5.3 配置 PMTU 的老化时间

通过合理配置 PMTU 的老化时间，可以改善网络的传输效率，提高网络性能。

背景信息

当同一网络上的主机互相进行通信时，该网络的 MTU 对通信双方非常重要。但当主机间要通过很多网络才能通信时，对通信双方最重要的是通信路径中最小的 MTU，因为在通信路径上不同网络的链路层 MTU 不同。通信路径中最小的 MTU 被称为路径 MTU（PMTU）。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp timer pathmtu-age** *age-time*，配置 PMTU 的老化时间。

PMTU 老化时间的取值范围是 10 ～ 100 分钟，缺省值是 0 分钟，即不进行老化。

----结束

7.5.4 配置 TCP 的滑动窗口大小

通过配置 TCP 的滑动窗口的大小，可以配置 TCP 的 Socket 接收和发送缓冲区的大小，提高网络的性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **tcp window** *window-size*，配置 TCP 的 Socket 接收和发送缓冲区的大小。

面向连接 Socket 的接收和发送缓冲区的大小 *window-size* 的取值范围是 1k ～ 32k 字节，缺省值是 8k 字节。

----结束

7.5.5 配置接口的 TCP 最大报文段长度

通过配置接口的 TCP 最大报文段长度，使该接口接收和发送的 TCP 报文的大小都不能超过该长度，提高网络的性能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **tcp adjust-mss** *value*，配置接口的 TCP 最大报文段长度。

接口的 TCP 最大报文段长度的取值范围是 128 ～ 2048 字节。

----结束

7.5.6 检查配置结果

可以查看 TCP 的配置信息。

操作步骤

- 执行 **display tcp status** [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ipv4-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv4-address*] [**remote-port** *remote-port-number*]]命令，查看 TCP 连接状态。
- 执行 **display tcp statistics** 命令，查看 TCP 流量统计信息。

----结束

任务示例

执行命令 **display tcp status**，可以查看 TCP 连接状态信息。

```
<Huawei> display tcp status
TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
0b148a24  90 /1    0.0.0.0:23             0.0.0.0:0             14849 Listening
0ba8fb2c  90 /11   100.1.1.116:23         100.1.1.4:1334        0     Established
0ba91254  90 /12   100.1.1.116:23         100.1.1.4:2266        0     Established
```

执行命令 **display tcp statistics**，可以查看 TCP 流量统计信息。

```
<Huawei> display tcp statistics
Received packets:
     Total: 34574
     Total(64bit high-capacity counter): 34574
     packets in sequence: 2852 (3242 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 6 (6 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 3757 (126230 bytes)
     duplicate ACK packets: 29083, too much ACK packets: 0

Sent packets:
    Total: 35094
     Total(64bit high-capacity counter): 35094
     urgent packets: 0
     control packets: 0 (including 1 RST)
     window probe packets: 0, window update packets: 0

     data packets: 5364 (126736 bytes),    data packets retransmitted: 0 (0 byte
s)
     ACK-only packets: 657 (626 delayed)
```

```
Other information:
    Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    Keep alive timeout: 29072, keep alive probe: 29072,     Keep alive timeout,
so connections disconnected : 0
    Initiated connections: 0,     accepted connections: 16, established connecti
ons: 16
    Closed connections: 13 (    dropped: 10, initiated dropped: 0)
    Packets dropped with MD5 authentication: 0
    Packets permitted with MD5 authentication: 0
    Send Packets permitted with Keychain authentication: 0
    Receive Packets permitted with Keychain authentication: 0
    Receive Packets Dropped with Keychain authentication: 0
```

7.6 维护 IP 性能

维护 IP 性能包括清除 IP 性能统计信息、监控 IP 性能运行状况。

7.6.1 清除 IP 性能统计信息

介绍了使用 reset 命令清除 IP 性能统计信息。

背景信息

清除 IP/TCP/UDP 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除 IP 统计信息后，请在用户视图下执行 **reset ip statistics** [**interface** *interface-type interface-number*]命令。
- 在确认需要清除 Socket Monitor 中的信息后，请在用户视图下执行 **reset ip socket monitor** [**task-id** *task-id* **socket-id** *socket-id*]命令。
- 在确认需要清除 TCP 统计信息后，请在用户视图下执行 **reset tcp statistics** 命令。
- 在确认需要清除 UDP 统计信息后，请在用户视图下执行 **reset udp statistics** 命令。

----结束

7.6.2 监控 IP 性能运行状况

介绍了使用 display 命令监控 IP 性能运行状况。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 IP 性能的运行情况。

操作步骤

- 在任意视图下执行 **display tcp status** [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ipv4-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv4-address*] [**remote-port** *remote-port-number*]]命令，查看 TCP 连接状态。
- 在任意视图下执行 **display tcp statistics** 命令，查看 TCP 流量统计信息。
- 在任意视图下执行 **display udp statistics** 命令，查看 UDP 流量统计信息。
- 在任意视图下执行 **display ip interface** [*interface-type interface-number*]命令，查看 IP 层接口信息。
- 在任意视图下执行 **display ip statistics** 命令，查看 IP 流量统计信息。
- 在任意视图下执行 **display icmp statistics** 命令，查看 ICMP 流量统计信息。
- 在任意视图下执行 **display fib acl** *acl-number* [**verbose**]命令，过滤显示 FIB 信息。
- 在任意视图下执行 **display fib** [*slot-id*] *destination-address1* [*desinationt-mask1*] [**longer**] [**verbose**]命令，按照目的地址进行匹配显示 FIB 表项。
- 在任意视图下执行 **display fib** [*slot-id*] *destination-address1 destination-mask1 destination-address2 destination-mask2* [**verbose**]命令，查看目的地址在输入的 *destination-address1 destination-mask1* 到 *destination-address2 destination-mask2* 范围内的 FIB 表项。
- 在任意视图下执行 **display fib ip-prefix** *prefix-name* [**verbose**]命令，根据所输入的 *prefix-name* 名字，把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 在任意视图下执行 **display fib interface** *interface-type interface-number* 命令，根据所输入的接口类型和编号，把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 在任意视图下执行 **display fib next-hop** *ip-address* 命令，根据所输入的下一跳 IP 地址，把通过了该过滤规则的 FIB 表项按照一定格式显示出来。
- 在任意视图下执行 **display fib** [*slot-id*] **statistics** 命令，查看 FIB 表项的总数目。
- 在任意视图下执行 **display fib** [*slot-id*]命令，查看转发信息表的信息。
- 在任意视图下执行 **display ip socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **sock-type** *socket-type*]命令，查看系统当前所有的套接口信息。

----结束

7.7 配置举例

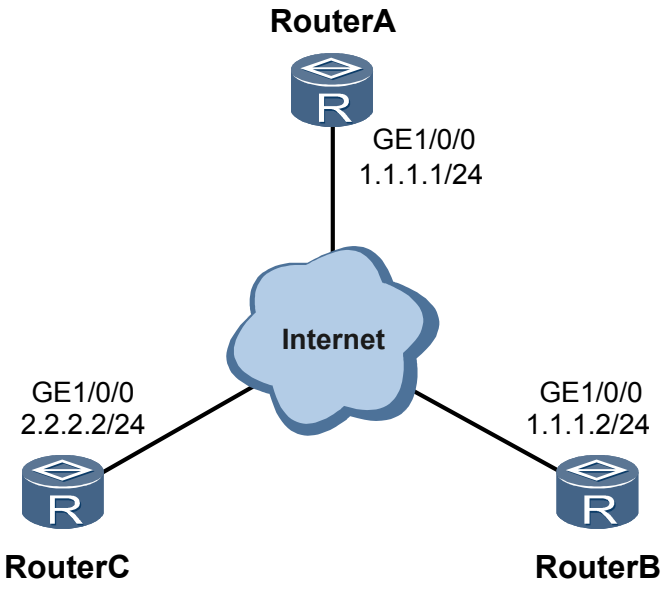
介绍 IP 性能的配置举例。

7.7.1 配置 ICMP 属性重定向报文示例

组网需求

如图 7-1 所示，为测试重定向报文的限制发送需要 RouterA、RouterB、RouterC 三台设备，并且这三台设备通过各自的三层接口相连。

图 7-1 配置 ICMP 属性重定向报文组网图



配置思路

配置限制发送 ICMP 重定向报文的思路如下：

1. 在各设备上的相应接口上配置 IP 地址。
2. 配置到达非直连设备的静态路由。
3. 在接口上使能限制发送 ICMP 重定向报文的功能。

数据准备

完成此配置，需准备如下的数据：

- 到达非直连设备的静态路由。
- 接口的 IP 地址。

操作步骤

步骤 1 配置接口的 IP 地址

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 1.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

配置 RouterC。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 2.2.2.2 24
[RouterC-GigabitEthernet1/0/0] quit
```

步骤 2 配置静态路由

配置 RouterA。

```
[RouterA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
```

配置 RouterB。

```
[RouterB] ip route-static 2.2.2.0 255.255.255.0 1.1.1.1
```

步骤 3 在 RouterB 的接口 GE1/0/0 上取消 ICMP 重定向报文的发送功能

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo icmp redirect send
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 4 验证配置结果

打开 RouterB 的 ICMP 报文调试开关。

