目 录

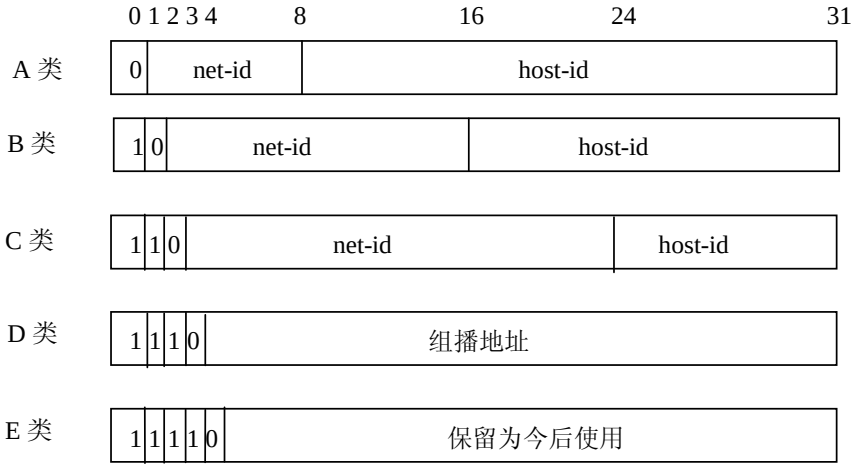
第1章 IP 地址配置

1.1 IP 地址介绍

所谓 IP 地址，是指分配给连接在 Internet 上的主机的一个唯一的 32 比特标识符。IP 地址一般由两部分组成：第一部分为网络号码，第二部分为主机号码。IP 地址的结构使我们可以在 Internet 上方便地进行寻址。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。

为了方便IP地址的管理以及组网，Internet的IP地址分成五类。如 图 1-1所示，IP地址由下列两个字段组成：

- 网络号码字段（net-id）；网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（host-id）。



net-id—网络号码，host-id—主机号码

图1-1 五类 IP 地址

D 类地址是一种组播地址，主要是留给 Internet 体系结构委员会 IAB（Internet Architecture Board）使用。E 类地址保留在今后使用。目前大量使用中的 IP 地址属于 A、B、C 三种中的一种。

在使用 IP 地址时要知道一些 IP 地址是保留作为特殊用途的，一般不使用。下表列出用户可配置的 IP 地址范围。

表1-1 IP 地址分类及范围

网络类型	地址范围	说明
A	0.0.0.0～127.255.255.255	所有形如 127.X.Y.Z 的地址都保留作回路测试，发送到这个地址的分组不会输出到线路上，它们被内部处理并当作输入分组。
B	128.0.0.0～191.255.255.255	-
C	192.0.0.0～223.255.255.255	-
D	224.0.0.0～239.255.255.255	D 类地址是一种组播地址。
E	240.0.0.0～255.255.255.255	255.255.255.255 用于广播地址，其它地址保留今后使用。

IP 地址有一些重要的特点：

(1) IP 地址是一种非等级的地址结构，和电话号码的结构不一样，也就是说，IP 地址不能反映任何有关主机位置的地理信息。

(2) 当一个主机同时连接到两个网络上时（作路由器用的主机即为这种情况），该主机就必须同时具有两个相应的 IP 地址，其网络号码 net-id 是不同的，这种主机成为多地址主机（multihomed host）。

(3) 按照 Internet 的观点，用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号码 net-id。

(4) 在 IP 地址中，所有分配到网络号码（net-id）的网络，不管是小的局域网还是很大的广域网，都是平等的。

从 1985 年起，为了使 IP 地址的使用更加灵活，只分配 IP 地址的网络号码 net-id，而后面的主机号码 host-id 则是受本单位控制。即某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 net-id，具体的各个主机号码 host-id 则由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。当一个单位的主机很多而且分布在很大的地理范围时，为了便于管理，可将单位内部的主机号码再进一步划分为多个子网。需要注意的是，子网的划分由单位内部决定，在本单位以外看不到单位内部的子网。从外部看，这个单位只有一个网络号码。只有当外面的报文进入到本单位范围后，本单位的路由器才根据子网号码再进行选路，找到目的主机。

如图 1-2 所示，为一个 B 类 IP 地址划分子网情况，其中子网掩码由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码和子网号码字段，而“0”对应于主机号码字段。

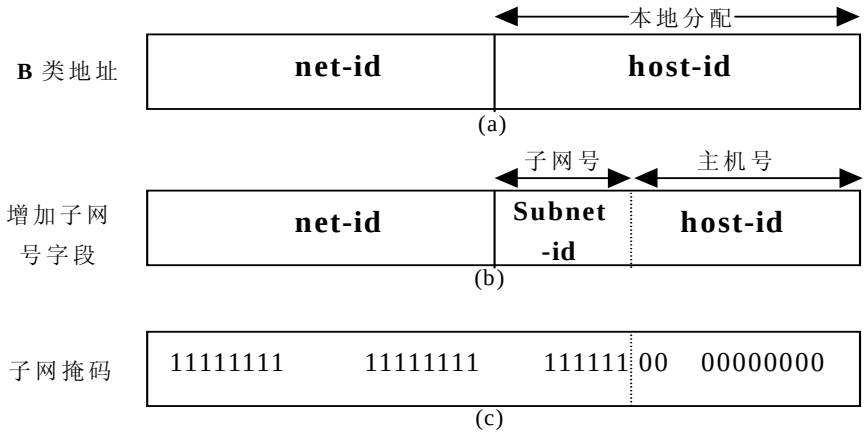


图1-2 IP 地址子网划分

多划分出一个子网号码字段是要付出代价的。举例来说，本来一个 B 类 IP 地址可以容纳 65534 个主机号码。但划分出 6bit 长的子网字段后，最多可有 64 个子网，每个子网有 10bit 的主机号码，即每个子网最多可有 1022（2^{10}-2，去掉全 1 和全 0 的主机号码）个主机号码。因此主机号码的总数是 64* 1022 = 65408 个，比不划分子网时要少 126 个。

若一个单位不进行子网的划分，则其子网掩码即为默认值，此时子网掩码中“1”的长度就是网络号码的长度。因此，对于 A，B 和 C 类的 IP 地址，其对应子网掩码的默认值分别为 255.0.0.0；255.255.0.0.和 255.255.255.0。

一台路由器用来连接多个网络，具有多个网络的 IP 地址。上面讲的 IP 地址还不能直接用来进行通信。这是因为：

- IP 地址只是主机在网络层中的地址，若要将网络层中传送的数据报交给目的主机，必须知道该主机的物理地址。因此必须将 IP 地址解析为物理地址。
- 用户平时不愿意使用难于记忆的 IP 地址，而是愿意使用易于记忆的主机名，因此也需要将主机名解析为 IP 地址。

下图表示了主机名、IP 地址和物理地址之间的关系。

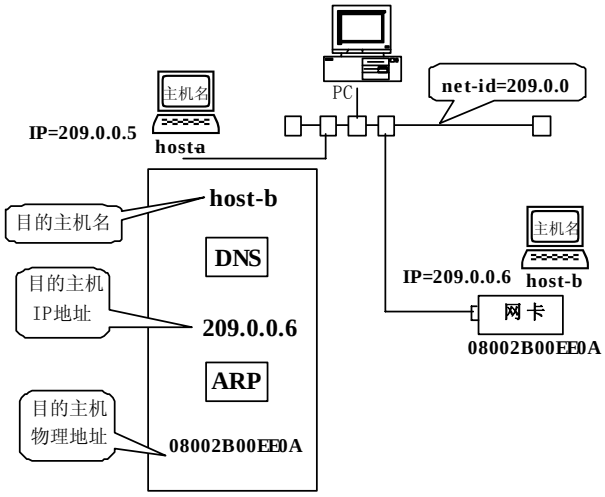


图1-3 主机名、IP 地址和物理地址之间的关系

1.2 IP 地址的配置

IP 地址配置包括：

- 配置接口 IP 地址
- 配置接口借用 IP 地址
- IP 地址的监控与维护

1.2.1 配置接口 IP 地址

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

IP 地址的配置支持如下情况：

- 父接口和子接口之间不可以是同一网段。
- 兄弟接口之间不可以是同一网段。
- 主从地址可以是同一网段。

1. 配置接口主 IP 地址

一个接口只能有一个主 IP 地址，用下面的命令可修改接口的主 IP 地址和网络的掩码。

请在接口视图下进行下列配置。

表1-2 配置接口主 IP 地址

操作	命令
配置接口主 IP 地址	**ip address** *ip-address net-mask*

通过掩码来标识 IP 地址包含的网号，例如：路由器以太网口的 IP 地址是 129.9.30.42，掩码是 255.255.0.0，将 IP 地址与掩码相“与”后，可知路由器以太网接口所在网段的地址为 129.9.0.0。

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。

缺省情况下，无主 IP 地址。

2. 配置接口从 IP 地址

除了主 IP 地址外，一个接口上还可配置多个从 IP 地址。配置从 IP 地址的主要目的在于使同一接口能位于不同的子网上，从而产生以同一接口为输出端口的网络路由，这样通过同一接口实现与多个子网相连。

请在接口视图下进行下列配置。

表1-3 配置接口从 IP 地址

操作	命令
配置接口从 IP 地址	**ip address** *ip-address net-mask* **sub**

缺省情况下，无从 IP 地址。

一个接口所能配置的 IP 地址总数最多为 32 个，包括主 IP 地址和从 IP 地址。

⚠ 注意：

当接口被配置为通过 BOOTP、DHCP 或 PPP 协商分配 IP 地址后，则不能再给该接口配置从 IP 地址。

3. 删除接口 IP 地址

请在接口视图下进行下列配置。

表1-4 删除接口 IP 地址

操作	命令
删除 IP 地址	**undo ip address** [*ip-address net-mask* [**sub**]]

使用该命令时若不带任何参数，将删除该接口的所有 IP 地址。

undo ip address 命令不带任何参数表示删除该接口的所有 IP 地址。**undo ip address** *ip-address net-mask* 表示删除主 IP 地址，**undo ip address** *ip-address net-mask* **sub** 表示删除从 IP 地址。在删除主 IP 地址前必须先删除完所有的从 IP 地址。

4. 设置接口 IP 地址可协商属性

若接口封装了 PPP，本端接口还未配置 IP 地址而对端已有 IP 地址时，可为本端接口配置 IP 地址可协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。该配置主要用于在通过 ISP 访问 Internet 时，得到由 ISP 分配的 IP 地址。

请在接口视图下进行下列配置。

表1-5 设置接口 IP 地址可协商属性

操作	命令
设置接口 IP 地址可协商属性	**ip address ppp-negotiate**
取消接口 IP 地址可协商属性	**undo ip address ppp-negotiate**

系统缺省为不允许接口 IP 地址的协商。关于 PPP 接口地址协商的详细配置请参见链路层部分的 PPP 协议。

⚠ 注意：

- 因 PPP 支持 IP 地址的协商，所以只有当接口封装了 PPP 时，才能设置接口 IP 地址的协商，当 PPP 协议 down 时，协商产生的 IP 地址将被删除。
- 若接口原来配有地址，在配置接口 IP 地址协商后，原 IP 地址将被删除。
- 配置接口 IP 地址协商后，不需再给该接口配置 IP 地址，IP 地址由协商获得。
- 配置接口 IP 地址协商后，再次配置该接口协商，原协商产生的 IP 地址将被删除，接口再次协商获得 IP 地址。
- 在协商地址被删除后，接口将处于无地址状态。

1.2.2 配置接口借用 IP 地址（IP Address Unnumbered）

1. IP Address Unnumbered 简介

借用 IP 地址这种功能，其最主要的目的就是节省宝贵的 IP 地址资源。一个接口如果没有 IP 地址就无法生成路由，也就无法转发报文。所谓“借用 IP 地址”，其实质就是：一个接口上没有配置 IP 地址，但是还想使用该接口。就向其它有 IP 地址的接口借一个 IP 地址过来，以使该接口能够正常使用。如果被借用接口有多个 IP 地址，则只能借用主 IP 地址。如果被借用接口没有 IP 地址，则借用接口的 IP 地址为 0.0.0.0。该功能通过 **ip address unnumbered** 命令来实现。

需要注意的是：

- 借用方不能为以太网接口。
- 被借用方接口的地址本身不能为借用地址。
- 被借用方的地址可以借给多个接口。

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

由于借用方接口本身没有 IP 地址，无法进行路由，所以必须为其手工配置两条路由才能实现路由器间的连通。具体的配置步骤请参见配置举例。

⚠ 注意：

在 Tunnel 接口配置地址借用后，必须手工配置到 Tunnel 对端接口的静态路由，且掩码必须为 32 位。

2. IP Address Unnumbered 配置任务列表

IP Address Unnumbered 属性在接口视图下进行，封装了 PPP、HDLC、帧中继、SLIP 的串口以及 Tunnel 接口可借用以太网口或其它接口的 IP 地址。

IP Address Unnumbered 配置任务列表如下：

- 激活和关闭 IP Address Unnumbered

3. 激活和关闭 IP Address Unnumbered

请在接口视图下进行下列配置。

表1-6 接口借用 IP 地址的配置

操作	命令
激活 IP Address Unnumbered	**ip address unnumbered interface** *interface-type interface-number*
关闭 IP Address Unnumbered	**undo ip address unnumbered**

缺省情况下，不借用其它接口的 IP 地址。

1.2.3 IP 地址显示和调试

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

表1-7 IP 地址显示和调试

操作	命令
显示接口 IP 信息	**display ip interface** [*interface-type interface-number*]
显示接口 IP 摘要信息	**display ip interface brief** [*interface-type interface-number*]

1.2.4 IP Address Unnumbered 显示和调试

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

表1-8 IP Address Unnumbered 显示和调试

操作	命令
显示接口信息，其中包括 IP Address Unnumbered 信息	**display interface** [*interface-type* [*interface-number*]]

1.2.5 IP 地址配置举例

1. 组网需求

为路由器串口 Serial1/0/1 配置 IP 地址，要求主 IP 地址为 129.2.2.1，从地址为 129.1.3.1。

2. 组网图

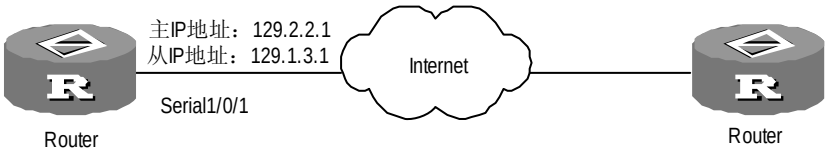


图1-4 为路由器接口配置主从 IP 地址

3. 配置步骤

配置路由器串口 Serial0/1 的主从 IP 地址。

```
[H3C] interface serial 1/0/1
[H3C-Serial1/0/1] ip address 129.2.2.1 255.255.255.0
[H3C-Serial1/0/1] ip address 129.1.3.1 255.255.255.0 sub
```

1.2.6 典型 IP Address Unnumbered 配置举例

1. 组网需求

假设有一家公司，总部在北京，在深圳、上海各有一个分公司。在武汉有一个办事处。它的网络情况如下图。R 是总部的路由器，它通过电话网（PSTN）与各个分公司、办事处的路由器 R1、R2、R3 相连。R、R1、R2、R3 四台路由器都有一个串口用于拨号，一个以太网口用于连接本地的网络。

2. 组网图

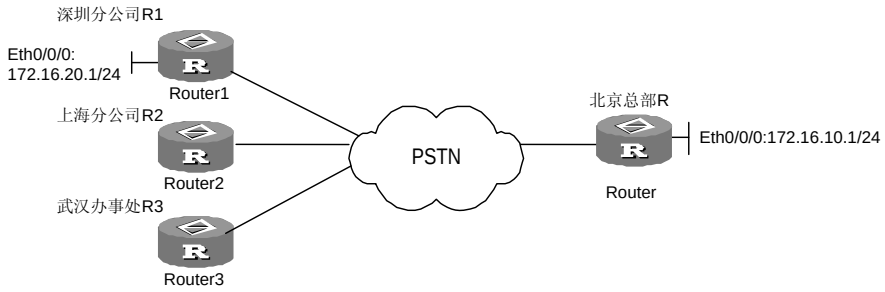


图1-5 某公司的网络拓扑图

3. 配置步骤

(1) 配置总部路由器 R

```
[H3C-Ethernet1/0/0] ip address 172.16.10.1 255.255.255.0
```

借用以太网的 IP 地址。

```
[H3C-Serial2/0/0] ip address unnumbered interface ethernet 1/0/0
[H3C-Serial2/0/0] link-protocol ppp
```

配置到深圳路由器 R1 以太网网段的路由。

```
[H3C] ip route-static 172.16.20.0 255.255.255.0 172.16.20.1
```

配置到深圳路由器 R1 串口的接口路由。

```
[H3C] ip route-static 172.16.20.0 255.255.255.0 serial2/0/0
```

(2) 配置深圳分公司的路由器 R1

```
[H3C-Ethernet1/0/0] ip address 172.16.20.1 255.255.255.0
```

借用以太网的 IP 地址。

```
[H3C-Serial2/0/0] ip address unnumbered ethernet 1/0/0
[H3C-Serial2/0/0] link-protocol ppp
```

配置到北京总部路由器 R 以太网网段的路由，该路由为缺省路由：

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 172.16.10.1
```

配置到北京路由器 R 串口的接口路由。

```
[H3C] ip route-static 172.16.10.1 255.255.255.255 serial2/0/0
```

1.2.7 IP 地址配置排错

路由器是网络互连设备，因而在给接口配置 IP 地址时，我们必须明白组网需求和子网的划分。一般应遵循如下原则：

- 路由器以太网接口 IP 地址必须与该以太网口所连的局域网在同一网段。
- 广域网两端的路由器的串口 IP 地址尽量在同一网段。

故障之一：从路由器 **ping** 局域网中某一主机不通。

故障排除：

- 首先检查路由器以太网口和局域网中主机的 IP 地址配置，是否位于同一网段。
- 如果配置正确，可以在路由器上打开 **arp** 调试开关，查看路由器是否正确地发送和接收 **arp** 报文，如果只有发送，没有接收到 **arp** 报文，则有可能以太网物理层有问题。

第2章 地址解析协议（ARP）的配置

2.1 静态/动态 ARP 配置

2.1.1 动态 ARP 简介

ARP 即地址解析协议，主要用于从 IP 地址到以太网 MAC 地址的解析。一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。

在 Comware 的实现中，如果收到的 ARP 报文满足以下任何一条条件，系统将创建或更新 ARP 表项：

- ARP 报文的源 IP 地址与入接口 IP 地址在同一网段，不是广播地址，目的 IP 地址是本接口 IP 地址。
- ARP 报文的源 IP 地址与入接口 IP 地址在同一网段，不是广播地址，目的 IP 地址是本接口的 VRRP 虚拟 IP 地址。
- ARP 报文的目的 IP 地址属于入接口上的配置的 NAT 地址池。

如果收到的 ARP 报文的源 IP 地址在入接口的 ARP 表中已经存在对应表项，也将对 ARP 表项进行更新。

2.1.2 静态 ARP 简介

在某些情况下，如将目的地址不在本网段的报文，绑定到某个特定网卡，使得到该 IP 地址的报文能通过该网关进行转发；或是当用户需要过滤掉一些非法 IP 地址（如将这些非法地址绑定到某个不存在的 MAC 地址），就需要用户手工配置静态 ARP 表中的映射项。

2.1.3 静态 ARP 的配置

静态 ARP 配置包括：

- 手工添加/删除静态 ARP 映射项

请在系统视图下进行下列配置。

表2-1 手工添加/删除静态 ARP 映射项

操作	命令
手工添加静态 ARP 映射项	**arp static** *ip-address ethernet-address* [*vpn-instance-name*]
手工删除静态 ARP 映射项	**undo arp** *ip-address* [*vpn-instance-name*]

静态 ARP 映射项在路由器正常工作时间一直有效，而动态 ARP 映射项的有效时间为 20 分钟。

缺省情况下，由动态 ARP 协议获取地址映射。

系统最多可以配置 2048 条静态 ARP 映射项。

2.1.4 动态 ARP 相关配置

1. 使能/关闭 ARP 表项的检查功能（可选）

可以使用下面的命令控制设备是否学习 MAC 地址为组播 MAC 的 ARP 表项。

请在系统视图下进行下列配置。

表2-2 使能/关闭 ARP 表项的检查功能

操作	命令
使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项	**arp check enable**
关闭 ARP 表项的检查功能，即学习 MAC 地址为组播 MAC 的 ARP 表项	**undo arp check enable**

缺省情况下，使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项。

2. 使能/关闭支持自然网段的 ARP 请求（可选）

可以使用下面的命令控制设备是否支持自然网段的 ARP 请求。

请在系统视图下进行下列配置。

表2-3 使能/关闭支持自然网段的 ARP 请求

操作	命令
使能支持自然网段的 ARP 请求	**naturemask-arp enable**
不支持自然网段的 ARP 请求	**undo naturemask-arp enable**

缺省情况下，不支持自然网段的 ARP 请求。

3. 配置动态 ARP 表项的超时时间

请在系统视图下进行下列配置。

表2-4 配置动态 ARP 表项的超时时间

操作	命令
配置动态 ARP 表项的超时时间	**arp timer aging** *minutes*

操作	命令
恢复动态 ARP 表项的超时时间为缺省值	**undo arp timer aging** *minutes*

缺省情况下，动态 ARP 表项的超时时间为 20 分钟。

2.1.5 ARP 显示和调试

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

在用户视图下，执行 **reset** 命令可以清除该运行情况，执行 **debugging** 命令可以对 ARP 进行调试。

表2-5 ARP 显示和调试

操作	命令
显示 ARP 映射表	**display arp** [**static** | **dynamic** | **all**]
显示动态 ARP 表项超时时间（仅 AR46 系列路由器支持）	**display arp timer aging**
清除 ARP 映射表中的 ARP 项	**reset arp** [**all** | **dynamic** | **static** | **interface** *interface-type interface-number*]
打开 ARP 调试信息开关	**debugging arp packet**
关闭 ARP 调试信息开关	**undo debugging arp packet**

2.2 代理 ARP 的配置

2.2.1 代理 ARP 简介

代理 ARP 的主要功能就是将处在同一网段（IP 地址在同一网段），却在不同的物理网络上的计算机或路由器连接起来，使它们互相通信，就好象在同一个物理网络上。

在 80 年代中后期，随着网络应用的发展，局域网的规模越来越大。一所大学的以太网中主机数目可以达到上百台，在这种情况下以太网中的碰撞和冲突的次数已经相当多了。此时新的应用需要继续扩大局域网的规模，若采用中继器的方式将新增的计算机连入局域网，将会使局域网过载，产生的碰撞和冲突将严重降低以太网的性能。为解决这一问题，提出了代理 ARP 解决方案。

2.2.2 代理 ARP 的应用环境

代理 ARP 主要是为连接两个在同一 IP 网段但位于不同物理位置上的网络。

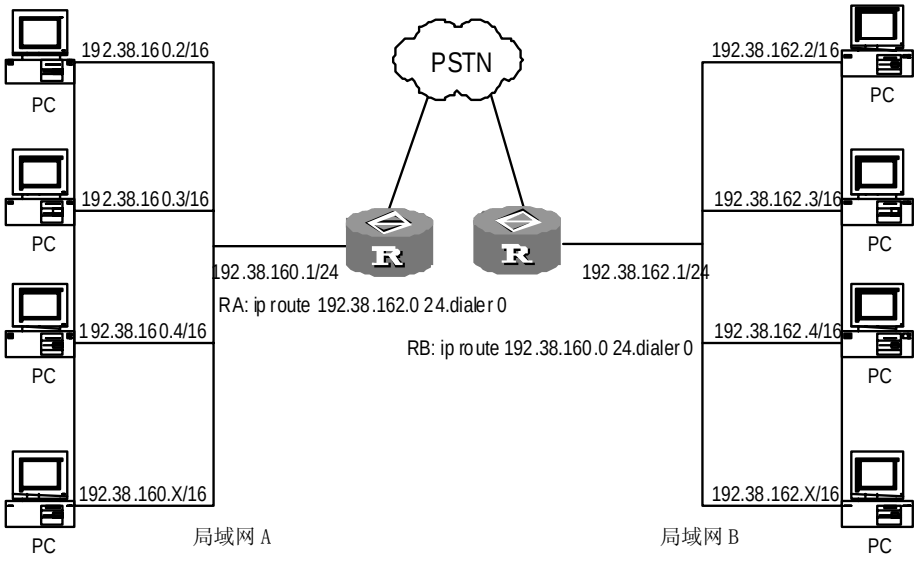


图2-1 代理 ARP 的应用环境

两个局域网分别与两台路由器的以太网口相连。两个局域网中的主机都在 192.38.0.0 网段上。实际上，局域网 A 占用了 192.38.160.0 这一子网段。局域网 B 占用了 192.38.162.0 这一子网段。但是两个局域网中主机的掩码一定是 16 位，即：只包括网络号（192.38.0.0），而不包括子网号（192.38.160.0 或 192.38.162.0）。两台路由器的以太网口都配置成 192.38.0.0 网段，并使能代理 ARP。两台路由器通过 PSTN 相连。在两台路由器上分别配置一条到对端局域网网段的静态路由。

当局域网 A 中的主机想访问局域网 B 中的主机，例如：IP 地址为 192.38.160.2 的主机（以下简称主机 A）想访问 192.38.162.2 的主机（以下简称主机 B）。其访问过程如下：

(1) 主机 A 发出对主机 B 的 ARP 请求报文。

(2) 路由器 A 收到该请求报文，查找路由表。若发现一条到主机 B 的路由项 (192.38.162.0)，就将自己的 MAC 地址添入 ARP 应答报文中，发送给主机 A。

(3) 主机 A 收到 ARP 应答报文后，就将 IP 报文发送给路由器 A。

(4) 路由器 A 接收到 IP 报文后，再查找路由表，将报文转发给路由器 B。

(5) 路由器 B 将接收到的 IP 报文转发给主机 B。

(6) 当主机 B 向主机 A 发送应答报文时，也将经过相同的过程。这样，两台处于不同物理网络上的主机相互访问，就好象处于同一物理网络上。

2.2.3 配置代理 ARP

请在以太网接口视图下进行下面配置。

表2-6 配置代理 ARP

操作	命令
配置代理 ARP	**arp-proxy enable**
禁用代理 ARP 功能。	**undo arp-proxy enable**

缺省情况下，禁用代理 ARP 功能。

2.3 免费 ARP 配置

2.3.1 免费 ARP 简介

免费 ARP 是指设备通过对外发送免费 ARP 报文，来实现以下功能：

网络中的设备可以通过发送免费 ARP 报文来确定其它设备的 IP 地址是否与自己冲突。

如果发送免费 ARP 报文的设备正好改变了硬件地址（很可能是设备关机了，并换了一块接口卡，然后重新启动），那么这个报文就可以使其他设备高速缓存中旧的硬件地址进行相应的更新。例如：设备收到某个 IP 地址的免费 ARP 请求，但在此设备的高速缓存中已经存在这个 IP 地址的 ARP 表项，那么就要用免费 ARP 请求中的发送端硬件地址（如以太网地址）对高速缓存中相应的内容进行更新。设备接收到任何 ARP 请求都要完成这个操作（ARP 请求是在网上广播的，因此每次发送 ARP 请求时网络上的所有主机都要这样做）。

免费 ARP 报文的特点：

报文的源和目的 IP 地址都是本机地址，报文源 MAC 地址是本机 MAC 地址

当其他设备收到免费 ARP 报文后，如果发现免费 ARP 报文中的 IP 地址和自己的 IP 地址冲突，则给发送免费 ARP 报文的设备返回一个 ARP 应答。

2.3.2 使能免费 ARP 报文学习功能

请在系统视图下进行下列配置。

表2-7 使能免费 ARP 报文学习功能

操作	命令
启用免费 ARP 报文的学习功能	**gratuitous-arp-learning enable**
关闭免费 ARP 报文的学习功能	**undo gratuitous-arp-learning enable**

缺省情况下，关闭免费 ARP 报文学习功能。

2.3.3 使能应答不同网段 ARP 请求报文的功能

请在系统视图下进行下列配置。

表2-8 使能应答不同网段 ARP 请求报文的功能

操作	命令
使能应答不同网段 ARP 请求报文的功能	**gratuitous-arp-sending enable**
关闭应答不同网段 ARP 请求报文的功能	**undo gratuitous-arp-sending enable**

缺省情况下，关闭应答不同网段 ARP 请求报文的功能。

2.3.4 使能周期性发送免费 ARP 报文功能并设置发送周期

请在以太网接口视图、以太网子接口视图、千兆以太网接口视图、千兆以太网子接口视图、桥模板视图、VLAN 接口视图或虚拟以太网接口视图下进行下列配置。

表2-9 使能周期性发送免费 ARP 报文的功能并设置发送周期

操作	命令
使能周期性发送免费 ARP 报文功能并设置发送周期	**arp send-gratuitous-arp** *seconds*
关闭周期性发送免费 ARP 报文的功能	**undo arp-gratuitous-arp**

缺省情况下，接口不会周期性发送免费 ARP 报文。

2.3.5 广域网接口 IP 地址与链路层协议地址的映射

在路由器中，除了维护以太网口 IP 地址到 MAC 地址的映射外，还需维护广域网口 IP 地址与链路层协议地址的映射，有以下两类：

- 在封装 X.25 接口上，IP 地址与 X.121 地址的映射，由 **x25 map ip** 命令维护。
- 在封装帧中继接口上，IP 地址与虚电路号（DLCI）的映射，由 **fr map ip** 命令来维护。

上述映射，又可称为二次路由，它们的正确配置，是保证路由器正常工作的关键。详细介绍请参见相关章节。

2.4 授权 ARP 配置

2.4.1 授权 ARP 简介

所谓授权 ARP（Authorized Address Resolution Protocol），即由 DHCP Server 或其他模块根据某种约定，自动在 ARP 表中添加的 ARP 表项。授权 ARP 可以阻止

DHCP Server 对非法 ARP 应答进行动态学习，即只有通过 DHCP Server 分配了 IP 地址的客户端能够依据 ARP 应答报文自动添加 ARP 表项（静态 ARP 表项不受影响），从而阻止非法用户上网。同时授权 ARP 提供了 ARP Ping 的探测机制，来确认 DHCP 客户端是否已下线并通知 DHCP Server 该用户已下线。因此授权 ARP 特性的引入增强了网络安全性并实现了快速发现用户下线的功能。

📖 说明：

- 授权 ARP 特性目前只在启用了 DHCP Server 功能的路由器上实现。
- 授权 ARP 特性目前只支持 DHCP Server 与 DHCP Client 在同一网段的情况。

2.4.2 基本概念

1. ARP cache

每一个主机上都有一个 ARP 高速缓存，称为 ARP cache。ARP cache 存放了最近学习到的 IP 地址到硬件地址之间的映射记录。缺省情况下，高速缓存中每一项的生存时间为 20 分钟。通常在进行 ARP 转换时先搜索 ARP cache，如果没有匹配成功再检查 ARP 表。

2. ARP 表

ARP 表就是记录 IP 地址转与物理地址对应关系的映射表。每一个设备上都维护的一张 ARP 表，表中有通过动态、静态或其他方式生成的 ARP 映射。表项中包括了 IF 索引、物理地址、IP 地址以及类型。

3. ARP Ping

授权 ARP 的老化是通过被称为 ARP ping 的机制来实现的。ARP ping 通过定期向授权表项中记录的客户端 IP 地址发送 ARP 请求报文来判断用户是否已经下线：当收到 ARP 回应报文（不论是否是 ARP ping 所触发）时，授权 ARP 将刷新自己的老化时间。ARP ping 为 DHCP Server 增加了主动询问客户端状态的机制，这样做的好处是使得 DHCP Server 得以在较短的时间内发现客户端离线并释放资源。

4. 授权 ARP 表项

授权 ARP 表项是一类特殊的表项，也是添加在设备端的 ARP 表中的，授权 ARP 同时具有静态 ARP 和动态 ARP 两者的特征。授权 ARP 具有较高的优先级，新添加的授权 ARP 表项可以覆盖相同的动态 ARP 表项而同时不被新添加的相同动态 ARP 所覆盖；但同时其优先级低于静态 ARP，其添加动作不可以覆盖相同的静态 ARP 表项而同时可以被相同的静态 ARP 表项所覆盖。

授权 ARP 具有类似于动态 ARP 的老化机制——通过记录和刷新每个表项的老化时间来判断该表项是否需要老化。授权 ARP 表项的老化时间是由 ARP Ping 来实现的，独立于动态 ARP 表项的老化。缺省的授权 ARP 表项老化时间为连续进行三次 ARP

Ping 后没有收到回应后的时间。ARP Ping 的时间间隔为 30 秒，所以授权 ARP 表项的缺省老化时间为 90 秒，即如果在 90 秒内没有收到任何对应于授权 ARP 表项的报文并且也没有被DHCP Server刷新该表项(当DHCP Server重新添加授权ARP时就认为是刷新该表项），则老化该表项并通知 DHCP Server。

授权 ARP 表项可以被手工删除或通过 DHCP 服务器的删除表项来删除

5. 禁止动态学习 ARP

出于安全性的考虑，授权 ARP 提供了禁止动态学习 ARP（ARP security）的功能，当该功能启动时，只有静态 ARP 表项和授权 ARP 表项被允许添加，动态 ARP 的学习将被禁止。禁止动态学习 ARP 与授权 ARP 之间并不互相依赖，可以独立使用。

2.4.3 ARP 报文结构

ARP 报文分为 ARP 请求和 ARP 应答报文，ARP 请求和应答报文的格式如下图所示，当一个 ARP 请求发出时，除了接收端硬件地址（正是请求方想要获取的地址）域为空外，其他所有的域都被使用。ARP 应答报文使用了所有的域。

图2-2 ARP 请求和应答报文格式

- 硬件类型

识别硬件接口的类型，合法的值为：

表2-10 合法硬件接口类型列表

类型	描述
1	以太网
2	实验以太网
3	X.25
4	Proteon ProNET（令牌环）
5	混沌网（chaos）
6	IEEE802.X

类型	描述
7	ARC 网络

- 协议类型

协议类型标识发送设备所使用的协议类型，TCP/IP 中，这些协议通常是 EtherType。

- 硬件地址长度：数据报文中硬件地址以字节为单位的长度。
- 协议地址长度：数据报文中所有协议地址以字节为单位的长度。
- 操作码：指明数据报是 ARP 请求还是 ARP 应答，假如是 ARP 请求，此值为 1；假如是 ARP 应答，此值为 2；RARP 请求，此值为 3；RARP 应答，此值为 4。
- 发送方硬件地址：发送方设备的硬件地址。
- 发送方 IP 地址：发送方设备的 IP 地址
- 接收方硬件地址：接收方设备的硬件地址。在 ARP 请求报文中这个域为空，在 ARP 应答报文中这个域为返回的接收方的硬件地址。
- 接收方 IP 地址：接收方设备的 IP 地址。

2.4.4 ARP 表

	IF索引	物理地址	IP地址	类型
表项1				
表项2				
表项3				
表项4				
表项5				
表项n				

图2-3 ARP 表

IF 索引：记录拥有表项中物理地址和 IP 地址的设备的物理接口或端口。

物理地址：设备的物理地址，即 MAC 地址。

IP 地址：设备的 IP 地址。

类型：该表项的类型。类型有四种可能的值。值 2 表示该表项是无效的，值 3 表示该表项是动态学习获得的，值 4 表示该表项是静态配置的，值 1 表示不是上面的任何一种情况。

2.4.5 授权 ARP 的工作机制

授权 ARP 的工作机制是 ARP 的工作机制和 DHCP 的工作机制的结合，由于目前授权 ARP 还不支持 DHCP 中继，下面将介绍 DHCP 客户端和 DHCP 服务器在同一网段的情况授权 ARP 的工作机制，具体如下：

(1) DHCP 客户端广播 DHCP_DISCOVER 报文，DHCP 服务器收到广播报文后回应 DHCP_OFFER 报文，同时在报文中携带了 DHCP 客户端的配置参数。

(2) 当网络中有多个 DHCP 服务器回应 DHCP_OFFER 报文，则 DHCP 客户端会接受最先到达的 DHCP 服务器的配置参数并向网络广播 DHCP_REQUEST 报文，该报文中携带了 DHCP 客户端的 MAC 地址和准备使用的 IP 地址。

(3) DHCP 服务器收到客户端的 DHCP_REQUEST 报文后，给 DHCP 客户端回应 DHCP_ACK 报文。同时 DHCP 服务器会在本地 ARP 表中添加一条包含了客户端 MAC 地址、IP 地址以及所在接口索引的授权 ARP 表项。

(4) 当 DHCP 服务器的 ARP 表中添加了授权 ARP 表项后，则通过 ARP Ping 机制来实现授权 ARP 表项的老化，即 ARP Ping 通过定期向授权 ARP 表项中记录的客户端 IP 地址发送 ARP 请求报文来判断该客户端是否已经下线，如果 ARP Ping 发送三次 ARP 请求报文都没有收到回应，则认为该客户端已经下线，将在 ARP 表中删除该授权表项。

(5) 为了提高安全性，授权 ARP 还提供了禁止动态学习 ARP（ARP Security）功能。当启动禁止动态学习 ARP 功能时，只有静态 ARP 表项和授权 ARP 表项可以在 DHCP 服务器的 ARP 表中被添加，动态学习的 ARP 表项不会被添加。因此，如果 DHCP 服务器同时作为代理上网的网关时，非法的固定 IP 用户就无法上网。

2.4.6 授权 ARP 配置

1. 配置准备

配置授权 ARP 前需要完成下列配置：

- 作为 DHCP 服务器的路由器已经启动了 DHCP Server 功能，并配置了地址池等相关的 DHCP 服务器参数。
- 客户端的设备配置通过为 DHCP 获取 IP 地址。

2. 配置授权 ARP

授权 ARP 的配置包括了 DHCP 服务器配置、ARP 的使能以及授权 ARP 表项老化时间的配置，以下的配置均在 DHCP 服务器端进行。

(1) 在系统视图下使能授权 ARP

表2-11 针对 DHCP 接口地址池使能授权 ARP

操作	命令	说明
进入系统视图	**system-view**	-
配置接口工作在 DHCP 服务器模式，并从接口地址池分配地址	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	必选
针对 DHCP 接口地址池使能授权 ARP	**dhcp server synchronize arp** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }	必选 缺省情况下，禁止使能授权 ARP
进入接口视图	**interface** *interface-type interface-number*	应对上面命令涉及的接口配置 IP 地址，才能创建接口地址池
配置接口 IP 地址	**ip address** *ip-address net-mask*	
配置禁止动态学习 ARP	**arp security**	可选 缺省情况使能动态学习 ARP
配置授权 ARP 表项老化时间	**arp security time-out** *seconds*	可选 缺省情况下授权 ARP 表项老化时间为 90 秒

📖 **说明：**

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式可以配置接口范围，所以可以同时在多个接口上配置 DHCP 支持授权 ARP 功能。

(2) 在接口视图下使能授权 ARP

表2-12 针对 DHCP 接口地址池使能授权 ARP

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口 IP 地址	**ip address** *ip-address net-mask*	-
配置接口工作在 DHCP 服务器模式，并从接口地址池分配地址	**dhcp select interface**	必选

操作	命令	说明
针对 DHCP 接口地址池使能授权 ARP	**dhcp server synchronize arp**	必选 缺省情况下，禁止使能授权 ARP
配置禁止动态学习 ARP	**arp security**	可选 缺省情况使能动态学习 ARP
配置授权 ARP 表项老化时间	**arp security time-out** *seconds*	可选 缺省情况下授权 ARP 表项老化时间为 90 秒

📖 **说明：**

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式是在接口视图下配置 DHCP 支持授权 ARP 功能的，适用于配置单个接口支持授权 ARP 功能。

(3) 在 DHCP 全局地址池视图下使能授权 ARP

表2-13 针对 DHCP 全局地址池使能授权 ARP

操作	命令	说明
进入系统视图	**system-view**	-
配置接口工作在 DHCP 服务器模式，并从全局地址池分配地址	**dhcp select global** [**subaddress**]	**interface** *interface-type interface-number* [**to** *interface-type interface-number*]	**all** }	必选
进入 DHCP 地址池视图	**dhcp server ip-pool** *pool-name*	必选
针对 DHCP 全局地址池使能授权 ARP	**synchronize arp**	必选 缺省情况下，禁止使能授权 ARP
退回到系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置禁止动态学习 ARP	**arp security**	可选 缺省情况使能动态学习 ARP
配置授权 ARP 表项老化时间	**arp security time-out** *seconds*	可选 缺省情况下授权 ARP 表项老化时间为 90 秒

📖 说明：

该方式适用于从 DHCP 全局地址池中给客户端分配 IP 地址的情况。

⚠ 注意：

- 只有配置了禁止动态学习 ARP 功能后，ARP Ping 机制才会启动。若 ARP Ping 机制没有启动，即使授权 ARP 表项已老化超时，也不会老化授权 ARP 表项。
- 当 ARP 表中已添加了一些授权 ARP 表项后才启动 **arp security**，则已存在的授权 ARP 表项的老化时间将被刷新。
- 若没有配置 **arp security** 命令而直接配置 **arp security time-out**，则会在配置信息中保存老化时间配置，但该老化时间并不会真正起作用。

2.4.7 授权 ARP 典型配置举例

1. 组网需求

- DHCP 客户端通过 DHCP 服务器获得 IP 地址
- 配置了 DHCP 服务器功能的路由器支持授权 ARP，授权 ARP 表项的老化时间为 120 秒。
- DHCP 服务器与客户端相连的以太网口 Ethernet1/0/0 的 IP 地址为 10.1.1.1/24，代理上网的以太网口 Ethernet1/0/1 的 IP 地址为 10.1.2.1/24。DHCP 服务器全局地址池为 10.1.1.0/24。
- DHCP 服务器同时作为代理网关服务器代理客户端访问 Internet。

2. 组网图

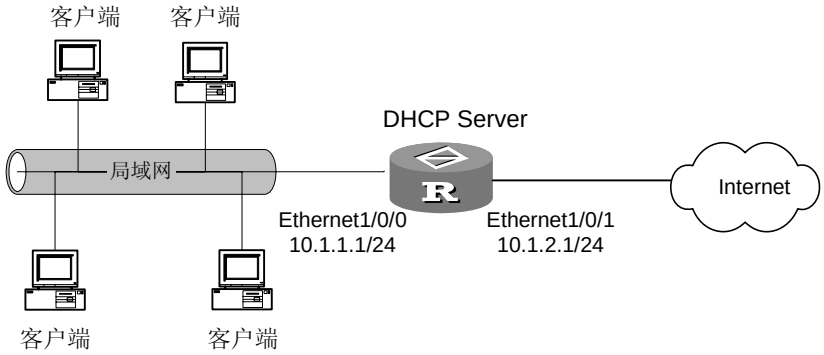


图2-4 ARP 授权组网图

3. 配置步骤

启动 DHCP 服务。