```
<RouterB> debugging ip icmp
```

在 RouterA 上执行 Ping 命令，会看到 RouterB 不发送主机重定向报文，debugging 命令的回显信息里没有 ICMP 重定向报文信息。

```
[RouterA] ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=255 time=3 ms

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

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
```

```
interface GigabitEthernet1/0/0
 ip address 1.1.1.2 255.255.255.0
 undo icmp redirect send
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.1
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 2.2.2.2 255.255.255.0
#
return
```

7.7.2 配置非等价负载分担示例

本举例介绍基于接口的非等价负载分担的配置示例。

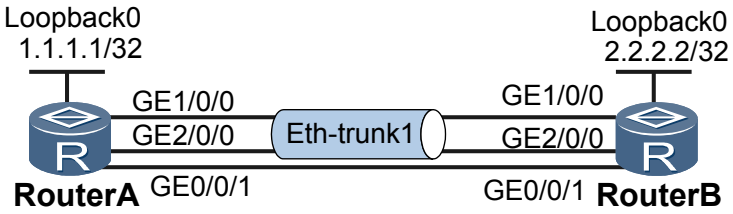
组网需求

如图 7-2 所示，RouterA 和 RouterB 之间通过两条链路连接。

- RouterA 上 Eth-Trunk1 接口的成员口是 GE1/0/0 和 GE2/0/0；RouterB 上 Eth-Trunk1 接口的成员口是 GE1/0/0 和 GE2/0/0。
- RouterA 的 GE0/0/1 到 RouterB 的 GE0/0/1 是一条实际物理链路。

因为 Eth-Trunk1 接口包含了两个 GE 接口，所以其带宽是单独一条物理链路的两倍。要求 RouterA 到 RouterB 的这两条链路上实现非等价负载分担。

图 7-2 配置非等价负载分担组网图



设备名称	接口名称	IP 地址
RouterA	Eth-Trunk1	30.1.1.1/24
	GE0/0/1	40.1.1.1/24
RouterB	Eth-Trunk1	30.1.1.2/24
	GE0/0/1	40.1.1.2/24

配置思路

非等价负载分担配置思路如下：

- 在 RouterA 和 RouterB 上配置静态路由。

- 在 RouterA 的接口上配置非等价负载分担功能，使 RouterA 和 RouterB 之间的流量基于不同的链路进行非等价负载分担。

数据准备

为完成此配置示例，需准备如下的数据：

- 接口类型和接口编号。
- 各接口的 IP 地址和子网掩码。
- Eth-Trunk 接口编号。
- Eth-Trunk 接口的带宽值。

操作步骤

步骤 1 配置各个接口的 IP 地址（略）。

步骤 2 配置静态路由。

在 RouterA 上配置静态路由。

```
[RouterA] ip route-static 2.2.2.2 32 30.1.1.2
[RouterA] ip route-static 2.2.2.2 32 40.1.1.2
```

在 RouterB 上配置静态路由。

```
[RouterB] ip route-static 1.1.1.1 32 30.1.1.1
[RouterB] ip route-static 1.1.1.1 32 40.1.1.1
```

步骤 3 检查路由配置。

在 RouterA 上查看静态路由信息。

```
<RouterA> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 3        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      2.1.1.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        2.2.2.0/24  Static  60   0           RD  30.1.1.1        Eth-
Trunk1
                    Static  60   0           RD  40.1.1.1        GigabitEthernet
0/0/1
        2.2.2.2/32  Static  60   0           RD  30.1.1.1        Eth-
Trunk1
                    Static  60   0           RD  40.1.1.1        GigabitEthernet
0/0/1
```

在 RouterA 上可以 ping 通 2.2.2.2。缺省情况下，RouterA 的出接口上实现了等价负载分担功能。

步骤 4 在 RouterA 的接口上使能非等价路由负载分担功能。

```
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] load-balance bandwidth 1500000
[RouterA-Eth-Trunk1] load-balance unequal-cost enable
[RouterA-Eth-Trunk1] quit
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] load-balance unequal-cost enable
[RouterA-GigabitEthernet0/0/1] quit
```

步骤 5 重启接口，使 RouterA 上的 UCMP 配置生效。

```
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] shutdown
[RouterA-Eth-Trunk1] undo shutdown
[RouterA-Eth-Trunk1] quit
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] shutdown
[RouterA-GigabitEthernet0/0/1] undo shutdown
[RouterA-GigabitEthernet0/0/1] quit
```

步骤 6 验证配置结果

在 RouterA 上仍可以 ping 通 20.1.1.1。

```
<RouterA> ping 2.2.2.2
PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=255 time=2 ms

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

在用户视图下执行命令 **display current-configuration**，可以看到接口 Eth-trunk1 和 GigabitEthernet0/0/1 已配置非等价负载分担功能。

```
<RouterA> display current-configuration
...
interface Eth-trunk1
 undo portswitch
 load-balance bandwidth 1500000
 load-balance unequal-cost enable
 ip address 30.1.1.1 255.255.255.0
interface GigabitEthernet0/0/1
 load-balance unequal-cost enable
 ip address 40.1.1.1 255.255.255.0
...
```

----结束

配置文件

RouterA 的配置文件。

```
#
 sysname RouterA
#
interface Eth-trunk1
 undo portswitch
 trunkport GigabitEthernet1/0/0
 trunkport GigabitEthernet2/0/0
 load-balance bandwidth 1500000
 load-balance unequal-cost enable
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 load-balance unequal-cost enable
 ip address 40.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
```

```
#
 ip route-static 2.2.2.2 32 30.1.1.2
 ip route-static 2.2.2.2 32 40.1.1.2
#
return
```

RouterB 的配置文件。

```
#
 sysname RouterB
#
interface Eth-trunk1
 undo portswitch
 trunkport GigabitEthernet1/0/0
 trunkport GigabitEthernet2/0/0
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 40.1.1.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255

#
 ip route-static 1.1.1.1 32 30.1.1.1
 ip route-static 1.1.1.1 32 40.1.1.1
#
return
```

8 IP 单播策略路由配置

关于本章

通过配置 IP 单播策略路由，可以用于提高网络的安全性能和负载分担。

8.1 IP 单播策略路由概述
策略路由可分为本地策略路由、接口策略路由和智能策略路由。

8.2 AR1200 支持的 IP 单播策略路由特性

8.3 配置本地策略路由
通过配置本地策略路由，可以控制特定的报文通过指定的出口进行转发。

8.4 配置接口策略路由
配置接口策略路由可以将到达接口的转发报文重定向到指定的下一跳地址。

8.5 配置智能策略路由
配置智能策略路由可以检测链路质量，根据业务对链路质量的要求进行链路切换。有效降低链路质量变坏对业务的影响，同时又提高了资源利用率。

8.6 配置举例
配置示例中包括组网需求、配置注意事项、配置思路等。

8.1 IP 单播策略路由概述

策略路由可分为本地策略路由、接口策略路由和智能策略路由。

与单纯根据 IP 报文的目的地址进行转发不同，策略路由是一种根据用户制定的策略进行路由转发的机制，通常用于安全、负载分担等目的。

8.2 AR1200 支持的 IP 单播策略路由特性

AR1200 策略路由不仅支持基于到达报文的源地址、报文长度等信息进行路由选择的本地策略路由和接口策略路由，还支持基于链路质量信息为业务数据流选择最佳链路的智能策略路由 SPR（Smart Policy Routing）。报文到达后，系统首先根据策略路由转发，若没有配置策略路由或配置了策略路由但找不到匹配的表项时，再根据路由表来转发报文。

三种策略路由的特点：

- 本地策略路由：仅对本设备发送的报文实现策略路由，比如本机下发的 ICMP、BGP 等协议报文。
- 接口策略路由：仅重定向目的地址为非本机的数据报文，此方式对主机上送报文不生效。多应用与负载分担和安全监控。
- SPR：周期性地校检链路的质量参数与业务的质量要求,如果链路质量满足不了业务需求，则 SPR 会把业务流切换到满足质量的链路。SPR 是一种业务性强、智能、高效的策略路由。

说明

SPR 功能需要使用 License 授权。缺省情况下，设备的 SPR 功能受限无法使用。如果需要使用 SPR 功能，请联系华为办事处申请并购买如下 License:

- AR1200 数据业务增值包

8.3 配置本地策略路由

通过配置本地策略路由，可以控制特定的报文通过指定的出口进行转发。

8.3.1 建立配置任务

介绍配置本地策略路由的应用环境、前置任务、数据准备和配置过程。

应用环境

内部网络通过一台路由器与外部网络连接，路由器有多个到外部网的出口，为了控制某些报文通过指定的出口，就需要配置接口的 IP 单播策略路由。

如果要对路由器本身产生的报文进行策略路由，就需要配置本地策略路由。

前置任务

在配置本地策略路由之前，需完成以下任务：

- 配置路由器与其他设备连接的接口

- 配置接口的链路层协议
- 配置用于匹配报文的 ACL
- 如果希望报文进入 VPN，则需要预先配置 VPN

数据准备

在本地策略路由之前，需准备以下数据。

序号	数据
1	策略路由名，策略的节点号以及对报文的默认动作是允许还是拒绝
2	报文的最小字节数和最大字节数
3	已配置的匹配报文的 ACL 编号
4	报文的新的优先级
5	指定策略中报文的默认的下一跳或出接口
6	指定策略中报文的下一跳或出接口编号
7	指定策略中报文所属 VPN 实例名

8.3.2 定义策略路由的匹配规则

通过该配置可以定义对何种报文进行策略路由。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **policy-based-route** *policy-name* { **deny** | **permit** } **node** *node-id*，创建策略或一个策略节点。

步骤 3 执行命令 **if-match packet-length** *min-length max-length* 或 **if-match acl** *acl-number*，设置 IP 报文匹配条件。

----结束

后续处理

在进行策略路由配置时，需要注意以下情况：

- 策略可以用来引入路由以及对 IP 报文转发进行策略路由。
- 策略路由的具体内容由 **if-match** 和 **apply** 子句来指定。
- 一条策略中可以包含多条 **if-match** 子句，即 **if-match acl** 、**if-match packet-length**，组合使用。
  - 重复创建 **if-match acl** *acl-number* 时，新的配置将覆盖旧的配置。
  - 重复创建 **if-match packet-length** *min-length max-length* 时，新的配置将覆盖旧的配置。

- **permit** 表示对满足匹配条件的报文进行策略路由，**deny** 表示对满足匹配条件的报文不进行策略路由。
- 由策略名称指定的策略可以包含若干策略节点，策略节点由顺序号 *node-id* 来指定，顺序号的值越小则优先级越高，相应策略优先执行。

8.3.3 定义策略路由的动作

包括设置报文出接口和下一跳。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **policy-based-route** *policy-name* { **deny** | **permit** } **node** *node-id*，创建策略或一个策略节点。

步骤 3 执行命令 **apply ip-precedence** *precedence*，设置报文优先级。

步骤 4 执行命令 **apply ip-address default next-hop** *ip-address1* [*ip-address2*]，指定报文的缺省下一跳。

说明

报文的缺省下一跳地址不能是本地 IP 地址。

步骤 5 执行命令 **apply default output-interface** *interface-type1 interface-number1* [*interface-type2 interface-number2*]，指定报文的缺省出接口。

说明

报文的缺省出接口不能为以太接口等广播型接口。

步骤 6 执行命令 **apply ip-address next-hop** *ip-address1* [*ip-address2*]，设置报文的下一跳。

说明

报文的下一跳地址不能是本地 IP 地址。

步骤 7 执行命令 **apply output-interface** *interface-type interface-number*，指定报文的出接口。

说明

报文的出接口不能为以太接口等广播型接口。

步骤 8 执行命令 **apply access-vpn vpn-instance** *vpn-instance-name* &<1-6>，设置访问 VPN 实例。

apply ip-precedence 命令用来设置报文的优先级。其中参数 *precedence* 的取值范围是 0～7。也可以使用优先级关键字代替优先级的值，它们之间的对应关系如表 8-1 所示。

表 8-1 参数 *precedence* 的优先级取值与关键字的对应关系

优先级取值	关键字
0	Routine
1	Priority
2	Immediate
3	Flash

优先级取值	关键字
4	Flash-override
5	Critical
6	Internet
7	Network

----结束

后续处理

定义策略路由的动作时请注意以下情况。

- 一条策略中可以包含多条 **apply** 子句，组合使用。
- 如果策略中只设置多个下一跳，那么报文转发只在多个下一跳之间负载分担。
- 如果策略中只设置多个出接口，那么报文转发只在多个出接口之间负载分担。
- 如果策略中同时设置了多个下一跳和多个出接口，那么报文转发仅在多个出接口之间负载分担。
- 如果先使用 **apply output-interface** 命令配置了两个出接口，然后又执行该命令配置了一个出接口，则后配置的出接口将覆盖前面配置的第一个出接口，而第二个出接口不会被覆盖。

8.3.4 应用策略路由

通过该配置使能策略路由。

操作步骤

- 启动本地策略路由
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ip local policy-based-route** *policy-name*，使能本地策略路由。

     本地策略路由只对本地产生的报文有效。只能配置一条本地策略。

----结束

8.3.5 检查配置结果

可以查看本地策略路由的配置信息。

前提条件

已经完成本地策略路由的所有配置。

操作步骤

- 使用 **display ip policy-based-route** 命令查看已使能的策略。
- 使用 **display ip policy-based-route setup local** 命令查看本地策略路由的设置情况。

- 使用 **display ip policy-based-route statistics local** 命令查看本地策略路由报文的统计信息。
- 使用 **display policy-based-route** [*policy-name*]命令查看已创建的策略内容。

----结束

任务示例

执行命令 **display ip policy-based-route** 命令查看已使能的策略。

```
<Huawei> display ip policy-based-route
 policy Name             interface
 aaa                     local
```

执行命令 **display ip policy-based-route setup local**，可以看到本地策略路由的配置情况。

```
<Huawei> display ip policy-based-route setup local
 policy-based-route aaa permit node 5
 if-match acl 2000
 apply output-interface Ethernet1/0/0
```

执行命令 **display ip policy-based-route statistics local**，可以看到本地策略路由的统计信息。

```
<Huawei> display ip policy-based-route statistics local
 Local policy based routing information:
 policy-based-route: aaa
   permit node 21
 Total denied: 0, forwarded: 0
```

8.4 配置接口策略路由

配置接口策略路由可以将到达接口的转发报文重定向到指定的下一跳地址。

8.4.1 建立配置任务

在配置接口策略路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在实际应用中，有时路由表转发满足不了业务需求，需要为特定的转发报文指定下一跳地址。接口策略路由可以将到达该接口的匹配重定向规则的转发报文指定特定的下一跳出口，不匹配重定向规则的转发报文则按路由表转发。

配置流分类可以为指定的数据流应用接口策略路由，AR1200 支持以下流分类：

- 传统流分类

  对于进入设备的各种流量，可以根据报文的 VLAN ID、802.1p 值、源 MAC、目的 MAC、二层封装的协议字段、FR DE、FR DLCI、ATM PVC、ACL 4000 ～ 4999 等二层信息，报文的 DSCP 优先级、IP 优先级、协议类型、ACL 2000 ～ 3999 等三层信息，报文的 RTP 端口号、TCP 报文的 TCP SYN 标志等四层信息以及报文的入接口等参数进行分类。
- 基于 SAC(Smart Application Control)的流分类

使用 DPI(Deep Packet Inspection)深度报文检测技术，对报文中第 4 ～ 7 层的内容和一些动态协议(如 HTTP、FTP、RTP)进行检测和识别，通过对报文进行深度的识别和分类，识别网络中运行的协议和应用。

将流分类和重定向绑定为流策略，在接口上应用该流策略，才能完成接口策略路由配置。

前置任务

在配置接口策略路由前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作
- 配置相关接口的 IP 地址和路由协议，保证路由互通
- 如果使用 ACL 作为接口策略路由的流分类规则，配置相应的 ACL
- （可选）SAC 特征库文件已经上传到设备，保存在设备的存储介质中

数据准备

在配置流分类之前，需要准备以下数据：

序号	数据
1	流分类名称及相关的参数
2	（可选）SAC 特征库文件的名称和存储路径

8.4.2 定义流分类

定义流分类，可以将符合一定规则的报文作为一类，对匹配同一流分类的报文进行相同的处理。

前提条件

如果要定义基于应用协议的匹配规则，必须使能 SAC 功能并加载特征库。

如果要定义基于 SAC 协议组的匹配规则，必须使能 SAC 功能、加载特征库且配置了 SAC 协议组。

说明

详细配置请参照《*Huawei AR1200 系列 企业路由器 配置指南-QoS*》中“（可选）配置 SAC 功能”部分。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

- **and** 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则以及其中一条 ACL 规则才能命中。

- **or** 表示流分类各规则之间是“逻辑或”，即报文只需匹配流分类中的一个规则即可命中。

缺省情况下，流分类中各规则之间的关系为“逻辑或”。

步骤 3 定义流分类中的匹配规则。能定义的匹配规则如下：

- 定义基于 VLAN 报文 802.1p 优先级的匹配规则，执行命令 **if-match 8021p** *8021p-value* &<1-8>。
- 定义基于 QinQ 报文内层 802.1p 优先级的匹配规则，执行命令 **if-match cvlan-8021p** *8021p-value* &<1-8>。
- 定义基于 ACL 的匹配规则，执行命令 **if-match acl** { *acl-number* | *acl-name* }。

  说明

  使用 ACL 作为流分类规则，必须先配置相应的 ACL 规则，AR1200 支持:

  - 基本 ACL，具体配置请参见配置基本 ACL。
  - 高级 ACL，具体配置请参见配置高级 ACL。
  - 二层 ACL，具体配置请参见配置二层 ACL。
- 定义基于所有报文的匹配规则，执行命令 **if-match any**。