```
[H3C] dhcp enable
```

配置接口工作在 DHCP 服务器模式下，并从全局地址池中分配 IP 地址。

```
[H3C] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

配置 DHCP 服务器网络参数和地址池。

```
<H3C> system-view
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[H3C-Ethernet1/0/1] quit
[H3C] dhcp server ip-pool 0
[H3C-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

针对 DHCP 全局地址池使能授权 ARP。

```
[H3C-dhcp-pool-0] synchronize arp
[H3C-dhcp-pool-0] quit
```

禁止动态 ARP 学习，配置授权 ARP 表项的老化时间为 120 秒。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] arp security
[H3C-Ethernet1/0/0] arp security time-out 120
[H3C-Ethernet1/0/0] quit
```

第3章 域名解析（DNS）的配置

3.1 域名解析简介

TCP/IP 不仅提供了 IP 地址来确定设备，而且还专门设计了一种字符串形式的主机命名机制，这就是所谓的域名系统。此系统使用一种有层次的命名方式，为网间网上的设备指定一个有意义的名字，并且在网络上设有域名解析服务器，完成域名与 IP 地址的对应关系。这样一来用户就可以使用便于记忆的、有意义的域名，而不必去记忆晦涩难懂的 IP 地址。

域名解析分为动态解析和静态解析，二者可以相辅相成，在解析域名时，可以首先采用静态解析的方法，如果静态解析不成功，再采用动态解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

- 动态解析有专用的域名解析服务器，负责接受客户提出的域名解析请求。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域名解析服务器，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客户机。
- 静态解析即手动建立域名和 IP 地址之间的对应关系。当客户机需要域名所对应的 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。

3.2 静态域名解析的配置

3.2.1 配置静态域名解析

静态域名解析是通过静态域名解析表进行的，静态域名解析表类似于 Windows 9X 操作系统之下的 hosts 文件，路由器可以通过查询此表而获取常见域名的 IP 地址，同时用户可以使用便于记忆的主机名而不是抽象的 IP 地址来访问相应的设备。

请在系统视图下进行下列操作。

表3-1 配置主机名和对应 IP 地址

操作	命令
配置主机名和对应 IP 地址	**ip host** *hostname ip-address*
取消主机名和对应的 IP 地址	**undo ip host** *hostname* [*ip-address*]

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，后配置的 IP 地址生效。

3.2.2 域名解析表显示和调试

表3-2 域名解析表显示和调试

操作	命令
显示静态域名解析表	**display ip host**

3.3 DNS Client 配置

3.3.1 DNS 系统组成简介

由于 Internet 协议（IP）地址结构（由 32 位组成不便于记忆，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域名服务器来完成的。

域名系统（DNS）是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名字和 IP 地址之间的转换及电子邮件的选路信息。从应用上来讲，对 DNS Server 的访问是通过一个地址解析器（Resolver）来完成的。DNS Client 主要完成 Resolver 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。

一般一个 DNS 系统的工作过程为应用程序首先向 DNS Client 发出请求，DNS Client 收到请求后，首先查询本地数据库，如果发现没有，就向域名服务器发送查询报文，收到响应后再解析域名服务器发回来的响应报文，并根据响应报文的内容决定下一步的操作。

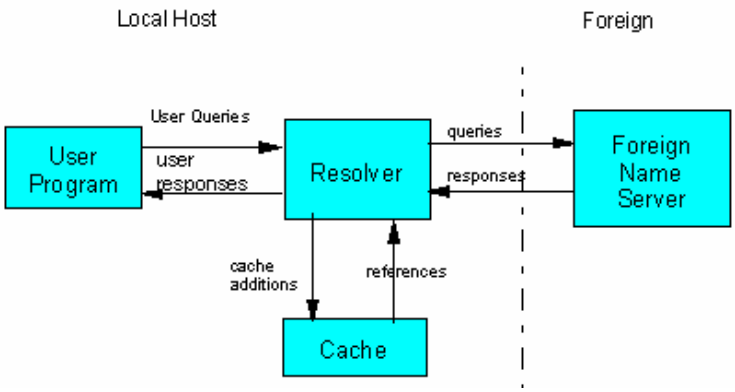


图3-1 DNS 系统组成框图

用户程序（User Program）依照自己的需要（需要域名或 IP 地址）向解析器（Resolver）发出询问，解析器首先查询本地缓冲区（Cache），如果在缓冲区中查到该映射项，则直接回复用户的请求。如果缓冲区中没有，它将根据查询的类型（需要 IP 地址还是需要域名)组织查询报文，该报文可以采用 TCP 或 UDP 格式（本程序中采用 UDP)，然后根据本机上的 DNS 配置向缺省的域名服务器发出 UDP（或 TCP）查询报文（域名服务器的端口号为 53），获得服务器的响应后，解析该响应报文并回答用户的请求。

应用程序、解析器和域名服务器以及解析器上的缓冲区关系如上图所示，其中，解析器和缓冲区集成在一起构成 DNS Client，它的作用是接受应用程序的 DNS 咨询，并对其作出应答。一般来说，“应用程序”和“域名解析器”是在同一台主机上，“域名服务器”可以和它们在同一台主机上，也可以在不同的主机上（一般情况下是在不同的主机上）。

3.3.2 DNS Client 的配置

DNS Client 的配置包括下面几个配置：

- 启动 DNS 解析
- 配置 DNS 服务器的 IP 地址
- 配置域名后缀搜索列表

其中必须的配置是启动 DNS 解析与配置 DNS 服务器的 IP 地址，如果设备上的接口使用 DHCP 客户端来分配 IP 地址，且 DHCP 服务器下发的给设备的信息中包括了 DNS 服务器的地址和域后缀搜索列表，那么只需要启动域名解析即可。

1. 启动 DNS 解析

要使用 DNS Client 功能，需要在设备上打开 DNS 解析的开关，使用下面的命令可以启动/关闭 DNS 解析。

请在系统视图下进行下面配置。

表3-3 启动/关闭 DNS 域名解析功能

操作	命令
启动 DNS 域名解析功能	**dns resolve**
关闭 DNS 域名解析功能	**undo dns resolve**

缺省情况下，关闭 DNS 域名解析功能。

2. 配置 DNS 服务器的 IP 地址

要进行 DNS 域名解析，需要知道域名服务器的地址，这样才能把查询请求报文发送到正确的服务器进行解析，使用下面的命令可以配置/删除 DNS 服务器的 IP 地址。

请在系统视图下进行下面配置。

表3-4 配置 DNS 服务器的 IP 地址

操作	命令
配置 DNS 服务器的 IP 地址	**dns server** *ip-address*
删除 DNS 服务器的 IP 地址	**undo dns server** [*ip-address*]

缺省情况下，未配置 DNS 服务器的 IP 地址。

3. 配置 DNS 域后缀搜索列表

用户在访问一些网站的时候，后缀往往都是相同的。如 sina.com.cn、h3c.com.cn、sohu.com.cn 等。

为了方便用户使用，可以设定一个 **domain** 为 com.cn，这样在用户敲入命令“ping sina”的时候，DNS 解析时会先查找字符串“sina.com.cn”对应的 IP 地址，如果没有得到回应，就发送 sina 的进行解析查找“sina”对应的 IP 地址。重复使用下面的命令可以配置域后缀搜索列表。

请在系统视图下进行下面配置。

表3-5 配置 DNS 域搜索后缀

操作	命令
配置 DNS 域搜索后缀	**dns domain** *domain-name*
删除 DNS 域搜索后缀	**undo dns domain** [*domain-name*]

📖 **说明：**

根据 RFC1034 的规定如果用户输入“ping sina.”，那么将会先查找“sina”对应的 IP 地址，如果没有回应，则会发送“sina.com.cn”对应的 IP 地址解析请求报文。

3.3.3 DNS Client 的显示和调试

1. DNS Client 的显示

请在任意视图下进行下列操作。

表3-6 DNS Client 的显示

操作	命令
查看 DNS 解析功能是否启动	**display current-configuration**
显示 DNS 服务器的配置	**display dns server** [**dynamic**]

操作	命令
显示 DNS 域后缀搜索列表的配置	**display dns domain** [**dynamic**]
显示动态的域名缓存的内容	**display dns dynamic-host**
显示 DNS 解析结果	**nslookup type** { **ptr ip-address** | **a domain-name** }

📖 **说明：**

如果使用 dynamic 参数，则显示的域名服务器是通过 DHCP 或者其它方式动态获取到的域名服务器的地址。

2. 清空动态的域名缓存的内容

在一次成功的域名解析之后，DNS Client 会把解析的结果放到缓存中。如果再有相同的域名解析请求，那么 DNS Client 会首先再缓存中查找，如果没有，再向 DNS 服务器发送域名解析请求，使用下面的命令可以清空当前缓存中的内容。

请在用户视图下进行下列操作。

表3-7 清空动态域名缓存的内容

操作	命令
清空动态的域名缓存的内容	**reset dns dynamic-host**

3. DNS Client 的调试

请在用户视图下进行下列操作。

表3-8 DNS Client 的调试

操作	命令
打开 DNS Client 调试开关	**debugging dns**
关闭 DNS Client 调试开关	**undo debugging dns**

缺省情况下，DNS Client 调试开关关闭。

3.3.4 使用 DNS 进行域名解析典型配置举例

1. 组网需求

在路由器上使用域名解析功能。路由器的 IP 地址是 10.110.10.1，DNS 服务器的 IP 地址是 10.110.66.66。

2. 组网图

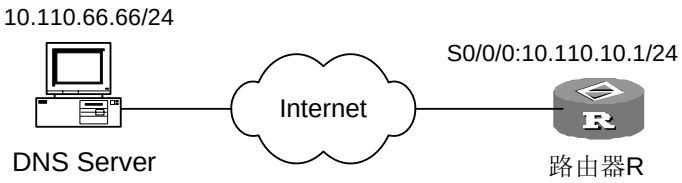


图3-2 使用 DNS Client 典型组网

3. 配置步骤

启动 DNS 域名解析功能。

```
[H3C] dns resolve
```

配置 DNS 服务器 IP 地址。

```
[H3C] dns server 10.110.66.66
```

配置 Serial0/0/0 的 IP 地址。

```
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] ip address 10.110.10.1 255.255.255.0
[H3C-Serial0/0/0] quit
```

配置到 DNS 服务器的静态路由。

```
[H3C] ip route-static 10.110.66.66 serial 0/0/0
```

3.3.5 故障诊断与排除

1. 故障之一：域名解析失败

一般情况下域名明解析失败的原因有如下几个：

(1) 软件原因

- 域名服务器的 IP 地址配置错误。
- 设备到域名服务器没有正确的路由
- 没有打开域名解析的开关

(2) 硬件原因

网络连接是否有故障，如网线折断，接口松动。

3.4 DNS Proxy 配置

3.4.1 DNS Proxy 简介

DNS Proxy 是指在作为代理网关的路由器上启动 DNS 代理功能，这样在局域网内部没有 DNS 服务器时，局域网内部客户端可以通过网关路由器连接到外部 DNS 服务器，进行正确的 DNS 解析后，可以访问 Internet。

3.4.2 DNS Proxy 的工作机制

(1) DNS 客户端将 DNS 请求报文发送给 DNS Proxy，此时请求报文的目的地址为 DNS Proxy 的 IP 地址；

(2) DNS Proxy 收到请求报文后，将报文中的目的地址替换为 DNS 服务器的 IP 地址，然后根据已配置的 DNS 服务器的地址将报文转发给 DNS 服务器。若在 DNS Proxy 上配置了多个 DNS 服务器的地址，则 DNS Proxy 先向第一个 DNS 服务器上发送请求，若第一个 DNS 服务器没有响应，则 DNS 客户端等待超时后会重新发送 DNS 请求报文，DNS Proxy 收到请求报文后向第二个 DNS 服务器转发，以此类推，直到 DNS 服务器发送响应报文为止。

(3) DNS 服务器的响应报文返回给 DNS Proxy 后，DNS Proxy 将报文中的源 IP 地址替换为 DNS Proxy 的 IP 地址后转发给 DNS 客户端。这时，DNS 客户端就可以使用 DNS 解析到的 IP 地址上网了。

3.4.3 DNS Proxy 的配置

1. 配置准备

在配置 DNS Proxy 功能前需要先进行如下配置：

- 在 DNS Proxy 上配置真实的 DNS 服务器的地址
- 在 PC 上指定 DNS Server 为使能了 DNS Proxy 的网关的 IP 地址
- 保证 DNS Proxy 与 DNS Client 及 DNS 服务器网络可达

2. 配置 DNS Proxy

DNS Proxy 功能是在作为网关的路由器上配置的。

表3-9 配置 DNS Proxy

操作	命令	说明
进入系统视图	**system-view**	-
启动 DNS 代理功能	**dns-proxy enable**	必选

3.4.4 DNS Proxy 典型配置举例

1. 组网需求

局域网内没有 DNS 服务器，要求内部 10.1.1.0/24 网段的 PC 可以通过外网的 DNS 服务器来解析域名。要求：

- 网关路由器支持 DNS Proxy；
- 外网 DNS 服务器 IP 地址为 10.72.66.36/24。

2. 组网图

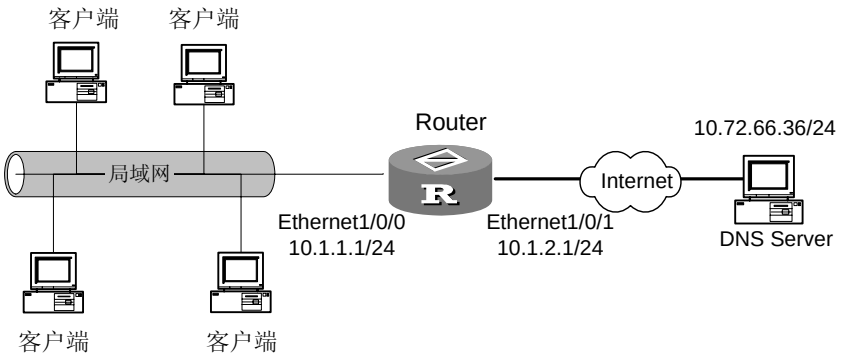


图3-3 DNS Proxy 典型配置举例

3. 配置步骤

(1) 配置路由器

配置 Ethernet 1/0/0 的 IP 地址。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet 1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置 NAT 服务，使客户端可以通过 DNS Proxy 访问 Internet。

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 10.1.1.0 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[H3C-Ethernet1/0/1] nat outbound 2000
[H3C-Ethernet1/0/1] quit
```

启动 DNS Proxy 功能。

```
[H3C] dns-proxy enable
```

配置 DNS 服务器地址。

```
[H3C] dns server 10.72.66.36
```

配置路由，保证 DNS 客户端与服务器路由可达（具体配置略）。

(2) 配置 PC

将网关及 DNS 服务器指定为 10.1.1.1。

第4章 DDNS 配置

4.1 DDNS 简介

DDNS（Dynamic Domain Name Service，动态域名服务）是建立静态域名和该域名对应主机的动态 IP 地址之间的绑定关系。

如图 图 4-1所示，服务器ServerA提供HTTP服务或者FTP服务，该服务器通过路由器连接到Internet上。当服务器ServerA是通过DHCP获取IP地址，或者该服务器通过PPPoE、PPTP或L2TP连接到Internet上时，该服务器的IP地址就是动态的，在每一次初始化连接的时候该设备的IP地址都可能改变。

因为 DNS 服务器提供的域名和 IP 地址的对应关系是静态的，不会随着服务器 IP 地址的更新而动态更新该对应关系，这样当 ServerA 的 IP 地址发生变化时，Internet 上的用户就不能通过域名访问到该服务器。

DDNS（动态域名服务）能够建立静态域名和分配给该服务器的动态 IP 地址之间的绑定关系，Internet 上的用户只要知道域名就能够进行访问服务器了。

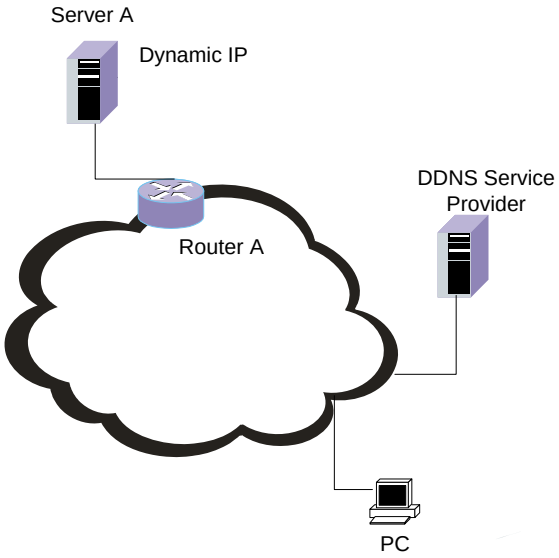


图4-1 DDNS 应用示意图

DDNS 分为如下两个方面：

- DDNS 用户侧

提供 HTTP 服务或者 FTP 服务的服务器作为 DDNS 用户侧，当 DDNS 用户侧的 IP 地址改变后，用户侧需要通过客户端程序或登录某个 HTTP 页面，通知 DDNS 服务提供商该服务器的域名和 IP 地址的对应关系已经改变。

用户一般使用 DDNS 服务提供商专门提供的客户端程序或登录某个特定的 HTTP 页面完成更新请求。更新的过程没有专门的协议，需要根据不同的 DDNS 服务提供商定制。

- DDNS 服务提供商

DDNS 服务提供商根据用户的 IP 地址更新请求，通知 DNS 服务器更新用户域名对应的 IP 地址。

H3C路由器实现了DDNS用户侧的需求，支持 www.3322.org DDNS服务提供商，当用户的IP地址改变后通知 3322.org，3322.org会通知相应的DNS服务器更新用户的域名与IP地址的对应关系。

4.2 配置 DDNS

4.2.1 配置准备

因为路由器需要访问DDNS服务提供商，需要根据域名 www.3322.org 来查找对应的IP地址，所以路由器需要获得DNS解析服务，并且确保在DNS上已经建立了域名与IP地址的对应关系。

4.2.2 配置 DDNS

表4-1 配置 DDNS

操作	命令	说明
进入系统视图	**system-view**	-
选择不同的 DDNS 服务商（目前只有 3322.org 一个服务商），并进入该 DDNS 服务商配置模式	**ddns-server 3322.org**	-
配置访问 DDNS 服务提供商的参数	请参见“4.2.3 配置访问DDNS服务提供商的参数”	必选
配置访问 DDNS 服务提供商所要更新的域名	**ddns domainname** *name*	必选
向 DDNS 服务提供商发送消息，通知 IP 地址和域名的对应关系已经改变	**ddns refresh**	必选

4.2.3 配置访问 DDNS 服务提供商的参数

表4-2 配置访问 DDNS 服务提供商的参数

操作	命令	说明
进入系统视图	**system-view**	-
选择不同的 DDNS 服务商（目前只有 3322.org 一个服务商），并进入该 DDNS 服务商配置模式	**ddns-server 3322.org**	-
配置访问 DDNS 服务提供商所使用的用户名	**ddns username** *name*	必选
配置访问 DDNS 服务提供商使用的密码	**ddns password** *password*	必选
配置访问 DDNS 服务提供商所使用的接口	**ddns source-interface** *interface-type interface-number*	必选

4.2.4 DDNS 典型配置举例

1. 组网需求

Server A通过Router A上提供的DHCP服务动态获得IP地址。ServerA为Internet上的用户提供WWW服务，使用的域名为 www.abc123.com，Internet上的用户通过该域名进行访问。

2. 组网图

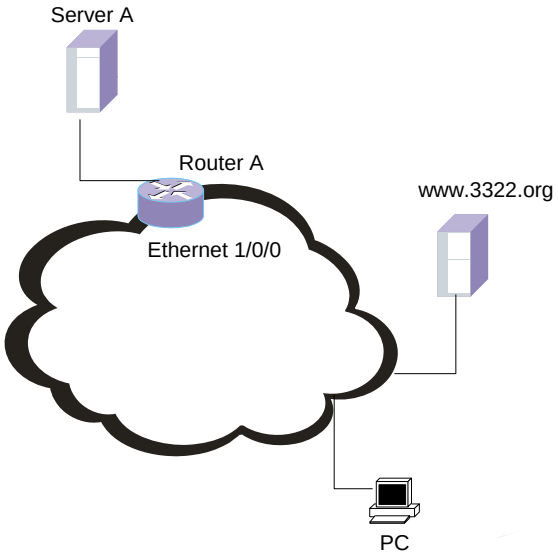


图4-2 DDNS 典型应用组网图

3. 配置步骤

进入系统视图。

```
<H3C> system-view
```

选择不同的 DDNS 服务商（目前只有 3322.org 一个服务商），并进入该 DDNS 服务商配置模式。

```
[H3C] ddns-server 3322.org
```

配置访问 DDNS 服务提供商所使用的用户名为 user。

```
[H3C-ddns-3322.org] ddns username user
```

配置访问 DDNS 服务提供商使用的密码为 pass。

```
[H3C-ddns-3322.org] ddns password pass
```

配置访问 DDNS 服务提供商所使用的接口为 Ethernet 1/0/0。

```
[H3C-ddns-3322.org] ddns source-interface ethernet 1/0/0
```

配置访问DDNS服务提供商所要更新的域名为 www.abc123.com。

```
[H3C-ddns-3322.org] ddns domainname www.abc123.com
```

向 DDNS 服务提供商发送消息，通知 IP 地址和域名的对应关系已经改变。

```
[H3C-ddns-3322.org] ddns refresh
```

第5章 URPF 配置

5.1 URPF 简介

5.1.1 URPF 基本介绍

URPF（Unicast Reverse Path Forwarding，单播反向路径查找），主要功能是用于防止基于源地址欺骗的网络攻击行为。

源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文，对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权用户以他人身份获得访问系统的目的。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。

一般的 URPF 检查有严格（Strict）型和 松散（Loose）型两种，此外，还可以支持 ACL 与缺省路由的检查。

5.1.2 URPF 处理流程

1. 首先，进行源地址合法性检查，如果报文源地址不是合法的主机地址，直接将报文丢弃。

2. 报文的源地址在路由器的 FIB 表中存在，且找到的转发表项中的出接口与该报文的入接口相同：

(1) 如果找到的转发项是缺省路由，则必须配置了 allow-default，报文才能通过，否则进入 ACL 检查流程。

(2) 如果找到的转发项不是缺省路由，则通过 URPF 检查，报文通过。

3. 报文的源地址在路由器的 FIB 表中存在，但找到的转发表项中的出接口与该报文的入接口不同：

(1) 对于 strict 型检查，直接进入 ACL 检查流程。

(2) 对于loose型检查，处理过程同 2. 。

4. 如果报文的源地址在路由器的 FIB 表中不存在，或者找到的转发项为 Blackhole 或者 Reject，则进入 ACL 检查流程。

5. ACL 检查流程：

(1) 如果配置了 ACL，则进行 ACL 过滤：

- ACL 允许通过，则报文可以通过
- ACL 不允许通过，则丢弃报文

(2) 如果没有配置 ACL，则直接丢弃报文。

📖 **说明：**

URPF 不支持快转，即在已经建立快转表的情况下，URPF 检查结果不生效，反向检查失败的报文仍然能够进行转发。

5.2 URPF 配置

请在接口视图下进行下列配置。

表5-1 使能或关闭 URPF 检查

操作	命令
使能 URPF 检查	**ip urpf** { **strict** | **loose** } [**allow-default-route**] [**acl** *acl-number*]
关闭 URPF 检查	**undo ip urpf**

缺省为关闭 URPF 检查。

5.3 URPF 的显示与调试

请在用户视图下进行下列配置。

表5-2 显示 URPF 的丢包情况

操作	命令
打开 URPF 的丢包调试开关	**debugging ip urpf discards** [**interface** *interface-type interface-num*]
关闭 URPF 的丢包调试开关	**undo debugging ip urpf discards** [**interface** *interface-type interface-num*]

第6章 IP Accounting 配置

6.1 IP Accounting 简介

IP Accounting 特性实现了对进出路由器的 IP 报文进行统计的功能，统计对象包括路由器自身发送和正常转发的 IP 报文，也包括被防火墙拒绝的 IP 报文，统计信息包括源 IP 地址和目的 IP 地址、协议号、报文个数和字节总数。根据 IP 报文是否通过防火墙、是否匹配用户配置的规则，将统计结果进行分类存储和显示。

用户配置的规则由一个 IP 地址和相应的掩码组成，规则表中记录的是 IP 地址和其掩码相“与”的结果，即网段的地址。IP 报文的源 IP 地址或目的 IP 地址中只要有一个匹配规则中的网段地址，就将该报文信息记录在“符合规则的合法报文（合法报文为未被防火墙过滤的报文）统计表（interior hash table）”中，否则就记录在“不符合规则的合法报文统计表（exterior hash table）”中；如果该 IP 报文在进出路由器接口时被此接口上配置的防火墙过滤掉了，那么就将其信息记录在“被防火墙拒绝的非法报文统计表（firewall-denied hash table）”中。

6.2 IP Accounting 配置

配置 IP Accounting 特性，首先需要配置启动该功能，然后在接口上使能统计报文的类型，这样，路由器就开始统计经过自身的 IP 报文了。

6.2.1 配置准备

需要使能统计报文的接口上已经正确配置了 IP 地址和掩码以及相应的防火墙。

6.2.2 IP Accounting 配置过程

IP Accounting 配置过程如下：

表6-1 IP Accounting 配置过程

操作	命令	说明
进入系统视图	**system-view**	-
启动 IP Count 报文统计功能	**ip count enable**	必选
设置老化时间	**ip count timeout** *minutes*	可选 缺省 720 分钟
设置匹配规则的统计表的表长	**ip count interior-threshold** *number*	可选 缺省 512

操作	命令	说明
设置不匹配规则的统计表的表长	**ip count exterior-threshold** *number*	可选 缺省为 0
添加匹配规则	**ip count rule** *ip-address net-mask*	必选 如果不配置规则，则认为任何报文都是不匹配规则的
进入接口视图	**interface** *interface-type interface-number*	必选
配置接口统计报文的类型	**ip count** [**firewall-denied**] { **inbound-packets** | **outbound-packets** }	必选
显示配置的规则信息	**display ip count rule**	**display** 命令可以在任意视图下执行
显示统计信息	**display ip count** { **inbound-packets** | **outbound-packets** } { **interior** | **exterior** | **firewall-denied** }	**display** 命令可以在任意视图下执行

⚠ 注意：

- 在接口配置了统计功能而不配置任何规则的情况下，若要统计经过路由器的 IP 报文信息，则必须设置“不符合规则的 IP 报文统计信息表（exterior）”的表长为一大于零的整数。例如，如果输入命令 **ip count exterior-threshold** *50*，则可以统计至多 50 个不同的源地址和目的地址组合的 IP 报文信息。
- 只有源地址和目的地址都相同的 IP 报文才统计在一个表项里面，对于合法的 IP 报文，这个表项下面再根据不同协议号进行细致的区分和存储，而对于非法的 IP 报文（即被防火墙拒绝的 IP 报文），则不再进行细致区分，忽略其协议信息，只记录报文个数和字节总数。
- IP Accounting 配置规则时最多可以配置 32 条。

6.2.3 IP Accounting 配置举例

1. 组网需求

路由器分别和两台主机通过以太网口连接起来，如下图所示，要求统计 PC1 到 PC2 的 IP 报文信息并且统计信息每 24 小时老化一次。

2. 组网图

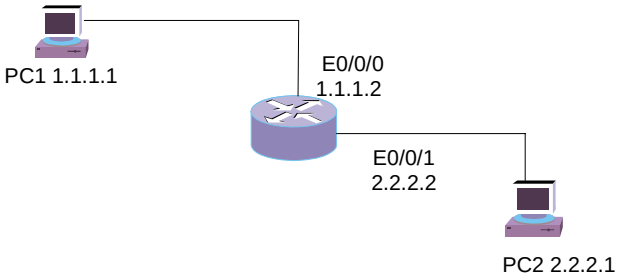


图6-1 IP Accounting 组网图

3. 配置步骤

启动 IP Accounting 统计功能。

```
[H3C] ip count enable
```

进入系统视图，配置一条匹配规则。

```
[H3C] ip count rule 1.1.1.1 24
```

配置老化时间为 1440 分钟（24 小时）。

```
[H3C] ip count timeout 1440
```

配置符合规则的统计信息表长为 100。

```
[H3C] ip count interior-threshold 100
```

配置不符合规则的统计信息表长为 20。

```
[H3C] ip count exterior-threshold 20
```

进入以太网口 0/0/0，配置 IP 地址，配置接口标志位，以统计进出的 IP 报文信息。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 1.1.1.2 24
[H3C-Ethernet0/0/0] ip count inbound-packets
[H3C-Ethernet0/0/0] ip count outbound-packets
[H3C-Ethernet0/0/0] quit
```

进入以太网口 0/0/1，配置 IP 地址。

```
[H3C] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] ip address 2.2.2.1 24
```

在 PC1 和 PC2 分别配置到对方的静态路由，并在 PC1 上执行 ping PC2 的操作。

显示统计信息。

```
[H3C] display ip count inbound-packets interior
 Inbound packets information in interior list:
  SrcIP           DstIP           Protocol  Pkts        Bytes
  1.1.1.1         2.2.2.2         ICMP      4           240
[H3C] display ip count outbound-packets interior
```

```
Outbound packets information in interior list:
 SrcIP           DstIP           Protocol  Pkts        Bytes
 2.2.2.2         1.1.1.1         ICMP      4           240
```

📖 **说明：**

可以使用路由器等其他网络设备来代替两台主机。

6.3 显示和维护

通过 **display** 命令对 IP Accounting 配置进行显示，**display** 命令可以在任意视图下执行。

表6-2 IP Accounting 配置显示和维护

配置	命令	说明
显示配置的信息	**display this**	该命令在系统视图和接口视图执行，可以看到用户配置的命令
显示用户配置的规则	**display ip count rule**	该命令可以在任意视图执行
显示统计信息	**display ip count { inbound-packets | outbound-packets } { interior | exterior | firewall-denied }**	该命令可以在任意视图执行

6.4 常见配置错误

- 在配置 interior 统计表和 exterior 统计表时，如果此时表中的表项数目已经大于用户设置或默认的数值时，需要先清空相应的统计信息表再进行配置。
- 统计信息表中存放的是用户配置后的报文信息，如果用户配置一条规则以后，原来不符合此规则的报文开始符合规则，从此之后，所有该地址的报文都被存放到 interior 统计表中，而 exterior 表中可能还有该地址的 IP 报文信息，只不过都是用户配置之前的统计信息。老化时间过后，这些表项就会被删除掉。

第7章 UDP HELPER 配置

7.1 UDP HELPER 简介

UDP HELPER 的主要功能是实现对指定 UDP 广播报文的中继转发，即它能将 UDP 广播报文转成单播报文发送给指定的服务器，起到一个中继的作用。

在启动 UDP HELPER 后，如果端口接收到 UDP 广播报文，则根据报文的 UDP 端口号来判断是否要对该报文进行中继转发，如果需要转发，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，将报文送给上层模块处理。对于 BOOTP/DHCP 广播报文的中继，如果客户端在请求报文中指明需要以广播报文的形式接收响应报文，则系统将以广播的方式向客户端发送响应报文；否则将以单播的方式向客户端发送响应报文。

7.2 UDP HELPER 配置

UDP HELPER 配置包括：

- 启动/关闭 UDP 中继转发功能
- 配置需要中继转发的 UDP 端口
- 配置广播报文中继转发的目的服务器

7.2.1 启动/关闭 UDP 中继转发功能

可以使用下面的命令启动/关闭 UDP 中继转发功能。当启动该功能后，用户就可以配置需要中继转发的 UDP 端口。在启动的同时，69、53、37、137、138、49 这六个默认的 UDP 端口的广播报文转发功能会被启动。当关闭该功能后，所有已配置的 UDP 端口都被取消，包括默认端口。

请在系统视图下进行下列配置。

表7-1 启动/关闭 UDP 中继转发功能

操作	命令
启动 UDP 中继转发功能	**udp-helper enable**
关闭 UDP 中继转发功能	**undo udp-helper enable**

缺省情况下，UDP 中继转发处于关闭状态。

7.2.2 配置需要中继转发的 UDP 端口

可以使用下面的命令配置需要中继转发的 UDP 端口。当启动 UDP 中继转发功能后，系统默认支持中继转发下面协议端口的广播报文，即这些默认 UDP 端口的广播报文会被单播转发到相应的目的服务器。系统最多支持配置 256 个需要中继转发的 UDP 端口。

表7-2 默认 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 Server)	137
NetBIOS-DS (NetBIOS Datagram Server)	138
TACACS (Terminal Access Controller Access Control System)	49

请在系统视图下进行下列配置。

表7-3 配置/删除需要中继转发的 UDP 端口

操作	命令
配置需要中继转发的 UDP 端口	**udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }
删除需要中继转发的 UDP 端口	**undo udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

需要注意的是：

- 只有先启动 UDP 中继转发功能后，才能配置需要中继转发的 UDP 端口。否则，将会有错误提示信息。
- 参数 **dns|netbios-ds|netbios-ns|tacacs|tftp|time** 指 6 个默认端口。对默认端口可以有两种配置方法：(1) 指定端口号配置；(2) 指定参数配置。例如：**udp-helper port** *53* 和 **udp-helper port dns** 的效果是一样的。
- 在用 **display current-configuration** 命令显示配置信息时，默认端口号是不显示的，只有当取消了一个默认端口的中继转发功能，该端口号才显示出来。

7.2.3 配置广播报文中继转发的目的服务器

可以使用下面的命令在以太网接口上配置广播报文被中继转发到的目的服务器。一个以太网接口最多对应 20 个目的服务器。在启动 UDP 中继转发功能，且在某个以

太网接口上配置了目的服务器后，则从该以太网接口接收的指定 UDP 端口的广播报文都被单播发送到以太网接口对应的目的服务器。

请在以太网接口视图下进行下列配置。

表7-4 配置/删除广播报文中继转发的目的服务器

操作	命令
配置广播报文中继转发的目的服务器	**udp-helper server** *ip-address*
删除广播报文中继转发的目的服务器	**undo udp-helper server** [*ip-address*]

缺省情况下，没有配置目的服务器。

7.3 UDP HELPER 的显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 UDP HELPER 的目的服务器，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **debugging** 命令对 UDP HELPER 进行调试。

表7-5 UDP HELPER 的显示和调试

操作	命令
显示以太网接口对应的目的服务器信息	**display udp-helper server** [**interface** *number*]
打开 UDP HELPER 的调试开关	**debugging udp-helper** { **event** | **packet** [**receive** | **send**] }
关闭 UDP HELPER 的调试开关	**undo debugging udp-helper** { **event** | **packet** [**receive** | **send**] }

第8章 BOOTP 客户端配置

8.1 BOOTP 客户端简介

BOOTP 客户端可以使用 BOOTP 协议向服务器请求分配一个 IP 地址。BOOTP 客户端主要包含两个过程：

- 向服务器发送 BOOTP 请求报文
- 处理服务器返回的 BOOTP 响应报文

BOOTP 客户端在使用 BOOTP 协议获取 IP 地址时，先向服务器发送 BOOTP 请求报文，服务器接收到请求报文后，将返回 BOOTP 响应报文。BOOTP 客户端从接收到响应报文中即可获取所分配到的 IP 地址。

BOOTP 协议报文是基于 UDP 的，为了保证报文的可靠传输，采取超时重传机制。BOOTP 客户端在向服务器发送请求报文时，同时启动一个重发定时器。若该定时器超时仍未收到服务器返回的响应报文，则要重传请求报文。重传报文每隔五秒重传一次，报文最多能传送三次，传送三次之后还不成功就不再重传报文。

8.2 BOOTP 客户端配置

BOOTP 客户端配置包括：

- 配置以太网接口通过 BOOTP 协议获取 IP 地址

8.2.1 配置以太网接口通过 BOOTP 协议获取 IP 地址

可以使用下面的命令配置以太网接口的 IP 地址通过 BOOTP 协议获取。

请在以太网接口视图下进行下列配置。

表8-1 配置以太网接口通过 BOOTP 协议获取 IP 地址

操作	命令
配置以太网接口通过BOOTP协议获取IP地址	**ip address bootp-alloc**
取消以太网接口通过BOOTP协议获取IP地址	**undo ip address bootp-alloc**

缺省情况下，以太网接口不通过 BOOTP 协议获取 IP 地址。

8.3 BOOTP 客户端的显示及调试

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

表8-2 BOOTP 客户端的显示及调试

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

第9章 DHCP 配置

9.1 DHCP 简介

9.1.1 DHCP 介绍

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。

与 BOOTP 相比，DHCP 也采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息，两种协议的报文都采用 UDP 进行封装，并使用基本相同的报文结构。

BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。

DHCP 从两方面对 BOOTP 进行了扩展：DHCP 可使计算机仅用一个消息就获取它所需要的所有配置信息；DHCP 允许计算机快速、动态地获取 IP 地址，而不是静态为每台主机指定地址。

9.1.2 DHCP 的 IP 地址分配

(1) IP 地址分配策略

对于 IP 地址的占用时间，不同主机有不同的需求：对于服务器，可能需要长期使用固定的 IP 地址；对于某些主机，可能需要长期使用某个动态分配的 IP 地址；而某些个人则可能只在需要时分配一个临时的 IP 地址就可以了。

针对这些不同的需求，DHCP 服务器提供三种 IP 地址分配策略：

- 手工分配地址：由管理员为少数特定主机（如 WWW 服务器等）配置固定的 IP 地址。
- 自动分配地址：为首次连接到网络的某些主机分配固定 IP 地址，该地址将长期由该主机使用。
- 动态分配地址：以“租借”的方式将某个地址分配给客户端主机，使用期限到期后，客户端需要重新申请地址。大多数客户端主机得到的是这种动态分配的地址。

(2) IP 地址分配的优先次序

DHCP 服务器按照如下次序为客户端选择 IP 地址：

- DHCP 服务器的数据库中与客户端 MAC 地址静态绑定的 IP 地址；
- 客户端以前曾经使用过的 IP 地址，即客户端发送的 DHCP-REQUEST 报文中请求 IP 地址选项（Requested IP Addr Option）的地址；
- 在 DHCP 地址池中，顺序查找可供分配的 IP 地址，最先找到的 IP 地址；
- 如果未找到可用的 IP 地址，则依次查询超过租期、发生冲突的 IP 地址，如果找到则进行分配，否则报告错误。

9.2 DHCP 服务器介绍

9.2.1 DHCP 服务器的应用环境

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。大量用户必须通过 DHCP 服务动态获得自己的 IP 地址，而且，对并发用户的数目也有限制。
- 网络中具有固定 IP 地址的主机比较少，大部分主机可以不使用固定的 IP 地址。

9.2.2 DHCP 服务器的基本原理

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如下图所示：

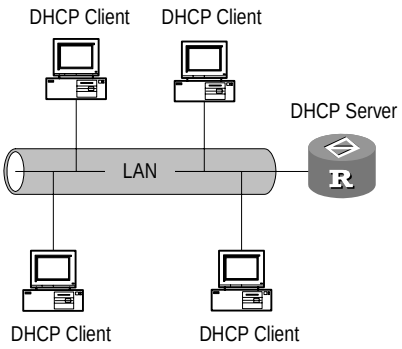


图9-1 DHCP 服务器典型组网应用

DHCP 客户端为了获取合法的动态 IP 地址，在不同阶段与服务器之间交互不同的信息，通常存在以下三种模式：

(1) DHCP 客户端首次登录网络

DHCP 客户端首次登录网络时，主要通过四个阶段与 DHCP 服务器建立联系。

- 发现阶段，即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCP_Discover 报文，只有 DHCP 服务器才会进行响应。
- 提供阶段，即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCP_Discover 报文后，从 IP 地址池中挑选一个尚未分配的 IP 地址分配给客户端，向该客户端发送包含出租 IP 地址和其它设置的 DHCP_Offer 报文。服务器在发送 DHCP_Offer 报文之前，会以广播的方式发送 ARP 报文进行地址探测，以保证发送给客户端的 IP 地址的唯一性。
- 选择阶段，即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP_Offer 报文，客户端只接受第一个收到的 DHCP_Offer 报文，然后以广播方式向各 DHCP 服务器回应 DHCP_Request 报文，该信息中包含 DHCP 服务器在 DHCP_Offer 报文中分配的 IP 地址。
- 确认阶段，即 DHCP 客户端确认所提供 IP 地址的阶段。客户端收到 DHCP_ACK 确认报文后，广播目的地址是被分配地址的 ARP 报文，如果在规定的时间内没有收到回应，客户端才使用此地址。

除 DHCP 客户端选中的服务器外，其它 DHCP 服务器本次未分配出的 IP 地址仍可用于其他客户端的 IP 地址申请。

(2) DHCP 客户端再次登录网络

当DHCP客户端再次登录网络时，主要通过以下几个步骤与DHCP服务器建立联系。

- DHCP 客户端首次正确登录网络后，以后再登录网络时，只需要广播包含上次分配 IP 地址的 DHCP_Request 报文即可，不需要再次发送 DHCP_Discover 报文。
- DHCP 服务器收到 DHCP_Request 报文后，如果客户端申请的地址没有被分配，则返回 DHCP_ACK 确认报文，通知该 DHCP 客户端继续使用原来的 IP 地址。
- 如果此 IP 地址无法再分配给该 DHCP 客户端使用（例如已分配给其它客户端），DHCP 服务器将返回 DHCP_NAK 报文。客户端收到后，重新发送 DHCP_Discover 报文请求新的 IP 地址。

(3) DHCP 客户端延长 IP 地址的租用有效期

DHCP 服务器分配给客户端的动态 IP 地址通常有一定的租借期限，期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 租约（如延长 IP 地址租约）。

实际使用中，在 DHCP 客户端启动或 IP 地址租约期限达到一半时，DHCP 客户端会自动向 DHCP 服务器发送 DHCP_Request 报文，以完成 IP 租约的更新。如果此

IP 地址有效，则 DHCP 服务器回应 DHCP_ACK 报文，通知 DHCP 客户端已经获得新 IP 租约。

(4) 在 PC 机上的配置（以 Window 操作系统为例）

在用户 PC 机（即 DHCP 客户端）的 DOS 环境下使用 **ipconfig /release** 命令或在图形界面下执行［winipcfg /释放］来主动释放 IP 地址，此时，用户 PC 机向 DHCP 服务器发送 DHCP_Release 报文。然后，在用户 PC 机的 DOS 环境下使用 **ipconfig /renew** 命令或在图形界面下执行［winipcfg /更新］来申请新的 IP 地址，此时，用户 PC 机向 DHCP 服务器发送 DHCP_Discover 报文。

在用户 PC 机（DHCP 客户端）上也可以使用 **ipconfig/renew** 命令或在图形界面下执行［winipcfg/更新］来更新其 IP 地址租约。

上述几个过程在下面的 DHCP 客户端状态迁移图中有完整体现：

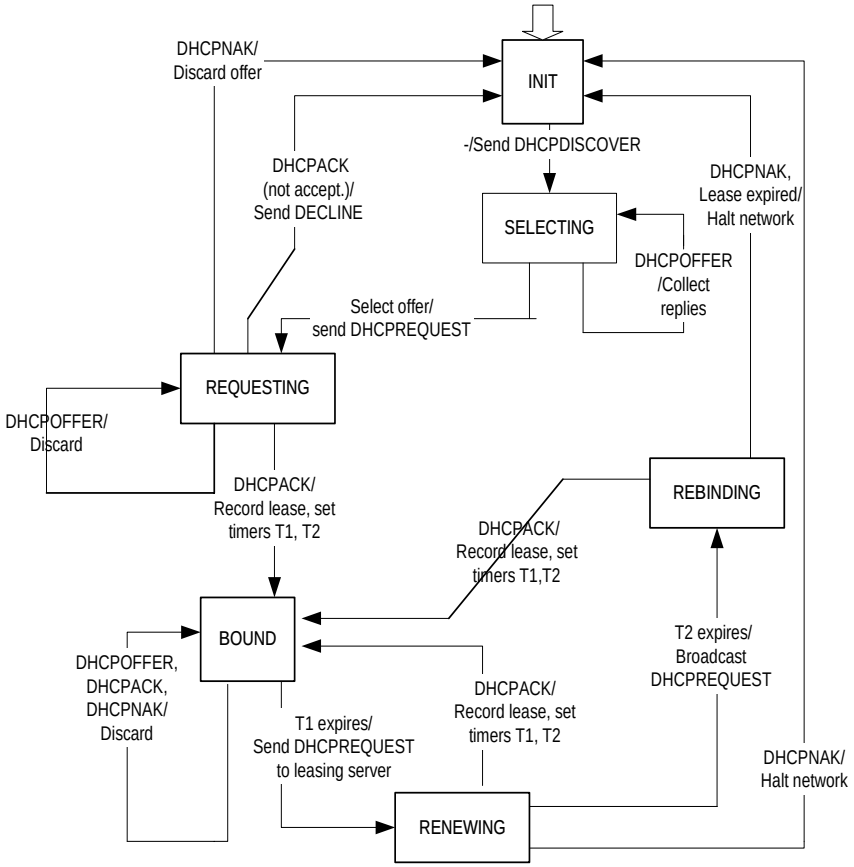


图9-2 DHCP 客户端状态迁移图

9.2.3 DHCP Accounting 简介

DHCP Accounting 又称为 DHCP 计费，是指 DHCP 服务器在分配和释放租约时，通知 RADIUS 服务器开始计费或停止计费。DHCP 服务器与 RADIUS 服务器配合使用，实现了网络计费功能，同时也在一定程度上保障了网络的安全性。

1. DHCP Accouting 报文结构

在 DHCP 服务器与 RADIUS 服务器进行交互主要是通过发送 Accounting start 和 Accounting stop 请求报文来进行的，这两种报文结构的结构大致相同，只是在 Attribute 字段稍有差别，报文结构如下：

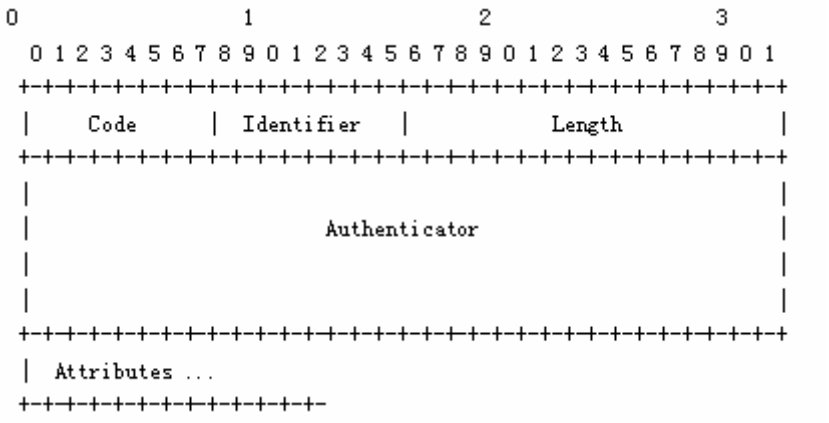


图9-3 Accounting 报文结构

- Code：Code 字段在报文中占用一个字节，用来表示 RADIUS 报文的类型。当收到的报文的 Code 字段非法时，该报文将会被丢弃。Code 值为 4 时表示是 Accounting start 报文，为 5 时表示是 Accounting stop 报文。
- Identifier：Identifier 字段在报文中占用一个字节，用来匹配请求和回应报文，RADIUS 服务器可以通过这个字段来检测从同一个客户端的相同 IP 地址和 UDP 端口发来的重复请求。
- Length：Length 字段在报文中占用两个字节，标识了整个 Accounting 报文的长度。
- Authenticator：Authenticator 字段在报文中占用 16 个字节。用来识别客户端和 RADIUS 计费服务器之间的信息。

2. DHCP Accounting 的工作机制

在运行 DHCP Server 功能的路由器上配置好 AAA 认证和 RADIUS，则 DHCP Server 作为 RADIUS 的客户端。对于 DHCP Server 作为 RADIUS 客户端的认证过程，请参考“安全/RADIUS 协议概述”部分，这里将指介绍 DHCP Server 与 RADIUS Server 的计费交互过程。

- DHCP 服务器通过 DHCP ACK 报文将 IP 配置信息发送给 DHCP 客户端后，会发送 Accounting start 请求报文给指定的 RADIUS 服务器，RADIUS 服务器将对 Accounting start 请求进行相应的处理，并进行记录。同时 RADIUS 服务器给 DHCP 服务器发送回应报文。

- 当由于某种原因，DHCP 服务器的租约被释放后，DHCP 服务器将立刻发送 Accounting stop 请求报文通知 RADIUS 服务器停止记录，然后 RADIUS 服务器对 Accounting stop 报文进行相应的处理并停止记录。同时 RADIUS 服务器给 DHCP 服务器发送回应报文。释放租约的原因有：租约过期、收到用户的 release 请求、手工删除租约、手工删除地址池等。
- 若由于种种原因，指定域的 RADIUS 服务器不可达，则 Accounting start 报文将在一定的时间间隔发送三次，若三次后仍没有收到正确的相应报文，则不再发送 Accounting start 报文。

9.2.4 DHCP 服务器支持 option 82 简介

option 82 是 DHCP 报文中的中继代理信息选项的一种。当 DHCP Client 发送请求报文到 DHCP Server 时，若需要经过 DHCP Relay，则由 DHCP Relay 将 Option 82 添加到请求报文中。option 82 包含很多 sub-option，目前 DHCP Server 只仅支持 option 82 中的 sub-option 5。即在当 DHCP Relay 在 option 82 的 sub-option 5 中添加某一网段的 IP 地址时，DHCP Server 端则可能根据 option 82 为用户分配地址或配置信息。

1. option 82 概念介绍

(1) options

DHCP 报文中的“选项”字段，该字段为可变长字段，包含部分租约信息、报文类型等。Options 字段最多可以包括 255 个 option，最少为 1 个 option。

(2) option 82

option 82 又称为中继代理信息选项（Relay Agent Information Option），是 DHCP 报文中 options 字段的一部分。在 RFC3046 中规定，option 82 的位置在 option 255 之前而在其他 option 之后。option 82 中最多可以包含 255 个 sub-option。若定义了 option 82，则至少要定义一个 sub-option。目前 option 82 中常用的 sub-option 有 sub-option 1、sub-option 2 和 sub-option 5。

(3) sub-option 1

sub-option 1 为代理电路 ID（即 Circuit ID）子项，是 option 82 的一个子选项。该子选项定义了在传输报文的时候要携带 DHCP 客户端所连接交换机端口的 VLAN-ID 及端口的 MAC 地址，通常在 DHCP 中继设备上配置。

通常 sub-option 1 与 sub-option 2 子选项要共同使用来标识 DHCP 源端的信息。

(4) sub-option 2

sub-option 2 为代理远程 ID（即 Remote ID）子项，也是 option 82 的一个子选项。该子选项定义了在传输报文的时候要携带中继设备的 MAC 地址信息，通常也在 DHCP 中继设备上配置。

通常 sub-option 1 与 sub-option 2 子选项要共同使用来标识 DHCP 源端的信息。

(5) sub-option 5

sub-option 5 为链路选择（Link Selection）子项，也是 option 82 的一个子选项。该选项中包含了 DHCP 中继添加的 IP 地址。这样 DHCP 服务器在分配 IP 地址给 DHCP 客户端的时候就可以分配与该地址同网段的 IP 地址。

🕮 **说明：**

目前我们的 DHCP 只实现了 option 82 的部分功能，即 DHCP 服务器仅支持 option 82 的 sub-option 5，DHCP 中继仅支持 option 82 的 sub-option1 和 sub-option2。

---

2. DHCP 服务器支持 option 82 工作机制

DHCP Server 支持 option 82 的 sub-option 5 的工作机制如下：

- 在有 DHCP Relay 的网络中，DHCP Relay 将 DHCP 客户端广播的 DHCP 请求报文发送给 DHCP Server；
- DHCP Server 收到 DHCP Relay 转发的请求报文后判断报文中是否有 DHCP Relay 添加的 option 82 的 sub-option 5，如果有则 DHCP Server 将查找本地地址池，并为 DHCP Client 分配与 sub-option 5 中的 IP 地址在同一网段的 IP 地址。然后 DHCP Server 在回应报文中回应 option 82；
- DHCP Relay 收到 DHCP Server 的回应报文后剥离 option 82 选项后转发给 DHCP Client。

3. 协议规范

与 DHCP Server 支持 option 82 相关的协议有：

- RFC2131 Dynamic Host Configuration Protocol
- RFC3527 Link Selection sub-option

9.2.5 DHCP 服务器支持 BIMS option 简介

DHCP 服务器支持 BIMS option 是指 DHCP 服务器在给 DHCP 客户端分配 IP 地址的同时将 BIMS（Branch Intelligent Management System） 服务器的信息也同时告知 DHCP 客户端，使 DHCP 客户端在得到 IP 地址后能够通过 BIMS 服务器进行软件备份和升级。BIMS option 的 option 号为 217。

1. BIMS option 的报文结构

BIMS option 是在 DHCP 服务器给 DHCP 客户端的回应报文的 options 字段中添加的，由于不同厂商的 DHCP 客户端对 DHCP 回应报文的处理机制不同，因此 DHCP 服务器在 DHCP_OFFER 和 DHCP_ACK 报文中都将携带 BIMS option 选项。BIMS option 报文结构如下：

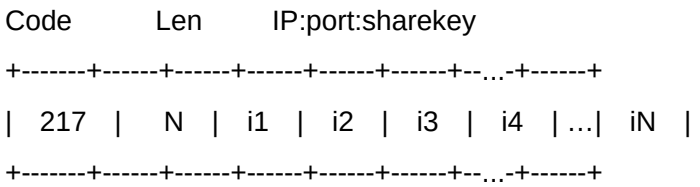


图9-4 BIMS option（option 217）报文结构

BIMS option 报文的结构与其他 option 报文的结构基本相同，也包含了 Code 和 Len 字段用来标识 option 的序号和 option 报文的长度。

i1～iN 字段主要用来携带 BIMS 服务器的 IP 地址、协议端口号以及 BIMS Server 的共享密钥。在该字段由字符串组成，例如 BIMS 服务器的 IP 地址为 192.168.1.1，端口号为 80，共享密钥为 abcdefg，则在 i 字段中表示为 192.168.1.1.80.abcdefg。

2. DHCP 服务器支持 BIMS option 工作机制

(1) DHCP 客户端向 DHCP 服务器发送请求报文申请 IP 地址以及配置参数。

(2) DHCP 服务器端收到请求报文后，查看本地配置的地址池，DHCP 服务器可以在全局地址池及接口地址池启动 BIMS option，若将要分配地址的地址池启动了 BIMS option，则 DHCP 服务器将在回应报文中除携带分配给客户端的 IP 配置信息外，还将携带 BIMS 服务器的 IP 地址、协议端口号以及共享密钥。

(3) DHCP 客户端收到服务器带有 BIMS option 的回应报文后解析出 option 中的 BIMS 服务器 IP 地址、协议端口号以及共享密钥。客户端获得 BIMS 服务器的信息后就向 BIMS 服务器定期发送连接请求，以便通过 BIMS 服务器进行软件的备份和升级。

9.2.6 DHCP 服务器支持 option184 简介

option 184 是 RFC 中规定的保留选项，用户可以自定义该选项中携带的信息。因此 3COM 使用该选项定义了四个私有的子选项，从而使 DHCP 服务器可以在回应 DHCP 客户端的请求时携带 DHCP 客户端需要的信息。option 184 中包含的子选项主要是携带了语音方面的信息，其子选项号和携带的信息具体如下：

- sub-option 1：NCP-IP（Network Call Processor IP Address），网络呼叫处理器 IP 地址。

- sub-option 2：AS-IP（Alternate Server IP Address），备选 NCP 服务器的 IP 地址。
- sub-option 3：Voice VLAN Configuration，语音 VLAN 配置。
- sub-option 4：Fail-Over Call Routing，Failover 呼叫路由。

1. option 184 中各子选项的含义

- NCP-IP

NCP-IP 子选项携带了 NCP（Network Call Processor，网络呼叫处理器）的 IP 地址。在 option 184 中若使用该子选项，必须将其作为第一个子选项（sub-option 1）。

option 184 的 sub-option 1 子选项携带的 NCP-IP 地址可以标识作为网络呼叫控制源的服务器及应用程序下载服务器。

- AS-IP

AS-IP 子选项携带了 AS（Alternate Server，备选服务器）的 IP 地址，该子选项为 option 184 的第二个子选项（sub-option 2）。只有定义了 sub-option 1，即只有定义了 NCP-IP 子选项，AS-IP 子选项才能生效。

option 184 中的 sub-option 2 子选项携带了备选 NCP 服务器的 IP 地址，用来作为 NCP-IP 的备份。当 NCP-IP 中携带的地址不可达或不合法时，才使用该选项指定的 NCP 服务器。

- Voice VLAN Configuration

Voice VLAN Configuration 子选项携带了语音 VLAN 是否使能的标记以及 VLAN ID，该子选项为 option 184 的第三个子选项（sub-option 3）。

option 184 的 sub-option 3 子选项共由两部分组成：一部分携带了语音 VLAN 识别是否使能的标记，另一部分携带了语音 VLAN 的 ID 信息。当语音 VLAN 使能域标记为 0 时，则表示没有使能语音 VLAN 识别功能，即使 VLAN ID 域中指定了语音 VLAN ID，也将忽略该 VLAN ID 信息；当语音 VLAN 使能域标记为 1 时，表示使能语音 VLAN 识别功能。

- Fail-Over Call Routing

Fail-Over Call Routing 子选项携带了 Failover 呼叫路由的 IP 地址及其关联的拨号串，该子选项为 option 184 的第四个子选项（sub-option 4）。

option 184 的 sub-option 4 子选项中的 Fail-Over 呼叫路由的 IP 地址和拨号串就是 SIP（Session Initiation Protocol，会话初始化协议）用户之间互相通信时对端的 IP 地址和呼叫号码。当 NCP 服务器不可达时，SIP 用户可以使用已配置的对端 IP 地址及呼叫号码直接与对端 SIP 用户建立连接并通信。

说明：

DHCP 服务器添加 option 184 的 sub-option 时，添加 sub-option 2、sub-option 3 或 sub-option 4 前必须先添加 sub-option 1 子选项，否则后面的子选项将无效。

2. DHCP 服务器支持 option 184 的工作机制

DHCP 服务器携带的 option 184 信息是添加在服务器给 DHCP 客户端的回应报文中。下面假设 DHCP 客户端与 DHCP 服务器在同一网段，DHCP 服务器支持 option 184 的工作机制如下：

(1) DHCP 客户端向 DHCP 服务器发送请求报文，请求报文中携带 option 184 选项，该选项中指明了请求 option 184 的配置参数。

(2) DHCP 服务器查看请求报文中的请求列表，然后在回应报文的 options 字段中添加 option 184 及相应的 sub-option 后返回给 DHCP 客户端。

说明：

只有 DHCP 客户端在请求报文的 option 55 选项中指明要求回应 option 184 选项，DHCP 服务器才会回应 option 184。

9.2.7 广域网口支持 DHCP 地址分配

传统的 DHCP 客户端功能只能在以太网接口上实现，但现在已经实现了在封装类型为 PPP、HDLC 以及帧中继的广域网接口上实现 DHCP Server/DHCP Relay/DHCP Client 功能。支持 DHCP 的广域网口目前包括同/异步串口、E1 接口。

下面将根据链路层封装的协议类型来分别介绍 DHCP Server 与 DHCP Client 之间的工作流程。

1. 在封装 PPP 的广域网接口上启用 DHCP 地址分配

当接口封装 PPP 并启动了 DHCP 后，将先进行 PPP 协议的协商，当 PPP 模块协商成功后再进行 DHCP 报文的交互，具体过程如下：

(1) 在 PPP 链路 LCP 协商成功后，本端（DHCP Client）向对端（DHCP Server）发送 DHCP-Discover 请求报文，此时 DHCP Server 丢弃此请求报文。

(2) 在IPCP协商阶段，本端使用本设备其它接口的IP地址或全 0 地址与对端进行IPCP协商，IPCP协商成功后，DHCP Client通过PPP链路以广播形式发送DHCP请求报文，其地址分配过程请参见 9.2.2 DHCP服务器的基本原理。

(3) 获得了 IP 地址的 DHCP 客户端将 IP 地址填充到相应的广域网接口，并通知 PPP 模块本端地址发生了变化，然后本端 PPP 模块重新进行 IPCP 协商以通知对端 IP 地址的变化。

2. 在封装为帧中继的广域网接口上启用 DHCP 地址分配

帧中继链路上的 DHCP 工作流程与以太网基本相同，其区别如下：

因一个帧中继接口上可能有多个逻辑通道，所以当帧中继接口作为 DHCP Client 申请 IP 地址的时候：

- 若帧中继接口配置为允许动态地址映射，则 DHCP Client 可以直接广播 DHCP 请求报文，从而可以进行正常的 DHCP 协商并获得 IP 地址；
- 若帧中继接口配置为静态地址映射，则必须同时配置 **broadcast** 关键字，使 DHCP 请求报文可以通过多条逻辑通道进行广播，从而获得 IP 地址。

3. 在封装为 HDLC 的广域网接口上启用 DHCP 地址分配

当链路协议封装为 HDLC 时，作为 DHCP Client 的一端发起 DHCP 请求后，DHCP Server 可以直接为其分配 IP 地址。

9.3 DHCP 中继介绍

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，不能跨网段。因此，为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能（DHCP Relay）的引入解决了这一难题：局域网内的客户端可以通过 DHCP 中继与其他子网的 DHCP 服务器通信，最终取得合法的 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

一般来说，DHCP 中继可以是主机，也可以是路由器，只要对它启动 DHCP 中继代理的服务程序即可。

9.3.1 DHCP 中继的基本原理

下图是 DHCP 中继的典型应用示意图。

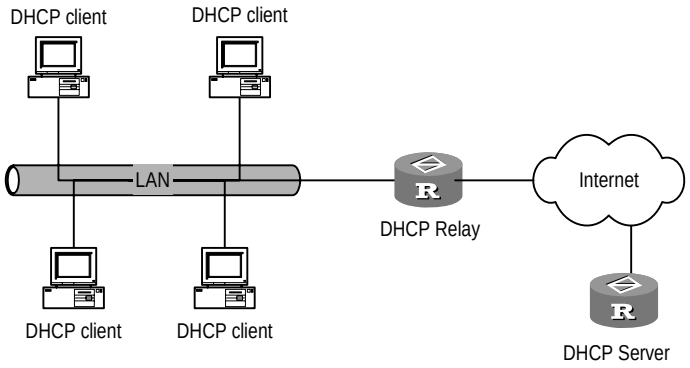


图9-5 DHCP 中继的典型组网应用

工作原理如下：

- 当 DHCP 客户端启动并进行 DHCP 初始化时，它在本地网络广播配置请求报文。
- 如果本地网络存在 DHCP 服务器，则可以直接进行 DHCP 配置，不需要 DHCP 中继；
- 如果本地网络没有 DHCP 服务器，则与本网络相连的、带 DHCP 中继功能的网络设备收到该广播报文后，进行适当处理并转发给指定的、其它网络上的 DHCP 服务器。
- DHCP 服务器根据客户端提供的信息进行相应的配置，并通过 DHCP 中继将配置信息发送给客户端，完成对客户端的动态配置。事实上，从开始配置到最终完成配置，可能存在多次这样的交互过程。

DHCP 中继提供了对 DHCP 广播报文的透明传输功能，能够把 DHCP 客户端（或服务器）的广播报文透明地传送到其它网段的 DHCP 服务器（或客户端）上。

在实际网络环境中，DHCP 中继功能一般是在路由器某个具体的接口上实现的。这时需要为该接口配置 IP 中继地址，用来指定 DHCP 服务器。

9.3.2 DHCP 中继支持 option 82 概述

option 82 是 DHCP 报文中的中继代理信息选项（Relay Agent Information Option）。当 DHCP 客户端发送请求报文到 DHCP 服务器时，若经过了 DHCP 中继，则 DHCP 中继可以对报文中的 option 82 选项字段进行处理，如：丢弃、用中继设备本身生成的 option 82 选项替代报文中原有的 option 82 选项或保持设备原有的 option 82 选项等。

option 82 包含很多 sub-option，目前我们的 DHCP 中继仅支持 sub-option 1 和 sub-option 2。

option 82 实现了 DHCP 客户端和 DHCP 中继设备的地址信息（如 MAC 地址、VLANID 等）在 DHCP 服务器上的记录，与其他软件配合使用可以实现 DHCP 分配的限制和计费功能。

1. DHCP 中继支持 option 82 工作机制

DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取 IP 地址的过程与 DHCP 客户端直接从 DHCP 服务器获取 IP 地址的过程完全相同，都要经历发现、提供、选择和确认四个阶段，详细的过程请参考本手册“网络层协议”的 DHCP 部分。这里将只介绍 DHCP 中继支持 option 82 时的工作机制，具体如下：

- DHCP 客户端在初始化时以广播的形式发送请求报文；
- 若本地网络没有 DHCP 服务器，则与本网络相连的 DHCP 中继设备接收到该广播报文后检查报文中是否已有 option 82 选项，如果报文中已有 option 82，则按照配置的策略对该报文进行处理（如：丢弃、用中继设备本身的 option 82 项替代报文中原有的 option 82 项或保持设备原有的 option 82 项等），然后将请求报文转发给 DHCP 服务器；若请求报文中没有 option 82 选项，则 DHCP 中继设备将 option 82 选项添加到报文中后转发给 DHCP 服务器。此时，请求报文中将包含了 DHCP 客户端所连接的交换机端口的 MAC 地址、所属的 VLAN 以及 DHCP 中继设备本身的 MAC 地址；
- DHCP 服务器收到 DHCP 中继设备转发的 DHCP 请求报文后，将记录报文中 option 选项所携带的信息，然后将带着 DHCP 配置信息以及 option 82 信息的报文回应给 DHCP 中继；
- DHCP 中继收到 DHCP 服务器的返回报文后将剥离报文中的 option 82 信息，然后将带有 DHCP 配置信息的报文转发给 DHCP 客户端。

📖 说明：

DHCP 客户端发送的请求报文有两种，分别为 DHCP_DISCOVER 报文和 DHCP_REQUEST 报文，DHCP 中继设备将在这两种报文中都添加 option 82 选项，因为不同厂商生产的 DHCP 服务器设备对请求报文的处理机制不同，有些设备处理 DHCP_DISCOVER 报文中的 option 82 信息，而有些处理 DHCP_REQUEST 报文中的 option 82 信息。

---

2. 协议规范

与 DHCP 中继支持 option 82 相关的协议有：

- RFC2131 Dynamic Host Configuration Protocol
- RFC3046 DHCP Relay Agent Information Option

9.4 DHCP 公共配置

DHCP 的公共配置是指对于 DHCP 服务器和 DHCP 中继功能都适用的配置，包括：

- 使能/禁止 DHCP 服务
- 配置伪 DHCP 服务器检测功能

9.4.1 使能/禁止 DHCP 服务

对于 DHCP 服务器和 DHCP 中继，在进行 DHCP 配置之前，都需要先使能 DHCP 服务。只有启动该服务后，其它相关的 DHCP 配置才能生效。

请在系统视图下进行下列配置。

表9-1 使能/禁止 DHCP 服务

操作	命令
使能 DHCP 服务	**dhcp enable**
禁止 DHCP 服务	**undo dhcp enable**

缺省情况下，使能 DHCP 服务。

📖 **说明：**

在正确配置系统时钟后，DHCP 才会正常运行。

9.4.2 配置伪 DHCP 服务器检测功能

在网络中，如果有私自架设的 DHCP 服务器，当其他用户申请 IP 地址时，这台 DHCP 服务器就会与 DHCP 客户端进行交互，导致用户获得错误的 IP 地址，无法正常上网，这种私设的 DHCP 服务器称为伪 DHCP 服务器。

可以配置伪 DHCP 服务器检测功能，记录 DHCP 服务器的 IP 地址和接口等信息，以便管理员及时发现并处理伪 DHCP 服务器。

请在系统视图下进行下列配置。

表9-2 配置伪 DHCP 服务器检测功能

操作	命令
使能伪 DHCP 服务器检测功能	**dhcp server detect**
禁止伪 DHCP 服务器检测功能	**undo dhcp server detect**

缺省情况下，禁止伪 DHCP 服务器检测功能。

9.5 DHCP 服务器配置

DHCP 服务器配置包括：

- 配置接口工作在 DHCP 服务器模式
- 创建 DHCP 地址池
- 配置 DHCP 地址池的地址分配
- 配置 DHCP 地址池中不参与自动分配的 IP 地址
- 配置 DHCP 地址池的 IP 地址租用有效期限
- 配置 DHCP 客户端的域名
- 配置 DHCP 客户端的 DNS 服务器的 IP 地址
- 配置 DHCP 客户端的 NetBIOS 服务器的 IP 地址
- 配置 DHCP 客户端的 NetBIOS 节点类型
- 配置 DHCP 自定义选项
- 配置 DHCP 客户端的出口网关路由器
- 配置 DHCP 服务器的 ping 包发送
- 清除 DHCP 相关信息

🕮 **说明：**

全局地址池与接口地址池:

- 全局地址池是通过系统视图下的 **dhcp server ip-pool** 命令创建的，在本路由器范围内有效。
- 接口地址池是在为以太网接口配置了合法的单播 IP 地址及 **dhcp select interface** 命令后自动创建的，它的地址段范围就是此以太网接口所在的网段，并且只在此接口下有效。与接口地址池相关的命令，只有在接口地址池已经存在的情况下才能配置。

9.5.1 配置接口工作在 DHCP 服务器模式

当收到 DHCP 客户端发出的、目的地址是本机的 DHCP 报文时，可以通过配置决定如何处理这些报文。如果配置为服务器模式，则将报文转给本地 DHCP 服务器；如果配置为中继模式，则将报文转给指定的外部 DHCP 服务器。

如果配置当前接口工作在服务器模式，请在以太网接口（含子接口）、虚拟以太网接口、封装 PPP/HDLC/FR 的同/异步串口、E1 接口视图下进行下列配置。

表9-3 配置当前接口工作在 DHCP 服务器模式

操作	命令
将 DHCP 报文发送到本地 DHCP 服务器，从全局地址池分配地址	**dhcp select global** [**subaddress**]
将 DHCP 报文发送到本地 DHCP 服务器，从接口地址池分配地址	**dhcp select interface**
恢复缺省设置	**undo dhcp select**

如果同时配置多个接口工作在服务器模式，请在系统视图下进行下列配置。

表9-4 配置指定范围的接口工作在 DHCP 服务器模式

操作	命令
将 DHCP 报文发送到本地 DHCP 服务器，从全局地址池分配地址	**dhcp select global** [**subaddress**] { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
将 DHCP 报文发送到本地 DHCP 服务器，从接口地址池分配地址	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
恢复缺省设置	**undo dhcp select** { **interface** *interface-type interface-number* [*to interface-type interface-number* | **all** }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。目前支持 DHCP Server 的接口可以为以太网接口（或子接口）、虚拟以太网接口、封装了 PPP/HDLC/FR 的同/异步串口、E1 接口等。

📖 说明：

- 如果需要使用接口地址池，必须将对 DHCP 报文的处理模式设置为 **interface**。
- **subaddress** 表示使能 DHCP Server 从地址分配功能，即服务器分配给客户端的 IP 地址为服务器上以太网口从地址网段的 IP 地址，该地址从全局地址池中分配。此时服务器端以太网接口下也要配置从 IP 地址，且要求全局地址池的网段与接口下从 IP 地址在同一网段，否则客户端以太网接口获得的 IP 地址与主 IP 地址在同一网段。
- 支持从地址分配的接口目前仅有以太网接口和虚拟以太网接口。
- 如果在一个接口上同时配置 DHCP Server 和 DHCP Client，会造成地址分配出现混乱。因此，请不要在同一接口下同时配置 DHCP Server 和 DHCP Client。

9.5.2 创建 DHCP 全局地址池

DHCP 服务器通过地址池给用户分配 IP 地址。当客户端向服务器发出 DHCP 请求时，DHCP 服务器选择合适的地址池，并从中挑选一个空闲的 IP 地址与其他相关参

数（如 DNS 服务器地址、地址租用期限等）一起传送给客户端。每个 DHCP 服务器可以配置多个地址池，Comware 目前支持 128 个全局地址池。

DHCP 服务器中的地址池采用树状结构：树根是自然网段地址，分支是该网段的子网地址，叶节点是手工绑定的客户端地址。这种树状结构实现了配置的继承性，即子网（子节点）配置继承自然网段（父节点）的配置，客户端（孙子节点）的配置继承子网（子节点）的配置。这样，对于一些通用参数（如域名），只需要在自然网段或者子网上配置即可。地址池的树状结构可以通过命令 **display dhcp server tree** 查看，同一级别地址池的顺序由配置的先后决定。

请在系统视图下进行下列配置。

表9-5 创建 DHCP 全局地址池

操作	命令
创建 DHCP 地址池或进入 DHCP 地址池视图	**dhcp server ip-pool** *pool-name*
删除 DHCP 地址池	**undo dhcp server ip-pool** *pool-name*

缺省情况下，没有创建任何 DHCP 全局地址池。

9.5.3 配置 DHCP 地址池的地址分配

根据客户端的实际需要，可以选择采用静态地址绑定方式或动态地址分配方式，但不能对同一个 DHCP 地址池同时配置这两种方式。

动态地址分配需要指定用于分配的地址范围，而静态地址绑定则可以看做是只包含一个地址的特殊的 DHCP 地址池。

1. 配置全局地址池的静态地址绑定

某些客户端可能需要固定的 IP 地址，即将客户端的 MAC 地址或 Identifier 与某个 IP 地址绑定。当此 MAC 地址或 Identifier 的客户端申请 DHCP 地址时，服务器根据客户端 MAC 地址或 Identifier 寻找到对应的固定 IP 地址分配给客户端。

请在 DHCP 地址池视图下进行下列配置。

表9-6 配置静态地址绑定

操作	命令
配置静态绑定的 IP 地址	**static-bind ip-address** *ip-address* [**mask** *netmask*]
删除静态绑定的 IP 地址	**undo static-bind ip-address**
配置静态绑定的客户端 MAC 地址或 Identifier	**static-bind** { **mac-address** *mac-address* | **client-identifier** *client-identifier* }
删除静态绑定的客户端 MAC 地址或 Identifier	**undo static-bind** { **mac-address** | **client-identifier** }

缺省情况下，未配置 DHCP 客户端 IP 地址与 MAC 地址或 Identifier 绑定。客户端的 MAC 地址或 Identifier 类型缺省为以太。

🕮 **说明：**

命令 **static-bind ip-address** 和 **static-bind { mac-address | client-identifier}**必须配合使用，并且，如果多次执行，新的配置会覆盖已有配置。

每一个 MAC 地址或 Identifier 对应的静态绑定仅允许配置一个。

---

2. 配置接口地址池的静态地址绑定

请在以太网接口（含子接口）视图下进行下列配置。

表9-7 配置接口地址池的静态地址绑定

操作	命令
配置当前接口地址池的静态地址绑定	**dhcp server static-bind ip-address** *ip-address* { **mac-address** *mac-address* | **client-identifier** *client-identifier* }
删除配置的静态地址绑定	**undo dhcp server static-bind** { **ip-address** *ip-address* | **mac-address** *mac-address* | **client-identifier** *client-identifier* }

在一个接口的所有静态绑定中，IP 地址和 MAC 地址/client-identifier 必须是唯一的，且 client-identifier 与 MAC 地址是互斥的，同一个 IP 地址不能既绑定 MAC 地址，又绑定 client-identifier。

3. 配置动态地址分配

对于动态分配给客户端的地址（包括永久的和租用期有限的动态地址），都需要配置地址池范围。目前，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。

请在 DHCP 地址池视图下进行下列配置。

表9-8 配置动态分配的 IP 地址范围

操作	命令
配置动态分配的 IP 地址范围	**network** *ip-address* [**mask** *netmask*]
删除动态分配的 IP 地址范围	**undo network**

缺省情况下，未配置 DHCP 地址池，即没有可供分配的地址。

多次执行 **network** 命令，新的配置会覆盖已有配置。

9.5.4 配置 DHCP 地址池中不参与自动分配的 IP 地址

DHCP 服务器在分配地址时，需要排除已经被占用的某些 IP 地址（如网关、FTP 服务器等），否则，同一地址分配给两台主机会造成 IP 地址冲突。

请在系统视图下进行下列配置。

表9-9 配置 DHCP 地址池中不参与自动分配的 IP 地址

操作	命令
配置 DHCP 地址池中不参与自动分配的 IP 地址	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]
删除 DHCP 地址池中不参与自动分配的 IP 地址	**undo dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行本命令，可以配置多个不参与自动分配的 IP 地址段。

9.5.5 配置 DHCP 地址池的 IP 地址租用有效期限

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 DHCP 地址池中的地址都具有相同的期限。

地址租用有效期限不具有继承关系。

为方便用户，系统提供不同范围的地址租用有效期限配置方式。

1. 全局 DHCP 地址池

请在 DHCP 地址池视图下进行下列配置。

表9-10 配置全局 DHCP 地址池的 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
恢复缺省的 IP 地址租用有效期限	**undo expired**

2. 接口 DHCP 地址池

请在以太网接口（含子接口）视图下进行下列配置。

表9-11 配置接口 DHCP 地址池的 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
恢复缺省的 IP 地址租用有效期限	**undo dhcp server expired**