  说明

  流分类中同时配置 **if-match any** 和其他规则时，报文流只匹配 **if-match any** 规则，而忽略其他规则。
- 定义基于目的 MAC 地址匹配规则，执行命令 **if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]。
- 定义基于源 MAC 地址的匹配规则，执行命令 **if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]。
- 定义基于 FR 报文中的 DLCI 信息的匹配规则，执行命令 **if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]。
- 定义基于 FR 报文中的 DE 标志位的匹配规则，执行命令 **if-match fr-de**。
- 定义基于 IP 报文 DSCP 优先级的匹配规则，执行命令 **if-match dscp** *dscp-value* &<1-8>。
- 定义基于 MPLS 报文 EXP 优先级的匹配规则，执行命令 **if-match mpls-exp** *exp-value* &<1-8>。
- 定义基于 IP 报文 IP 优先级的匹配规则，执行命令 **if-match ip-precedence** *ip-precedence-value* &<1-8>。

  说明

  不能在一个逻辑关系为“与”的流分类中同时配置 **if-match dscp** 和 **if-match ip-precedence**。
- 定义基于入接口的匹配规则，执行命令 **if-match inbound-interface** *interface-type interface-number*
- 定义基于以太网帧头中协议类型字段的匹配规则，执行命令 **if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }。
- 定义基于报文三层协议类型的匹配规则，执行命令 **if-match protocol ip**。
- 定义基于 ATM 报文中的 PVC 信息的匹配规则，执行命令 **if-match pvc** *vpi-number*/*vci-number*。
- 定义基于 RTP 端口号的匹配规则，执行命令 **if-match rtp start-port** *start-port-number* **end-port** *end-port-number*。

- 定义基于 TCP 报文 SYN Flag 的匹配规则，执行命令 **if-match tcp syn-flag** *syn-flag* &<1-6>。
- 定义基于 VLAN ID 匹配规则，执行命令 **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]。
- 定义基于 QinQ 报文内层 VLAN ID 的匹配规则，执行命令 **if-match cvlan-id** *start-cvlan-id* [**to** *end-cvlan-id*]。
- 定义基于应用协议的匹配规则，执行命令 **if-match app-protocol** *protocol-name* [**time-range** *time-name*]。

  说明

  当流分类中包含 **if-match app-protocol** 时，流分类各规则之间的关系必须是 **or**。
- 定义基于 SAC 协议组的匹配规则，执行命令 **if-match protocol-group** *protocol-group* [**time-range** *time-name*]。

  说明

  当流分类中包含 **if-match protocol-group** 时，流分类各规则之间的关系必须是 **or**。

----结束

8.4.3 配置重定向

通过配置重定向，将符合流分类规则的报文重定向到指定的下一跳地址。

背景信息

通过在流行为中配置重定向，可以实现策略路由功能。

包含重定向动作的流策略只能在接口的入方向上应用。

如果设备上没有指定的下一跳 IP 地址对应的 ARP 表项，设备会触发 ARP 学习，如果一直学习不到 ARP，则报文按原始路径转发，如果设备上有或学习到了此 ARP 表项，则按照指定的 IP 进行报文转发。

NQA（Network Quality Analysis）是网络故障诊断和定位的有效工具，配置 NQA 与重定向联动功能，可以在网络链路出现故障时，实现路由快速切换，保障用户数据流量正常转发：

- 当 NQA 检测到与目的 IP 可达时，按照指定的 IP 进行报文转发，即重定向生效。
- 当 NQA 检测到与目的 IP 不可达时，系统将按原来的转发路径转发报文，即重定向不生效。

说明

NQA 测试例必须为 ICMP 类型，具体配置请参见《*Huawei AR1200 系列企业路由器 配置指南-网络管理*》中“NQA 配置”部分的配置 ICMP 测试、配置测试例的通用参数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **redirect ip-nexthop** *ip-address* [**track nqa** *admin-name test-name*]，将符合流分类的报文重定向到下一跳，并配置重定向与 NQA 测试例联动。

----结束

8.4.4 配置流策略

配置完流分类和重定向后需要将流分类与重定向绑定，并应用在接口上,从而实现接口策略路由。

应用环境

流分类提供了有区别地进行服务的前提和基础，重定向用来定义针对某类报文所做的重定向动作，只有将流分类和重定向关联起来才能形成完整的接口策略路由。AR1200 支持在 LAN 接口、WAN 接口或子接口应用接口策略路由。

每个接口上能且只能应用一个策略路由，但同一个策略路由可以同时应用在不同的接口上。

前置任务

在配置策略路由之前，需要完成以下任务：

- 配置流分类
- 配置重定向

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic policy** *policy-name*，创建流策略并进入流策略视图。

步骤 3 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在策略中关联流分类和重定向动作。

步骤 4 执行命令 **quit**，退出流策略视图。

步骤 5 执行命令 **interface** *interface-type interface-number*[.*subinterface-number*]，进入接口视图或子接口视图。

步骤 6 执行命令 **traffic-policy** *policy-name* **inbound**，在接口或子接口的入方向应用策略路由。

----结束

8.4.5 检查配置结果

配置流行为后，可查看流行为信息。

前提条件

已经完成流行为的配置。

操作步骤

- 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。

----结束

8.5 配置智能策略路由

配置智能策略路由可以检测链路质量，根据业务对链路质量的要求进行链路切换。有效降低链路质量变坏对业务的影响，同时又提高了资源利用率。

8.5.1 建立配置任务

在配置智能策略路由前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

在实际应用中，由于网络应用的多样性和业务需求的多样性等原因，传统的基于逐跳的路由协议已不能满足需求。越来越多的用户的关注点从原来的只关注的网络的联通性转换到关注业务性能指标上，如业务的可获取性、质量等。

智能策略路由 SPR（Smart Policy Routing）周期性地检测链路的质量参数与业务的质量要求，如果链路质量不能满足业务需求，SPR 会将业务流切换至满足业务需求的链路上，保障业务的转发质量，提高链路的使用效率。

前置任务

在配置只能策略路由之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up
- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up
- 配置接口的 IP 地址，保证探测链路的路由可达。
- 配置区分业务流的 ACL
- 配置用于检测链路的 NQA 实例

数据准备

在配置智能策略路由之前，需准备以下数据。

序号	数据
1	业务流 ACL 编号
2	业务需求的质量指标，如：delay、jitter 和 loss 的阀值。
3	测试实例名和管理用户

8.5.2 配置 SPR 的路由参数

配置 SPR 的路由参数可以设定 SPR 的切换周期、探测链路和逃生链路等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-policy-route**，创建智能策略路由并进入智能策略路由视图。

步骤 3 执行命令 **period** *period-value*，配置 SPR 的切换周期。

步骤 4 （可选）执行命令 **route flapping suppression** *period-value*，配置振荡抑制周期。

说明

当链路质量不稳定时可能会引起 SPR 频繁切换链路，会严重影响业务数据转发效率。配置振荡抑制周期规定了链路切换的最短时间间隔，链路在下次切换前至少会等待振荡抑制周期配置的时间，避免链路频繁切换。

步骤 5 执行命令 **prober** *interface-type interface-number* **NQA** *admin-name test-name*，配置探测链路。

说明

探测链路所使用的 NQA 测试实例是 NQA 客户端，探测链路的对端是 NQA 服务器。

步骤 6 （可选）执行命令 **backup-interface** { *interface-type interface-number* } [*next-hop-address*]，配置逃生链路。

说明

当逃生链路为 PPP 链路时可以只指定逃生链路的出接口，如果是其他链路，比如以太网链路时，必须指定逃生链路的下一跳 IP 地址，否则无法转发报文。

步骤 7 执行命令 **link-group** *name*，创建链路组并进入链路组视图。

步骤 8 执行命令 **link-member** *interface-type interface-number*，将指定链路接口加入链路组。

说明

加入链路组的接口必须是已经被配置成探测链路的接口。

----结束

8.5.3 配置 SPR 与业务关联

配置 SPR 的业务参数，包括指定需要策略路由的业务流，配置业务的质量需求，绑定业务的探测链路等内容。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **smart-policy-route**，创建智能策略路由并进入智能策略路由视图。

步骤 3 执行命令 **service-map** *name*，创建 SPR 的业务模板并进入业务模板视图。

步骤 4 （可选）执行命令 **description** *information*，配置业务模板的描述信息。

步骤 5 执行命令 **match acl** *acl-number*，绑定业务流 ACL。

说明

SPR 通过匹配 ACL 规则区分不同的业务流。支持的 ACL 范围是编号 2000 ~ 3999 的基本 ACL 和高级 ACL。

步骤 6 根据实际业务需求，设置业务需求各质量参数的阀值，从如下操作步骤中选择一项或多项执行：

1. 执行命令 **set delay threshold** *threshold-value*，配置业务的时延阀值。
2. 执行命令 **set jitter threshold** *threshold-value*，配置业务的抖动时间阀值。
3. 执行命令 **set loss threshold** *threshold-value*，配置业务的丢包率阀值。
4. 执行命令 **set cmi threshold** *threshold-value*，配置业务的综合度量指标 CMI（Composite Measure Indicator）的阀值。

步骤 7 （可选）执行命令 **cmi-method** *cmi-method*，配置 CMI 计算方法。

步骤 8 执行命令 **set link-group** *name*，配置业务的主链路组。

步骤 9 （可选）执行命令 **set link-group** *name* **backup**，配置业务的备份链路组。

----结束

8.5.4 检查配置结果

配置 SPR 功能后，可查看 SPR 的各类配置信息。

前提条件

已经完成 SPR 功能的配置。

操作步骤

- 执行命令 **display smart-policy-route**，查看 SPR 的路由配置信息。
- 执行命令 **display smart-policy-route service-map** *name*，查看业务模板的配置信息。
- 执行命令 **display smart-policy-route link-state** [*interface-type interface-number*]，查看查看探测链路的链路状态信息。

----结束

8.6 配置举例

配置示例中包括组网需求、配置注意事项、配置思路等。

8.6.1 配置 IP 单播策略路由示例

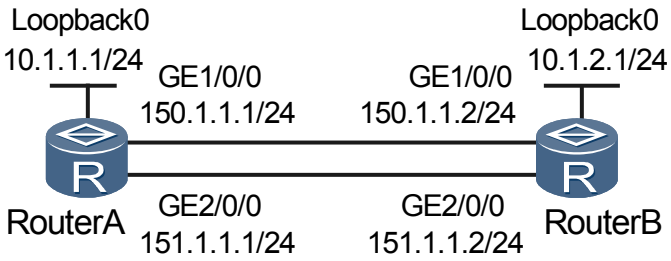
介绍 IP 单播策略路由示例的配置过程。

组网需求

如图 8-1 所示，在 RouterA 上应用 IP 单播策略路由：

- 对大小为 64 ～ 1400 字节的报文设置 150.1.1.2 作为下一跳地址。
- 对大小为 1401 ～ 1500 字节的报文设置 151.1.1.2 作为下一跳地址。
- 所有其它长度的报文都按基于目的地址的方法进行路由。

图 8-1 配置基于报文长度的策略路由组网图



配置思路

IP 单播策略路由配置思路如下：

- 首先指定各接口的 IP 地址。
- 配置静态路由。
- 配置策略路由，包括匹配规则和动作。

数据准备

为完成此配置示例，需准备如下的数据：

- 各接口的 IP 地址和子网掩码。
- 策略路由的匹配规则中使用的报文长度，动作中使用的下一跳。

操作步骤

步骤 1 配置各接口的 IP 地址。

配置 RouterA 的各接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 150.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 151.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterB 的各接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 150.1.1.2 255.255.255.0
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 151.1.1.2 255.255.255.0
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 2 配置静态路由。

在 RouterA 上配置静态路由。

```
[RouterA] ip route-static 10.1.2.0 24 150.1.1.2
```

```
[RouterA] ip route-static 10.1.2.0 24 151.1.1.2
```

在 RouterB 上配置静态路由。

```
[RouterB] ip route-static 10.1.1.0 24 150.1.1.1
[RouterB] ip route-static 10.1.1.0 24 151.1.1.1
```

步骤 3 配置策略路由。

配置名称为 lab1 的策略路由。

```
[RouterA] policy-based-route lab1 permit node 10
[RouterA-policy-based-route-lab1-10] if-match packet-length 64 1400
[RouterA-policy-based-route-lab1-10] apply ip-address next-hop 150.1.1.2
[RouterA-policy-based-route-lab1-10] quit
[RouterA] policy-based-route lab1 permit node 20
[RouterA-policy-based-route-lab1-20] if-match packet-length 1401 1500
[RouterA-policy-based-route-lab1-20] apply ip-address next-hop 151.1.1.2
[RouterA-policy-based-route-lab1-20] quit
```

使能本地策略路由。

```
[RouterA] ip local policy-based-route lab1
```

步骤 4 验证配置结果

在 RouterA 用 **debugging ip policy-based-route** 命令监视策略路由。

```
<RouterA> debugging ip policy-based-route
<RouterA> terminal debugging
<RouterA> terminal monitor
```

在 RouterA 上 Ping RouterB 的 Loopback0，并将报文数据字段长度设为 80 字节。

```
<RouterA> ping -s 80 10.1.2.1
 PING 100.1.2.1: 80  data bytes, press CTRL_C to break
Mar  9 2011 15:00:35.40.2 RouterA PBR/7/POLICY-ROUTING:IP Policy routing success
 : next-hop : 150.1.1.2
    Reply from 100.1.2.1: bytes=80 Sequence=1 ttl=254 time=1 ms
    Reply from 100.1.2.1: bytes=80 Sequence=2 ttl=254 time=1 ms
    Reply from 100.1.2.1: bytes=80 Sequence=3 ttl=254 time=1 ms
    Reply from 100.1.2.1: bytes=80 Sequence=4 ttl=254 time=1 ms
    Reply from 100.1.2.1: bytes=80 Sequence=5 ttl=254 time=1 ms

  --- 100.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

RouterA 上显示的策略路由信息如下：

```
<RouterA>
Mar  9 2011 15:00:37.50.2 RouterA PBR/7/POLICY-ROUTING:IP Policy routing success
 : next-hop : 150.1.1.2
Mar  9 2011 15:00:37.50.3 RouterA PBR/7/POLICY-ROUTING:IP Policy routing success
 : next-hop : 150.1.1.2
Mar  9 2011 15:00:37.50.4 RouterA PBR/7/POLICY-ROUTING:IP Policy routing success
 : next-hop : 150.1.1.2
Mar  9 2011 15:00:37.50.5 RouterA PBR/7/POLICY-ROUTING:IP Policy routing success
 : next-hop : 150.1.1.2
```

以上策略路由信息显示，RouterA 在接收到报文后，根据策略路由确定的下一跳为 150.1.1.2，也就是说将报文从端口 GigabitEthernet1/0/0 转发出去。

在 RouterA 上 PingRouterB 的 Loopback0，并将报文数据字段长度设为 1401 字节。

```
<RouterA> ping -s 1401 10.1.2.1
```

```
  PING 100.1.2.1: 1401  data bytes, press CTRL_C to break
Mar  9 2011 15:41:26.350.2 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
Mar  9 2011 15:41:26.350.3 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
    Reply from 100.1.2.1: bytes=1401 Sequence=1 ttl=254 time=2 ms
Mar  9 2011 15:41:26.850.1 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
    Reply from 100.1.2.1: bytes=1401 Sequence=2 ttl=254 time=2 ms
Mar  9 2011 15:41:27.340.1 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
    Reply from 100.1.2.1: bytes=1401 Sequence=3 ttl=254 time=2 ms
Mar  9 2011 15:41:27.840.1 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
    Reply from 100.1.2.1: bytes=1401 Sequence=4 ttl=254 time=2 ms
Mar  9 2011 15:41:28.340.1 RouterA PBR/7/POLICY-ROUTING:IP Policy routing succes
s : next-hop : 151.1.1.2
    Reply from 100.1.2.1: bytes=1401 Sequence=5 ttl=254 time=2 ms

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

以上策略路由信息显示，RouterA 在接收到报文后，根据策略路由确定的下一跳为 151.1.1.2，也就是说将报文从端口 GigabitEthernet2/0/0 转发出去。

----结束

配置文件

RouterA 的配置文件。

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 150.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 151.1.1.1 255.255.255.0
#
 ip route-static 10.1.2.0 255.255.255.0 150.1.1.2
 ip route-static 10.1.2.0 255.255.255.0 151.1.1.2
#
 policy-based-route lab1 permit node 10
  if-match packet-length 64 1400
  apply ip-address next-hop 150.1.1.2
 policy-based-route lab1 permit node 20
  if-match packet-length 1401 1500
  apply ip-address next-hop 151.1.1.2
#
 ip local policy-based-route lab1
```

RouterB 的配置文件。

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 150.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 151.1.1.2 255.255.255.0
```

```
#
 ip route-static 10.1.1.0 255.255.255.0 150.1.1.1
 ip route-static 10.1.1.0 255.255.255.0 151.1.1.1
```

8.6.2 配置 NQA for 重定向示例

通过配置重定向与 NQA 的联动，实现在各链路无故障时不同部门的报文通过不同的链路访问 WAN 侧网络，当 NQA 测试例检测到链路出现故障时，实现快速切换，取消重定向按照正常转发路径转发报文，保障用户数据流量正常转发。