3. 多个接口的 DHCP 地址池

系统提供对指定范围的多个以太网子接口的 DHCP 地址池同时进行配置的功能，以减少某些应用中的重复配置工作。

请在系统视图下进行下列配置。

表9-12 配置多个接口的 DHCP 地址池 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
恢复缺省的 IP 地址租用有效期限	**undo dhcp server expired** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

缺省情况下，IP 地址租用有效期限为 1 天。

📖 **说明：**

为方便用户，对某些 DHCP 配置选项，系统提供不同范围的 DHCP 地址池的配置方式。用户可以分别对全局 DHCP 地址池、接口 DHCP 地址池或指定接口范围的多个以太网子接口的接口 DHCP 地址池进行配置，最后一种配置方式对于减少某些应用中的重复配置尤其有用。

这类配置任务包括：配置 DHCP 客户端的域名、DHCP 客户端的 DNS 服务器的 IP 地址、DHCP 客户端的 NetBIOS 服务器的 IP 地址、DHCP 客户端的 NetBIOS 节点类型以及 DHCP 自定义选项。

租期所能表示的最大时间范围截止到 2106 年。

9.5.6 配置 DHCP 客户端的域名

在 DHCP 服务器上，可以为每个地址池分别指定客户端使用的域名。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表9-13 配置全局 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	**domain-name** *domain-name*
删除分配给 DHCP 客户端的域名	**undo domain-name**

如果配置接口 DHCP 地址池，请在以太网接口（含子接口）视图下进行下列配置。

表9-14 配置接口 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	**dhcp server domain-name** *domain-name*
删除分配给 DHCP 客户端的域名	**undo dhcp server domain-name**

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表9-15 配置多个接口的 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
删除分配给 DHCP 客户端的域名	**undo dhcp server domain-name** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

缺省情况下，未配置分给 DHCP 客户端的域名。

9.5.7 配置 DHCP 客户端的 DNS 服务器的 IP 地址

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。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 DNS 服务器地址。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表9-16 配置全局 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	**dns-list** *ip-address* [*ip-address*]
删除 DHCP 客户端的 DNS 服务器的 IP 地址	**undo dns-list** { *ip-address* | **all** }

如果配置接口 DHCP 地址池，请在以太网接口（含子接口）视图下进行下列配置。

表9-17 配置接口 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	**dhcp server dns-list** *ip-address* [*ip-address*]
删除 DHCP 客户端的 DNS 服务器的 IP 地址	**undo dhcp server dns-list** { *ip-address* | **all** }

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表9-18 配置多个接口的 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	**dhcp server dns-list** *ip-address* [*ip-address*] { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
删除 DHCP 客户端的 DNS 服务器的 IP 地址	**undo dhcp server dns-list** { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

缺省情况下，未配置 DNS 服务器的 IP 地址。

9.5.8 配置 DHCP 客户端的 NetBIOS 服务器的 IP 地址

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

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 NetBIOS 地址。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表9-19 配置全局 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	**nbns-list** *ip-address* [*ip-address*]
删除 DHCP 客户端的 NetBIOS 服务器地址	**undo nbns-list** { *ip-address* | **all** }

如果配置接口 DHCP 地址池，请在以太网接口（含子接口）视图下进行下列配置。

表9-20 配置接口 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	**dhcp server nbns-list** *ip-address* [*ip-address*]
删除 DHCP 客户端的 NetBIOS 服务器地址	**undo dhcp server nbns-list** { *ip-address* | **all** }

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表9-21 配置多个接口的 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	**dhcp server nbns-list** *ip-address* [*ip-address*] { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
删除 DHCP 客户端的 NetBIOS 服务器地址	**undo dhcp server nbns-list** { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

缺省情况下，未配置 NetBIOS 服务器的 IP 地址。

9.5.9 配置 DHCP 客户端的 NetBIOS 节点类型

DHCP 客户端在广域网上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，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。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表9-22 配置全局 DHCP 地址池的客户端 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	**undo netbios-type**

如果配置接口 DHCP 地址池，请在以太网接口（含子接口）视图下进行下列配置。

表9-23 配置接口 DHCP 服务器的客户端的 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }

操作	命令
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	**undo dhcp server netbios-type**

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表9-24 配置多个接口的 DHCP 地址池客户端的 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	**undo dhcp server netbios-type** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

缺省情况下，客户端采用 h 类节点（**h-node**）。

9.5.10 配置 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。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表9-25 配置 DHCP 自定义选项

操作	命令
配置 DHCP 自定义选项	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }
删除 DHCP 自定义选项	**undo option** *code*

如果配置接口 DHCP 地址池，请在以太网接口（含子接口）视图下进行下列配置。

表9-26 配置 DHCP 自定义选项

操作	命令
配置 DHCP 自定义选项	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }
删除 DHCP 自定义选项	**undo dhcp server option** *code*

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表9-27 配置 DHCP 自定义选项

操作	命令
配置 DHCP 自定义选项	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
删除 DHCP 自定义选项	**undo dhcp server option** *code* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

9.5.11 配置 DHCP 客户端的出口网关路由器

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。

请在 DHCP 地址池视图下进行下列配置。

表9-28 配置 DHCP 客户端的出口网关路由器

操作	命令
配置 DHCP 客户端的出口网关	**gateway-list** *ip-address* [*ip-address*]
删除 DHCP 客户端的出口网关	**undo gateway-list** { *ip-address* | **all** }

缺省情况下，未配置 DHCP 客户端的出口网关地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个出口网关地址。

📖 **说明：**

当指定多个出口网关地址时，需要多个 ip-address 参数。

9.5.12 配置 DHCP 服务器的 ping 包发送

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

地址探测是通过 ping 命令实现的，检测是否能在指定时间内得到 ping 应答。如果没有得到应答，则继续发送 ping 报文，直到发送 ping 包数量达到最大值；如果仍然超时，则可以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 地址唯一。

请在系统视图下进行下列配置。

表9-29 配置 DHCP 服务器的 ping 包发送

操作	命令
配置 DHCP 服务器发送 ping 包的最大数量	**dhcp server ping packets** *number*
恢复 DHCP 服务器发送 ping 包的缺省最大数量	**undo dhcp server ping packets**
配置DHCP服务器发送ping包的最长等待响应时间	**dhcp server ping timeout** *milliseconds*
恢复DHCP服务器发送ping包的缺省最长等待响应时间	**undo dhcp server ping timeout**

缺省情况下，发送 ping 包的最大数量为 2，等待 ping 响应的最长时间为 500 毫秒。

DHCP 服务器通过 **ping** 包的发送检测是否发生地址冲突，而 DHCP 客户端则通过 ARP 报文检测是否发生地址冲突。

9.5.13 配置 DHCP 服务器计费

DHCP 服务器计费功能用于 DHCP 服务器在分配和释放租约时，向指定域的 RADIUS 模式的计费服务器发送计费报文。

配置了 DHCP 服务器计费功能后，当用户申请 IP 地址时，DHCP 服务器会给用户分配带有 IP 地址、租约期限和其它配置信息的租约，成功分配租约后，会立刻通知指定域的 RADIUS 计费服务器，发送一个 RADIUS START 计费请求报文；当由于某种原因，DHCP Server 的租约被释放（释放租约的原因可能有租约过期，收到用户的 release 请求，手工删除租约，手工删除地址池等），那么 DHCP 服务器会立刻通知指定域的 RADIUS 计费服务器，发送一个 RADIUS STOP 计费结束报文。

此时 RADIUS 服务器只是记录了用户使用 IP 地址的情况，并不真正进行计费。

1. 配置准备

在配置 DHCP 服务器计费前需要先进行下列配置：

- 完成 DHCP 服务器及客户端的相关配置，保证 DHCP 能够为客户端分配 IP 地址；
- 完成域及 RADIUS 计费服务器的相关配置，这里仅在指定域下配置 RADIUS 方案，并在 RADIUS 方案下面配置 RADIUS 服务器即可。

域及 RADIUS 计费服务器的相关配置请参考“安全”部分。

2. 在系统视图下配置 DHCP 服务器计费

表9-30 在系统视图下配置 DHCP 服务器计费

操作	命令	说明
进入系统视图	**system-view**	-
配置接口工作在 DHCP 服务器模式，并从指定接口地址池中分配地址	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	必选
针对指定接口地址池中的地址启动 DHCP 计费功能，并配置 DHCP 计费所使用的域	**dhcp server accounting domain** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	必选
进入相应接口视图	**interface** *interface-type interface-number*	应对上面命令涉及的接口配置 IP 地址，才能创建接口地址池
配置接口 IP 地址	**ip address** *ip-address net-mask*	

📖 说明：

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式可以配置子接口范围，所以可以同时在多个子接口上配置 DHCP 服务器计费功能。

3. 在接口视图下配置 DHCP 服务器计费

表9-31 接口视图下配置 DHCP 服务器计费

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	必选
配置接口 IP 地址	**ip address** *ip-address net-mask*	必选
配置接口工作在 DHCP 服务器模式，并从接口地址池中分配地址	**dhcp select interface**	必选
针对接口地址池中的地址启动 DHCP 计费功能，并配置 DHCP 计费所使用的域	**dhcp server accounting domain** *domain-name*	必选

📖 说明：

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式是在接口视图下配置 DHCP 服务器计费的，适用于配置单个接口支持 DHCP 服务器计费功能。

4. 在 DHCP 全局地址池视图下配置 DHCP 服务器计费

表9-32 DHCP 全局地址池视图下配置 DHCP 服务器计费

操作	命令	说明
进入系统视图	**system-view**	-
配置指定接口工作在 DHCP 服务器模式，并从 DHCP 全局地址池中分配地址	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*]}	必选
进入 DHCP 地址池视图	**dhcp server ip pool** *pool-name*	-
配置动态分配的 IP 地址范围	**network** *ip-address* [**mask** *netmask*]	-
针对 DHCP 地址池中的地址启动 DHCP 服务器计费功能，并配置 DHCP 服务器计费所使用的域	**accounting domain** *domain-name*	缺省情况下，未启动 DHCP 服务器计费功能。

📖 说明：

该方式适用于从 DHCP 全局地址池中给客户端分配 IP 地址的情况。

9.5.14 配置 DHCP 服务器支持 BIMS option

1. 配置准备

在配置 DHCP 服务器支持 BIMS option 前应先进行如下配置：

- 在路由器上启动 DHCP Server 服务器并配置地址池
- 配置 DHCP 客户端
- 保证 DHCP 客户端、DHCP 服务器以及 BIMS 服务器之间网络可达

2. 配置 BIMS option

表9-33 配置 BIMS option

操作	命令	说明
进入系统视图	**system-view**	-
在系统视图下启动并配置 BIMS option	**dhcp server bims-server ip** *ip-address* **port** *port-number* **sharekey** *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	必选 三种配置方法，在实际应用中任选其一
在接口视图下启动并配置 BIMS option	**dhcp server bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key* **undo dhcp server bims-server**	
在 DHCP 全局地址池下启动并配置 BIMS option	**dhcp server ip-pool** *pool-name*	
	bims-server ip *ip-address* **port** *port-number* **sharekey** *key*	

📖 说明：

若在全局地址池中配置了 BIMS option，则 DHCP 服务器从全局地址池分配 IP 地址给客户端时将携带 BIMS option。若在指定接口上配置了 BIMS option，则 DHCP 服务器从接口地址池中分配 IP 地址时携带 BIMS option。若在 **dhcp server bims-server ip** 命令中使用 **all** 关键字，则 DHCP 服务器从所有接口地址池中分配 IP 地址时都将携带 BIMS option。

9.5.15 配置 DHCP 服务器支持 option184

DHCP 服务器支持在系统视图、接口视图或在 DHCP 地址池视图下分别配置 option 184 的各 sub-option。无论是在系统视图下还是在接口视图下配置 option 184，都要在相应的接口上配置接口地址池。

1. 配置准备

在配置 DHCP 服务器支持 option184 特性前需要先进行下列配置：

- 配置 DHCP 服务器的网络参数、地址池及地址分配租期等分配策略
- 配置 DHCP 服务器与 DHCP 客户端网络可达

上述详细配置请参考本手册“网络层协议”的 DHCP 部分。

2. 在系统视图下配置 DHCP 服务器支持 option 184

表9-34 系统视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	**system-view**	-
配置接口工作在 DHCP 服务器模式，并从指定接口地址池中分配地址	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	必选
配置 option 184 的子选项 NCP-IP	**dhcp server voice-config ncp-ip** *ip-address* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	必选
配置 option 184 的子选项 AS-IP	**dhcp server voice-config as-ip** *ip-address* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	**dhcp server voice-config voice-vlan** *vlan-id* { **enable** | **disable** } { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	**dhcp server voice-config fail-over** *ip-address dialer-string* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
进入相应接口视图	**interface** *interface-type interface-number*	应对上面命令涉及的接口配置 IP 地址，才能创建接口地址池
配置接口 IP 地址	**ip address** *ip-address net-mask*	

📖 **说明：**

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式可以配置接口范围，所以可以同时在多个接口上配置 DHCP 支持 option 184 功能。

3. 在接口视图下配置 DHCP 服务器支持 option 184

表9-35 接口视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	必选
配置接口 IP 地址	**ip address** *ip-address net-mask*	必选
配置接口工作在 DHCP 服务器模式，并从接口地址池中分配地址	**dhcp select interface**	必选
配置 option 184 的子选项 NCP-IP	**dhcp server voice-config ncp-ip** *ip-address*	必选
配置 option 184 的子选项 AS-IP	**dhcp server voice-config as-ip** *ip-address*	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	**dhcp server voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	**dhcp server voice-config fail-over** *ip-address dialer-string*	可选 只有配置了 NCP-IP 子选项才能配置该子选项

📖 **说明：**

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式是在接口视图下配置 DHCP 支持 option 184 功能的，适用于配置单个接口支持 option 184 功能。

4. 在 DHCP 全局地址池视图下配置 DHCP 服务器支持 option 184

表9-36 DHCP 全局地址池视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	**system-view**	-
配置指定接口工作在 DHCP 服务器模式，并从 DHCP 全局地址池中分配地址	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*]}	必选
进入 DHCP 地址池视图	**dhcp server ip pool** *pool-name*	必选

操作	命令	说明
配置动态分配的 IP 地址范围	**network** *ip-address* [**mask** *netmask*]	必选
配置 option 184 的子选项 NCP-IP	**voice-config ncp-ip** *ip-address*	必选
配置 option 184 的子选项 AS-IP	**voice-config as-ip** *ip-address*	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	**voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	**voice-config fail-over** *ip-address dialer-string*	可选 只有配置了 NCP-IP 子选项才能配置该子选项

📖 **说明：**

该方式适用于从 DHCP 全局地址池中给客户端分配 IP 地址的情况。

9.5.16 配置 DHCP 服务器支持 option 82

1. 配置准备

在配置 DHCP 服务器支持 option 82 特性前需要先进行下列配置：

- DHCP 服务器功能
- DHCP 服务器的网络参数、地址池及地址分配租期等分配策略
- 配置网络路由可达

上述详细配置请参考本手册“网络层协议”的 DHCP 部分。

2. 使能 DHCP 服务器支持 option82

表9-37 配置 DHCP 服务器支持 option82

操作	命令	说明
进入系统视图	**system-view**	-
使能 DHCP 服务器支持 option 82	**dhcp server relay information enable**	必选 缺省情况下使能 DHCP Server 支持 option 82

9.5.17 清除 DHCP 相关信息

在任意视图下执行 **display dhcp server ip-in-use** 命令可以查看到地址池的动态地址绑定信息，这些信息也可以通过命令清除。

在任意视图下执行 **display dhcp server conflict** 命令可以查看到 DHCP 地址冲突的统计信息，这些信息也可以通过命令清除。

在任意视图下执行 **display dhcp server statistics** 命令可以查看到 DHCP 服务器的统计信息，这些信息也可以通过命令清除。

请在用户视图下进行下列配置。

表9-38 清除 DHCP 相关信息

操作	命令
清除指定 IP 地址的绑定信息	**reset dhcp server ip-in-use ip** *ip-address*
清除全局地址池的动态地址绑定信息	**reset dhcp server ip-in-use pool** [*pool-name*]
清除接口地址池的动态地址绑定信息	**reset dhcp server ip-in-use interface** [*interface-type interface-number*]
清除所有地址池的地址绑定信息	**reset dhcp server ip-in-use all**
清除指定 IP 地址的冲突统计信息	**reset dhcp server conflict** *ip-address*
清除所有地址池的地址冲突统计信息	**reset dhcp server conflict all**
清除 DHCP 服务器的统计信息	**reset dhcp server statistics**

9.6 DHCP 中继配置

DHCP 中继配置包括：

- 配置接口工作在 DHCP 中继模式
- 配置 DHCP 中继指定的外部服务器地址
- 通过 DHCP 中继配置 DHCP 服务器负载分担
- 通过 DHCP 中继释放客户端的 IP 地址
- 清除 DHCP 中继的统计信息

9.6.1 配置接口工作在 DHCP 中继模式

当收到 DHCP 客户端发出的、目的地址是本机的 DHCP 报文时，可以通过配置决定如何处理这些报文。如果配置为服务器模式，则将报文转给本地 DHCP 服务器；如果配置为中继模式，则将报文转给指定的外部 DHCP 服务器。

如果配置当前接口工作在中继模式，请在以太网接口（含子接口）、封装 PPP/HDLC/FR 的同/异步串口、E1 接口视图下进行下列配置。

表9-39 配置当前接口工作在 DHCP 中继模式

操作	命令
将 DHCP 报文通过中继发送给外部 DHCP 服务器，由外部 DHCP 服务器分配地址	**dhcp select relay**
恢复缺省设置	**undo dhcp select**

如果同时配置多个接口工作在中继模式，请在系统视图下进行下列配置。

表9-40 配置指定范围的接口工作在 DHCP 中继模式

操作	命令
将 DHCP 报文通过中继发送给外部 DHCP 服务器，由外部 DHCP 服务器分配地址	**dhcp select relay** { **interface** *interface-type interface-number [to interface-type interface-number* | **all** }
恢复缺省设置	**undo dhcp select** { **interface** *interface-type interface-number [to interface-type interface-number* | **all** }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。目前支持 DHCP Relay 的接口可以为以太网接口（或子接口）、虚拟以太网接口、封装了 PPP/HDLC/FR 的同/异步串口、E1 接口等。

📖 **说明：**

以太网子接口支持 DHCP Relay 时，如果是 PC 通过该子接口获得 IP 地址，则 PC 需要通过交换机连接到路由器，并在交换机上做相应的链路配置。

9.6.2 配置 DHCP 中继指定的外部服务器地址

当配置 DHCP 中继功能时，从接口上收到的 DHCP 广播报文将被送到指定的外部 DHCP 服务器。

如果只需要在当前接口上指定外部 DHCP 服务器地址，请在接口视图下进行下列配置。

表9-41 配置当前接口的外部 DHCP 服务器地址

操作	命令
配置当前接口的外部 DHCP 服务器地址	**ip relay-address** *ip-address*
删除当前接口的外部 DHCP 服务器地址	**undo ip relay address** { *ip-address* | **all** }

如果在指定范围的多个接口上指定外部 DHCP 服务器地址，请在系统视图下进行下列配置。

表9-42 配置指定范围的多个接口上的外部 DHCP 服务器地址

操作	命令
配置指定范围的多个接口上的外部 DHCP 服务器地址	**ip relay address** *ip-address* [**interface** *interface-type interface-number [to interface-type interface-number* | **all**]
删除指定范围的多个接口上的外部 DHCP 服务器地址	**undo ip relay address** { *ip-address* | **all** } { **interface** *interface-type interface-number [to interface-type interface-number* | **all** }

📖 **说明：**

由于 DHCP 客户端在 DHCP 配置的某些阶段发送的报文为广播报文，因此相应接口应当支持广播方式。

每个接口最多可以支持 20 个外部 DHCP 服务器地址。

9.6.3 通过 DHCP 中继配置 DHCP 服务器负载分担

使用 DHCP 中继功能可以配置多个 DHCP 服务器，并可以配置它们之间进行负载分担。

如果配置了多个 DHCP 服务器，DHCP 中继可以通过负载分担的方式将 DHCP 客户端的请求按 HASH 算法分给不同的 DHCP 服务器进行处理，实现多个 DHCP 服务器的负载分担。

请在系统视图下进行下列配置。

表9-43 配置 DHCP 服务器的负载分担

操作	命令
配置 DHCP 服务器的负载分担	**ip relay address cycle**
取消 DHCP 服务器的负载分担	**undo ip relay address cycle**

缺省情况下，DHCP 服务器之间不进行负载分担。

9.6.4 通过 DHCP 中继释放客户端的 IP 地址

在某些情况下，可能需要通过 DHCP 中继手工释放客户端申请到的 IP 地址。

请在接口视图或系统视图下进行下列配置。

表9-44 通过 DHCP 中继释放客户端的 IP 地址

操作	命令
向 DHCP 服务器请求释放客户端申请到的 IP 地址	**dhcp relay release** *client-ip mac-address*
向指定的 DHCP 服务器请求释放客户端申请到的 IP 地址	**dhcp relay release** *client-ip mac-address server-ip*

当不指定 DHCP 服务器时，如果在系统视图下，则向所有 DHCP 服务器发送释放申请，如果在接口视图下，向该接口下的所有中继地址发送释放申请。

🕮 **说明：**

在 DHCP Relay 中配置手工释放 IP 地址后，会通知 DHCP Server 释放 DHCP ip-in-use 地址池中的地址，该 IP 地址在释放后会放入过期队列，一般情况下不会马上被分配出去；此时仅仅释放的是 DHCP ip-in-use 地址池中的地址，Client 端主机是无法真正释放该地址的，所以 Client 端主机会使用该地址直到租约超时。

只有当服务器端用 MAC 地址来标识用户时，Release 报文才能生效。对于路由器提供的 DHCP 服务器，可以使用 **display dhcp server ip-in-use** 命令查看一下，如显示为 Hardware address，表示用 MAC 地址来标识用户；如果显示为 Client identifier/Hardware address，表示用 Client identifier 地址来标识用户。

9.6.5 配置 DHCP 中继支持 option 82

1. 配置准备

在配置 DHCP 中继支持 option 82 特性前需要先进行下列配置：

- DHCP 中继功能
- DHCP 服务器的网络参数、地址池及地址分配租期等分配策略
- 配置网络路由可达

上述详细配置请参考本手册“网络层协议”的 DHCP 部分。

2. 配置 DHCP 中继支持 option82

本节的配置需要在启动了 DHCP 中继的网络设备上进行。

表9-45 配置 DHCP 中继支持 option82

操作	命令	说明
进入系统视图	**system-view**	-
使能 DHCP 中继支持 option 82	**dhcp relay information enable**	必选

操作	命令	说明
配置 DHCP 中继对包含 option 82 的请求报文的处理策略	**dhcp relay information strategy { drop | keep | replace }**	可选 缺省情况下 DHCP Relay 对包含 option 82 的请求报文的处理策略为 replace，即用 Relay 本身的 option 82 替换原有报文中的 option 82

9.6.6 清除 DHCP 中继的统计信息

在任意视图下执行 **display dhcp relay statistics** 命令可以查看到 DHCP 中继的统计信息，这些信息也可以通过命令清除。

请在用户视图下进行下列配置。

表9-46 清除 DHCP 中继的统计信息

操作	命令
清除 DHCP 中继的统计信息	**reset dhcp relay statistics**

9.7 DHCP 客户端配置

DHCP 客户端的配置很简单，仅包括下面一条配置命令，目前在以太网接口（包括子接口）、封装 PPP/HDLC/FR 的同/异步串口或 E1 接口上均可通过 DHCP 方式获取地址。

请在以太网接口（包括子接口）、同/异步串口、E1 接口视图下进行下列配置。

表9-47 DHCP 客户端配置

操作	命令
启动 DHCP 客户端，以获取本地 IP 地址	**ip address dhcp-alloc**
关闭 DHCP 客户端功能	**undo ip address dhcp-alloc**

缺省情况下，关闭 DHCP 客户端功能。

🕮 说明：

- 接口在配置 DHCP 动态获取 IP 地址后不再允许配置从 IP 地址，即命令 **ip address dhcp-alloc** 与命令 **ip address** *ip-address mask* **sub** 不能同时配置在一个以太网接口下，两者只能取其一。
- 若在 DHCP Server 上配置了 **gateway-list** 命令，那么 DHCP Client 在获得接口 IP 地址且接口 UP 后其路由表中会出现一条下一跳为指定网关的缺省路由。若 DHCP Client 通过 DHCP Server 获得了多个网关地址，并且 DHCP Client 使用的是 H3C 系列路由器，那么 DHCP Client 在获得接口 IP 地址且接口 UP 后只取 DHCP Server 地址池 gateway-list 中的第一个地址添加到缺省路由，如下：

```
[H3C] display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol   Pre  Cost      Nexthop         Interface
0.0.0.0/0          DHCPDEF 255  0         23.23.0.2       Ethernet2/1.1
```

该缺省路由的优先级为 255、花费为 0。

- 当在封装 FR 的接口上启动 DHCP Client 时，要么 FR 接口采用帧中继动态地址映射，要么采用广播方式的帧中继静态地址映射。
- 虚拟以太口支持 DHCP Server，但目前还不支持 DHCP Client。

9.8 DHCP 显示和调试

在完成上述配置后，可在任意视图下执行 **display** 命令显示配置后 DHCP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 DHCP 进行调试。

1. DHCP 服务器的显示和调试

表9-48 DHCP 服务器的显示和调试

操作	命令
查看 DHCP 地址池的空闲地址信息	**display dhcp server free-ip**
查看 DHCP 的地址冲突统计信息	**display dhcp server conflict** [**ip** *ip-address* | **all**]
查看 DHCP 地址池中超期的租约	**display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] **all** }
查看 DHCP 的地址绑定信息	**display dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] }
查看 DHCP 服务器的统计信息	**display dhcp server statistics**
查看 DHCP 地址池的树状结构信息	**display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

操作	命令
打开 DHCP 服务器的调试开关	**debugging dhcp server** { **error** | **event** | **packet** | **all** }
关闭 DHCP 服务器的调试开关	**undo debugging dhcp server** { **event** | **packet** | **error** | **all** }
清除 DHCP 动态地址绑定信息。	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-num*] | **all**]
清除 DHCP 地址冲突的统计信息	**reset dhcp server conflict** [*ip-address* | **all**]
清除 DHCP 服务器的统计信息	**reset dhcp server statistics**

🕮 说明：

dhcp sever 的租约信息不会在执行 **save** 命令时保存到 flash 中，故系统重启或用 **reset dhcp server ip-in-use** 命令清除租约后配置文件中没有任何租约的信息，此时客户端如果发出续约请求将会被拒绝，系统会让客户端重新申请 IP 地址。

2. DHCP 中继的显示和调试

表9-49 DHCP 中继的显示和调试

操作	命令
查看 DHCP 中继的 IP 信息	**display ip interface** [*interface-type interface-number*]
查看 DHCP 中继的相关统计信息	**display dhcp relay statistics**
查看接口的 DHCP 中继地址配置	**display dhcp relay address** { **interface** *interface-name* | **all** }
查看通过 DHCP Relay 动态获取 IP 的客户端的 IP 地址和 MAC 地址的对应关系	**display dhcprelay-security**
打开 DHCP 中继调试开关	**debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }
关闭 DHCP 中继调试开关	**undo debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

3. DHCP 客户端的显示和调试

表9-50 DHCP 客户端的显示和调试

操作	命令
显示 DHCP 客户端统计信息	**display dhcp client** [**verbose**]
打开 DHCP 客户端的调试开关	**debugging dhcp client** { **error**| **event** | **packet** | **all**}

操作	命令
关闭 DHCP 客户端的调试开关	**undo debugging dhcp client** { **error**| **event**	**packet**	**all**}

9.9 DHCP 典型配置举例

9.9.1 DHCP 服务器典型配置举例

常见的DHCP组网方式可分为两类：一种是DHCP服务器和客户端都在一个子网内，直接进行 DHCP 协议的交互；第二种是 DHCP 服务器和客户端分别处于不同的子网中，必须通过 DHCP 中继代理实现 IP 地址的分配。无论那种情况下，DHCP 的配置都是相同的。

1. 组网需求

DHCP 服务器为同一网段中的客户端动态分配 IP 地址，地址池网段 10.1.1.0/24 分为两个网段：10.1.1.0/25 和 10.1.1.128/25。DHCP 服务器两个 Ethernet 接口地址分别为 10.1.1.1/25 和 10.1.1.129/25。

网段 10.1.1.0/25 内的地址租用期限为 10 天 12 小时，域名为 h3c.com，DNS 地址为 10.1.1.2，无 NetBIOS 地址，出口路由器地址为 10.1.1.126；网段 10.1.1.128/25 网段内的地址租用期限为 5 天，DNS 地址为 10.1.1.2，NetBIOS 地址为 10.1.1.4，出口路由器的地址为 10.1.1.254。

2. 组网图

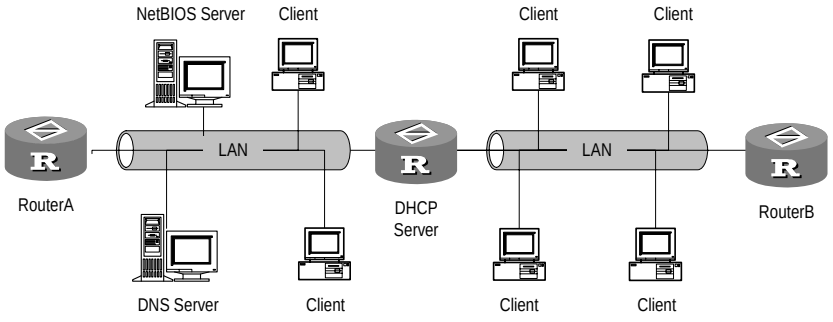


图9-6 DHCP 服务器与客户端在同一网络中

3. 配置步骤

启动 DHCP 服务。

```
[H3C] dhcp enable
```

配置接口工作在 DHCP 服务器模式下，并从全局地址池中分配 IP 地址。

```
[H3C] dhcp select global interface ethernet 0/0/0 to ethernet 0/0/1
```

配置不参与自动分配的 IP 地址（DNS、NetBIOS 和出口网关地址）。

```
[H3C] dhcp server forbidden-ip 10.1.1.2
[H3C] dhcp server forbidden-ip 10.1.1.4
[H3C] dhcp server forbidden-ip 10.1.1.126
[H3C] dhcp server forbidden-ip 10.1.1.254
```

配置 DHCP 地址池 0 的共有属性（地址池范围、DNS 地址）。

```
[H3C] dhcp server ip-pool 0
[H3C-dhcp-0] network 10.1.1.0 mask 255.255.255.0
[H3C-dhcp-0] dns-list 10.1.1.2
[H3C-dhcp-0] quit
```

配置 DHCP 地址池 1 的属性（地址池范围、出口网关、地址租用期限）。

```
[H3C] dhcp server ip-pool 1
[H3C-dhcp-1] network 10.1.1.0 mask 255.255.255.128
[H3C-dhcp-1] domain-name h3c.com
[H3C-dhcp-1] gateway-list 10.1.1.126
[H3C-dhcp-1] expired day 10 hour 12
```

配置 DHCP 地址池 2 的属性（地址池范围、出口网关、NetBIOS 地址、地址租用期限）。

```
[H3C] dhcp server ip-pool 2
[H3C-dhcp-2] network 10.1.1.128 mask 255.255.255.128
[H3C-dhcp-2] expired day 5
[H3C-dhcp-2] nbns-list 10.1.1.4
[H3C-dhcp-2] gateway-list 10.1.1.254
```

9.9.2 DHCP 中继典型配置举例

1. 组网需求

DHCP 客户端所在的网段为 10.110.0.0，而 DHCP 服务器所在的网段为 202.38.0.0。需要通过带 DHCP 中继功能的路由器中继 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。

DHCP 服务器应当分配一个 10.110.0.0 网段的 IP 地址池，以便将适当的 IP 地址分配给该网段上的 DHCP 客户端，并且 DHCP 服务器上应当配置有到 10.110.0.0 网段的路由。

2. 组网图

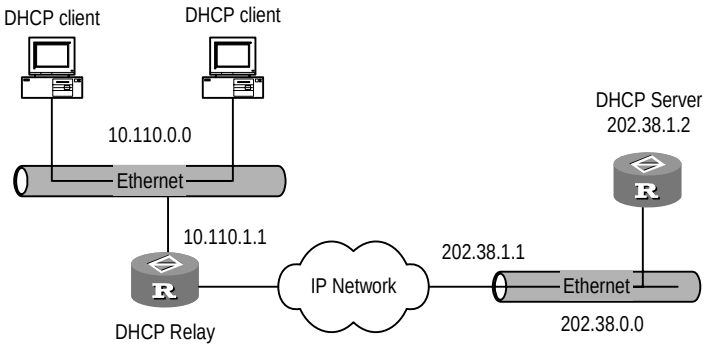


图9-7 DHCP 中继配置

3. 配置步骤

配置路由器：

使能 DHCP 服务

```
[H3C] dhcp enable
```

进入要实现 DHCP 中继功能的接口，为其配置 IP 地址和地址掩码以使其和 DHCP 客户端属于同一个网段

```
[H3C] interface ethernet 6/0/0
[H3C-Ethernet6/0/0] ip address 10.110.1.1 255.255.0.0
```

为该接口配置 IP 中继地址以指明 DHCP 服务器的位置

```
[H3C-Ethernet6/0/0] dhcp select relay
[H3C-Ethernet6/0/0] ip relay address 202.38.1.2
```

DHCP 服务器的配置略。

9.9.3 DHCP 客户端典型配置举例

介绍两种 DHCP 客户端典型配置：一种是以太网主接口动态获取 IP 地址；第二种是以太网子接口动态获取 IP 地址(支持 VLAN)。

1. 以太网主接口作 DHCP 客户端

(1) 组网需求

路由器 RTA 的以太口 Ethernet0/0/0、Ethernet2/0/0 分别接入 LAN1、LAN2 中，在两个 LAN 中分别有 DHCP 服务器 server1、server2。LAN1 所在网段为 200.254.0.0/16，LAN1 所在网段为 172.10.0.0/16，要求配置 RTA 的上述两个以太口通过 DHCP 的方式获取地址。

(2) 组网图

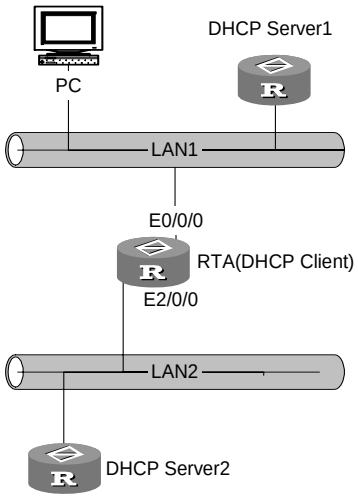


图9-8 主接口作 DHCP 客户端

(3) 配置步骤

以下同时列出 DHCP 服务器和客户端的配置过程。

- 配置 server1。

```
[H3C] dhcp enable
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 200.254.0.1 16
[H3C] dhcp server ip-pool 1
[H3C-dhcp1] network 200.254.0.0 mask 255.255.0.0
```

- 配置 server2。

```
[H3C] dhcp enable
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 172.10.0.1 16
[H3C] dhcp server ip-pool 2
[H3C-dhcp2] network 172.10.0.0 mask 255.255.0.0
```

- 配置 Client。

配置 RTA 的 Ethernet0/0/0 通过 DHCP 动态获取地址。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address dhcp-alloc
```

配置 RTA 的 Ethernet2/0/0 通过 DHCP 动态获取地址。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address dhcp-alloc
```

2. 以太网子接口动态获取 IP 地址

(1) 组网需求

DHCP 服务器 1 和 2 分别接在不同的 VLAN 中，server1 在 VLAN10，server2 在 VLAN20，要求在路由器 RTA（DHCP client）的以太口 Ethernet0/0/0 上创建子接口，并分别从上述两个 DHCP 服务器中动态获取 IP 地址。

(2) 组网图

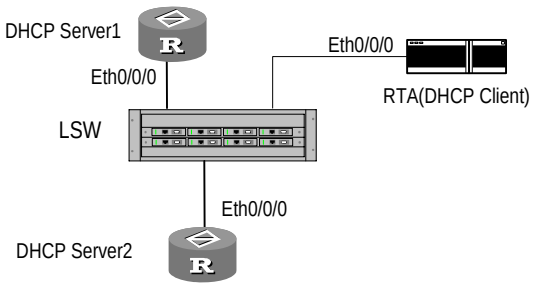


图9-9 子接口作 DHCP 客户端

(3) 配置步骤

LANSWITCH 的配置不在这里列出，但要保证 sever1 接入到 VLAN10 中，server2 接入到 VLAN20 中，接作 DHCP client 的 RTA 路由器的端口配置为 TRUNK 端口，并能透传 vlan id 为 10 和 20 的报文。

DHCP 服务器 server1、server2 的配置过程同上例，以下仅列出 DHCP 客户端的配置过程。

配置从 server1 获取地址的子接口

```
[H3C] interface ethernet 0/0/0.1
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 10
[H3C-Ethernet0/0/0.1] ip addr dhcp-alloc
```

配置从 server1 获取地址的子接口

```
[H3C] interface ethernet 0/0/0.2
[H3C-Ethernet0/0/0.2] vlan-type dot1q vid 20
[H3C-Ethernet0/0/0.2] ip addr dhcp-alloc
```

9.9.4 DHCP Accounting 配置举例

1. 组网需求

要求 RADIUS 计费服务器记录 DHCP Client 使用 IP 地址的情况，具体要求如下：

- DHCP Server 通过 Ethernet1/0/0 和 Ethernet1/0/1 分别连接 DHCP Client 及 RADIUS Server。
- RADIUS Server 的 IP 地址为 10.1.2.2/24。
- DHCP 全局地址池为 10.1.1.0，并在全局地址池下指定 DHCP Server 计费使用的域为 123；

- DHCP Server 启动 DHCP Accounting 功能，由 RADIUS 计费服务器通过域 123 对 DHCP Client 使用 IP 地址的情况进行记录。

2. 组网图

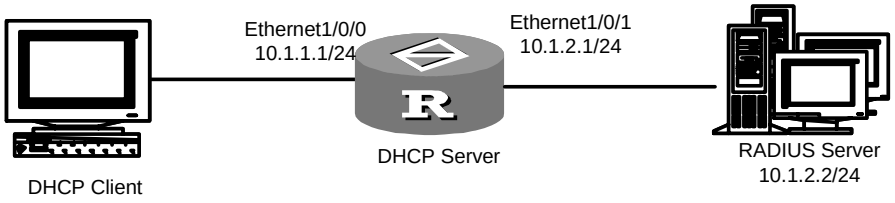


图9-10 DHCP Accounting 配置举例组网图

3. 配置步骤

配置 DHCP Server 的网络参数。

```
<H3C> system-view
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[H3C-Ethernet1/0/1] quit
```

使能 DHCP Server。

```
[H3C] dhcp enable
[H3C] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

配置 Domain、创建 RADIUS 方案并配置 Domain 和 RADIUS 关联。

```
[H3C] radius scheme 123
[H3C-radius-123] primary accounting 10.1.2.2
[H3C-radius-123] quit
[H3C] domain 123
[H3C-isp-123] scheme radius-scheme 123
[H3C-isp-123] quit
```

配置 DHCP server 的地址池。

```
[H3C] dhcp server ip-pool test
[H3C-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0
```

配置 DHCP Accounting 计费使用的域为 123。