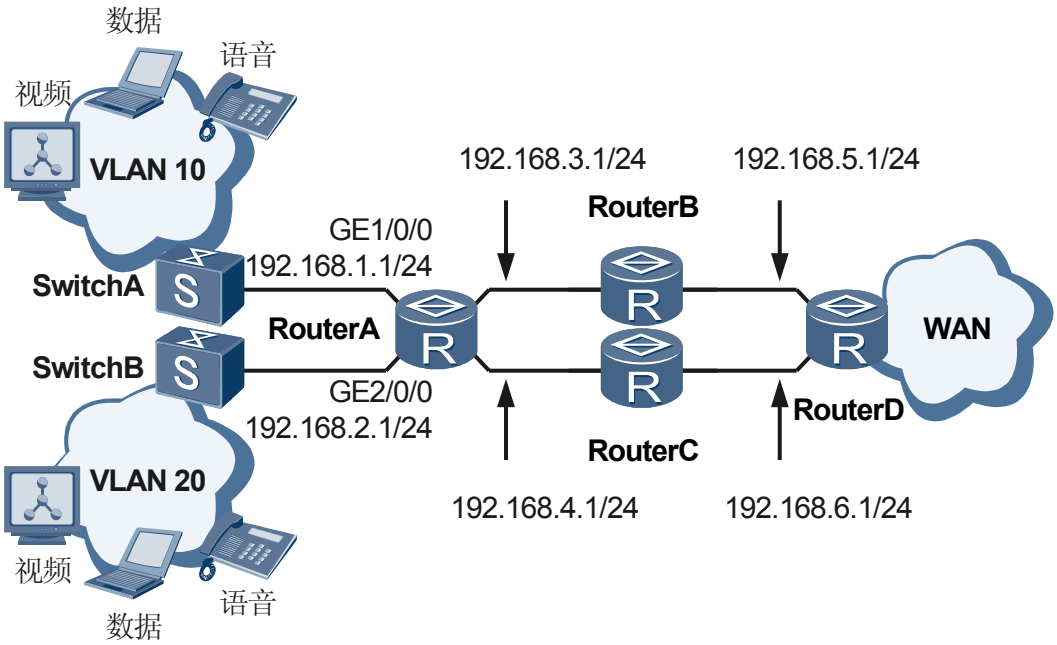
组网需求

如图 8-2 所示，VLAN 10 和 VLAN 20 是企业内部的两个部门，分别通过交换机连接到 RouterA 的 GE1/0/0 和 GE2/0/0。

RouterA 可以通过 RouterA→RouterB→RouterD 链接到 WAN 侧，也可以通过 RouterA→RouterC→RouterD 链接到 WAN 侧，现要求：

- 在两条链路都正常时，各部门的报文通过不同的链路连接到 WAN 侧；
- 当一条链路发生故障时，两个部门的报文都走无故障的链路，避免长时间的业务中断；
- 当故障解决后，恢复报文从不同链路连接到 WAN 侧。

图 8-2 配置 NQA for 重定向的组网图



配置思路

采用如下的思路配置 NQA for 重定向：

1. 配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。

2. 配置 NQA 测试例，检测链路 RouterA→RouterB→RouterD 和 RouterA→RouterC→RouterD 是否正常。
3. 配置流分类，匹配规则为匹配报文的入接口。
4. 配置流行为，即配置 NQA 与重定向联动：当 NQA 测试例检测到链路 RouterA→RouterB→RouterD 正常时，将满足规则的报文重定向到 192.168.3.1/24，当 NQA 测试例检测到链路 RouterA→RouterC→RouterD 正常时，将满足规则的报文重定向到 192.168.4.1/24。
5. 配置流策略，绑定上述流分类和流行为，并应用到相应的接口。

数据准备

为完成此配置示例，需准备如下的数据：

- 各接口的 IP 地址。
- NQA 测试例参数：

NQA 测试例类型	管理者	测试例名	目的地址
ICMP	admin	vlan10	192.168.5.1/24
ICMP	admin	vlan20	192.168.6.1/24

- 流分类参数：

名称	匹配规则
vlan10	匹配入接口为 GE1/0/0 的报文。
vlan20	匹配入接口为 GE2/0/0 的报文。

- 流行为参数：

名称	重定向下一跳 IP	与重定向联动的 NQA 测试例
vlan10	192.168.3.1/24	admin vlan10
vlan20	192.168.4.1/24	admin vlan20

- 流策略的名称为 vlan10 和 vlan20，应用于接口 GE1/0/0 和 GE2/0/0 的入方向。

操作步骤

步骤 1 配置各接口

配置 RouterA 接口 GE1/0/0 的 IP 地址为 192.168.1.1/24。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

说明

其他接口的 IP 地址配置方法相同，此处省略。

请配置 SwitchA 和 SwitchB，使其能与 RouterA 互通。

步骤 2 在 RouterA 上配置 NQA 测试例

```
[RouterA] nqa test-instance admin vlan10
[RouterA-nqa-admin-vlan10] test-type icmp
[RouterA-nqa-admin-vlan10] destination-address ipv4 192.168.5.1
[RouterA-nqa-admin-vlan10] frequency 10
[RouterA-nqa-admin-vlan10] start now
[RouterA-nqa-admin-vlan10] quit
[RouterA] nqa test-instance admin vlan20
[RouterA-nqa-admin-vlan20] test-type icmp
[RouterA-nqa-admin-vlan20] destination-address ipv4 192.168.6.1
[RouterA-nqa-admin-vlan20] frequency 10
[RouterA-nqa-admin-vlan20] start now
[RouterA-nqa-admin-vlan20] quit
```

步骤 3 配置流分类

在 RouterA 上创建流分类 vlan10、vlan20，分别匹配入接口为 GE1/0/0 和 GE2/0/0 的报文。

```
[RouterA] traffic classifier vlan10
[RouterA-classifier-vlan10] if-match inbound-interface gigabitethernet 1/0/0
[RouterA-classifier-vlan10] quit
[RouterA] traffic classifier vlan20
[RouterA-classifier-vlan20] if-match inbound-interface gigabitethernet 2/0/0
[RouterA-classifier-vlan20] quit
```

步骤 4 配置流行为

在 RouterA 上创建流行为 vlan10，配置 NQA 测试例 admin vlan10 与重定向到下一跳 192.168.3.1/24 联动，当 NQA 测试例检测到链路正常时，重定向生效；NQA 测试例检测到链路故障时，按正常转发路径转发报文。

```
[RouterA] traffic behavior vlan10
[RouterA-behavior-vlan10] redirect ip-nexthop 192.168.3.1 track nqa admin vlan10
[RouterA-behavior-vlan10] quit
```

在 RouterA 上创建流行为 vlan20，配置 NQA 测试例 admin vlan20 与重定向到下一跳 192.168.4.1/24 联动，当 NQA 测试例检测到链路正常时，重定向生效；NQA 测试例检测到链路故障时，按正常转发路径转发报文。

```
[RouterA] traffic behavior vlan20
[RouterA-behavior-vlan20] redirect ip-nexthop 192.168.4.1 track nqa admin vlan20
[RouterA-behavior-vlan20] quit
```

步骤 5 配置流策略并应用到接口上

在 RouterA 上创建流策略 vlan10、vlan20，将流分类和对应的流行为进行绑定。

```
[RouterA] traffic policy vlan10
[RouterA-trafficpolicy-vlan10] classifier vlan10 behavior vlan10
[RouterA-trafficpolicy-vlan10] quit
[RouterA] traffic policy vlan20
[RouterA-trafficpolicy-vlan20] classifier vlan20 behavior vlan20
[RouterA-trafficpolicy-vlan20] quit
```

将流策略 vlan10 应用到接口 GE1/0/0 入方向，将流策略 vlan20 应用到接口 GE2/0/0 入方向。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] traffic-policy vlan10 inbound
```

```
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] traffic-policy vlan20 inbound
[RouterA-GigabitEthernet2/0/0] quit
```

步骤 6 验证配置结果

查看 RouterA 接口的配置信息。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] display this
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 traffic-policy vlan10 inbound
#
return
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] display this
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 traffic-policy vlan20 inbound
#
return
```

查看在接口上应用的流策略的配置信息。

```
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: vlan10
   Classifier: vlan10
    Operator: OR
     Behavior: vlan10
      Redirect:
        Redirect ip-nexthop 192.168.3.1 track nqa admin vlan10

  Policy: vlan20
   Classifier: vlan20
    Operator: OR
     Behavior: vlan20
      Redirect:
        Redirect ip-nexthop 192.168.4.1 track nqa admin vlan20
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
traffic classifier vlan10 operator or
 if-match inbound-interface GigabitEthernet1/0/0
traffic classifier vlan20 operator or
 if-match inbound-interface GigabitEthernet2/0/0
#
traffic behavior vlan10
 redirect ip-nexthop 192.168.3.1 track nqa admin vlan10
traffic behavior vlan20
 redirect ip-nexthop 192.168.4.1 track nqa admin vlan20
#
traffic policy vlan10
 classifier vlan10 behavior vlan10
traffic policy vlan20
 classifier vlan20 behavior vlan20
```

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 traffic-policy vlan10 inbound
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 traffic-policy vlan20 inbound
#
nqa test-instance admin vlan10
 test-type icmp
 destination-address ipv4 192.168.5.1
 frequency 10
 start now
nqa test-instance admin vlan20
 test-type icmp
 destination-address ipv4 192.168.6.1
 frequency 10
 start now
#
return
```

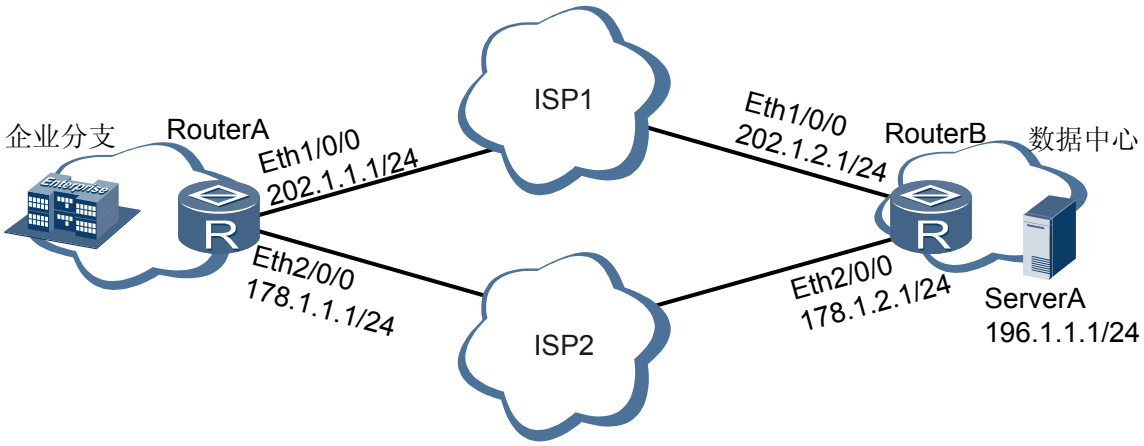
8.6.3 配置智能策略路由示例

介绍智能策略路由示例的配置过程。

组网需求

如图 8-3 所示，某金融企业分支通过 ISP1 的网络和 ISP2 的网络和企业的数据中心相连。企业用 ISP1 的网络作为高速主链路，用 ISP2 的网络作为备份链路。其中，RouterA 的 Eth1/0/0 和 ISP1 相连，IP 地址为 202.1.1.1/24，Eth2/0/0 与 ISP2 相连，IP 地址为 178.1.1.1/24。RouterB 的 Eth1/0/0 和 ISP1 相连，IP 地址为 202.1.2.1/24，Eth2/0/0 与 ISP2 相连，IP 地址为 178.1.2.1/24。企业分支需要将交易数据及时保存到数据中心的 ServerA 上，ServerA 的 IP 地址为 196.1.1.1/24。为了保证交易数据能及时反馈到数据中心，交易数据要求链路的时延不能大于 1000 毫秒。

图 8-3 配置智能策略路由组网图



配置思路

智能策略路由配置思路如下：

- 首先指定各接口的 IP 地址。
- 配置静态路由，保证企业分支和数据中心间路由可达。
- 配置 ISP1 的链路为主链路组，ISP2 的链路为备份链路组。

数据准备

为完成此配置示例，需准备如下的数据：

- 各接口的 IP 地址和子网掩码。
- RouterA 和 RouterB 之间路由可达。
- 配置 ACL，区分需要智能策略路由的数据流。
- 配置 NQA 实例。

操作步骤

步骤 1 配置各接口的 IP 地址

配置 RouterA 的各接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 1/0/0
[RouterA-Ethernet1/0/0] ip address 202.1.1.1 255.255.255.0
[RouterA-Ethernet1/0/0] quit
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] ip address 178.1.1.1 255.255.255.0
```

配置 RouterB 的各接口的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface ethernet 1/0/0
[RouterB-Ethernet1/0/0] ip address 202.1.2.1 255.255.255.0
[RouterB-Ethernet1/0/0] quit
[RouterB] interface ethernet 2/0/0
[RouterB-Ethernet2/0/0] ip address 178.1.2.1 255.255.255.0
```

步骤 2 配置 NQA 实例

在 RouterA 上配置 NQA 客户端。

```
[RouterA] nqa test-instance admin nqa1
[RouterA-nqa-admin-nqa1] test-type jitter
[RouterA-nqa-admin-nqa1] destination-address ipv4 202.1.2.1
[RouterA-nqa-admin-nqa1] destination-port 10000
[RouterA-nqa-admin-nqa1] hardware-based enable
[RouterA-nqa-admin-nqa1] frequency 10
[RouterA-nqa-admin-nqa1] source-interface Ethernet 1/0/0
[RouterA-nqa-admin-nqa1] start now
[RouterA-nqa-admin-nqa1] quit
[RouterA] nqa test-instance admin nqa2
[RouterA-nqa-admin-nqa2] test-type jitter
[RouterA-nqa-admin-nqa2] destination-address ipv4 178.1.2.1
[RouterA-nqa-admin-nqa2] destination-port 10001
[RouterA-nqa-admin-nqa2] hardware-based enable
[RouterA-nqa-admin-nqa2] frequency 10
[RouterA-nqa-admin-nqa2] source-interface Ethernet 2/0/0
[RouterA-nqa-admin-nqa2] start now
```

在 RouterB 上配置 NQA 服务器。

```
[RouterB] nqa-server udpecho 202.1.2.1 10000
[RouterB] nqa-server udpecho 178.1.2.1 10001
```

步骤 3 配置区分业务流的 ACL

在 RouterA 上配置 ACL 3000，允许目的地址为 196.1.1.1 的数据流做智能策略路由。

```
[RouterA] acl 3000
[RouterA-acl-adv-3000] rule permit ip destination 196.1.1.1 0.0.0.0
```

步骤 4 配置 RouterA 的智能策略路由的路由参数

```
[RouterA] smart-policy-route
[RouterA-smart-policy-route] period 50
[RouterA-smart-policy-route] route flapping suppression 100
[RouterA-smart-policy-route] prober ethernet 1/0/0 nqa admin nqa1
[RouterA-smart-policy-route] prober ethernet 2/0/0 nqa admin nqa2
[RouterA-smart-policy-route] link-group group1
[RouterA-smart-policy-route-link-group group1] link-member ethernet 1/0/0
[RouterA-smart-policy-route-link-group group1] quit
[RouterA-smart-policy-route] link-group group2
[RouterA-smart-policy-route-link-group group2] link-member ethernet 2/0/0
[RouterA-smart-policy-route-link-group group2] quit
```

步骤 5 配置智能策略路由的业务参数

```
[RouterA-smart-policy-route] service-map map1
[RouterA-smart-policy-route-service-map-map1] match acl 3000
[RouterA-smart-policy-route-service-map-map1] set delay threshold 1000
[RouterA-smart-policy-route-service-map-map1] set link-group group1
[RouterA-smart-policy-route-service-map-map1] set link-group group2 backup
```

步骤 6 验证配置结果

在 RouterA 上查看探测链路的探测结果。

```
[RouterA] display smart-policy-route link-state
------------------------------------------------------------------------------
link-name                               Delay     Jitter    Loss      CMI
------------------------------------------------------------------------------
Ethernet1/0/0                           1000      0         0         8000
Ethernet2/0/0                           1000      0         0         8000
------------------------------------------------------------------------------
```

在 RouterA 上查看业务 map1 的选路信息。

```
[RouterA] display smart-policy-route service-map map1
------------------------------------------------------------------------------
Match acl         : 3000
DelayThreshold    : 1000
LossThreshold     : -
JitterThreshold   : -
CmiThreshold      : 1000
GroupName         : group1
BackupGroupName   : group2
Description       :
Cmi-Method        : d+l+j
CurLinkName       : Ethernet1/0/0
------------------------------------------------------------------------------
```

----结束

配置文件

RouterA 的配置文件。

```
#
 sysname RouterA
```

```
#
acl number 3000
 rule 5 permit ip destination 196.1.1.1 0
#
interface Ethernet1/0/0
 ip address 202.1.1.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 178.1.1.1 255.255.255.0
#
nqa test-instance admin nqa1
 test-type jitter
 destination-address ipv4 202.1.2.1
 destination-port 10000
 hardware-based enable
 frequency 10
 source-interface Ethernet1/0/0
 start now
nqa test-instance admin nqa2
 test-type jitter
 destination-address ipv4 178.1.2.1
 destination-port 10001
 hardware-based enable
 frequency 10
 source-interface Ethernet2/0/0
 start now
#
smart-policy-route
 period 50
 route flapping suppression 100
 prober Ethernet1/0/0 nqa admin nqa1
 prober Ethernet2/0/0 nqa admin nqa2
 link-group group1
  link-member Ethernet1/0/0
 link-group group2
  link-member Ethernet2/0/0
 service-map map1
  match acl 3000
  set delay threshold 1000
  set link-group group1
  set link-group group2 backup
#
```

RouterB 的配置文件。