```
[H3C-dhcp-pool-test] accounting domain 123
```

9.9.5 3COM VCX 请求 option 184 组网案例

1. 组网需求

3COM VCX 设备作为 DHCP 客户端从 DHCP 服务器请求 option 184 的所有子选项配置，H3C 路由器作为 DHCP 服务器，并在全局地址池下配置支持 option 184 功能。其中 NCP-IP 地址为 3.3.3.3；Alternate Server IP 地址为 2.2.2.2；使能语音 VLAN，且语音 VLAN ID 为 1。Fail-Over IP 地址为 1.1.1.1，呼叫号码为 99*。

2. 组网图

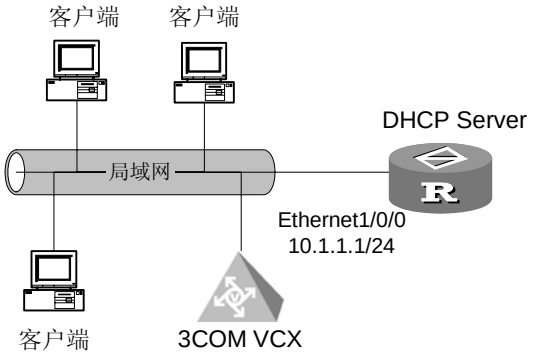


图9-11 3COM VCX 请求 option184 组网图

3. 配置步骤

(1) DHCP 客户端配置

作为 DHCP 客户端的 3COM VCX 使能 DHCP Client 功能，并配置请求 option 184 的所有子选项，配置过程略。

(2) DHCP 服务器配置

```
<H3C> system-view
[H3C] dhcp enable
[H3C] dhcp select global interface ethernet 1/0/0
[H3C] dhcp server ip-pool 123
[H3C-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
[H3C-dhcp-pool-123] voice-config as-ip 2.2.2.2
[H3C-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
[H3C-dhcp-pool-123] voice-config voice-vlan 1 enable
[H3C-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
[H3C-dhcp-pool-voice] quit
```

9.9.6 DHCP Relay 支持 option 82 典型组网举例

1. 组网需求

两台 DHCP Client 设备在网段 10.110.1.0，通过 DHCP Relay 设备从 DHCP Server 获取 IP 地址。DHCP Relay 支持 option 82 选项，且处理策略为 **keep**。

本例中假设 DHCP Relay 到 DHCP Server 的路由可达。下面将只介绍作为 DHCP 中继的配置。

2. 组网图

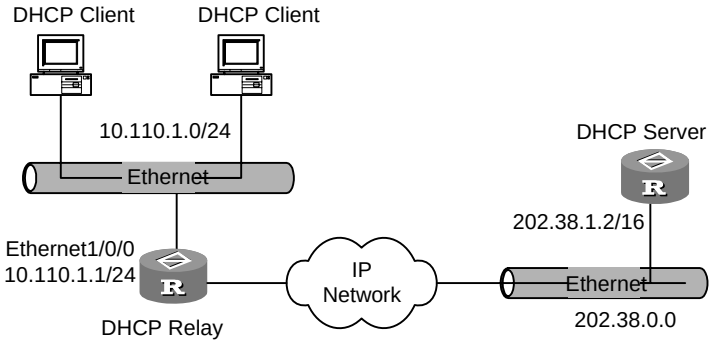


图9-12 DHCP Relay 支持 option82 组网图

3. 配置步骤

使能 DHCP 服务。

```
<H3C> system-view
[H3C] dhcp enable
```

配置 DHCP 中继接口，并为其配置 IP 地址/地址掩码以使其和 DHCP 客户端属于同一个网段。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] dhcp select relay
[H3C-Ethernet1/0/0] ip address 10.110.1.1 255.255.255.0
```

为 DHCP 中继接口指定 DHCP 服务器。

```
[H3C-Ethernet1/0/0] ip relay address 202.38.1.2
[H3C-Ethernet1/0/0] quit
```

使能 DHCP 中继支持 option 82 功能，并指定策略为 **keep**。

```
[H3C] dhcp relay information enable
[H3C] dhcp relay information strategy keep
```

DHCP 服务器配置略。

9.9.7 封装 PPP 的串口支持 DHCP 配置举例

1. 组网需求

如下图所示：DHCP Client 通过串口 Serial2/0/0 与 DHCP Relay 的串口 Serial2/0/1 连接，DHCP Relay 通过串口 Serlal2/0/0 与 DHCP Server 连接。要求 DHCP Client 的串口 Serial2/0/0 通过 DHCP Relay 从 DHCP Server 自动获得 IP 地址。

- DHCP Server 的地址池网段为 20.20.0.0/24；
- DHCP Client 与 DHCP Relay 以及 DHCP Relay 与 DHCP Server 之间的链路均为 PPP 链路。

2. 组网图

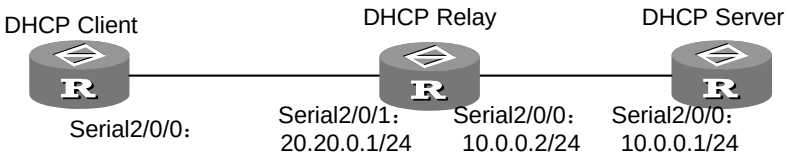


图9-13 封装 PPP 的串口支持 DHCP 配置举例示意图

3. 配置步骤

(1) 配置 DHCP Server

```
<H3C> system-view
[H3C] dhcp enable
[H3C] dhcp select global interface serial 2/0/0
[H3C] dhcp server ip-pool 1
[H3C-dhcp-pool-1] network 20.20.0.0 mask 255.255.255.0
[H3C-dhcp-pool-1] gateway-list 20.20.0.1
[H3C-dhcp-pool-1] domain-name h3c.com
[H3C-dhcp-pool-1] quit
[H3C] interface serial 2/0/0
[H3C-serial2/0/0] link-protocol ppp
[H3C-serial2/0/0] ip address 10.0.0.1 255.255.255.0
[H3C-serial2/0/0] quit
[H3C] ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

(2) 配置 DHCP Relay

```
<H3C> system-view
[H3C] dhcp enable
[H3C] interface serial 2/0/0
[H3C-serial2/0/0] link-protocol ppp
[H3C-serial2/0/0] ip address 10.0.0.2 255.255.255.0
[H3C-serial2/0/0] quit
[H3C] interface serial 2/0/1
```

```
[H3C-serial2/0/1] link-protocol ppp
[H3C-serial2/0/1] ip address 20.20.0.1 255.255.255.0
[H3C-serial2/0/1] ip relay address 10.10.0.1
[H3C-serial2/0/1] dhcp select relay
[H3C-serial2/0/1] quit
```

(3) 配置 DHCP Client

```
<H3C> system-view
[H3C] dhcp enable
[H3C] interface serial 2/0/0
[H3C-serial2/0/0] link-protocol ppp
[H3C-serial2/0/0] ip address dhcp-alloc
[H3C-serial2/0/0] quit
```

第10章 IP 性能配置

10.1 IP 性能配置

10.1.1 配置接口最大传输单元（MTU）

接口最大传输单元决定了在该接口上的报文是否需要分片。

请在接口视图下进行下列操作。

表10-1 配置接口最大传输单元

操作	命令
配置接口最大传输单元	**mtu** *mtu-size*
恢复接口最大传输单元的缺省值	**undo mtu**

接口最大传输单元的缺省值为 1500 字节。

10.1.2 配置 TCP 报文分片

该命令用来配置 TCP 最大报文分片的长度，这个长度决定了该接口上的 TCP 报文是否需要分片。

请在接口视图下进行下列操作。

表10-2 配置 TCP 报文分片

操作	命令
配置 TCP 报文分片	**tcp mss** *value*
取消 TCP 报文分片	**undo tcp mss**

缺省情况下，TCP 报文不分片。

10.1.3 配置 TCP 属性

可以配置的 TCP 属性包括：

- synwait 定时器：当发送 syn 报文时，TCP 启动 synwait 定时器，若 synwait 超时前未收到回应报文，则 TCP 连接将被终止。synwait 定时器的超时时间取值范围为 2～600 秒，缺省值为 75 秒。

- finwait 定时器：当 TCP 的连接状态由 FIN_WAIT_1 变为 FIN_WAIT_2 时启动 finwait 定时器，若 finwait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。finwait 的取值范围为 76～3600 秒，finwait 的缺省值为 675 秒。
- 面向连接 Socket 的接收和发送缓冲区的大小：范围为 1～32K 字节，缺省值为 8K 字节。

请在系统视图下进行下列配置。

表10-3 配置 TCP 属性

操作	命令
配置 TCP 连接建立 synwait 定时器时间	**tcp timer syn-timeout** *time-value*
恢复 TCP 连接建立 synwait 定时器时间为缺省值	**undo tcp timer syn-timeout**
配置 TCP 的 FIN_WAIT_2 定时器时间	**tcp timer fin-timeout** *time-value*
恢复 TCP 的 FIN_WAIT_2 定时器时间为缺省值	**undo tcp timer fin-timeout**
配置 TCP 的 Socket 接收和发送缓冲区的大小	**tcp window** *window-size*
恢复 TCP 的 Socket 接收和发送缓冲区的大小为缺省值	**undo tcp window**

缺省情况下，TCP finwait 定时器缺省为 675 秒，TCP synwait 定时器缺省值为 75 秒，面向连接 Socket 的收发缓冲区大小缺省为 8K 字节。

10.1.4 配置 ICMP 发送重定向报文

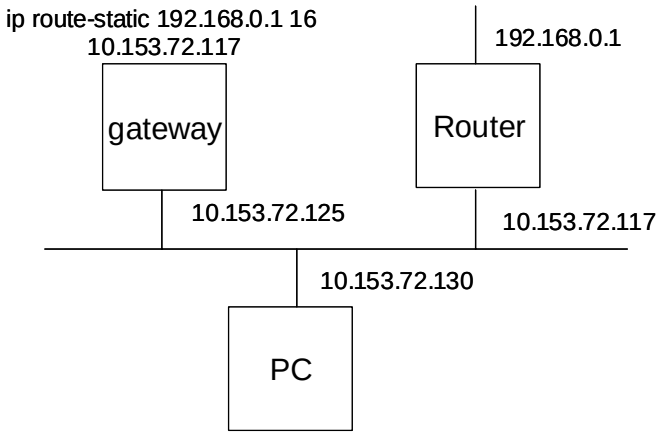


图10-1 配置 ICMP 发送重定向报文示意图

如上图示连接情况，PC 要发送报文到 Router，会先将报文发送到网关，再由网关转发给 Router。这种情况下可以在网关上使能 ICMP 发送重定向报文功能，这样网关会发送重定向报文给 PC，使 PC 直接将报文发送给 Router。

请在系统视图下进行下列配置。

表10-4 配置 ICMP 发送重定向报文

操作	命令
打开 ICMP 发送重定向报文功能	**icmp redirect send**
关闭 ICMP 发送重定向报文功能	**undo icmp redirect send**

缺省情况下，打开 ICMP 发送重定向报文功能。

10.1.5 IP 性能显示和调试

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

执行 **reset** 命令可以清除该运行情况的统计信息。

在用户视图下，执行 **debugging** 命令可以对 IP 性能进行调试。

表10-5 IP 性能显示和调试

操作	命令
显示 TCP 连接状态	**display tcp status**
显示 TCP 流量统计信息	**display tcp statistics**
显示 UDP 流量统计信息	**display udp statistics**
显示系统当前所有的套接口信息	**display ip socket** [**socktype** *sock_type*] [*task_id socket_id*]
显示 IP 层接口表信息	**display ip interface** [*interface-type interface-number*]
显示接口板的 FIB 表	**display fib**
据正则表达式输出缓冲区中与包含字符串 *text* 相关的行	**display fib** | { **begin** | **include** | **exclude** } *text*
显示过滤 FIB 信息	**display fib acl** *acl-number*
按照目的地址进行匹配显示 FIB 表项	**display fib** *dest-addr1* [*dest-mask1*] [**longer**]
显示目的地址在输入的 *dest-addr1 dest-mask1* 到 *dest-addr2 dest-mask2* 范围内的 FIB 表项	**display fib** *dest-addr1 dest-mask1 dest-addr2 dest-mask2*
根据所输入的 ip-prefix 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	**display fib ip-prefix** *listname*
显示 FIB 表项的总数目	**display fib statistics**
打开 IP 报文调试信息开关	**debugging ip packet** [**acl** *acl-number*]
关闭 IP 报文调试信息开关	**undo debugging ip packet**
打开 ICMP 报文调试信息开关	**debugging ip icmp**

操作	命令
关闭 ICMP 调试信息开关	**undo debugging ip icmp**
打开 TCP 报文调试信息开关	**debugging tcp packet** [*task_id socket_id*]
关闭 TCP 报文调试信息开关	**undo debugging tcp packet** [*task_id socket_id*]
打开 UDP 连接的调试信息	**debugging udp packet** [*task_id socket_id*]
关闭 UDP 连接的调试信息	**undo debugging udp packet** [*task_id socket_id*]
打开 TCP 事件的调试开关	**debugging tcp event** [*task_id socket_id*]
关闭 TCP 事件的调试开关	**undo debugging tcp event** [*task_id socket_id*]
打开 TCP 连接的 MD5 认证调试开关	**debugging tcp md5**
关闭 TCP 连接的 MD5 认证调试开关	**undo debugging tcp md5**
清除 IP 统计信息	**reset ip statistics**
清除 TCP 流量统计信息	**reset tcp statistics**
清除 UDP 流量统计信息	**reset udp statistics**

10.2 接口转发广播报文配置

10.2.1 配置接口转发广播报文

正常情况下路由器不会转发二层广播报文，但某些特殊应用希望路由器能够转发二层广播报文，如：跨网络的远程唤醒（Wake On Lan，WOL）应用，需要路由器将运行远程唤醒程序的服务器发出的唤醒帧（为二层广播帧）转发到某个指定的网络中，此时请在接口视图下进行下列配置。

表10-6 配置所在接口转发广播报文

操作	命令
配置所在接口转发广播报文	**ip forward-broadcast** [*acl-number*]
取消接口转发广播报文	**undo ip forward-broadcast**

缺省情况下，路由器不转发广播报文。

10.2.2 利用路由器实现远程 WOL 组网应用

1. 组网需求

在 PC1 上运行远程唤醒软件（如 magic packet.exe）唤醒远端 192.168.1.0/24 网段中的所有 PC。

- 保证 PC1 与 192.168.1.0/24 网段之间路由可达；
- 保证 192.168.1.0/24 网段中的所有 PC 都支持远程唤醒（需要电源、网卡、主板都支持）；
- 在路由器的 Ethernet1/0/1 接口上使能接口转发广播报文的功能；
- 保证仅来自于 192.168.2.1 的“唤醒”报文被转发到 192.168.1.0/24 网段中。

2. 组网图

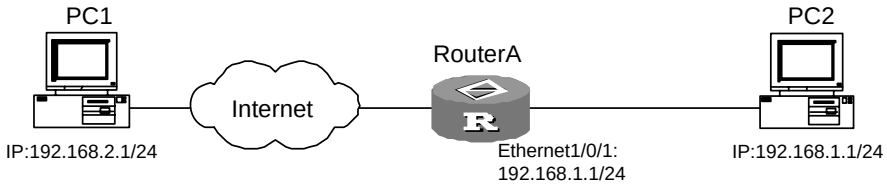


图10-2 利用路由器实现远程 WOL 组网应用

3. 配置过程

路由器 A 的配置：

```
<H3C> system-view
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 192.168.1.2 24
[H3C-Ethernet1/0/1] ip forward-broadcast 2100
[H3C-Ethernet1/0/1] quit
[H3C] acl number 2100
[H3C-acl-basic-2100] rule 1 permit source 192.168.2.1 0
[H3C-acl-basic-2100] rule 2 deny source any
```

10.3 单播快速转发配置

10.3.1 单播快速转发简介

报文转发效率是衡量路由器性能的一项关键指标。按照常规流程，路由器在一个报文到达后，将它从接口存储器拷贝至主 CPU 中，CPU 从 IP 地址中确定网络号，查找路由表以确定一条最佳的路径将报文转发出去，同时为报文封装链路层帧头，封装后的帧再通过 DMA（直接内存访问）拷贝到输出队列中，这个过程两次经过主系统总线。每一个报文的转发都要重复这个过程。

单播快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。我们知道在 Internet 网上的数据基本上都是基于数据流的。一个数据流就是指在网上两个特定主机之间的一次特定的应用，比如一次 FTP 操作传输一个文件。我们一般用一个 5 元组描述一个数据流：源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号。当一个数据流的第一个报文通过查找路由表转发后，在高速缓存中生成相应的交换信息，后续相同的报文的转发，就可以通过直接查找高速缓存来实现转发。这样便大大缩减了 IP 报文的排队流程，减少路由查找时间，提高了 IP 报文的转发吞吐量。由于高速缓存中的转发表已经做过优化，因此查找速度将大大提高。

Comware 实现的单播快速转发，具有下列特性：

- 支持在各类高速链路接口上（包括子接口）提供单播快速转发，包括以太网、同步 PPP、帧中继、HDLC 等。
- 支持在配置了普通防火墙的情况下，提供单播快速转发的功能。
- 支持在配置了 ASPF 防火墙的情况下，提供单播快速转发的功能。
- 支持在配置了地址转换的情况下，提供单播快速转发的功能。
- 支持在配置了 GRE 的情况下，提供单播快速转发的功能
- 能大幅度提高报文的转发效率。

单播快速转发的性能有时会受到某些特性的影响，比如报文的队列管理，报文头压缩等。另外，单播快速转发能处理已经分片的 IP 报文，但不支持对 IP 报文的再分片。

10.3.2 单播快速转发配置

用户可根据需要禁止快速转发，如对报文转发要求使用负载分担时，要在相应方向上禁止接口进行快速转发。

请在接口视图下进行下列配置。

表10-7 允许/禁止接口进行单播快速转发

操作	命令
允许接口双向进行单播快速转发	**ip fast-forwarding**
允许在入接口方向上进行单播快速转发	**ip fast-forwarding inbound**
允许在出接口方向上进行单播快速转发	**ip fast-forwarding outbound**
禁止接口进行单播快速转发	**undo ip fast-forwarding** [**inbound** | **outbound**]

缺省情况下，接口在入/出的双向上都使能单播快速转发。

⚠ 注意：

- 如果要求对报文转发要求使用负载分担，必须在相应方向上禁止接口进行快速转发。
- 在接口上配置了快速转发后，该接口上的 IP 报文的调试信息将不再输出， 即 **debugging ip packet** 不起作用。

10.3.3 单播快速转发的显示和调试

表10-8 单播快速转发的显示和调试

操作	命令
显示单播快速转发表信息	**display ip fast-forwarding cache**[*ip-address*]
清除单播快速转发缓冲区中的内容	**reset ip fast-forwarding cache**

10.4 组播快速转发配置

10.4.1 组播报文快速转发简介

报文转发效率是衡量路由器性能的一项关键指标。按照常规流程，路由器在一个报文到达后，将它从接口存储器拷贝至主 CPU 中，CPU 从 IP 地址中确定网络号，查找路由表以确定一条最佳的路径，同时为报文封装链路层帧头，封装后的帧再从 DMA（直接内存访问）拷贝到输出队列中。这个过程两次经过主系统总线，且每一个报文的转发都要重复这个过程。

快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。Internet 上的数据基本上都是基于数据流的，一个数据流就是指在网上两个特定主机之间的一次特定的应用，比如一次 FTP 操作传输一个文件。我们一般用一个 5 元组描述一个数据流：源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号。当一个数据流的第一个报文通过查找路由表转发后，在高速缓存中生成相应的交换信息，后续报文的转发，就可以通过直接查找高速缓存来实现转发。这样便大大缩减了 IP 报文的排队流程、减少路由查找时间，提高了 IP 报文的转发吞吐量，由于高速缓存中的转发表已经做过优化，因此查找速度特别快。

组播报文快速转发，具有下列特性：

- 支持在各类高速链路接口上提供快速转发，包括以太网、ATM、同步 PPP、帧中继、HDLC 等。
- 支持在配置了包过滤防火墙的情况下，提供快速转发的功能。
- 支持在配置了 QoS 的情况下，提供快速转发的功能。

- 能大幅度提高报文的转发效率。

10.4.2 组播报文快速转发配置

用户可根据需要使能快速转发。

请在接口视图下进行下列配置。

表10-9 允许/禁止接口进行组播报文快速转发

操作	命令
允许接口进行组播报文快速转发	**ip multicast-fast-forwarding**
禁止接口进行组播报文快速转发	**undo ip multicast-fast-forwarding**

缺省情况下，接口未使能组播快速转发。

10.4.3 组播报文快速转发的显示和调试

表10-10 组播报文快速转发的显示和调试

操作	命令
显示组播快速转发表信息	**display ip multicast-fast-forwarding cache** [*multicast-group*]
清除组播快速转发缓冲区中的内容	**reset ip multicast-fast-forwarding cache**

10.5 IP 性能配置排错

故障之一：TCP 和 UDP 协议不能正常工作。

故障排除：可以打开相应的调试开关，查看调试信息。

- 用 **debugging udp packet** 命令打开 UDP 调试开关，跟踪 UDP 的数据包。当路由器发送或接收到 UDP 数据包，就可以实时显示出数据报的内容格式。根据数据报的内容，来发现问题之所在。

以下为 UDP 数据报的格式：

```
*0.377770-SOCKET-8-UDP:
1043494431: Output: task = ROUT(6), socketid = 3,
src = 1.1.1.1:520, dst = 255.255.255.255:520, datalen = 24
```

- 用 **debugging tcp packet** 命令打开 TCP 调试开关，跟踪 TCP 的数据包。TCP 可以有两种数据报的格式供选择。一种是调试跟踪所有以本设备为一端的 TCP 连接的 TCP 报文收发。操作如下：

```
[H3C] info-center enable
```

```
[H3C] quit
<H3C> debugging tcp packet
```

即可实时查看接收或发送的 TCP 报文，其具体报文格式如下：

```
*0.100070-SOCKET-8-TCP PACKET:
1043204051:  Input: Co0(5) socketId = 2, state = SYN_SENT,
src = 127.0.0.1:1025, dst = 2.2.2.2:23,
seq = 11084380, ack = 0, optlen = 4, flag = SYN ,
window = 8192
```

另外一种是调试跟踪其中 SYN、FIN 或 RST 置位的报文。

操作如下：

```
[H3C] info-center enable
[H3C] quit
<H3C> debugging tcp event
```

这样即可实时查看接收或发送的 TCP 报文，其具体报文格式同上。

第11章 地址转换（NAT）的配置

11.1 地址转换（NAT）简介

11.1.1 地址转换概述

如 RFC1631 所描述，NAT（Network Address Translation，地址转换）是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问外部网络的功能。这种通过使用少量的公有 IP 地址代表多数的私有 IP 地址的方式将有助于减缓可用 IP 地址空间枯竭的速度。

🕮 **说明：**

私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的 IP 地址。RFC1918 为私有网络预留出了三个 IP 地址块，如下：

A 类：10.0.0.0 ~ 10.255.255.255

B 类：172.16.0.0 ~ 172.31.255.255

C 类：192.168.0.0 ~ 192.168.255.255

上述三个范围内的地址不会在因特网上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。

下图描述了一个基本的 NAT 应用。

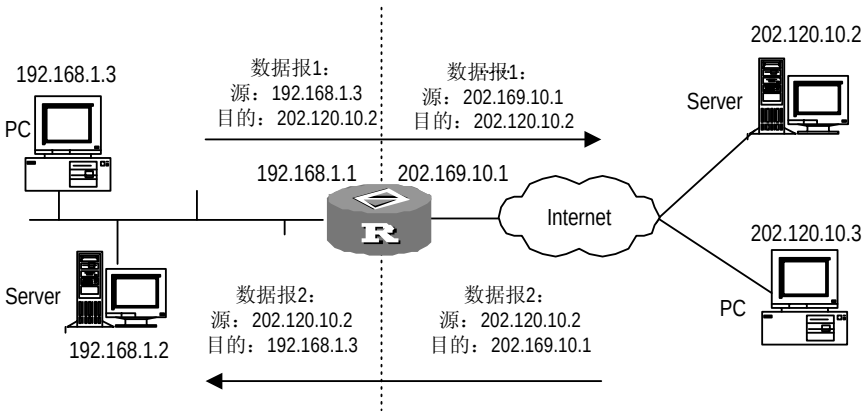


图11-1 地址转换的基本过程

NAT 服务器处于私有网络和公有网络的连接处。当内部 PC（192.168.1.3）向外部服务器（202.120.10.2）发送一个数据报 1 时，数据报将通过 NAT 服务器。NAT 进程查看报头内容，发现该数据报是发往外网的，那么它将数据报 1 的源地址字段的私有地址 192.168.1.3 换成一个可在 Internet 上选路的公有地址 202.169.10.1，并将该数据报发送到外部服务器，同时在网络地址转换表中记录这一映射；外部服务

器给内部 PC 发送应答报文 2（其初始目的地址为 202.169.10.1），到达 NAT 服务器后，NAT 进程再次查看报头内容，然后查找当前网络地址转换表的记录，用原来的内部 PC 的私有地址 192.168.1.3 替换目的地址。

上述的 NAT 过程对终端（如图中的 PC 和服务器）来说是透明的。对外部服务器而言，它认为内部 PC 的 IP 地址就是 202.169.10.1，并不知道有 192.168.1.3 这个地址。因此，NAT“隐藏”了企业的私有网络。

地址转换的优点在于，为内部主机提供了“隐私”（Privacy）保护前提下，实现了内部网络的主机通过该功能访问外部网络资源。但它也有一些缺点：

- 由于需要对数据报文进行 IP 地址的转换，涉及 IP 地址的数据报的报头不能被加密。在应用协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的 FTP 连接，否则 FTP 的 port 命令不能被正确转换。
- 网络调试变得更加困难。比如，某一台内部网络的主机试图攻击其它网络，则很难指出究竟是哪一台机器是恶意的，因为主机的 IP 地址被屏蔽了。
- 在链路的带宽低于 10Mbit/s 速率时，地址转换对网络性能基本不构成影响，此时，网络传输的瓶颈在传输线路上；当速率高于 10Mbit/s 时，地址转换将对路由器性能产生一些影响。

11.2 地址转换实现的功能

11.2.1 多对多地址转换及地址转换的控制

从上图的地址转换过程可见，当内部网络访问外部网络时，地址转换将会选择一个合适的外部地址，替代内部网络数据报文的源地址。在上图中是选择 NAT 服务器出接口的 IP 地址（公有地址）。这样所有内部网络的主机访问外部网络时，只能拥有一个外部的 IP 地址，因此，这种情况只允许最多有一台内部主机访问外部网络，这称为“一对一地址转换”。当内部网络的主机并发的要求访问外部网络时，“一对一地址转换”仅能够实现其中一台主机的访问请求。

NAT 的一种变形实现了并发性。允许 NAT 服务器拥有多个公有 IP 地址，当第一个内部主机访问外网时，NAT 选择一个公有地址 IP1，在地址转换表中添加记录并发送数据报；当另一内部主机访问外网时，NAT 选择另一个公有地址 IP2，以此类推，从而满足了多台内部主机访问外网的请求。这称为“多对多地址转换”。

🕮 **说明：**

NAT 服务器拥有的公有 IP 地址数目要远少于内部网络的主机数目，因为所有内部主机并不会同时访问外网。公有 IP 地址数目的确定，应根据网络高峰期可能访问外网的内部主机数目的统计值来确定。

在实际应用中，我们可能希望某些内部的主机具有访问 Internet（外部网络）的权利，而某些主机不允许访问。即当 NAT 进程查看数据报报头内容时，如果发现源 IP 地址是为那些不允许访问网络的内部主机所拥有的，它将不进行 NAT 转换。这就是一个对地址转换进行控制的问题。

H3C 系列路由器可以通过定义地址池来实现多对多地址转换，同时利用访问控制列表来对地址转换进行控制的。

- 地址池：用于地址转换的一些公有 IP 地址的集合。用户应根据自己拥有的合法 IP 地址数目、内部网络主机数目以及实际应用情况，配置恰当的地址池。地址转换的过程中，将会从地址池中挑选一个地址做为转换后的源地址。
- 利用访问控制列表限制地址转换：只有满足访问控制列表条件的数据报文才可以进行地址转换。这可以有效地控制地址转换的使用范围，使特定主机能够有权利访问 Internet。

11.2.2 NAPT——网络地址端口转换

还有一种 NAT 变形－－这就是 NAPT（Network Address Port Translation），NAPT 允许多个内部地址映射到同一个公有地址上，非正式的也可称之为“多对一地址转换”或地址复用。

NAPT 映射 IP 地址和端口号，来自不同内部地址的数据报可以映射到同一外部地址，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。也就是<私有地址+端口>与<公有地址+端口>之间的转换。

下图描述了 NAPT 的基本原理。

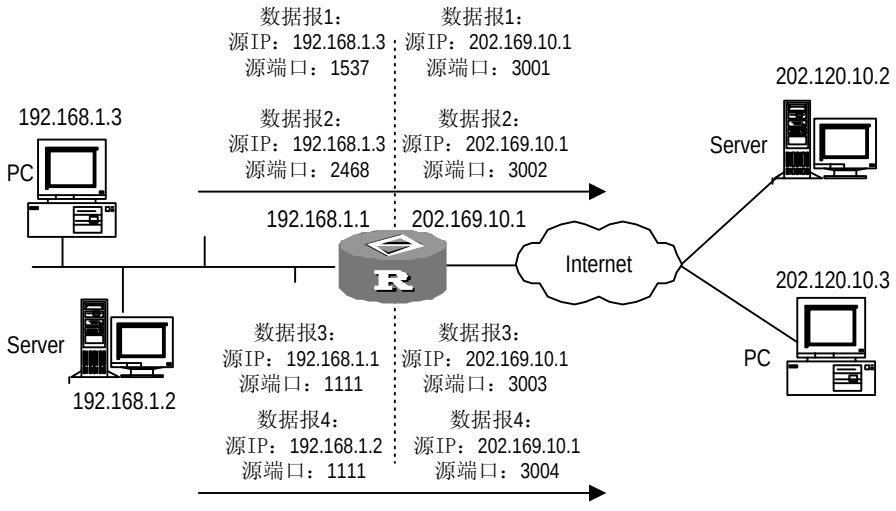


图11-2 NAPT 地址复用示意图

如图所示，四个带有内部地址的数据报到达 NAT 服务器，其中数据报 1 和 2 来自同一个内部地址但有不同的源端口号，数据报 3 和 4 来自不同的内部地址但具有相同

的源端口号。通过 NAT 映射，四个数据报都被转换到同一个外部地址，但每个数据报都赋予了不同的源端口号，因而仍保留了报文之间的区别。当回应报文到达时，NAT 进程仍能够根据回应报文的目的地址和端口号来区别该报文应转发到的内部主机。

11.2.3 静态网段地址转换

该特性实现了一种新的 NAT 静态地址转换方式，即将指定范围内的内部主机地址转换为指定的公网网段地址，转换过程中只对网段地址进行转换，保持主机地址不变。当内部主机访问外部网络时，如果主机地址在指定的内部主机地址范围内，会被转换为对应的公网地址；同样当通过公网网段地址对内部主机进行访问时，可以直接访问到内部主机（该公网地址在转换后在指定的内部主机地址范围内）。

通过 NAT 网段地址转换功能实现了内部主机地址和公网地址的直接映射关系，且同时提供了类似 NAT Server 的功能。

静态网段地址转换方式中公网 IP 地址与私网 IP 地址一一对应，因此比较浪费 IP 地址空间，故可以考虑与传统的静态地址转换或动态地址转换配合使用，只要不存在地址冲突即可。

静态地址转换还支持 NAT 多实例的配置，使得外部主机可以访问 MPLS VPN 内主机。

11.2.4 双向地址转换

常规地址转换技术只转换报文的源地址或目的地址，而双向地址转换（Bidirectional 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重叠的情况。如图所示：内部网络主机 PC1 和主机 PC3 的地址重叠。这种情况下，内部网络主机 PC1 或 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。双向 NAT 技术通过在 RouterA 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。

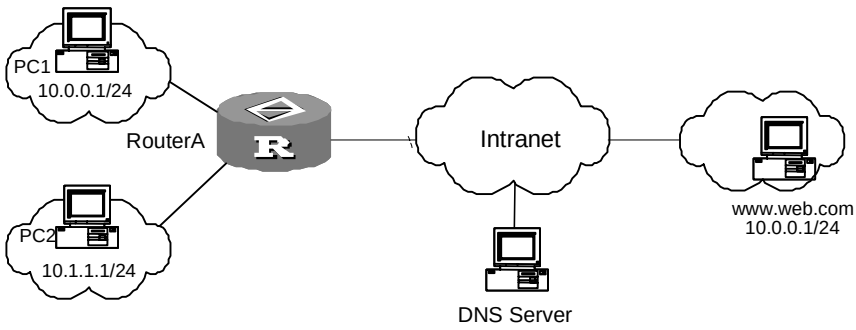


图11-3 双向地址转换应用组网图

例如，在 RouterA 上配置双向地址转换：

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，子网掩码为 24 位。

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 直接用域名访问主机 PC3 时，报文的处理流程如下：

(1) PC2 发送解析 www.web.com的DNS请求，经私网DNS服务器解析后，RouterA 收到 DNS服务器的响应报文。RouterA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 向 www.web.com发起方问（即向对应的临时地址 3.0.0.1 发起访问），当报文到达RouterA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 RouterA 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。

11.2.5 内部服务器

NAT 隐藏了内部网络的结构，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 的服务器，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 202.169.10.10 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）。

H3C 系列路由器的 NAT 功能提供了内部服务器功能供外部网络访问。外部网络的用户访问内部服务器时，NAT 将请求报文内的目的地址转换成内部服务器的私有地址。对内部服务器回应报文而言，NAT 要将回应报文的源地址（私网地址）转换成公网地址。

11.2.6 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。

11.2.7 地址转换应用网关

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，将会严重影响后继的协议交互。

地址转换应用网关（NAT Application Level Gateway，NAT ALG）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 Comware 的 NAT ALG 支持 PPTP、DNS、FTP、ILS、MSN、NBT、SIP、H.323 等协议。

11.2.8 支持 NAT 多实例

NAT 多实例允许分属于不同 MPLS VPN 的用户通过同一个出口访问外部网络（Internet），同时允许不同的 VPN 用户使用相同的私网地址。当 MPLS VPN 用户访问 Internet 时，Comware 的地址转换将内部网络主机的 IP 地址和端口替换为路由器的外部网络地址和端口，同时还记录了用户的 MPLS VPN 信息（如协议类型和路由标识符 RD 等）。报文还原时，地址转换将外部网络地址和端口还原为内部网络主机的 IP 地址和端口，同时获得了是哪一个 MPLS VPN 用户的访问。无论 PAT 方式的地址转换，还是 NO-PAT 方式的地址转换都支持多实例。

Comware 的地址转换支持内部服务器的多实例，提供给外部访问 MPLS VPN 内主机的机会。例如，VPN1 内提供 WWW 服务的主机地址是 10.110.1.1，可以使用 202.110.10.20 作为 web 服务器的外部地址，Internet 的用户使用 202.110.10.20 的地址就可以访问到 MPLS VPN1 提供的 WWW 服务。

11.3 NAT 限制最大连接数

如果局域网内的某台 PC 感染病毒，它会发起大量的连接，迅速消耗路由器资源，导致路由器效率下降，影响其他用户使用。NAT 限制最大连接数可以避免出现这种情况。通过连接数限制功能，可以设置某种特征的连接数上限，从而可以实现 NAT 限制最大连接数的功能。

连接数限制的配置相当灵活，用户可以通过配置策略实现针对不同的连接进行限制。用户配置的策略包括两方面的内容：

1. 符合什么特征的报文需要被限制。

可以通过 ACL 来指定报文的特征，如基于报文的源地址、基于报文的目的地址、基于服务，用户可以根据自己的需要使用 ACL 灵活地指定。

2. 对于符合指定特征的连接如何进行限制。

用户可以通过指定上限和下限两个阈值来控制是否允许建立连接。当符合某种特征的连接数达到上限时禁止建立该种连接。当连接数降低到小于等于下限时，允许建立连接。

11.4 NAT 的配置

NAT 配置包括：

- 配置地址池
- 配置地址转换
- 配置 Easy IP
- 配置静态地址转换
- 配置多对多地址转换
- 配置 NAPT
- 配置内部服务器
- 配置地址转换应用网关
- 配置地址转换有效时间（选配）
- 配置最大连接数限制（选配）

11.4.1 配置地址池

地址池是一些连续的 IP 地址集合，当内部数据包通过地址转换到达外部网络时，将会选择地址池中的某个地址作为转换后的源地址。

请在系统视图下进行下列配置。

表11-1 配置地址池

操作	命令
定义一个地址池	**nat address-group** *group-number start-addr end-addr*
删除一个地址池	**undo nat address-group** *group-number*

⚠ 注意：

当某个地址池已经和某个访问控制列表关联进行地址转换，是不允许删除这个地址池的。

📖 说明：

如路由器仅提供 easy IP 功能，则不需要配置 NAT 地址池，直接使用接口地址作为转换后的 IP 地址。

11.4.2 配置地址转换

将访问控制列表和地址池关联（或接口地址）后，即可实现地址转换。这种关联指定了“具有某些特征的 IP 报文”才可以使用“这样的地址池中的地址(或接口地址)”。当内部网络有数据包要发往外部网络时，首先根据访问列表判定是否是允许的数据包，然后根据转换关联找到与之对应的地址池（或接口地址）进行转换。

访问控制列表的配置请参见相关章节.

不同形式的形式地址转换，配置方法稍有不同。

1. Easy IP

如果地址转换命令不带 **address-group** 参数，即仅使用 **nat outbound** *acl-number* 命令，则实现了 easy-ip 的特性。地址转换时，直接使用接口的 IP 地址作为转换后的地址，利用访问控制列表控制哪些地址可以进行地址转换。

请在接口视图下进行下列配置。

表11-2 配置 Easy IP

操作	命令
配置访问控制列表和接口地址关联	**nat outbound** *acl-number*
删除访问控制列表和接口地址的关联	**undo nat outbound** *acl-number*

2. 使用指定 loopback 接口进行地址转换

请在接口视图下进行下列配置。

表11-3 使用指定 loopback 接口进行地址转换

操作	命令
配置访问控制列表和指定的 loopback 接口地址关联	**nat outbound** *acl-number* **interface** *interface-type interface-number*

操作	命令
删除访问控制列表和指定 loopback 接口地址的关联	**undo nat outbound** *acl-number* **interface** *interface-type interface-number*

匹配访问控制列表的数据报文的源地址将转换为指定的 loopback 接口的 IP 地址。

3. 配置静态地址转换表

(1) 配置一对一静态地址转换表

请在系统视图下进行下列配置。

表11-4 配置一对一静态地址转换表

操作	命令
配置从内部地址到外部地址的一对一静态地址转换表	**nat static** [**vpn-instance** *vpn-instance-name*] *inside-ip global-ip*
删除已经配置得 NAT 一对一静态地址转换表	**undo nat static** [**vpn-instance** *vpn-instance-name*] *inside-ip global-ip*

(2) 配置静态网段地址转换表

使用静态网段地址转换时， 只进行网段地址的转换，而保持主机地址不变。

请在系统视图下进行下列配置。

表11-5 配置网段地址静态转换表

操作	命令
配置从内部地址到外部地址的静态网段地址转换表	**nat static inside** [**vpn-instance** *vpn-instance-name*] **ip** *inside-start-address inside-end-address* **global ip** *global-ip* { *mask* | *prefix-length* }
删除已经配置的 NAT 网段地址转换表	**undo nat static inside** [**vpn-instance** *vpn-instance-name*] **ip** *inside-start-address inside-end-address* **global ip** *global-ip* { *mask* | *prefix-length* }

nat static inside 和 **nat static** 会分别创建两种不同的 NAT 静态表项，在具体的配置中，两种 NAT 静态表项不存在冲突即可。

🕮 **说明：**

使用 **nat static inside** 配置地址转换时，必须确保转换后的 **global** 地址不包含网络设备已使用的 IP 地址。

---

(3) 使静态地址转换在接口上生效

表11-6 使静态地址转换在接口上生效

操作	命令
使已经配置的 NAT 静态地址转换在接口上生效	**nat outbound static**

4. 配置多对多地址转换

将访问控制列表和地址池关联后，即可实现多对多地址转换。请在接口视图下进行下列配置。

表11-7 配置多对多地址转换

操作	命令
配置访问控制列表和地址池关联	**nat outbound** *acl-number* **address-group** *group-number* [**no-pat**]
删除访问控制列表和地址池的关联	**undo nat outbound** *acl-number* **address-group** *group-number* [**no-pat**]

5. 配置 NAPT

将访问控制列表和 NAT 地址池关联时，如果选择 **no-pat** 参数，则表示只转换数据包的 IP 地址而不使用端口信息，即不使用 NAPT 功能；如果不选择 no-pat 参数，则启用 NAPT 功能。缺省情况是启用。

请在接口视图下进行下面配置。

表11-8 配置 NAPT

操作	命令
配置访问控制列表和地址池关联	**nat outbound** *acl-number* [**address-group** *group-number*]
删除访问控制列表和地址池的关联	**undo nat outbound** *acl-number* [**address-group** *group-number*]

6. 配置 NAT 多实例

无论 Easy IP、多对多地址转换，还是 NAPT，都可以支持 NAT 多实例的配置。只要在访问控制列表的规则 **rule** 中配置 **vpn–instance** *vpn-instance-name*，指明那些 MPLS VPN 用户需要进行地址转换，即可以实现对 **MPLS VPN** 的支持。

11.4.3 配置双向地址转换

请在系统视图下进行下面配置。

表11-9 配置双向地址转换

操作	命令
配置重叠地址池到临时地址池的映射	**nat overlapaddress** *number overlappool-startaddress temppool-startaddress* { **pool-length** *pool-length* | **address-mask** *mask* }
删除重叠地址池到临时地址池的映射	**undo nat overlapaddress** *number*

11.4.4 配置内部服务器

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，提供了外部网络可访问内部服务器的功能。内部服务器与外部网络的映射表是由 **nat server** 命令配置的。

用户需要提供的信息包括：外部地址、外部端口、内部服务器地址、内部服务器端口以及服务协议类型。

H3C 系列路由器支持使用接口地址作为 NAT Server 的公网地址。当路由器的公网接口通过拨号或 DHCP 方式获取公网地址时，其 NAT Server 的公网地址可以动态更新，方便用户配置。

当内部服务器位于 MPLS VPN 时，还应指定所属的 *vpn-instance-name*。如果不设置该值，表示内部服务器属于一个普通的私网，不属于某一个 MPLS VPN。

请在接口视图下进行下列配置。

表11-10 配置内部服务器

操作	命令
配置一个内部服务器	**nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* [*global-port*] | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-addr* [*host-port*] **nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr global-port*1 *global-port2* | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-addr1 host-addr2 host-port*

操作	命令
删除一个内部服务器	**undo nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* [*global-port*] | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-addr* [*host-port*] **undo nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr global-port1 global-port2* | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-addr1 host-addr2 host-port*

⚠ 注意：

- *global-port* 和 *inside-port* 只要有一个定义了 any，则另一个要么不定义，要么是 any。
- 配置 tftp 的 **nat server** 时，为了保证 NAT 正常转换，应该对内网的 tftp 服务器配置 **nat outbound**。

11.4.5 配置地址转换应用网关

请在系统视图下进行下面配置

表11-11 配置地址转换应用网关

操作	命令
配置地址转换应用网关	**nat alg** { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** | **sip** }
禁用地址转换应用网关功能	**undo nat alg** { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** | **sip** }

缺省情况下，使能地址转换应用网关功能。

11.4.6 配置内部主机通过域名区分并访问其对应的内部服务器

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，请在系统视图下进行下面配置。

表11-12 配置内部主机通过域名区分并访问其对应的内部服务器

操作	命令
配置一条域名到外部 IP 地址、端口号、协议类型的映射	**nat dns-map** *domain-name global-addr global-port* [**tcp** | **udp**]

操作	命令
删除一条域名到外部 IP 地址、端口号、协议类型的映射。	**undo nat dns-map** *domain-name*

最多允许配置 16 条映射。

11.4.7 配置地址转换有效时间

由于地址转换所使用的 HASH 表不能永久存在，该命令支持用户可为 TCP、UDP、ICMP 协议分别设置 HASH 表有效的时间，若在设定的时间内未使用该 HASH 表，将失效。举例来说，某个 IP 地址为 10.110.10.10 的用户利用端口 2000 进行了一次对外 TCP 连接，地址转换为它分配了相应的地址和端口，但是若在一定时间内他一直未使用这个 TCP 连接，系统将把这个连接删除。

请在系统视图下进行下列配置。

表11-13 配置地址转换的有效时间

操作	命令
配置地址转换有效时间	**nat aging-time** { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

参数 default 表示采用系统缺省的地址转换有效时间。

缺省情况下，dns 协议地址转换有效时间为 60 秒，ftp 协议控制链路地址转换有效时间为 7200 秒，ftp 协议数据链路地址转换有效时间为 240 秒，PPTP 协议地址转换有效时间为 86400 秒，TCP 地址转换有效时间为 86400 秒，TCP 协议 fin 、rst 或 syn 连接地址转换有效时间为 60 秒， UDP 地址转换有效时间为 300 秒，ICMP 地址转换有效时间为 60 秒。

11.4.8 配置最大连接数限制

表11-14 配置最大连接数限制

操作	命令	说明
进入系统视图	**system-view**	-
创建 ACL 并进入 ACL 视图	**acl number** *acl-number*	必选
在 ACL 下定义规则	**rule** [*rule-id*] { **permit** | **deny** | **comment** *text* } **source** [*sour-addr sour-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]	必选
退出 ACL 视图	**quit**	-

操作	命令	说明
使能连接数限制功能	**connection-limit enable**	必选 缺省情况下，关闭连接数限制功能
设置在查不到连接数限制策略时的动作	**connection-limit default { permit | deny }**	可选 缺省为 deny
设置连接数限制的缺省阀值	**connection-limit default amount { upper-limit** *upper-limit* **| lower-limit** *lower-limit* **}***	可选 缺省情况下，上限为 50，下限为 20。
创建连接数限制策略并进入策略视图	**connection-limit policy** *policy-number*	必选
定义连接限制策略的规则	**limit** *limit-id* **acl** *acl-number* **[{ per-source | per-destination | per-service }* amount** *upper-limit lower-limit*]	必选
退出连接数限制策略视图	**quit**	-
指定和 NAT 绑定的连接数数限制策略	**nat connection-limit-policy** *policy-number*	必选

11.4.9 配置报文匹配方式

用户可以通过以下命令改变报文的匹配方式。

请在系统视图下进行下列配置。

表11-15 配置报文匹配方式

操作	命令	说明
进入系统视图	**system-view**	-
配置报文匹配方式为三元组匹配	**undo nat match factor-all**	必选
配置报文匹配方式为五元组匹配	**nat match factor-all**	必选

缺省情况下，报文匹配方式为五元组匹配。

📖 **说明：**

当匹配方式为三元组匹配时，将只对报文协议类型，目的 ip 地址和目的端口地址进行匹配，且只对 UDP 报文有效。

11.5 地址转换显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示地址转换配置后的运行情况，通过查看显示信息验证配置的效果。

执行 **reset** 命令可以清除该运行情况。

在用户视图下，执行 **debugging** 命令可以对地址转换进行调试。

表11-16 地址转换显示和调试

操作	命令
查看地址转换的状况	**display nat** { **address-group** | **aging-time** | **all** | **outbound** | **server** | **statistics** | **session** [**vpn-instance** *vpn-instance-name*] [**slot** *slot-number*] [**source global** *global-addr* | **source inside** *inside-addr*] [**destination** *ip-addr*]}
显示连接数限制信息	**display connection-limit statistics** [**source** *source-addr* { *source-wildcard* | *source-mask-len* }] [**destination** *destination-addr* { *destination-wildcard* | *destination-mask-len* }] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }] [**vpn-instance** *vpn-name*]
显示连接数限制策略	**display connection-limit policy** { *policy-number* | **all** }
显示与 NAT 相关的连数限制信息	**display nat connection-limit** [**source** *source-addr* { *source-wildcard* | *source-mask-len* }] [**destination** *destination-addr* { *destination-wildcard* | *destination-mask-len* }] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }] [**vpn-instance** *vpn-name*]
打开 NAT 的调试开关	**debugging nat** { **alg** | **event** | **packet** [**interface** *interface-type interface-number*] }
关闭 NAT 的调试开关	**undo debugging nat** { **alg** | **event** | **packet** [**interface** *interface-type interface-number*] }
打开连接数限制的调试开关	**debugging connection-limit**
关闭连接数限制的调试开关	**undo debugging connection-limit**
清除地址转换映射表	**reset nat session**

11.6 NAT 配置举例

11.6.1 典型 NAT 配置举例

1. 组网需求

如下图所示，一个公司通过 H3C 路由器的地址转换功能连接到广域网。要求该公司能够通过 H3C 路由器串口 3/0/0 访问 internet，公司内部对外提供 www、ftp 和 smtp 服务，而且提供两台 www 的服务器。公司内部网址为 10.110.0.0/16。其中，内部 ftp 服务器地址为 10.110.10.1，内部 www 服务器 1 地址为 10.110.10.2，内部 www 服务器 2 地址为 10.110.10.3，内部 smtp 服务器地址为 10.110.10.4，并且希望可以对外提供统一的服务器的 IP 地址。内部 10.110.10.0/24 网段可以访问 Internet，其它网段的 PC 机则不能访问 Internet。外部的 PC 可以访问内部的服务器。公司具有 202.38.160.100 至 202.38.160.105 六个合法的 IP 地址。

选用 202.38.160.100 作为公司对外的 IP 地址，www 服务器 2 对外采用 8080 端口。

2. 组网图

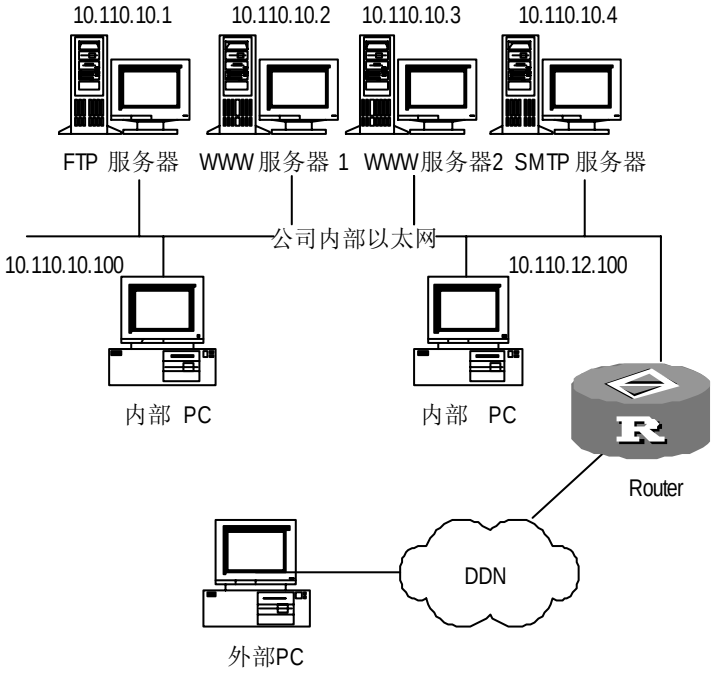


图11-4 地址转换配置案例组网图

3. 配置步骤

配置地址池和访问控制列表。