```
#
 sysname RouterB
#
interface Ethernet1/0/0
 ip address 202.1.2.1 255.255.255.0
#
interface Ethernet2/0/0
 mode user-termination
 ip address 178.1.2.1 255.255.255.0
#
nqa-server udpecho 178.1.2.1 10001
nqa-server udpecho 202.1.2.1 10000
#
```

9 UDP helper 配置

关于本章

介绍 UDP Helper 的基本原理，并提供配置过程和配置实例。

9.1 UDP helper 概述
介绍 UDP Helper 的基本原理。

9.2 AR1200 支持的 UDP helper 特性
介绍 UDP Helper 特性在 AR1200 中的支持情况。

9.3 配置 UDP helper
介绍 UDP Helper 的配置，以实现对指定 UDP 端口的广播报文进行中继转发。

9.4 维护 UDP Helper
介绍如何清除 UDP Helper 统计信息。

9.5 配置举例
介绍 UDP helper 的配置举例。

9.1 UDP helper 概述

介绍 UDP Helper 的基本原理。

企业网的主机有时需要通过发送广播报文，例如 UDP 广播报文，从服务器中获得配置信息。但是，当主机与待查询的服务器不在同一个广播域时，无法利用广播报文进行通信，从而使主机无法从服务器中获取所需要的信息。

为解决上述问题，AR1200 提供了 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，将广播报文转换为单播报文发送给指定的目的服务器。

9.2 AR1200 支持的 UDP helper 特性

介绍 UDP Helper 特性在 AR1200 中的支持情况。

AR1200 在使能 UDP Helper 功能后，默认对 6 个 UDP 端口的广播报文进行中继转发，其他 UDP 端口必须要在使能 UDP Helper 功能后手动配置。

默认端口列表如表 9-1 所示。

表 9-1 UDP Helper 使能后默认对广播报文中继转发的 UDP 端口列表

协议	UDP 端口号
TFTP (Trivial File Transfer Protocol)	69
DNS (Domain Name System)	53
Time Service	37
NetBIOS-NS (NetBIOS Name Service)	137
NetBIOS-DS (NetBIOS Datagram Service)	138
TACACS (Terminal Access Controller Access Control System)	49

UDP Helper 功能不支持对 DHCP 报文的中继，即中继转发的 UDP 端口不能配置为 67 和 68。如果要中继 DHCP 报文，需要使能 DHCP Relay 特性。

9.3 配置 UDP helper

介绍 UDP Helper 的配置，以实现对指定 UDP 端口的广播报文进行中继转发。

9.3.1 建立配置任务

在配置 UDP Helper 前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

企业网的主机有时需要通过发送广播报文,例如 UDP 广播报文，从服务器中获得配置信息。但是，当主机与待查询的服务器不在同一个广播域时，无法利用广播报文进行通信，从而使主机无法从服务器中获取所需要的信息。

为解决上述问题，AR1200 提供了 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，将广播报文转换为单播报文发送给指定的目的服务器。

前置任务

在配置 UDP Helper 功能之前，需完成以下任务：

- 配置 AR1200 到目的服务器的路由信息，使得 AR1200 到目的服务器路由可达。

数据准备

在配置 UDP Helper 功能之前，需要准备以下数据。

序号	数据
1	（可选）中继转发的 UDP 端口
2	需要配置中继转发目的服务器的接口和中继转发的目的服务器 IP 地址

9.3.2 使能 UDP helper 功能

介绍使能 UDP helper 功能的配置。

背景信息

使能 UDP Helper 功能后，如果设备接收到广播报文，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，且目的 MAC 为广播 MAC，则修改 IP 报文头的目的 IP 地址，将报文发给指定的目的服务器。
- 否则，直接将报文丢弃。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **udp-helper enable**，使能 UDP Helper 功能。

----结束

9.3.3 (可选)配置中继转发的 UDP 端口

介绍中继转发的 UDP 端口的配置。

前提条件

已经使能 UDP Helper 功能。

背景信息

UDP Helper 功能使能后，AR1200 默认对 6 个 UDP 端口号 37（Time）、49（TACACS）、53（DNS）、69（TFTP）、137（NetBIOS-NS）、138（NetBIOS-DS）的广播报文进行中继转发，如果需要配置的端口号在上述端口号范围内，可以跳过该配置步骤。

AR1200 不支持对 DHCP 报文即 UDP 端口号 67 和 68 的中继转发。

请在 AR1200 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }，配置需要中继转发的 UDP 端口。

----结束

9.3.4 配置中继转发的目的服务器

介绍中继转发的目的服务器的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

目前支持 UDP Helper 功能的接口有 VLANIF 接口、WAN 侧 GE 接口和 WAN 侧 GE 子接口。

步骤 3 执行命令 **udp-helper server** *ip-address*，配置中继转发的目的服务器。

UDP Helper 功能使能后，如果接口收到报文的 UDP 目的端口号与需要中继转发的 UDP 端口号相匹配，则将报文转发给该接口下所配置的目的服务器。

----结束

9.3.5 检查配置结果

操作步骤

- 执行命令 **display udp-helper server**，查看 UDP 中继转发的接口号、目的服务器 IP 地址和转发的 UDP 报文数量。

- 执行命令 **display udp-helper port**，查看当前设备上已经配置的需要中继转发的 UDP 端口号信息。

----结束

任务示例

查看 UDP Helper 中继转发相关信息。

```
<Huawei> display udp-helper server
Server-interface                Server-Ip                    packet-num
------------------------------------------------------------------------------
Vlanif20                          1.1.1.2                             0
GigabitEthernet1/0/0.1        192.168.1.200                           0
```

查看当前设备上已经配置的需要中继转发的 UDP 端口号信息。

```
<Huawei> display udp-helper port
Udp-Port-Number       Description
------------------------------------------------------------
       1              TCP Port Service Multiplexer
      37              Time
      49              Login Host Protocol
      53              Domain Name Server
      69              Trivial File Transfer
     137              NETBIOS Name Service
     138              NETBIOS Datagram Service
```

9.4 维护 UDP Helper

介绍如何清除 UDP Helper 统计信息。

9.4.1 清除 UDP Helper 统计信息

背景信息

注意

清除 UDP Helper 统计信息后，以前的信息将无法恢复，清除前请务必仔细确认。

操作步骤

步骤 1 在确认需要清除 UDP Helper 统计信息后，请在用户视图下执行命令 **reset udp-helper packet**。

----结束

9.5 配置举例

介绍 UDP helper 的配置举例。

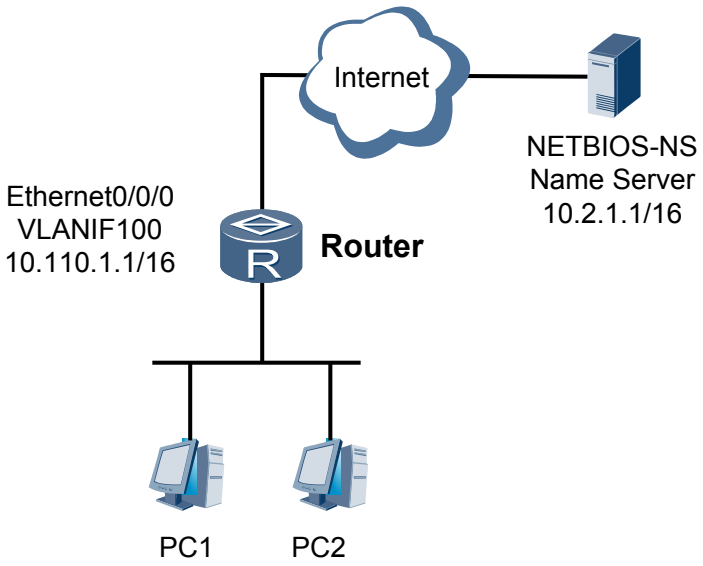
9.5.1 配置 UDP Helper 示例

组网需求

如图 9-1 所示，Router 的接口 VLANIF100 的 IP 地址为 10.110.1.1/16。NetBIOS-NS name 服务器的 IP 地址为 10.2.1.1/16。Router 与 NetBIOS-NS name 服务器不在同一网段，但 Router 到 NetBIOS-NS name 服务器路由可达。

配置将目的 UDP 端口号为 137、目的 IP 地址为 255.255.255.255 和 10.110.255.255 的广播 UDP 报文中继转发到指定的目的 NetBIOS-NS name 服务器上。这样如果 Router 接收到 NetBIOS-NS Register 的广播报文，将修改 IP 报文头的目的 IP 地址为 NetBIOS-NS name 服务器的 IP 地址，从而将报文发给指定的 NetBIOS-NS name 服务器。

图 9-1 配置 UDP Helper 组网图



配置思路

采用如下的思路配置 UDP Helper 功能：

1. 使能 Router 的 UDP Helper 功能。
2. 创建 VLAN 并在 VLANIF 接口下配置接口 IP 地址及中继转发的目的服务器。

说明

因为 Router 在启动 UDP Helper 功能后默认支持将目的 UDP 端口号为 137 的广播报文进行中继转发，所以此处不需要配置中继转发的 UDP 端口号。

数据准备

为完成此配置示例，需准备如下的数据：

- Router 中继转发广播报文的 VLANIF 接口
- 目的服务器的 IP 地址

操作步骤

步骤 1 使能 UDP Helper 功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] udp-helper enable
```

步骤 2 配置 Router 接口 Ethernet0/0/0 加入 VLAN100

```
[Router] vlan 100
[Router-Vlan100] quit
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port hybrid pvid vlan 100
[Router-Ethernet0/0/0] port hybrid untagged vlan 100
[Router-Ethernet0/0/0] quit
```

步骤 3 配置中继转发的目的服务器。

```
[Router] interface vlanif 100
[Router-Vlanif100] ip address 10.110.1.1 16
[Router-Vlanif100] udp-helper server 10.2.1.1
[Router-Vlanif100] quit
[Router] quit
```

步骤 4 检查配置结果。

接口 VLANIF100 中继转发的目的服务器为配置的 NetBIOS-NS name 服务器。

```
<Router> display udp-helper server
Server-interface        Server-Ip        packet-num
Vlanif100               10.2.1.1                0
```

----结束

配置文件

Router 的配置文件。

```
#
 sysname Router
#
 udp-helper enable
#
vlan batch 100
#
interface Ethernet0/0/0
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface Vlanif100
 ip address 10.110.1.1 255.255.0.0
 udp-helper server 10.2.1.1
#
return
```