```
[H3C] nat address-group 1 202.38.160.100 202.38.160.105
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
```

```
[H3C-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[H3C-acl-basic-2001] quit
```

允许 10.110.10.0/24 网段地址转换。

```
[H3C] interface serial 3/0/0
[H3C-Serial3/0/0] nat outbound 2001 address-group 1
```

设置内部 ftp 服务器。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

设置内部 www 服务器 1。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

设置内部 www 服务器 2。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
10.110.10.3 www
```

设置内部 smtp 服务器。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

11.6.2 使用 loopback 接口地址进行地址转换典型配置举例

1. 组网需求

如下图所示，公司通过 H3C 路由器串口 3/0/0 访问 internet，内部 10.110.10.0/24 网段可以访问 Internet，其它网段的 PC 机则不能访问 Internet，内部 10.110.10.0/24 网段使用 loopback 接口 IP 地址 202.38.160.106 做为地址转换后 IP 地址。公司内部对外提供 www、ftp 和 smtp 服务，三个服务器对外使用统一的服务器 IP 地址 202.38.160.100。

2. 组网图

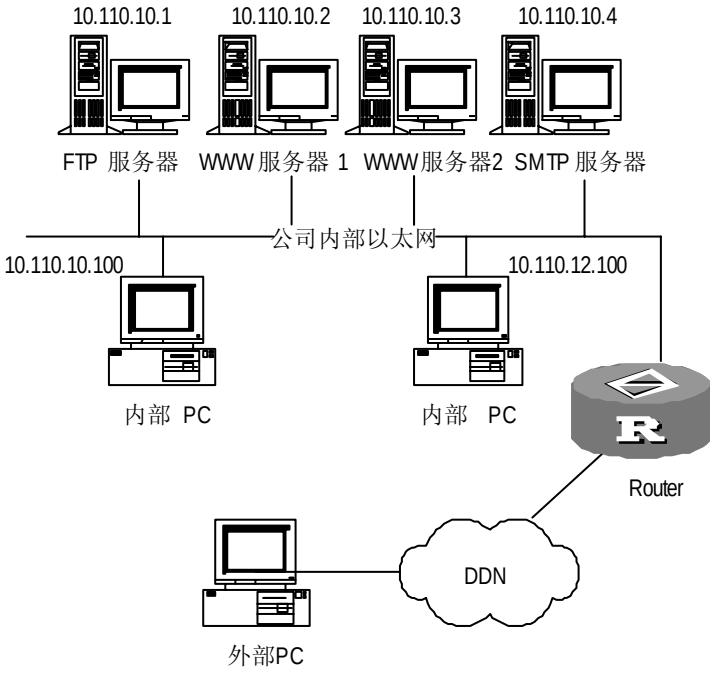


图11-5 地址转换配置举例组网图

3. 配置步骤

配置访问控制列表。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[H3C-acl-basic-2001] quit
```

配置 loopback 接口

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 202.38.160.106
[H3C-LoopBack0] quit
```

设置内部 ftp 服务器。

```
[H3C] interface serial 3/0/0
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

设置内部 www 服务器 1。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

设置内部 www 服务器 2。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
```

```
10.110.10.3 www
```

设置内部 smtp 服务器。

```
[H3C-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

配置使用 loopback 接口作为转换后的 IP 地址。

```
[H3C-Serial3/0/0] nat outbound 2001 interface loopback 0
```

11.6.3 静态网段地址转换典型组网应用

1. 组网需求

私网 A 的网络地址为 10.1.1.0/24 网段，私网 B 的网络地址也为 10.1.1.0/24 网段。假设 PC1 的地址为 10.1.1.2，PC 2 的地址也是 10.1.1.2。RouterA 的广域网接口 IP 地址为 201.1.1.1/24，RouterB 的广域网接口 IP 地址为 201.2.2.2/24。RouterA 和 B 上配置网段地址转换，将私网 A 的网络地址 10.1.1.0/24 转换为 211.2.1.0/24，将私网 B 的网络地址 10.1.1.0/24 转换为 211.2.2.0/24。在 RouterA 和 RouterB 上配置动态路由，保证 RouterA 到 211.2.2.0/24 的路由及 RouterB 到 211.2.1.0/24 的路由可达。

要求能够实现私网对公网的访问，而且实现私网 A 的 PC1 可以通过 PC2 在 Router2 上的公网地址 211.2.2.2 访问到 PC2；同样私网 B 的 PC2 可以通过 PC1 在 Router1 上的公网地址 211.2.1.2 访问到 PC1。

2. 组网应用

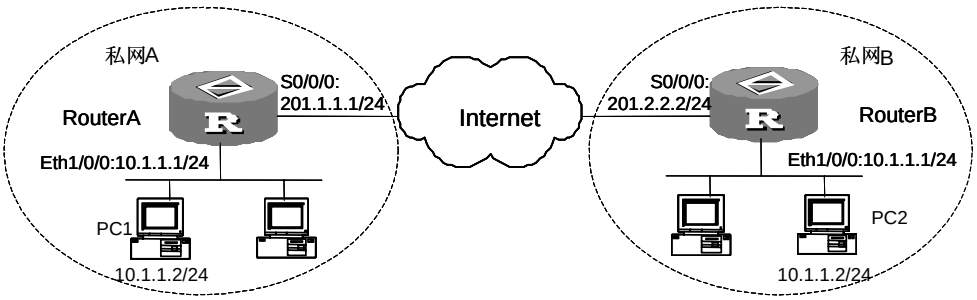


图11-6 静态网段地址转换应用组网图

3. 配置步骤

(1) 配置 RouterA

配置网段地址静态转换。

```
[H3C] nat static inside ip 10.1.1.1 10.1.1.254 global 211.2.1.0 255.255.255.0
```

配置网段地址转换在接口 Serial0/0/0 上生效。

```
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] ip address 201.1.1.1 255.255.255.0
```

```
[H3C-Serial0/0/0] nat outbound static
[H3C-Serial0/0/0] quit
```

配置 Ethernet1/0/0 接口。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置动态路由，保证到 211.2.2.0 网段的路由可达（略）。

(2) 配置 RouterB

配置网段地址静态转换。

```
[H3C] nat static inside ip 10.1.1.1 10.1.1.255 global 211.2.2.0 255.255.255.0
```

配置网段地址转换在接口 Serial0/0/0 上生效。

```
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] ip address 201.2.2.2 255.255.255.0
[H3C-Serial0/0/0] nat outbound static
[H3C-Serial0/0/0] quit
```

配置 Ethernet1/0/0 接口。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置动态路由，保证到 211.2.1.0 网段的路由可达（略）。

11.6.4 双向地址转换配置举例

1. 组网需求

公司原有内部局域网使用 10.0.0.0/24 和 10.1.1.0/24 网段地址，后合入一个网段，也使用 10.0.0.0/24 网段地址。当PC1 的IP地址 10.0.0.1 与 PC3 的IP地址相同时，要求PC1、PC2 可以用域名www.web.com或IP地址 3.0.0.1/24 访问PC3。域名服务器IP地址为 192.168.0.0/24 网段。

2. 组网图

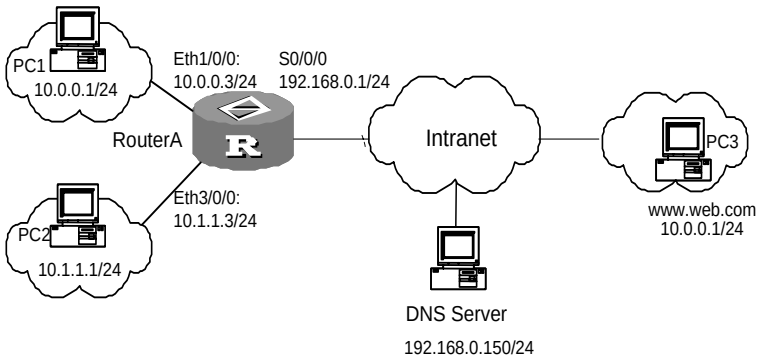


图11-7 双向地址转换配置举例组网图

3. 配置步骤

(1) 配置 RouterA

配置 NAT 地址池。

```
[H3C] nat address-group 1 2.0.0.1 2.0.0.200
```

配置双向 NAT 映射。

```
[H3C] nat overlapaddress 3 10.0.0.0 3.0.0.0 address-mask 24
```

配置访问控制列表。

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[H3C-acl-basic-2000] rule 1 permit source 10.1.1.0 0.0.0.255
[H3C-acl-basic-2000] quit
```

在广域网接口上绑定 NAT outbound。

```
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] ip address 192.168.0.1 255.255.255.0
[H3C-Serial0/0/0] nat outbound 2000 address-group 1
```

配置局域网口 IP 地址。

```
[H3C-Serial0/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.3 255.255.255.0
[H3C-Ethernet1/0/0] interface ethernet 3/0/0
[H3C-Ethernet3/0/0] ip address 10.1.1.3 255.255.255.0
[H3C-Ethernet3/0/0] quit
```

配置静态路由。

```
[H3C] ip route-static 3.0.0.0 255.255.255.0 serial 0/0/0
[H3C] ip route-static 192.168.1.0 255.255.255.0 serial 0/0/0
```

DNS 服务器的地址为 192.168.0.150/24。

11.6.5 内部服务器与 IPSec VPN 结合应用配置举例

1. 组网需求

总公司通过网关 Router1 连接到公网上，并通过公网建立 IPSec VPN 连接分公司网络。总公司和分公司之间的所有数据流均通过 IPSec 实现安全保护，采用 manual 方式建立安全联盟，安全协议采用 ESP 协议，加密算法采用 DES，验证算法采用 SHA1-HMAC-96。

总公司的 www 服务和 FTP 服务器位于 10.110.10.0 网段，通过 Router1 实现内部服务器功能，www 服务器和 FTP 服务器可以对公网用户提供访问服务，即公网上的 PC 可以通过公网地址访问内部服务器；也可以为公司内部用户提供服务，且公司的 PC 可以通过私网地址访问内部服务器。

总公司和分公司内部的 PC 分别位于 10.110.20.0/24 和 10.110.30.0/24 网段，均由 Router1 实现地址转换，通过 S1/0/0 的公网地址访问 Internet。

2. 组网图

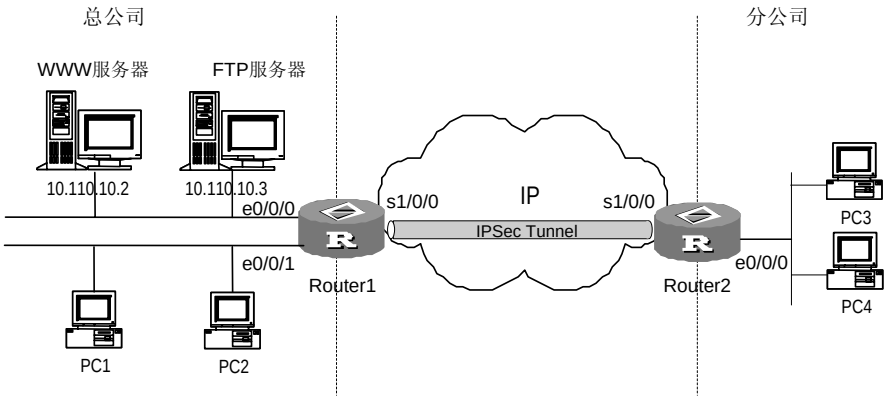


图11-8 内部服务器与 IPSec VPN 结合应用配置举例

3. 配置步骤

(1) 配置 Router1

配置以太网口 IP 地址。

```
[H3C] interface ethernet 0/0/0
[H3C-ethernet 0/0/0] ip address 10.110.10.1 255.255.255.0
[H3C-ethernet 0/0/0] interface ethernet 0/0/1
[H3C-ethernet 0/0/1] ip address 10.110.20.1 255.255.255.0
```

配置用于实现 PC 地址转换的访问控制列表。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit ip source 10.110.20.0 0.0.0.255
[H3C-acl-basic-2001] rule permit ip source 10.110.30.0 0.0.0.255
[H3C-acl-basic-2001] rule deny ip source any destination any
```

配置用于实现内部服务器地址转换的访问控制列表。

```
[H3C-acl-basic-2001] acl number 2002
[H3C-acl-basic-2002] rule permit ip source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2002] rule deny ip source 10.110.0.0 0.0.255.255 destination
10.110.30.0 0.0.0.255
[H3C-acl-basic-2002] rule deny ip source any destination any
```

配置用于实现 IPSec 的访问控制列表。

```
[H3C-acl-basic-2002] acl number 2003
[H3C-acl-basic-2003] rule permit ip source 10.110.0.0 0.0.255.255 destination
10.110.30.0 0.0.0.255
[H3C-acl-adv-2003] rule deny ip source any destination any
```

```
[H3C-acl-adv-2003] quit
```

配置 Easy IP。

```
[H3C] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[H3C-Serial1/0/0] nat outbound 2001
```

配置内部 ftp 及 www 内部服务器。

```
[H3C-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.3 ftp
[H3C-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.2 www
[H3C-Serial1/0/0] quit
```

配置 IPSec。

```
[H3C] ipsec proposal tran1
[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
[H3C-ipsec-proposal-tran1] transform esp
[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
[H3C-ipsec-proposal-tran1] quit
[H3C] ipsec policy map1 10 manual
[H3C-ipsec-policy-manual-map1-10] security acl 2003
[H3C-ipsec-policy-manual-map1-10] proposal tran1
[H3C-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
[H3C-ipsec-policy-manual-map1-10] tunnel local 202.38.160.1
[H3C-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[H3C-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
[H3C-ipsec-policy-manual-map1-10] sa string-key outbound esp
[H3C-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[H3C-ipsec-policy-manual-map1-10] quit
```

配置在串口上应用安全策略组。

```
[H3C] interface serial 1/0/0
[H3C-Serial1/0/0] ipsec policy map1
[H3C-Serial1/0/0] quit
```

配置到 Router2 以太网口的静态路由。

```
[H3C] ip route-static 10.110.30.0 255.255.255.0 202.38.162.1
```

(2) 配置 Router2

配置以太网口 IP 地址。

```
[H3C] interface ethernet 0/0/0
[H3C-ethernet 0/0/0] ip address 10.110.30.1 255.255.255.0
[H3C-ethernet 0/0/0] quit
```

配置用于实现 IPSec 的访问控制列表。

```
[H3C] acl number 2003
[H3C-acl-basic-2003] rule permit ip source 10.110.30.0 0.0.0.255 destination
10.110.0.0 0.0.255.255
[H3C-acl-adv-2003] rule deny ip source any destination any
[H3C-acl-adv-2003] quit
```

配置 IPSec。

```
[H3C] ipsec proposal tran1
[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
[H3C-ipsec-proposal-tran1] transform esp
[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
[H3C-ipsec-proposal-tran1] quit
[H3C] ipsec policy use1 10 manual
[H3C-ipsec-policyl-manual-use1-10] security acl 2003
[H3C-ipsec-policyl-manual-use1-10] proposal tran1
[H3C-ipsec-policyl-manual-use1-10] tunnel remote 202.38.160.1
[H3C-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
[H3C-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[H3C-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
[H3C-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[H3C-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
[H3C-ipsec-policyl-manual-use1-10] quit
```

配置串口地址并在串口上应用安全策略组。

```
[H3C] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 202.38.162.1 255.0.0.0
[H3C-Serial1/0/0] ipsec policy use1
[H3C-Serial1/0/0]quit
```

配置到 Router1 以太网口的静态路由。

```
[H3C] ip route-static 10.110.0.0 255.255.0.0 202.38.160.1
```

11.6.6 内部主机通过域名区分并访问对应的内部服务器组网应用

1. 组网需求

公司内部网络位于 10.0.0.0/8 网段，提供FTP及WWW内部服务器，域名分别为www.zc.com和 ftp.zc.com，域名可以被外部DNS服务器正确解析。连接外部网络的接口Serial0/0/0 的IP地址为 1.1.1.1/8。要求内部主机可以通过域名区分并访问对应的内部服务器。

2. 组网图

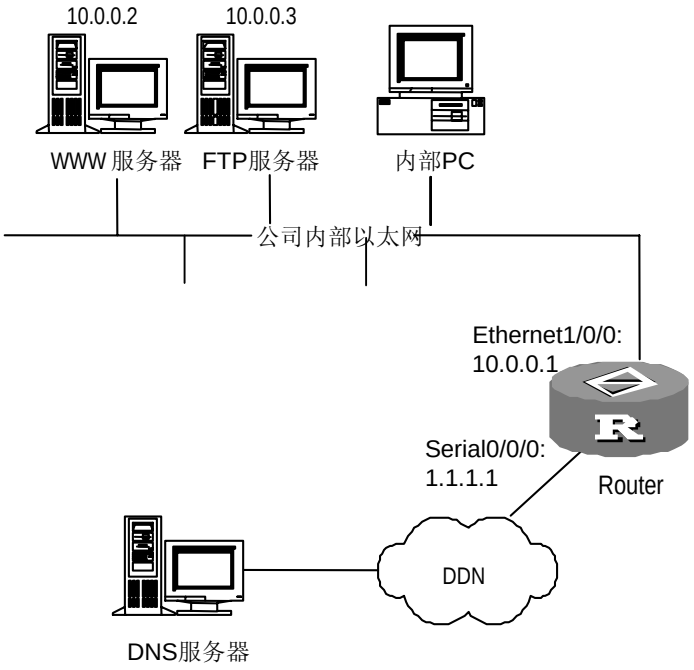


图11-9 内部主机通过域名区分并访问对应的内部服务器

3. 配置步骤

在 Serial0/0/0 接口上配置 FTP 及 WWW 内部服务器。

```
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] ip address 1.1.1.1 255.0.0.0
[H3C-Serial0/0/0] nat outbound 2000
[H3C-Serial0/0/0] nat server protocol tcp global 1.1.1.1 www inside 10.0.0.2
www
[H3C-Serial0/0/0] nat server protocol tcp global 1.1.1.1 ftp inside 10.0.0.3
ftp
[H3C-Serial0/0/0] quit
```

配置访问控制列表，允许 10.0.0.0/8 网段访问 Internet。

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[H3C-acl-basic-2000] rule 1 deny
```

配置 ethernet1/0/0。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

此时外部主机可以通过域名 www.zc.com和 ftp.zc.com访问其对应的内部服务器。加上如下配置后，内部主机也可以通过域名 www.zc.com和 ftp.zc.com访问其对应的内部服务器。

配置域名与外部地址、端口号、协议类型之间的映射。

```
[H3C] nat dns-map www.zc.com 1.1.1.1 80 tcp
[H3C] nat dns-map ftp.zc.com 1.1.1.1 21 tcp
```

11.6.7 NAT 限制最大连接数典型配置举例

1. 组网需求

如 图 11-10所示，路由器Router的Ethernet0/0/0 接口连接了局域网 192.168.1.0/24，Serial1/0/1 直接连接到Internet，在Router上配置了NAT以实现局域网内的PC都能访问Internet。

为了限制局域网内主机对外发起的连接数，路由器上配置 NAT 限制最大连接数特性，对单一源地址发起的连接数进行限制,连接数上限为 10，下限为 1。

2. 组网图

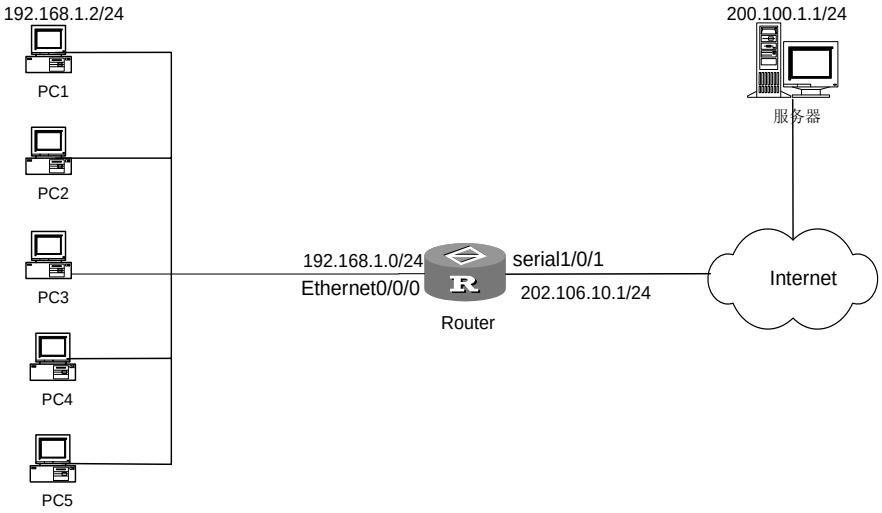


图11-10 NAT 限制最大连接数组网图

3. 配置步骤

在 Router 上配置 NAT。

略。

创建 ACL 并配置规则，来匹配源 IP 地址为 192.168.1.2/24 的数据。

```
<H3C> system-view
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 192.168.1.2 0
[H3C-acl-basic-2000] quit
```

创建连接数限制策略，并配置子规则，对单一源地址发起的连接数进行限制。

```
[H3C] connection-limit enable
```

```
[H3C] connection-limit policy 0
[H3C-connection-limit-policy-0] limit 0 acl 2000 per-source amount 10 1
[H3C-connection-limit-policy-0] quit
```

NAT 引用连接数限制策略 0。

```
[H3C] nat connection-limit-policy 0
```

11.7 NAT 排错

故障之一：地址转换不正常。

故障排除：打开 NAT 的 Debug 开关，具体操作请参见 **debugging** 命令中的 **debugging nat**。根据路由器上的 Debug 调试信息，初步定位错误，然后使用其它命令作进一步的判断。调试时，注意观察转换后的源地址，要保证这个地址是希望转换的地址，否则可能会是地址池配置错误。同时要注意想要访问的网络必须要有回到地址池中地址段的路由。注意防火墙以及地址转换本身的访问控制列表对地址转换造成的影响，同时注意路由的配置。

故障之二：内部服务器工作不正常。

故障排除：如果外部主机不能正常访问内部服务器，请检查是否是内部服务器主机的配置有错或路由器上对内部服务器的配置有错，如对内部服务器的 IP 地址指定错误等等。同时也有可能是防火墙禁止了外部主机对内部网络的访问，可以用 **display acl** 命令来查看，请参见防火墙的配置。

第12章 IP 单播策略路由配置

12.1 IP 单播策略路由简介

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由选择的机制。本系统的策略路由支持基于到达报文的源地址、地址长度等信息，灵活地指定路由。

本系统的策略路由配置需要做两方面的工作，一是定义那些需要使用策略路由的报文，二是为这些报文指定路由，这可以通过对一个 **route-policy** 的定义来实现。**route-policy** 的配置在用作策略路由的定义时，**if-match** 子句定义了那些需要使用策略路由的报文，当报文满足 **route-policy** 中的 **if-match** 子句时，则执行策略中的 **apply** 子句，以完成报文的转发。

一个 **route-policy** 由若干节点组成，每一节点由一些 **if-match** 子句和 **apply** 子句组成。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义通过该节点过滤后进行的动作。

节点的 if-match 子句之间的过滤关系是“与”的关系，即报文必须满足该节点的所有 if-match 子句，才会执行 apply 子句。目前 route-policy 提供了两种 if-match 子句，分别为 if-match packet-length 和 if-match acl；提供了 6 种 route-policy 的 apply 子句：**apply ip-precedence**，**apply ip-dscp**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。在满足所有 if-match 子句的情况下，apply 子句执行情况如下：

- 配置报文的 DSCP 值：**apply ip-dscp**，只要配置了该子句，该子句就一定会执行；
- 配置优先级：**apply ip-precedence**，优先级仅低于 **apply ip-dscp** 子句；
- 配置出接口和下一跳：**apply output-interface** 和 **apply ip-address next-hop**，其中 **apply output-interface** 命令的优先级高于 **apply ip-address next-hop**。当两条命令同时配置并且都有效时，系统只会执行 **apply output-interface** 命令；
- 配置缺省出接口和下一跳：apply default output-interface 和 apply ip-address default next-hop，同样，apply default output-interface 命令的优先级高于 apply ip-address default next-hop 。当两条命令同时配置并且都有效时，系统只会执行 apply default output-interface 命令。执行缺省出接口和下一跳命令的前提是，在策略路由中报文没有配置出接口或者下一跳，或者配置的出接口和下

一跳无效，并且报文在路由表中没有查到相应的路由，这时才会使用策略路由配置的缺省下一跳或者出接口。

本系统提供的策略路由可以分为接口策略路由和本地策略路由。前者在接口视图下配置（应用于报文到达的接口上），作用于到达该接口的报文；后者在系统视图下配置，对本机产生的报文进行策略路由。对于一般转发和安全等方面的使用需求，大多数情况下使用的是接口策略路由。

策略路由可应用于安全、负载分担等目的。

12.2 IP 单播策略路由的配置

IP 单播策略路由配置包括：

(1) 配置策略

- 创建策略
- 定义 Route-policy 的 **if-match** 子句
- 定义 Route-policy 的 **apply** 子句

(2) 使能策略路由

- 使能/禁止本地策略路由
- 使能/禁止接口策略路由

12.2.1 配置策略

1. 创建策略

由策略名称指定的策略可以包含若干策略点，每个策略点由 *sequence-num* 来指定，*sequence-num* 的值越小优先级越高，其定义的策略会被先执行。该策略可以用来引入路由以及对 IP 报文转发进行策略路由。该策略的具体内容由 if-match 和 apply 子句来指定。

请在系统视图下进行下列配置。

表12-1 创建策略

操作	命令
创建策略或一个策略节点	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
删除策略或一个策略节点	**undo route-policy** *policy-name* [**permit** | **deny** | **node** *sequence-number*]

permit 表示满足匹配条件的报文进行策略路由；**deny** 表示满足匹配条件的报文不进行策略路由。

缺省情况下，没有 route-policy 和相关的节点设置被定义。

2. 设置 Route-policy 的 if-match 子句

if-match 子句用来匹配需要使用策略路由的报文。IP 单播策略路由提供两种 **if-match** 子句，**if-match packet-length** 子句和 **if-match acl** 子句，当同时配置这两条子句时，子句之间是“与”的关系。

请在 **route-policy** 视图下进行下列配置。

表12-2 设置 Route-policy 的 if-match 子句

操作	命令
设置 IP 报文长度匹配条件	**if-match packet-length** *min-len max-len*
设置 ACL 匹配条件	**if-match acl** *acl-number*

缺省情况下，没有 **if-match** 子句被定义。

3. 设置 Route-policy 的 apply 子句

请在 **route-policy** 视图下进行下列配置。

IP 策略路由提供六种 **apply** 子句：**apply ip-precedence**，**apply ip-dscp**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。一条策略节点中可以包含多条 **apply** 子句，系统按配置顺序执行 **apply** 子句（无效的子句会跳过，继续去执行下一个子句）；当执行了一条有效的子句后，该策略即实施完毕。

表12-3 设置 Route-policy 的 apply 子句

操作	命令
设置报文的优先级	**apply ip-precedence** *precedence*
设置报文的 DSCP 值	**apply ip-dscp** { *value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **be** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** }
设置报文的发送接口	**apply output-interface** *interface-type interface-number* [*interface-type interface-number*]
设置报文的下一跳	**apply ip-address next-hop** *ip-address* [*ip-address*]
设置报文缺省发送接口	**apply default output-interface** *interface-type interface-number* [*interface-type interface-number*]
设置报文缺省下一跳	**apply ip-address default next-hop** *ip-address* [*ip-address*]

用户可指定多个下一跳或者设置多个出接口，此时，报文的转发将在多个合法参数中负载分担，即轮流在每一个下一跳或者出接口上发送一个报文。以上叙述只对于同种配置的多个参数有效，如果同时配置了出接口和下一跳，仅在出接口的设置中进行负载分担。

缺省情况下，没有 **apply** 子句被定义。

🕮 **说明：**

配置策略路由的 **apply** 子句时，对于点到点接口（如封装了 PPP 协议的 Serial 接口），既可以设置报文的发送接口也可以设置下一跳；对于广播类型或 NBMA 类型接口（如 Ethernet、ATM 接口），支持点到多点，则必须设置报文的下一跳地址。

12.2.2 使能策略路由

1. 使能/禁止本地策略路由

在系统视图下使能/禁止本地策略路由。最多只能配置一条本地策略。

表12-4 使能/禁止本地策略路由

操作	命令
使能本地策略路由	**ip local policy route-policy** *policy-name*
禁止本地策略路由	**undo ip local policy route-policy** *policy-name*

缺省情况下，禁止本地策略路由。

2. 使能/禁止接口策略路由

在指定接口上使能/禁止策略路由。每个接口最多配置一个策略。

请在接口视图下进行下列配置。

表12-5 使能/禁止接口策略路由

操作	命令
使能接口策略路由	**ip policy route-policy** *policy-name*
禁止接口策略路由	**undo ip policy route-policy** *policy-name*

缺省情况下，禁止接口策略路由。

12.3 IP 单播策略路由显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IP 单播策略路由配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可以对 IP 单播策略路由进行调试。

表12-6 表 IP 单播策略路由显示和调试

操作	命令
显示本地和接口设置的策略路由的策略	**display ip policy**
显示本地策略路由的设置情况	**display ip policy setup local**
显示接口策略路由的设置情况	**display ip policy setup interface** *interface-type interface-number*
显示本地策略路由报文的统计信息	**display ip policy statistic local**
显示接口策略路由报文的统计信息	**display ip policy statistic interface** *interface-type interface-number*
打开策略路由的调试开关	**debugging ip policy**

12.4 IP 单播策略路由典型配置举例

12.4.1 配置基于源地址的策略路由

1. 配置需求

定义策略 aaa 的策略路为由控制所有从以太网口 E3/0/0 接口接收的 TCP 报文，使用串口 serial1/0/0 发送，对其它报文，仍然按照查找路由表的方式进行转发。

- 5 号节点，表示匹配 **acl 3101** 的以太网报文将被发往串口 serial1/0/0；
- 10 号节点，表示匹配 **acl 3102** 的任何报文不做策略路由处理；

来自 Ethernet3/0/0 的报文将依次试图匹配 5、10 号节点的 **if-match** 子句。如果匹配了 **permit** 语句的节点，执行相应的 **apply** 子句；如果匹配了 **deny** 语句的节点，退出策略路由处理。

2. 组网图

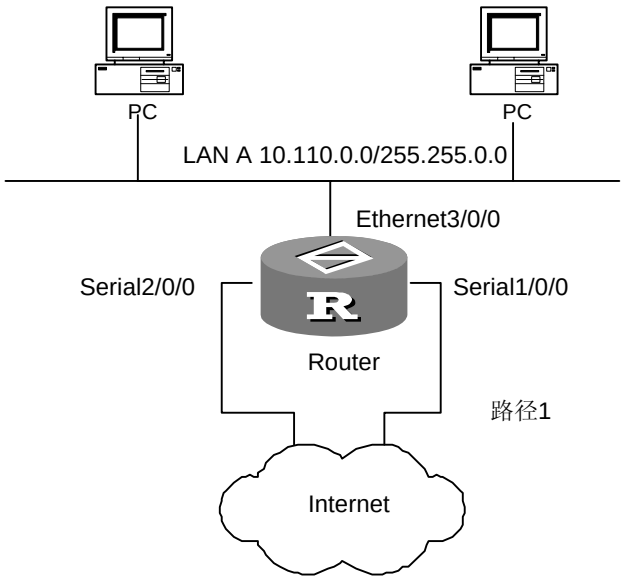


图12-1 配置基于源地址的策略路由组网图

3. 配置步骤

设置防火墙的缺省过滤方式为“禁止”。

```
[H3C] firewall default deny
```

定义访问控制列表。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit tcp
[H3C-acl-adv-3101] quit
[H3C] acl number 3102
[H3C-acl-adv-3102] rule permit ip
[H3C-acl-adv-3102] quit
```

定义 5 号节点，使匹配 acl 3101 的任何 TCP 报文被发往串口 serial 1/0/0。

```
[H3C] route-policy aaa permit node 5
[H3C-route-policy] if-match acl 3101
[H3C-route-policy] apply output-interface serial 1/0/0
[H3C-route-policy] quit
```

定义 10 号节点，表示匹配 acl 3102 的报文不做策略路由处理。

```
[H3C] route-policy aaa deny node 10
[H3C-route-policy] if-match acl 3102
[H3C-route-policy] quit
```

在以太网口上应用策略 aaa。

```
[H3C] interface ethernet 3/0/0
```

```
[H3C-Ethernet3/0/0] ip policy route-policy aaa
```

12.4.2 配置基于报文大小的策略路由

1. 配置需求

路由器 A 将大小为 64～100 字节的报文从 serial 2/0/0 发送；而将大小为 101～1000 字节的报文从 serial 2/0/1 发送；所有其它长度的报文均按正常方式路由。

在路由器 A 的 E1/2/0 接口上应用 IP 策略路由 lab1。这个策略将将大小为 64～100 字节的报文设置 150.1.1.2 作为下一转发 IP 地址；而将大小为 101～1000 字节的报文设置 151.1.1.2 作为下一转发 IP 地址。所有其它长度的报文都按基于目的地址的路由方法路由。

2. 组网图

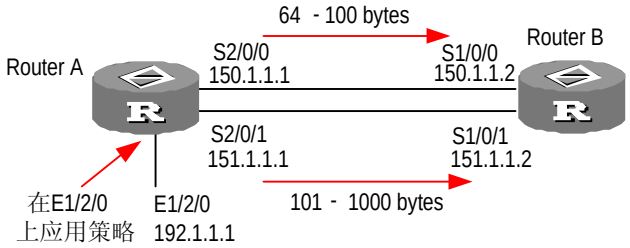


图12-2 配置基于报文大小的策略路由组网图

3. 配置步骤

配置路由器 Router A

```
[H3C] interface ethernet 1/2/0
[H3C-Ethernet1/2/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet1/2/0] ip policy route-policy lab1
[H3C] interface serial 2/0/0
[H3C-Serial2/0/0] ip address 150.1.1.1 255.255.255.0
[H3C] interface serial 2/0/1
[H3C-Serial2/0/1] ip address 151.1.1.1 255.255.255.0
[H3C] rip
[H3C-rip] network 192.1.1.0
[H3C-rip] network 150.1.0.0
[H3C-rip] network 151.1.0.0
[H3C] route-policy lab1 permit node 10
[H3C-route-policy] if-match packet-length 64 100
[H3C-route-policy] apply ip-address next-hop 150.1.1.2
[H3C] route-policy lab1 permit node 20
[H3C-route-policy] if-match packet-length 101 1000
[H3C-route-policy] apply ip-address next-hop 151.1.1.2
```

配置路由器 Router B

```
[H3C] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 150.1.1.2 255.255.255.0
[H3C] interface serial 1/0/1
[H3C-Serial1/0/1] ip address 151.1.1.2 255.255.255.0
[H3C] rip
[H3C-rip] network 150.1.0.0
[H3C-rip] network 151.1.0.0
```

在路由器 A 用 **debugging ip policy** 命令监视策略路由。注意 64 字节的报文与路由策略 lab1 的序号为 10 的入口项匹配，因此向 150.1.1.2 转发。

```
<H3C> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
150.1.1.2
```

在路由器 A，改变报文长为 101 字节，再用 **debugging ip policy** 命令监视策略路由。注意 101 字节的报文与路由策略 lab1 的序号为 20 的入口项匹配，从而向 151.1.1.2 转发。

```
<H3C> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
151.1.1.2
```

在路由器 A，改变报文长为 1001 字节，再用 **debugging ip policy** 命令监视策略路由。注意这个报文不匹配 lab1 中的任何入口项，所以按正常方式转发，策略路由没有输出转发报文的调试信息。

第13章 IP 组播策略路由配置

13.1 IP 组播策略路由简介

13.1.1 IP 组播策略路由概述

IP 组播策略路由是对组播通常的按照路由表进行报文转发功能的一种补充和增强，它依照用户指定的策略来转发组播报文。

IP 组播策略路由通过配置 route-policy 来实现，它是单播策略路由的一种扩展，由用户输入的一组 if-match 和 apply 语句来描述。if-match 子句定义匹配准则，也就是通过当前 route-policy 规定所需满足的过滤条件，它规定当组播报文满足匹配条件时，不再按照通常的流程来转发，而是按照用户设置的方案（由 apply 语句描述）进行转发。

13.1.2 与 IP 组播策略路由相关的几个概念

- route-policy

IP 组播策略路由的策略，通过配置 route-policy 实现。在路由器上可以配置多个 route-policy。

- 策略节点（node）

一个策略节点（node）就是一条完整的策略，它通过 **if-match** 命令来设置报文需要匹配的条件，通过 **apply** 命令来配置对满足匹配条件的报文需要执行的转发动作。在每个 node 中，包含最多一个用于定义报文匹配条件的访问控制列表（ACL），最多一个指定转发出接口的 ACL 和一个指定转发下一跳的 ACL。

一个 route-policy 中可以配置条件与动作不同的多个策略节点。每个 route-policy 中不同的策略节点通过一个序列号（sequence-number）进行标识。

- 匹配规则

组播报文的匹配条件由 if-match 子句描述，通过配置标准的或扩展的 ACL（2000～3999）来设置。

- 组播报文的转发动作

组播报文的转发动作由 apply 子句描述，包括设置转发的出接口和下一跳 IP 地址两种方式。其中，出接口列表通过一个基于接口的 ACL（1000～1999）来指定，下一跳 IP 地址列表通过一个标准的 ACL（2000～2999）来指定。

13.1.3 应用 IP 组播策略路由后的报文转发过程

对于组播报文，如果报文入接口上配置了 IP 组播策略路由，且该报文满足 IP 组播策略路由的匹配条件，则该报文将按照策略路由设置的动作进行转发；否则，该报文将按照组播通常的转发流程进行转发。

13.2 IP 组播策略路由配置

IP 组播策略路由配置包括：

- 定义 route-policy
- 定义 IP 组播路由策略的 if-match 子句
- 定义 route-policy 的 apply 子句
- 在接口上使能 IP 组播策略路由

13.2.1 定义 route-policy

一个 route-policy 中可以配置条件与动作不同的多个策略节点，每个策略节点都有自己的 **if-match** 子句与 **apply** 子句，由 *sequence-number* 指定这几个部分的匹配顺序。

请在系统视图下进行下列配置。

表13-1 定义 route-policy

操作	命令
定义 route-policy 节点	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
删除 route-policy 节点	**undo route-policy** *policy-name* [**permit** | **deny**]

当在路由器一个接口上配置了 IP 组播策略路由以后，对于所有从该接口进入路由器的组播数据报文，都将进行过滤处理。过滤方法是：对于该策略路由所指定的 route-policy 的所有策略节点，按照 *sequence-number* 从小到大的顺序，依次进行处理。

需要注意的是，不同 *sequence-number* 的各个部分之间的关系是“或”的关系，即报文依次经过具有不同 *sequence-number* 的各个节点, 如果报文的特征能够与某一个节点中的 if-match 子句相匹配，就会通过该节点的 apply 子句进行转发，报文不会再到达后续的所有节点。

13.2.2 定义 route-policy 的 if-match 子句

if-match 子句定义匹配准则，也就是需要通过当前 route-policy 的路由信息所需满足的过滤条件。

请在 route-policy 视图下进行下列配置。

表13-2 定义匹配条件

操作	命令
设置组播报文需要匹配的条件	**if-match acl** *acl-number*
取消设置的匹配条件	**undo if-match acl**

如果报文满足某个策略节点中指定的 If-match 条件，则执行该节点所指定的动作；如果报文不满足某个策略节点中指定的 If-match 条件，则继续检查下一个节点；如果所有的策略节点的条件都不满足，则报文将回到正常的转发流程中处理。

需要注意的是：

- 对于一个 route-policy 节点，在匹配的过程中，同一节点中的所有 **if-match** 子句之间的关系是“与”的关系。
- 组播策略路由只考虑策略节点中的 **if-match acl** 与 **if-match interface** 配置，其它任何 **if-match** 子句与组播策略路由的转发无关。
- 如不指定 **if-match** 子句，则所有路由信息都会通过该节点的过滤。

13.2.3 定义 route-policy 的 apply 子句

apply 子句指定动作，也就是在满足由 **if-match** 子句指定的过滤条件后所执行的一些配置命令。

请在 route-policy 视图下进行下列配置。

表13-3 定义 SET 子句

操作	命令
为策略节点中配置出接口列表	**apply output-interface acl** *acl-number*
取消配置的出接口列表	**undo apply output-interface** [**acl** *acl-number*]
为策略节点中配置下一跳 IP 地址列表	**apply ip-address next-hop** { **acl** *acl-number* | *ip-address* [*ip-address*] }
取消配置的下一跳 IP 地址列表	**undo apply ip-address next-hop** [**acl** *acl-number* | *ip-address* [*ip-address*]]

通过访问控制列表（ACL）来为 IP 组播策略路由指定出接口列表和下一跳 IP 地址列表。对于下一跳 IP 地址，指定的 ACL 是基本 ACL（2000～2999），对于出接口设置，指定的是基于接口的 ACL（1000～1999）。

13.2.4 在接口上使能 IP 组播策略路由

请在接口视图下进行下列配置。

表13-4 在接口上使能 IP 组播策略路由

操作	命令
在接口上使能 IP 组播路由策略	**ip multicast-policy route-policy** *policy-name*
取消在接口上应用的某条 IP 组播路由策略	**undo ip multicast-policy route-policy** *policy-name*

当在路由器一个接口上配置了 IP 组播策略路由以后，对于所有从该接口进入路由器的组播数据报文（不包括组播协议报文，例如组播路由协议产生的报文），都将进行过滤处理。

过滤方法是：对于该策略路由所指定的 route-policy 的所有策略节点，按照序列号从小到大的顺序，依次进行处理；如果报文满足某个策略节点中指定的 if-match 条件，则执行该节点所指定的动作；如果报文不满足某个策略节点中指定的 if-match 条件，则继续检查下一个节点；如果所有的策略节点的条件都不满足，则报文将回到正常的转发流程中处理。

13.3 IP 组播策略路由显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IP 组播策略路由配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可以对 IP 组播策略路由进行调试。

表13-5 IP 组播策略路由显示和调试

操作	命令
显示 IP 组播策略路由信息	**display ip multicast-policy** [**setup interface** *type number* | **statistic interface** *type number*]
打开 IP 组播策略路由调试开关	**debugging ip multicast-policy** [*acl-number*]
关闭 IP 组播策略路由调试开关	**undo debugging ip multicast-policy**

第14章 QLLC 配置

14.1 QLLC 简介

QLLC（Qualified Logical Link Control）是逻辑链路质量控制协议，它是通过 X25 网络传送 SDLC 协议内容的一种解决方案，即在 X25 链路上承载 SDLC 协议。因此可以理解为 QLLC 就是“SDLC over X25”，是将 SDLC 帧封装在 X25 的帧中进行传输。

QLLC 使得 SNA 的设备可以跨越 X25 网络和远端的 SNA 设备进行通讯。（SNA 是 IBM 提出的一个网络体系结构，与 ISO 的 TCP/IP 体系结构相对应。SNA 的链路层定义了：LLC2、SDLC、QLLC 等链路层协议。）

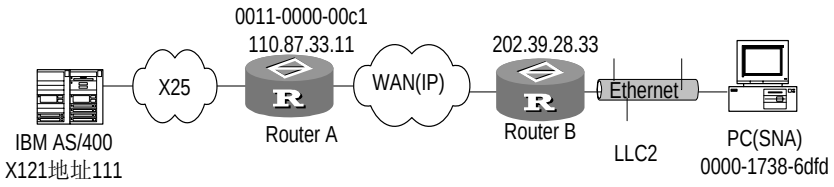


图14-1 QLLC 典型组网图

如上图所示，QLLC 作为链路层，负责交换 UNIX 和 IBM 主机之间的 SNA 协商报文。在 SNA 协商成功之后，UNIX 和 RouterA 之间交换的是普通 X25 报文。

14.2 QLLC 的配置

配置 QLLC 功能只需要在路由器上配置 QLLC 的交换表项就可以了。交换表项是对端 X.121 地址、本地接口的虚 MAC 地址与对端 SNA 设备的 MAC 地址之间的一个映射。当路由器接收到来自对端的 SNA 协商请求 时，根据虚 MAC 地址查找交换表，如果匹配成功，则根据交换表中的 X.121 地址发起 X.25 呼叫，如果呼叫成功，则开始进行 SNA 的协商。

当路由器接收到来自 X.25 网络的呼叫时，根据呼入的 X.121 地址和交换表进行匹配，如果匹配成功，则建立 X.25 虚电路，并根据交换表项中的远端 MAC 地址开始进行 SNA 的协商。

这里的虚 MAC 地址意义是将路由器虚拟为 SNA 设备，对端 SNA 设备利用该虚 MAC 地址进行 SNA 的协商，也即对端的 SNA 设备要探询的目的 MAC 地址就是我们为路由器配置的虚 MAC 地址。

说明：

每个同步接口只可以运行一条 QLLC 链路，即每个物理接口只可以配置一条交换表项。

一般情况下，SNA 设备是作为客户端，而 X.25 主机是作为服务器的。因此一般是由 SNA 设备首先向 X.25 主机发起协商请求。这种情况下，作为 QLLC 交换的路由器只需要配置 X.121 地址与虚拟 MAC 地址之间的映射，而不需要配置 X.121 地址与对端 SNA 设备的 MAC 地址的映射。

只有在服务器有首先发起 X.25 呼叫请求的情况下才需要配置 X.121 地址与对端 SNA 设备的 MAC 地址的映射。

请在同步接口视图下进行下列配置。

表14-1 创建 QLLC 的交换表现

操作	命令
创建 QLLC 的交换表项	**X25 qllc-switch** *x.121-address* **virtual-mac** *mac-address* [**partner-mac** *mac-address*]
删除 QLLC 的交换表项	**X25 qllc-switch** *x.121-address*

缺省情况下，没有交换表项。

14.3 QLLC 的显示和调试

请在用户视图下进行下来操作。

表14-2 QLLC 的显示和调试

操作	命令
打开 QLLC 调试信息开关	**debugging qllc** { **packet** | **event** | **all** }

14.4 QLLC 典型配置举例

1. 组网需求

RouterA 连接到 UNIX 主机所在以太网，启动 DLSw 功能。RouterB 连接到服务器所在的 X.25 网络，启动 DLSw 及 QLLC 功能。两台路由器通过 IP 网络相连。要求实现 UNIX 主机（SNA 的设备）要跨越 IP 网络和 X.25 网络与远端的服务器（SNA 设备）进行通讯。

2. 组网图

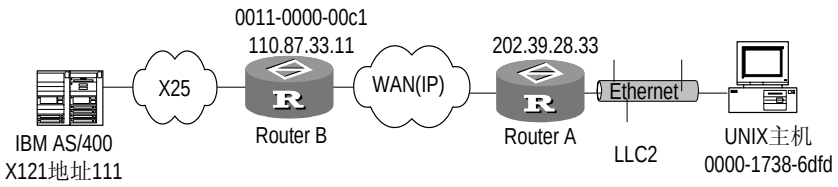


图14-2 QLLC 典型配置组网图

3. 配置步骤

📖 说明：

本例假设两个路由器之间的路由可达。

---

(1) 路由器 A 的配置

```
[H3C] dlsw local 202.39.28.33
[H3C] dlsw remote 110.87.33.11
[H3C] dlsw bridge-set 1
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] bridge-set 1
```

(2) 路由器 B 的配置

```
[H3C] dlsw local 110.87.33.11
[H3C] dlsw remote 202.39.28.33
[H3C] interface serial 0/0/0
[H3C-Serial1/0/0] link-protocol x25 dce ietf
[H3C-Serial1/0/0] x25 x121-address 222
[H3C-Serial1/0/0] x25 qllc-switch 111 virtual-mac 0011-0000-00c1 partner-mac
0000-1738-6dfd
```

第15章 SOT 配置

15.1 SOT 简介

SOT（SDLC over TCP/IP）是解决 SNA 与 TCP/IP 集成的一种隧道技术，实现 SDLC 协议在广域网上传输。SOT 通过把 SDLC 帧封装成 TCP/IP，实现 SDLC 帧通过 TCP/IP 的传输。SOT 是 SNA 多协议路由器在数据链路层的一种解决方案。

SOT 通常应用于两种场合，一个是前端处理机与远程通讯控制器相连，另一个是 IBM 主机与远程通讯控制器相连。

SOT 有三种不同的工作模式：

基本模式（Simple Sot Mode）：在这种模式下，路由器对接收到的报文不做任何修改，不考虑报文的地址，所有的帧都被直接发送到对端，相当于路由器两侧的IBM设备直接相连。此种应用只能用于点对点的通讯，如 图 15-1所示：

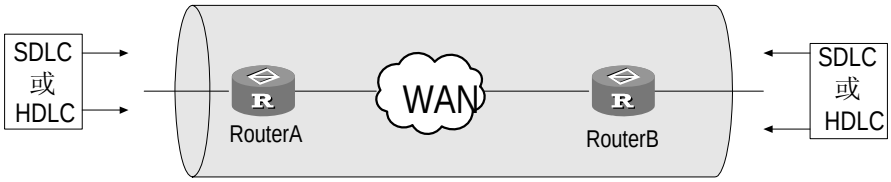


图15-1 Simple SOT Mode

穿透模式（SDLC Pass Through Mode）：在这种模式下，路由器对接收到的SDLC帧不做任何修改，SOT只负责将SDLC帧原样发送到目的地，包括监控帧。SDLC会话由通讯两端的IBM设备来维护。与Simple Sot Mode不同的是，路由器对于接收到的SDLC帧要检查它的终端的SDLC地址，然后用该终端的SDLC地址与**sot send address** 命令匹配，找出对应的IP地址，然后把该SDLC帧打成TCP包发送到该IP地址对应的路由器。此种应用可以提供点到多点的通讯。如 图 15-2所示：

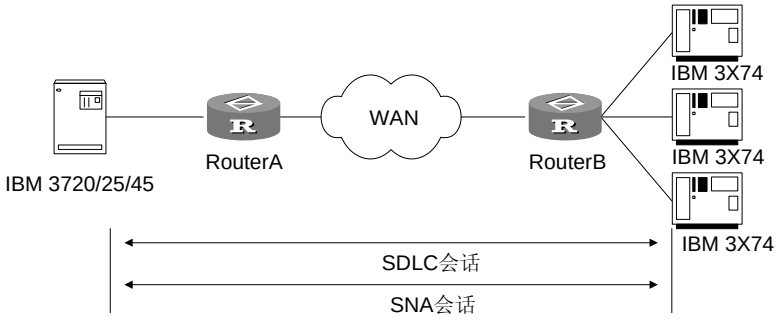


图15-2 SDLC Pass Through Mode

本地应答模式（SOT local acknowledgment mode）：在这种模式下，路由器需要参与SDLC会话，处理所有SDLC监控帧，包括接收端未就绪、接收端就绪、拒绝帧等。如 图 15-3所示：

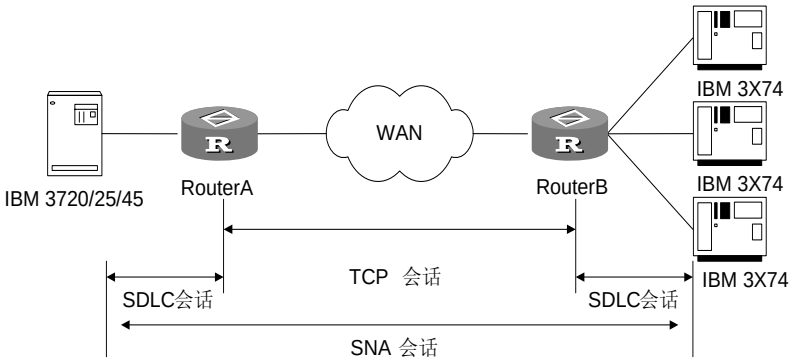


图15-3 SOT local acknowledgment mode

穿透模式和本地应答模式统称为 SDLC 模式，二者在具体配置上有所不同。

15.2 SOT 配置

SOT 的配置包括：

1. 全局配置

- 配置 SOT 本地实体的 IP 地址
- 配置 SOT 协议组
- 配置 SOT 连接检测的最大次数（可选，仅在本地应答模式的 primary 角色下配置）
- 配置超时定时器（可选，仅在本地应答模式下配置）

2. 接口配置

(1) **simple** 模式

- 封装 SOT 协议
- 将接口加入 SOT 协议组
- 配置转发所有 SDLC 帧

(2) **sdlc** 模式

穿透模式（含广播发送方式）：

- 封装 SOT 协议
- 将接口加入 SOT 协议组
- 配置终端的 SDLC 地址

- 配置 SDLC 的角色（仅广播发送方式必配）
- 配置向特定终端发送 SDLC 帧的路由

本地应答模式：

- 封装 SOT 协议
- 将接口加入 SOT 协议组
- 配置终端的 SDLC 地址
- 配置 SDLC 的角色（仅本地应答方式及穿透模式下的广播方式配置）
- 配置向特定终端发送 SDLC 帧的路由

15.2.1 指定 SOT 本地实体的 IP 地址

首先，在本端和对端路由器上分别配置 **sot peer** 命令，指定 SOT 隧道的两个端点，实现通过 TCP/IP 传送 SDLC 帧。

请在系统视图下进行下列配置。

表15-1 配置 SOT 本地实体的 IP 地址

操作	命令
指定 SOT 本地实体的 IP 地址	**sot peer** *ip-address*
删除 SOT 本地实体	**undo sot peer**

本命令配置的 IP 地址，必须是路由器上某一接口的 IP 地址，例如 Loopback 接口的 IP 地址，并且该接口必须处于“UP”状态，否则隧道无法建立，并且系统会给出 IP 地址非本地地址的提示。

15.2.2 配置 SOT 的协议组

协议组分为 simple 模式和 sdlc 模式两种。

请在系统视图下进行下列配置。

1. 配置 simple 协议组

表15-2 配置 simple 协议组

操作	命令
配置 simple 模式的协议组	**sot group-set** *group-number* **simple**
删除指定的协议组	**undo sot group-set** *group-number*

2. 配置 SDLC 协议组

表15-3 配置 SDLC 协议组

操作	命令
配置 SDLC 模式的协议组	**sot group-set** *group-number* **sdlc**
删除指定的协议组	**undo sot group-set** *group-number*

15.2.3 封装 SOT 协议

请在同步串口视图下进行下列配置。

表15-4 封装 SOT 协议

操作	命令
在同步串行接口上封装 SOT 协议	**link-protocol sot**

15.2.4 将串口加入到 SOT 协议组

sot gather 命令用来将串口加入到 SOT 协议组，并且每个串口只能配置一个 SOT 协议组，加入 simple 模式的协议组即指定接口工作在基本模式，只能提供点到点的数据传输；加入 SDLC 模式的协议组即指定接口工作在穿透模式或本地应答模式，可以提供点到多点的数据传输。

只有配置了该命令才可配置除 **link-protocol sot** 以外的其他的接口命令，并且根据配置的不同协议组（simple 协议组和 sdlc 协议组），配置不同的协议组参数。

📖 **说明：**

当在一个串口加入到多个 SOT 协议组时，只有最后配置的协议组生效。

当一个串口配置的 SOT 协议组类型变更时（simple 变为 sdlc，或相反），接口下原有的 SOT 配置将被删除。

同步串口视图下进行下面配置。

表15-5 将接口加入 SOT 协议组

操作	命令
将接口加入预先定义好的 SOT 协议组	**sot gather** *group-number*
删除接口下的 SOT 协议组	**undo sot gather** *group-number*

15.2.5 配置 SOT 连接检测的最大次数

当 SOT 实体双方的 TCP 连接中断后，角色为 primary 的一端进行连接检测，如果检测了 *count* 次数后仍未连接成功，则断开与该 SOT 实体的连接；如果在角色为 primary 一端未配置检测次数，则系统将等待一段时间后超时断开 SOT 连接（超时时间由 **sot timer keepalive** 命令配置）。

请在系统视图下进行下列配置。

表15-6 配置 SOT 连接检测的最大次数

操作	命令
配置 SOT 连接检测的最大次数	**sot counter keepalive** *count*
取消断开连接前的检测功能	**undo sot counter keepalive** *count*

该命令在本地应答模式的 primary 角色下起作用，并且可以和 **sot timer keepalive** 配合使用。缺省情况下，不检测直接断开 SOT 连接。

15.2.6 配置 keepalive 帧超时定时器

当 SOT 实体双方的 TCP 连接中断后，角色为 primary 的一端进行连接检测，如果在角色为 primary 一端未配置检测次数，则系统将等待 *seconds* 时间后超时断开 SOT 连接。

请在系统视图下进行下面配置。

表15-7 配置 keepalive 帧超时定时器

操作	命令
配置 keepalive 帧超时定时器	**sot timer keepalive** [*seconds*]
恢复 keepalive 帧超时定时器的缺省设置	**undo sot timer keepalive** [*seconds*]

超时定时器的缺省设置为 30 秒。

本命令应在 SOT 本地应答模式下使用，且可以与 **sot counter keepalive** 命令配合使用。

15.2.7 在接口下配置协议组的相关参数

请在同步串口视图下进行下面配置。

1. 配置终端的 SDLC 地址

本命令在穿透模式（非广播方式）和本地应答模式下使用。

在同一接口下可以配置多个终端的 SDLC 地址。只有配置了终端的 SDLC 地址之后，才可以执行路由命令 **sot send address**。

undo sot sdlc controller 命令用来删除串行链路上的终端的 SDLC 地址，如果已经配置了 **sot send address**，应先删除 **sot send address** 命令，再删除终端的 SDLC 地址。

表15-8 配置终端的 SDLC 地址

操作	命令
配置串行链路上的终端的 SDLC 地址	**sot sdlc controller** *sdlc-address*
删除串行链路上的终端的 SDLC 地址	**undo sot sdlc controller** *sdlc-address*

终端的 SDLC 地址不能为 0 和 FF，因为 FF 地址为广播地址专用，0 用于其他用途。

对于穿透模式下的广播发送方式，应使用下面命令配置终端 SDLC 地址。

表15-9 配置终端的 SDLC 地址为广播地址

操作	命令
为 SDLC 终端配置广播地址	**sot sdlc broadcast**
删除 SDLC 终端的广播地址	**undo sot sdlc broadcast**

2. 配置 SDLC 的角色

该命令仅在本地应答模式和穿透模式的广播方式下配置才有意义。

如果是本地应答模式，必须配置角色，角色需遵从主（IBM 主机）、从（路由器）、主（路由器）、从（终端）这样的次序，即与 IBM 主机相连的路由器是从节点，与终端相连的路由器是主节点（注意：这种模式下同一协议组的终端的 SDLC 地址不能重复）；如果是广播模式，也必须配置角色，角色需遵从主（IBM 主机）、从（路由器）、从（路由器）、从（终端）这样的次序，即与 IBM 主机和终端相连的路由器都是从节点；其他模式下不需要配置角色。

表15-10 配置 SDLC 角色

操作	命令
配置 SDLC 主角色	**sot sdlc-status primary**
配置 SDLC 从角色	**sot sdlc-status secondary**
删除 SDLC 角色	**undo sot sdlc-status**

3. 配置 SOT 的路由

(1) **simple** 模式

simple 模式下路由器将向指定地址转发所有的 SDLC 帧，故配置下面命令。**simple** 模式下的终端的 SDLC 地址缺省为 01，不需要配置。

表15-11 发送 SDLC 帧的路由配置命令

操作	命令
配置向指定地址转发接口上的所有 SDLC 帧	**sot send all tcp** *ip-address*
取消转发接口上的所有 SDLC 帧	**undo sot send all tcp** *ip-address*

(2) **SDLC** 模式

表15-12 配置向特定终端发送 SDLC 帧的路由

操作	命令
配置向特定终端发送 SDLC 帧的路由	**sot send address** *sdlc-address* **tcp** *ip-address* [**local**] [**send-queue**]
删除指定的 SDLC 帧路由表项	**undo sot send address** *sdlc-address* **tcp** *ip-address* [**local**] [**send-queue**]

- 非本地应答模式下

非本地应答模式（即透传模式）下，路由器对收到的 SDLC 帧要检查其终端的 SDLC 地址，然后用这个终端的 SDLC 地址与 SOT 路由表进行匹配，再将 SDLC 帧打成 TCP 包在 IP 网上进行传送。在非本地应答模式下，可以配置广播模式，向所有终端发送 SDLC 帧。

在穿透模式下，若以广播方式发送数据，则 *sdlc-address* 配置为广播地址 0xFF 即可。

- 本地应答模式下（**local**）

本地应答模式下，路由器对收到的 SDLC 帧不仅要检查其终端的 SDLC 地址，而且还要检查数据包的内容，对于某些内容不必进行传送。然后用终端的 SDLC 地址与 SOT 路由表进行匹配，再将 SDLC 帧打成 TCP 包在 IP 网上进行传送。在本地应答模式下，不能够配置广播方式。

15.3 SOT 的显示和调试

请在任意视图下使用下面命令。

表15-13 SOT 的显示和调试

操作	命令
显示当前 SOT 的连接状态	**display sot**
显示当前串口的状态	**display interface serial** *number*

操作	命令
显示 TCP 连接的状态	**display tcp status**

15.4 SOT 典型配置举例

15.4.1 SOT 基本模式典型配置举例

1. 组网需求

RouterA 通过串口 Serial0/0/0 连接 IBM 主机，RouterB 通过串口 Serial0/0/0 连接终端，RouterA 和 RouterB 的串口 Serial1/0/0 通过广域网互连。在 RouterA 和 RouterB 上配置 SOT 基本模式实现 IBM 主机与终端的互通。

2. 组网图

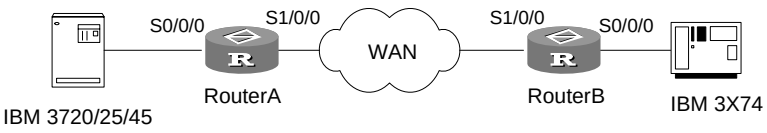


图15-4 SOT 基本模式典型配置举例

3. 配置步骤

(1) 路由器 A

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.1 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.1
[H3C] sot group-set 8 simple
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 8
[H3C-Serial0/0/0] sot send all tcp 1.0.0.2
[H3C-Serial0/0/0] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 100.1.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 200.2.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.2 serial 1/0/0
```

(2) 路由器 B

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.2 24
[H3C-LoopBack0] quit
```

```
[H3C] sot peer 1.0.0.2
[H3C] sot group-set 8 simple
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 8
[H3C-Serial0/0/0] sot send all tcp 1.0.0.1
[H3C-Serial0/0/0] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 200.2.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 100.1.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.2 SOT 穿透模式典型配置举例

1. 组网需求

RouterA 通过串口 Serial0/0/0 连接 IBM 主机，RouterB 通过串口 Serial0/0/0、Serial0/0/1 分别连接终端 C1、C2，RouterA 和 RouterB 的串口 Serial1/0/0 通过广域网互连。在 RouterA 和 RouterB 上配置 SOT 穿透模式实现 IBM 主机与终端 C1、C2 互通。

2. 组网图

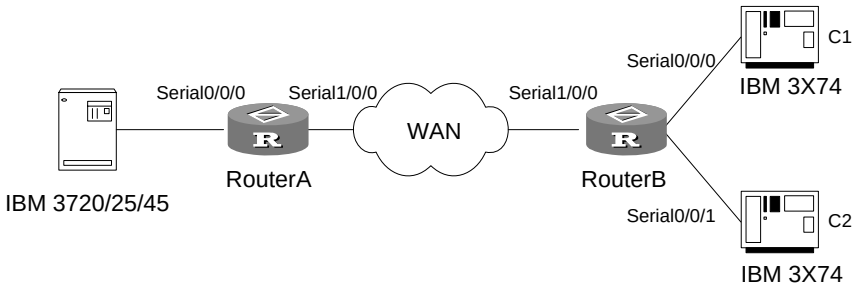


图15-5 SOT 穿透模式典型配置举例

3. 配置步骤

(1) 路由器 A

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.1 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.1
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc controller c1
```

```
[H3C-Serial0/0/0] sot send address c1 tcp 1.0.0.2
[H3C-Serial0/0/0] sot sdlc controller c2
[H3C-Serial0/0/0] sot send address c2 tcp 1.0.0.2
[H3C-Serial0/0/0] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 100.1.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 200.2.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.2 serial 1/0/0
```

(2) 路由器 B

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.2 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.2
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc controller c1
[H3C-Serial0/0/0] sot send address c1 tcp 1.0.0.1
[H3C-Serial0/0/0] interface serial 0/0/1
[H3C-Serial0/0/1] link-protocol sot
[H3C-Serial0/0/1] sot gather 1
[H3C-Serial0/0/1] sot sdlc controller c2
[H3C-Serial0/0/1] sot send address c2 tcp 1.0.0.1
[H3C-Serial0/0/1] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 200.2.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 100.1.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.3 SOT 穿透模式下的广播发送方式配置举例

1. 组网需求

RouterA 通过串口 Serial0/0/0 连接 IBM 主机，RouterB 通过串口 Serial0/0/0、Serial0/0/1 分别连接终端 C1、C2，RouterA 和 RouterB 的串口 Serial1/0/0 通过广域网互连。在 RouterA 和 RouterB 上配置 SOT 穿透模式并按广播方式向终端 C1、C2 发送数据。

2. 组网图

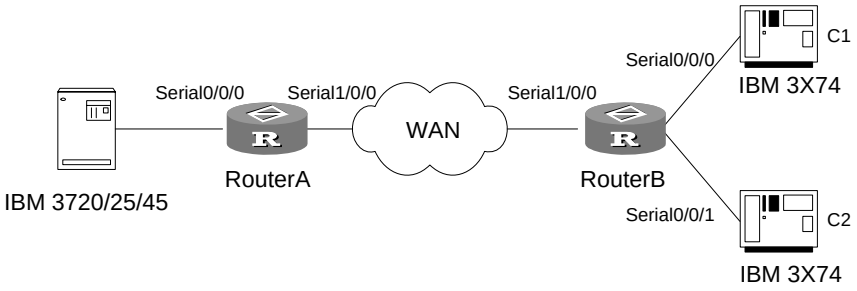


图15-6 SOT 穿透模式下的广播发送方式配置举例

3. 配置步骤

(1) 路由器 A

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.1 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.1
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc-status secondary
[H3C-Serial0/0/0] sot sdlc broadcast
[H3C-Serial0/0/0] sot send address ff tcp 1.0.0.2
[H3C-Serial0/0/0] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 100.1.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 200.2.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.2 serial 1/0/0
```

(2) 路由器 B

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.2 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.2
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc-status secondary
[H3C-Serial0/0/0] sot sdlc broadcast
[H3C-Serial0/0/0] sot send address ff tcp 1.0.0.1
[H3C-Serial0/0/0] interface serial 0/0/1
```

```
[H3C-Serial0/0/1] link-protocol sot
[H3C-Serial0/0/1] sot gather 1
[H3C-Serial0/0/1] sot sdlc-status secondary
[H3C-Serial0/0/1] sot sdlc broadcast
[H3C-Serial0/0/1] sot send address ff tcp 1.0.0.1
[H3C-Serial0/0/1] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 200.2.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 100.1.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.1 serial 1/0/0
```

15.4.4 SOT 本地应答模式的配置举例

1. 组网需求

RouterA 通过串口 Serial0/0/0 连接 IBM 主机，RouterB 通过串口 Serial0/0/0、Serial0/0/1 分别连接终端 C1、C2，RouterA 和 RouterB 的串口 Serial1/0/0 通过广域网互连。在 RouterA 和 RouterB 上配置本地应答模式实现 IBM 主机与终端 C1、C2 互通。

2. 组网图

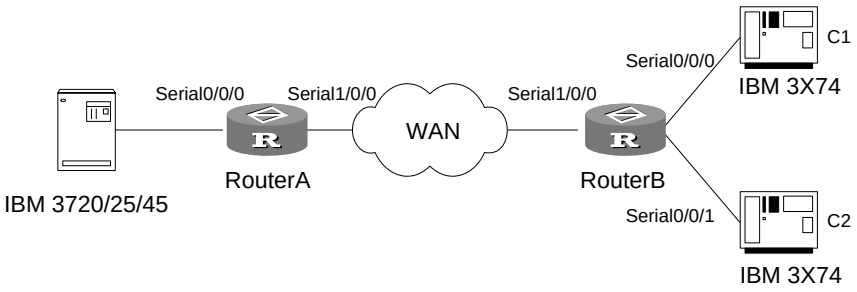


图15-7 SOT 本地应答模式的配置举例

3. 配置步骤

(1) 路由器 A

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.1 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.1
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc-status secondary
[H3C-Serial0/0/0] sot sdlc controller c1
```

```
[H3C-Serial0/0/0] sot send address c1 tcp 1.0.0.2 local
[H3C-Serial0/0/0] sot sdlc controller c2
[H3C-Serial0/0/0] sot send address c2 tcp 1.0.0.2 local
[H3C-Serial0/0/1] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 100.1.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 200.2.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.2 serial 1/0/0
```

(2) 路由器 B

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.0.0.2 24
[H3C-LoopBack0] quit
[H3C] sot peer 1.0.0.2
[H3C] sot group-set 1 sdlc
[H3C] interface serial 0/0/0
[H3C-Serial0/0/0] link-protocol sot
[H3C-Serial0/0/0] sot gather 1
[H3C-Serial0/0/0] sot sdlc-status primary
[H3C-Serial0/0/0] sot sdlc controller c1
[H3C-Serial0/0/0] sot send address c1 tcp 1.0.0.1 local
[H3C-Serial0/0/0] interface serial 0/0/1
[H3C-Serial0/0/1] link-protocol sot
[H3C-Serial0/0/1] sot gather 1
[H3C-Serial0/0/1] sot sdlc-status primary
[H3C-Serial0/0/1] sot sdlc controller c2
[H3C-Serial0/0/1] sot send address c2 tcp 1.0.0.1 local
[H3C-Serial0/0/1] interface serial 1/0/0
[H3C-Serial1/0/0] ip address 200.2.1.1 16
[H3C-Serial1/0/0] quit
[H3C] ip route-static 100.1.1.1 serial 1/0/0
[H3C] ip route-static 1.0.0.1 serial 1/0/0
```

第16章 NetStream 配置

16.1 NetStream 简介

16.1.1 NetStream 概述

NetStream 提供报文统计功能，它根据报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS、输入/输出接口来区分流，并针对不同的流进行独立的数据统计。

NetStream 的统计信息定期发送给 NSC（NetStream Collector，网络流数据收集器），由 NSC 进一步处理后，交给 NDA（NetStream Data Analyzer，网络流数据分析器）进行数据分析、计费、网络规划等多种应用。

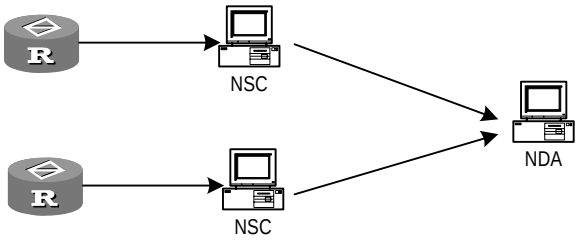


图16-1 NetStream 数据采集和分析图

上图是 NetStream 进行数据采集和分析的一个过程示意：路由器把采集到的关于流的详细信息输出给 NSC，NSC 初步处理后输出给 NDA，由 NDA 进行分析。同时，NetStream 对于防火墙和策略路由可以在流交换的基础上实现快速处理。

16.1.2 NetStream 实现

启用 NetStream 后，流信息首先被存储在 NetStream 缓冲区中，当流老化后，流信息通过 UDP 报文发送给 NSC。

NetStream 使用两种版本的 UDP 报文：版本 5 的报文和版本 8 的报文。

通常情况下，流老化后直接通过版本 5 的 UDP 报文发送。

如果配置了 NetStream 聚合（NetStream Aggregation），流信息将按照一定的规则分类、合并后生成聚合信息，再通过版本 8 的 UDP 报文发送。

16.2 NetStream 配置

配置 NetStream 功能时，首先需要在接口上启用 NetStream，然后指定统计信息输出的接口地址和 UDP 端口号。

如果使用 NetStream 聚合功能，则在接口上启用 NetStream 后，还需要配置 NetStream 聚合，并指定统计信息输出的接口地址和 UDP 端口号。

- 启用 NetStream 功能
- 配置 NetStream 聚合功能
- 配置 NetStream 输出的 UDP 报文
- 配置 NetStream 日志报文的时间戳

以下几项由用户根据实际情况决定是否需要设置，可以使用缺省配置。

- 配置 NetStream 版本 5 的 UDP 报文
- 配置 NetStream 的流老化
- 配置 NetStream 每秒最大老化流数
- 配置 NetStream 的最大流数
- 取消 NetStream 日志报文的日志头中的流方向标记

16.2.1 启用 NetStream 功能

NetStream 功能是在接口上启用的，由接口对接收的报文或发送的报文进行统计。一个接口上可以同时进行报文的入统计和出统计。

请在接口视图或桥模板视图下进行下列配置。

表16-1 启用 NetStream 功能

操作	命令
启用接口的 NetStream 入统计	**ip netstream inbound**
关闭接口的 NetStream 入统计	**undo ip netstream inbound**
启用接口的 NetStream 出统计	**ip netstream outbound**
关闭接口的 NetStream 出统计	**undo ip netstream outbound**

缺省情况下，接口上不启用 NetStream 入统计功能和出统计功能。

16.2.2 配置 NetStream 聚合功能

NetStream 支持聚合功能。老化的流在输出前先按照一定的规则进行分类，生成聚合的信息后再通过版本 8 的 UDP 报文发送出去。

在目前的实现中，支持五种聚合方式：

表16-2 NetStream 的五种聚合方式

聚合方式	分类依据
自治系统聚合	源 AS 号、目的 AS 号，输入接口索引、输出接口索引

聚合方式	分类依据
协议－端口聚合	协议号、源端口、目的端口
源前缀聚合	源 AS 号、源地址掩码长度、源前缀、输入接口索引
目的前缀聚合	目的 AS 号、目的地址掩码长度、目的前缀、输出接口索引
源和目的前缀聚合	源 AS 号、目的 AS 号、源地址掩码长度、目的地址掩码长度、源前缀、目的前缀、输入接口索引、输出接口索引

系统根据所选择聚合方式的分类依据，将多条流合并为一条聚合流，对应一条聚合记录。

配置 NetStream 的聚合功能时，首先进入某种聚合视图，然后在此聚合视图中使能该聚合功能。五种聚合功能相互独立，可以同时配置。

表16-3 配置 NetStream 聚合功能

操作	命令
进入 NetStream 的聚合视图（系统视图）	**ip netstream aggregation** { **as** | **protocol-port** | **source-prefix** | **destination-prefix** | **prefix** } *
使能聚合功能（聚合视图）	**enable**
取消聚合功能（聚合视图）	**undo enable**

缺省情况下，不使能任何 NetStream 聚合功能。

16.2.3 配置 NetStream 输出的 UDP 报文

NetStream 统计的流信息老化后通过 UDP 报文发送给 NSC。

用户可以对 NetStream 生成的 UDP 报文的源接口和目的地址及目的 UDP 端口号进行设置，其中源接口地址将做为 UDP 报文的源地址。

请在系统视图或聚合视图下进行下列配置。

表16-4 配置 NetStream 输出的 UDP 报文

操作	命令
配置 NetStream 输出的 UDP 报文源接口	**ip netstream export source interface** *interface-name*
恢复 UDP 报文的源接口缺省设置	**undo ip netstream export source**
配置 NetStream 输出的 UDP 报文的目的地址和端口号	**ip netstream export host** *ip-address udp-port*
恢复 UDP 报文的缺省目的地址和端口号	**undo ip netstream export host**

操作	命令
配置 UDP 报文的版本号及 Netstream 记录的被统计报文 IP 地址的自治系统号选项	**ip netstream export version** *version-number* [**origin-as** | **peer-as**]
恢复缺省设置	**undo ip netstream export version**

缺省情况下，系统视图下的源接口为 0，目的地址和目的 UDP 端口号都为 0，UDP 报文的版本号为 5，并以邻接自治系统号作为 UDP 报文的自治系统号（**peer-as**），聚合视图缺省使用系统视图下配置的源接口、目的地址和 UDP 端口号。

用户可以选择以起始自治系统号还是以邻接自治系统号作为 UDP 报文的自治系统号。

聚合视图缺省使用系统视图下配置的目的地址和 UDP 端口号。

需要说明的是：聚合视图下的配置只影响版本 8 的 UDP 报文；系统视图下的配置影响版本 5 的 UDP 报文，并在聚合视图下没有配置源接口和目的参数时，对版本 8 的 UDP 报文生效。

ip netstream export version 命令中 AS 类型的选项设置针对的是被统计报文，而不是统计上报的 UDP 报文。

在 FIB 表中，每个 IP 地址有两个 AS 号，一个是 origin-as，一个是 peer-as。而 Netstram 统计流的时候对于源 IP 和目的 IP 都只记录一个 AS 号。例如，缺省是 peer-as，则启动流统计时候 NetStream 只记录源 IP 和目的 IP 地址的 peer 型 AS 号。

16.2.4 配置 Netstream 日志报文的时间戳

Netstream 日志报文的时间戳为本地时间，在采用其它厂商的 NDA 如 CISCO 的 ManageEngine's NetFlow Analyzer 5，日志报文是按 UTC 时间解析的，当需要与其它厂商 NDA 兼容时，必须将 Netstream 日志报文的时间戳设置为 UTC 时间。

请在系统视图下进行下列配置。

表16-5 Netstream 日志报文的时间戳为 UTC 时间

操作	命令
配置 Netstream 日志报文的时间戳为 UTC 时间	**ip netstream format utc-time**
恢复缺省设置	**undo ip netstream format utc-time**

缺省情况下，Netstream 日志报文的时间戳为本地时间。

16.2.5 配置 NetStream 的流老化

在实际网络环境中，可能在很短的时间内产生大量流，这就需要根据一定的算法把当前一部分流从缓冲区中删除，称为老化（aging）。

NetStream 的老化机制有三种：按时老化、强制老化、TCP 的 FIN 和 RST 报文触发老化。

1. 配置按时老化

有两种按时老化方式：

- 按不活跃时间老化：对从最后一个报文流过到当前的时间超过 inactive timeout 的流进行老化；
- 按活跃时间老化：对从第一个报文流过到当前的时间超过 active timeout 的流进行老化。

请在系统视图下进行下列配置。

表16-6 配置按时老化

操作	命令
配置 NetStream 的活跃老化时间	**ip netstream timeout active** *minutes*
恢复 NetStream 的缺省活跃老化时间	**undo ip netstream timeout active**
配置 NetStream 的不活跃老化时间	**ip netstream timeout inactive** *seconds*
恢复 NetStream 的缺省不活跃老化时间	**undo ip netstream timeout inactive**

缺省情况下，流的活跃老化时间为 30 分钟，不活跃老化时间为 30 秒。

📖 **说明：**

配置老化时间时，需要注意：活跃老化时间的单位是分钟，而不活跃老化时间的单位是秒。

2. 执行强制老化

执行强制老化命令，用户可以将 NetStream 缓冲区中所有流老化输出，不必等待流老化超时就清除 NetStream 统计信息。

请在用户视图下进行下列操作。

表16-7 执行强制老化

操作	命令
清除 NetStream 统计信息，并老化流缓存区中所有流	**reset ip netstream statistics**

3. TCP 的 FIN 和 RST 报文触发老化

在 TCP 连接断掉或重启的时候 NetStream 缓冲区中相应的流会自动老化输出。这种老化方式不需要配置，由 NetStream 模块自动实现。

16.2.6 配置 NetStream 每秒最大老化流数

NetStream 流老化，首先进行老化处理对老化的流进行统计并仍存放在路由器 NetStream 缓冲区中，在日志输出处理时再生成 UDP 报文输出给 NSC。

根据实际需要，用户可以手工调整路由器每秒进行老化处理的最大流数。

请在系统视图下进行下列配置。

表16-8 配置 NetStream 每秒最大老化流数

操作	命令
配置 NetStream 每秒最大老化流数	**ip netstream process** *max-entries*
恢复缺省设置	**undo ip netstream process**

缺省情况下，每秒进行老化处理的最大流数为 100 条。

说明：

当 NetStream 流缓存区中的流数没有到达其所能容纳流的最大数量，每秒输出日志的流数仍为 100 条。

16.2.7 配置 NetStream 的最大流数

NetStream 统计的流信息首先存放在路由器 NetStream 流缓冲区中，当这些流老化后生成 UDP 报文输出给 NSC。

根据实际需要，用户可以手工调整路由允许存放的最大流数。

请在系统视图下进行下列配置。

表16-9 配置 NetStream 最大流数

操作	命令
配置 NetStream 流的缓存区大小	**ip netstream max-entry** *max-entries*

操作	命令
恢复缺省设置	**undo ip netstream max-entry**

缺省情况下，不同产品 NetStream 流缓冲区有所不同，请以实际产品规格为准。

16.2.8 取消 Netstream 日志报文的日志头中的流方向标记

在 Netstream 日志报文的日志头的第一个字节用来标记流方向，第二个字节用于标记版本号。但 Cisco 的日志报文中的前两个字节都是用来标记版本号的，没有标记流方向。当需要与 Cisco 兼容时，需要使用该命令去掉流方向的标记。

请在系统视图下进行下列配置。

表16-10 取消 NetStream 日志报文的日志头总的流方向标记

操作	命令
取消 Netstream 日志报文的日志头中的流方向标记	**ip netstream format no-direction**
恢复缺省设置	**undo ip netstream format no-direction**

缺省情况下，Netstream 日志报文的日志头中标记流方向。

16.3 NetStream 显示和调试

在完成上述配置后，可在任意视图下执行 **display** 命令显示配置后 NetStream 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **debugging** 命令可对 NetStream 进行调试。

表16-11 NetStream 显示和调试

操作	命令
查看 NetStream 流缓存区的配置和状态信息	**display ip netstream cache**
查看 NetStream 统计输出报文信息	**display ip netstream export**
打开 NetStream 调试开关	**debugging ip netstream** { **packet** | **event** }
关闭 NetStream 调试开关	**undo debugging ip netstream** { **packet** | **event** }

16.4 NetStream 典型配置举例

16.4.1 配置 NetStream 分类统计功能

1. 组网需求

在路由器 RouterA 上配置 NetStream 入统计和出统计。

2. 组网图

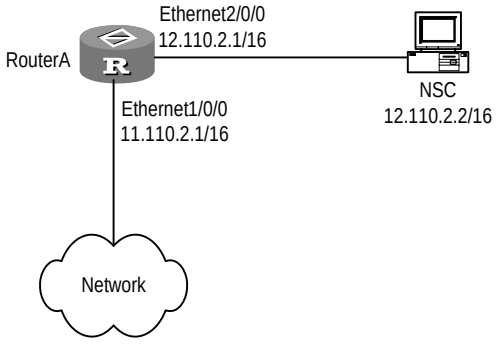


图16-2 配置 NetStream 分类统计功能

3. 配置步骤

配置接口 Ethernet 1/0/0，在此接口上启动 NetStream 入统计。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 11.110.2.1 255.255.0.0
[H3C-Ethernet1/0/0] ip netstream inbound
```

配置接口 Ethernet 2/0/0，在此接口上启动 NetStream 出统计。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 12.110.2.1 255.255.0.0
[H3C-Ethernet2/0/0] ip netstream outbound
```

配置 UDP 报文的目的地址和目的端口，源接口采用缺省配置。

```
[H3C] ip netstream export host 12.110.2.2 5000
```

16.4.2 配置版本 5 和版本 8 报文输出

1. 组网需求

在路由器 RouterA 上配置 NetStream，配置版本 5 报文输出和 5 种聚合的报文输出。

RouterA、RouterB 和 RouterC 之间建立 EBGP 邻居关系。

2. 组网图

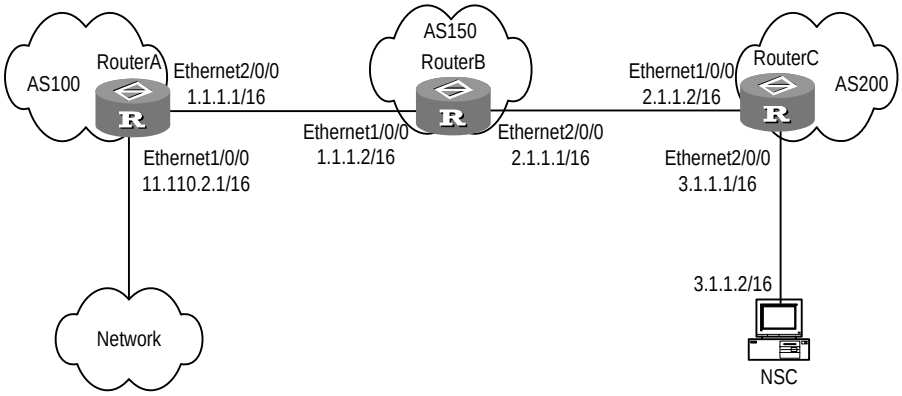


图16-3 配置版本 5 和版本 8 报文输出

3. 配置步骤

(1) 配置路由器 RouterA

配置接口 Ethernet 1/0/0，在出、入方向启动 NetStream 统计。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 11.110.2.1 255.255.0.0
[H3C-Ethernet1/0/0] ip netstream inbound
[H3C-Ethernet1/0/0] ip netstream outbound
```

配置接口 Ethernet 2/0/0。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 1.1.1.1 255.255.0.0
```

配置 BGP。

```
[H3C] bgp 100
[H3C-bgp] peer 1.1.1.2 as-number 150
[H3C-bgp] network 11.110.0.0 255.255.0.0
```

配置 NetStream 版本号和自治系统选项

```
[H3C] ip netstream export version 5 origin-as
```

配置 NetStream 最大流数。

```
[H3C] ip netstream max-entry 5000
```

配置版本 5 输出目的地址、目的端口、源接口。

```
[H3C] ip netstream export host 3.1.1.2 5000
[H3C] ip netstream export source interface ethernet 1/0/0
```

配置自治系统聚合模式。

```
[H3C] ip netstream aggregation as
[H3C-aggregation-as] enable
```

```
[H3C-aggregation-as] ip netstream export host 3.1.1.2 2000
[H3C-aggregation-as] ip netstream export source interface ethernet 2/0/0
[H3C-aggregation-as] quit
```

配置协议－端口聚合模式。

```
[H3C] ip netstream aggregation protocol-port
[H3C-aggregation-protport] enable
[H3C-aggregation-protport] ip netstream export host 3.1.1.2 3000
[H3C-aggregation-protport] ip netstream export source interface ethernet 2/0/0
[H3C-aggregation-protport] quit
```

配置源前缀聚合模式。

```
[H3C] ip netstream aggregation source-prefix
[H3C-aggregation-srcpre] enable
[H3C-aggregation-srcpre] ip netstream export host 3.1.1.2 4000
[H3C-aggregation-srcpre] ip netstream export source interface ethernet 2/0/0
[H3C-aggregation-srcpre] quit
```

配置目的前缀聚合模式。

```
[H3C] ip netstream aggregation destination-prefix
[H3C-aggregation-dstpre] enable
[H3C-aggregation-dstpre] ip netstream export host 3.1.1.2 5000
[H3C-aggregation-dstpre] ip netstream export source interface ethernet 0/1/1
```

配置前缀聚合模式。

```
[H3C] ip netstream aggregation prefix
[H3C-aggregation-prefix] enable
[H3C-aggregation-prefix] ip netstream export host 3.1.1.2 7000
[H3C-aggregation-prefix] ip netstream export source interface ethernet 2/0/0
[H3C-aggregation-prefix] quit
```

(2) 配置路由器 RouterB

配置接口 Ethernet 1/0/0。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 1.1.1.2 255.255.0.0
```

配置接口 Ethernet 2/0/0。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 2.1.1.1 255.255.0.0
```

配置 BGP。

```
[H3C] bgp 150
[H3C-bgp] peer 1.1.1.1 as-number 100
[H3C-bgp] peer 2.1.1.2 as-number 200
```

(3) 配置路由器 RouterC

配置接口 Ethernet 1/0/0。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 2.1.1.2 255.255.0.0
```

配置接口 Ethernet 2/0/0。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 3.1.1.1 255.255.0.0
```

配置 BGP。

```
[H3C] bgp 200
[H3C-bgp] peer 2.1.1.1 as-number 150
```

第17章 RCR 配置

17.1 RCR 简介

等值路由是指目的地址、优先级、metric 值等完全相同而下一跳不同的多条路由（对应多个出口链路），等值路由可以通过动态路由协议生成，也可通过配置产生。

RCR （Resilient Controllable Routing，弹性可控路由）是在转发层面对基于等值路由的流量进行合理分配，分配的依据主要是接口的当前负载情况，并且可以实时监控接口的负载信息，通过调整数据流的转发接口从而对负载进行动态优化调整。

RCR 包含两种模式：本地模式和分布式工作模式，目前 Comware 仅支持 RCR 本地模式，主要实现了对数据流在多条等值路由链路上的动态调整。

17.1.1 RCR 本地模式的基本概念

RCR 本地模式应用于单一路由器设备，当该设备存在到达同一目的地址的多个等值路由时，路由器将按照这些等值路由对应的不同出接口链路的负载状况来分配流量，负载相对较轻的出接口被用于发送新的数据流。

当这些出接口上的负载状况不符合预期状况时，可以按照用户配置启动针对数据流的动态调整功能，将可被调整的数据流按照策略调整至合适的出接口进行转发。为了确保调整的可靠性、稳定性，RCR 本地模式还提供了预调整和无效调整消除等方法。

17.1.2 RCR 本地模式的调整对象

运行 RCR 本地模式的基本要求是在设备接口上启动了 Netstream 出方向流量统计，Netstream 数据流就是 RCR 本地模式调整的数据流对象的来源，此外，每条数据流的出入接口（出接口可以是等值路由对应的任意出接口）IP 快速转发也必须使能，否则 RCR 本地模式将不对这些数据流或等值路由接口进行数据流动态调整。

RCR 本地模式的调整对象来源是 Netstream 出方向数据流，将 Netstream 数据流进行处理之后得到调整对象数据流。

17.1.3 RCR 本地模式的策略

RCR 本地模式的策略分为两类：

(1) 按照接口的实时负载状况分配新流量

当路由器通过等值路由接口转发新的数据流时，RCR 本地模式特性将检查各接口的当前负载状况，选择负载相对较少的出接口转发数据流。

(2) 按照接口的实时负载状况和接口负载带宽动态调整现有流量分配

当路由器上同时存在多条同一目的地址的等值路由时，这些数据流在这多条等值路由对应的出接口上进行转发。RCR 将按照命令配置的周期检查这些出接口的负载状况，判断负载比例是否按照带宽分配，不符合则进行调整。

判断过程如下：通过 NetStream 统计结果获得接口上负载的实时分布情况，根据相关的等值路由接口负载数据计算比例，与接口带宽进行比较，若不符合度超过某个定值，则将负载较重接口上的数据流调整至负载最轻的接口上转发。这样，当接口的负载比例与接口的负载带宽比例相差较大时，RCR 本地特性就对这些数据流进行调整，使调整后的各接口的负载比例更接近于接口的带宽比例。

两种策略的区别是：第一种策略其工作方式是针对每个报文的，也就是说每个报文进入转发时，都会触发选择出接口的过程。第二种不会针对每个报文进行计算，而是进行定时调整。

例如，企业出口路由器中存在两条目的网段为 11.2.2.0 的等值路由，两条出口链路带宽分别为 Ethernet 1/0/0（带宽为 10M）和 Serial 2/0/0（带宽为 2M），此时两条链路的负载分别为 5M 和 1M。目的网段为 11.2.2.0 的数据流的转发过程为：转发模块根据目的地址查找路由表，发现存在等值路由。由于启动了 RCR，路由器首先查找两条出口链路的带宽，再通过查找 Netstream 网络流量统计结果得到两条链路的负载分布，从而得知 Ethernet 1/0/0 接口可发送 5M 流量，在 Serial 2/0/0 接口可以发送 1M，根据 RCR 算法，由于 Ethernet 1/0/0 的可用带宽比较大，所以该数据流将通过 Ethernet 1/0/0 对应的链路发送。

当两个接口的流量分布发生变化时，负载分担算法会根据最新的流量分布情况做出动态调整。例如接口 Ethernet 1/0/0 和 Serial 2/0/0 分别有 9.5M 和 1.5M 的流量，某时刻接口 Serial 2/0/0 的流量结束了，2M 带宽空闲下来，RCR 算法会感知到这一变化，把 Ethernet 1/0/0 上的部分流量调整到 Serial 2/0/0 上来。使两个接口的负载比例接近 10M:2M，即 5:1。

17.1.4 RCR 本地模式的启动和运行过程

RCR 本地模式的启动和运行的整个过程可描述如下：

- 路由器启动 RCR 本地模式，第一种策略立即被使用，该策略将代替 RCR 启动前的负载均担模式。
- 启动 RCR 本地模式后，用户即可配置待调整路由，最多可配置 50 个待调整路由项，这样的多个待调整路由项称作待调整路由列表。
- 当采用命令行设置了不为零的动态调整时间间隔后，路由器将按照该间隔启动定时器，周期检查待调整路由列表对应的路由，针对每个对应等值路由的待调整路由判断其对应的各出接口负载是否符合要求，若不符合，则进行动态调整。

17.1.5 防止无效调整

RCR 本地模式在执行动态调整时，采用预调整与实际调整分离的方法，预调整结果满足预期值时才进行实际调整，实际调整之前将检查需要被调整的数据流，对于那些流量相同的数据流而言，交换位置是没有意义的，这种调整将被杜绝。

17.2 启动 RCR 本地模式

配置路由器设备启动 RCR 本地模式，之后将采用第一类策略对新数据流进行转发。

17.2.1 配置准备

若当前的负载分担模式是负载均担模式（默认），则可以直接启动 RCR 本地模式。若当前的负载分担模式不是负载均担模式（例如：当前采用了等值路由根据带宽动态调整的负载分担模式），则必须关闭当前的负载分担模式，然后才能启动 RCR 本地模式。

17.2.2 启动 RCR 本地模式配置过程

表17-1 启动 RCR 配置过程

操作	命令	说明
进入系统视图	**system-view**	-
进入 RCR 视图	**rcrlocal**	必选
设置对 Netstream 流的流量和接口的 IP 流量的监测周期	**check-term** *seconds*	可选 缺省情况下，检测周期的缺省值为 3 秒

⚠ 注意：

启动 RCR 本地模式，必须先关闭其他的负载分担模式。

17.3 使能 RCR 本地模式动态调整

使用本配置可以启动 RCR 本地模式的动态调整，系统将周期性的检查待调整路由列表，对每一个待调整路由项进行接口负载情况统计，对于那些存在等值路由的待调整路由项，如果对应的接口负载情况不符合要求则进行动态调整。

17.3.1 配置准备

RCR 本地模式已经启动，当前视图为 rcrlocal 视图。

17.3.2 使能 RCR 本地模式动态调整配置过程

表17-2 使能 RCR 本地模式动态调整配置过程

操作	命令	说明
进入系统视图	**system-view**	-
启动 RCR 本地模式	请参见 17.2 启动RCR本地模式	必选
设置待调整路由项	**adjust-route** *ip-address* { *mask-length* | *net-mask* }	必选
启动动态调整，即设置动态调整时间间隔	**adjust-interval** *seconds*	可选 在缺省情况下，对等值路由接口带宽负载进行动态调整的时间间隔为 10 秒钟
设置 RCR 特性判断接口负载是否满足预期条件和调整是否达到预期条件的比例因子	**adjust-ratio** *value*	可选 在缺省情况下，比例因子的值为 1
显示 RCR 配置的信息	**display rcrlocal** { **interface-load** | **statistics** [*ip-address* { *mask-length* | *net-mask* }] }	**display** 命令可以在任意视图执行

17.3.3 RCR 典型配置举例

1. 组网需求

RouterA 存在三个到网络地址 10.2.1.0 的等值路由，分别对应出接口 Ethernet 3/0/0，Atm1/0/0，Serial 2/0/0，带宽分别为 10M、155M 和 64K。要求按照三个接口的带宽比例动态调整到该目的地址的流量。

2. 组网图

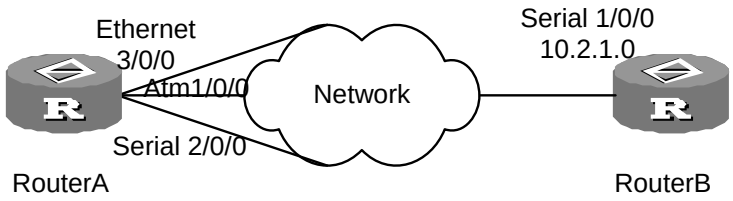


图17-1 RCR 本地模式动态调整组网图

3. 配置步骤

📖 说明：

三条链路的类型可以调整，但要确保 RouterA 路由表中存在三条可用的等值路由。所有接口的负载带宽可以在接口视图下使用命令 **loadbandwidth** 进行调整，使用 **loadbandwidth** 命令配置的带宽不影响接口属性，只对分配负载产生影响。

配置 Router A：

```
<H3C> system-view
[H3C] rcrlocal
[H3C-rcrlocal] adjust-route 10.2.1.0 24
[H3C-rcrlocal] adjust-interval 60
```

17.4 RCR 显示和维护

通过 **display** 命令对 RCR 本地模式配置进行显示，**display** 命令可以在任意视图下执行。

表17-3 RCR 配置显示和维护

配置	命令
显示所有接口的负载状况	**display rcrlocal interface-load**
显示全部或指定目的地址的等值路由的相关接口的负载状况和接口带宽情况	**display rcrlocal statistics** [*ip-address* { *mask-length* | *net-mask* }]

17.5 常见配置错误

- 出接口上的 Netstream 出方向数据流统计没有打开
- 数据流出/入接口上的 IP 快速转发没有全部打开

第18章 移动 IP

📖 **说明：**

该特性目前仅 AR 46 系列路由器及 AR 28 系列路由器支持。

18.1 移动 IP 简介

随着网络技术的发展，互联网的规模不断扩大，越来越多的移动用户希望能够以更加灵活的方式接入到互联网络中，因而提出了快速移动中的通信需求。在原有的 TCP/IP 网络中，一个子网内的移动节点进行了跨网段的漫游之后，在另外的子网中将无法使用原有网络（即家乡网络）中的固定 IP 地址进行通信，针对这种需求，移动 IP（Mobile IP，MIP）技术应运而生，它能够使移动用户在移动自己位置的同时无需中断正在进行的网络通信。

在移动 IP 系统中，移动节点始终使用固定的 IP 地址进行通信，这样在移动过程中可以保证已经建立的 TCP 连接不会中断。由于使用固定 IP 地址，使得网络位置的移动对用户是透明的；同时由于移动 IP 和网络介质无关，因此可以实现异质网络间的无缝漫游。

使用移动 IP 技术可以突破无线局域网（Wireless LAN，WLAN）的地域范围限制，并且克服了跨网段时使用动态主机配置协议（DHCP）方式所造成的通信中断等问题。

18.1.1 基本概念

1. 名词解释

- 家乡网络（Home Network）：其网络前缀与移动节点家乡地址的网络前缀匹配的网络，家乡网络可能是虚拟的。标准的 IP 路由机制将把发往移动节点家乡地址的报文发送到移动节点的家乡网络上。
- 家乡代理（Home Agent，HA）：指移动节点所在的本地网络的某一个主机或路由器，它保存有移动节点的位置信息，当移动节点离开本地网络时能够将发往移动节点的报文传给移动终端。
- 家乡地址（Home Address）：给移动节点分配的家乡网络中的 IP 地址，不管节点在何处接入 Internet，它都将保持不变。
- 外地网络（Foreign Network）：除移动节点的家乡网络外的任何其他网络。

- 外地代理（Foreign Agent，FA）：指移动节点当前所在的外地网络上的某一个主机或路由器，它能够把由家乡代理送来的数据包转发给移动节点。
- 转交地址（Care-of Address）：用于移动节点不在家乡网络时家乡代理把报文转交到移动节点。MIP 可以使用两种不同类型的转交地址：“外地代理转交地址”（Foreign Agent Care-of Address）是移动节点所注册的外地代理的地址；“配置转交地址”（Collocated Care-of Address）是移动节点从外部获得（通过手工配置或者通过 DHCP 获得等）的外地网络中的 IP 地址。
- 移动节点（Mobile Node，MN）：指一个主机或路由器，当它进行跨网段的漫游时可以不改变原有 IP 地址，并且仍能保持正在进行的通信。
- 移动路由器（Mobile Router，MR）：具备移动节点功能的路由器。
- 对端节点（Correspondent Node，CN）：与移动节点进行通信的同位体（peer），对端节点可为移动节点或固定节点。
- 移动代理（Mobility Agent）：包括家乡代理和外地代理。
- 移动绑定（Mobility Binding）：建立家乡地址与转交地址之间的绑定关系，以及确立该绑定关系的生存期。
- 访问者列表（Visitor List）：访问一个外地代理的移动节点的列表。

2. 安全联合

在移动节点进行注册的过程中，可以使用安全联合中定义的 SPI、密钥串对报文进行验证和加密、解密（使用 MD5 加密解密算法），以保证通信过程中的安全性。

安全联合包括六种：

- home-agent host（HA 与 MN 的安全联合）
- home-agent foreign-agent（HA 与 FA 的安全联合）
- foreign-agent visitor（FA 与 MN 的安全联合）
- foreign-agent home-agent（FA 与 HA 的安全联合）
- mobile-router home-agent（MR 与 HA 的安全联合）
- mobile-router foreign-agent（MR 与 FA 的安全联合）

3. Binding 表

Binding 表（绑定表）位于 HA，主要记录了移动节点的家乡地址和转交地址的对应关系，HA 根据移动节点的注册事件更新其绑定表信息。

4. Pending 表

Pending 表位于 FA，主要记录该 FA 上正在进行注册的移动节点的信息，包括节点的家乡地址、MAC 地址、家乡代理的地址等等。当某个移动节点注册成功后，该节

点的信息会从 Pending 表中删除并且在 Visitor 表中增加该节点的相应记录；如果移动节点注册失败，该节点的信息会直接从 Pending 表中删除。

5. Visitor 表

Visitor 表（访问者表）位于 FA，主要记录了在 FA 所在网络进行访问的移动节点的信息，包括节点的家乡地址、MAC 地址、家乡代理的地址等等，FA 根据移动节点的注册事件更新其 Visitor 表信息。

6. 多重绑定

当移动路由器支持多重绑定时，如果家乡代理也支持多重绑定，则 HA 会保留以前的移动绑定信息（包括转交地址等信息），也就是说 HA 上保存了 MR 多个转交地址的信息。否则，HA 会删除以前的移动绑定信息并用注册请求中指定的新的绑定信息来取代。

当至少使用一个无线网络接口的移动节点在多于一个外地代理的无线传输范围内移动时，多重绑定可能有用。当 HA 允许多重绑定时，它会把到达的每一个数据报的拷贝送到 HA 保存的该 MR 的每个转交地址，MR 将收到数据报的多个拷贝。

18.1.2 MIP 协议工作原理

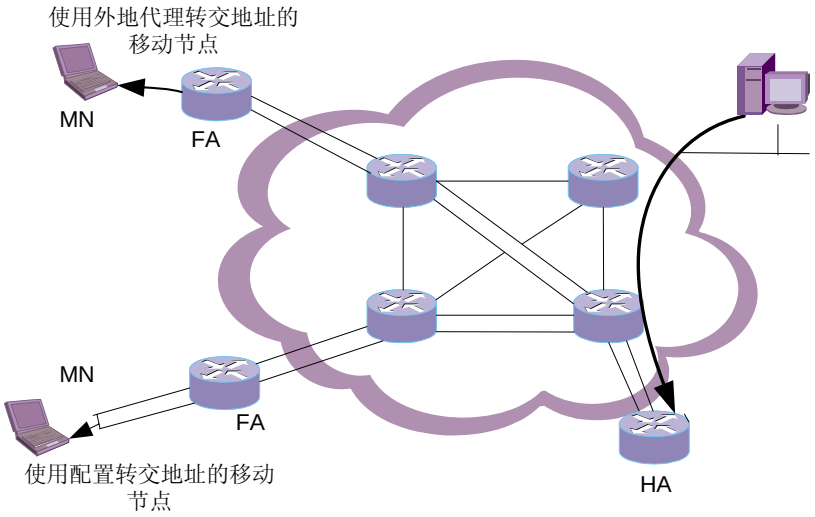


图18-1 移动 IP 原理图示

(1) HA 和 FA 在各自的本地网络上发送代理公告（Agent Advertisement）消息，以声明自己的存在。MN 根据收到的代理公告消息来判断自己是处于家乡网络还是外地网络。当 MN 处于家乡网络时，仍按传统的 TCP/IP 方式进行通信，不需要使用移动 IP 协议。

(2) 当移动终端判断自己已经漫游到一个外地网络时，启动 MIP 功能。为了能够收到通信对端发给它的 IP 数据包，移动终端需要向 HA 注册当前的位置地址，

这个位置地址就是转交地址。移动 IP 可以通过两种方式获得转交地址：借用外地代理的地址（即外地代理转交地址）和动态获得一个地址（即配置转交地址，例如使用 DHCP 等动态获得 IP 地址）。

(3) HA 接收来自转交地址的注册后，会构建一条通向转交地址的隧道，将截获的发给移动终端的 IP 数据包通过隧道送到外地网络的转交地址处。隧道技术有三种：IP in IP 封装、IP 的最小封装和 GRE（Generic Routing Encapsulation，通用路由封装）。

- IP in IP 封装用于将整个原始 IPv4 数据包放在另一个 IPv4 数据包的数据部分中。它在原始 IPv4 数据包的现有报头前插入了一个外层 IP 报头，外层报头中的源地址和目的地址分别标识隧道中的两个边界节点，即 HA 地址和转交地址。内层 IP 报头（即原始 IPv4 数据包报头）中的源地址和目的地址则分别标识原始数据包的发送节点和接收节点的 IP 地址。
- IP 的最小封装是移动 IP 中可选的隧道方式。它通过将 IP in IP 封装中内层 IP 报头和外层 IP 报头的冗余部分去掉，以减少实现隧道所需的开销。但使用这种封装技术有一个前提，就是原始的数据包不能已经被分片，因为 IP 的最小封装技术在新的 IP 报头和净荷之间插入了一个最小转发报头，它不保存有关分片的情况。
- 通用路由封装是移动 IP 采用的最后一种隧道技术。除了 IP 协议，它还可以支持其它网络层协议，它允许一种协议的数据包封装在另一种协议数据包中。

本模块支持两种隧道技术：IP in IP 封装和 GRE。

(4) 在转交地址处解除隧道封装，恢复出原始的 IP 数据包，如果 MN 使用的是外地代理转交地址，则由 FA 解除隧道封装，并将原始的 IP 数据报转发给 MN；如果 MN 使用的是配置转交地址，则由 MN 解除隧道封装，并继续解析 IP 数据报。这样 MN 在外地网络就能够收到这些发送给它的 IP 数据包

(5) 当 MN 在外地网络时，通过外地网络的路由器或者外地代理向通信对端发送 IP 数据包。如果使用反向隧道技术，则 MN 通过隧道将 IP 数据包发送到 HA（如采用配置转交地址）；或者先发送到 FA，由 FA 对数据包进行封装并传送给 HA（如采用外地代理转交地址），然后 HA 对数据包进行拆封，并通过正常路由发给通信对端。

(6) 当 MN 来到另一个外地网络时，只需要向家乡代理更新注册的转交地址，就可以继续通信。

(7) 当 MN 回到家乡网络时，移动终端向家乡代理注销转交地址，这时移动终端又将使用传统的 TCP/IP 方式进行通信。

18.1.3 移动 IP 模块实现的功能

移动 IP 模块实现了代理发现、注册、选路、虚拟网络以及移动路由器等功能：

1. 代理发现

FA 和 HA 通过 IRDP（ICMP Router Discovery Protocol）协议在自己所连接的本地网络上广播代理公告消息，以声明自己的存在。移动终端监听到这些消息后，就可以判断自己是在本地网络上还是在外地网络上，并且判断有哪些家乡代理或是外地代理连接在它目前所在的网络上。如果移动终端发现自己仍在本地网络上，即收到家乡代理发来的代理广告消息，则不启动移动 IP 功能。如果是从外地网络返回本地网络，则向家乡代理注销。如果移动终端检测到它已移动到一个新的外地网络上，则移动终端在得到转交地址后向家乡代理进行更新注册，以便让家乡代理存储移动终端的当前位置。

缺省情况下，FA 或 HA 并不周期性地发布代理公告报文，只有接到 MN 的代理请求报文后才会发送代理公告报文。通过设置 IRDP（ICMP Router Discovery Protocol，ICMP 路由发现协议）的相关属性，FA 或者 HA 会通过 IRDP 协议在各自的本地网络上周期性地广播代理公告消息，以声明自己的存在。

2. 注册

(1) 当 MN 发现自己从一个子网切换到另一个子网时，或发现所连接的 FA 进行重启时，或当前的注册就要过期时，MN 就向 FA（当 MN 的转交地址是代理转交地址时）或直接向 HA（当 MN 的转交地址是配置转交地址时）发送注册请求消息进行注册。如果直接向 HA 发送注册请求消息则直接转到第 3 步。

(2) FA 接收到注册请求后，要对它进行一系列的有效性检查，如果其中有一项检查失败，FA 就向 MN 发送一条注册应答消息拒绝这次注册请求，注册应答的 Code 域给出了拒绝的原因。如果检查有效，那么 FA 就将该消息中继到 MN 的 HA 那里，并建立一个 Pending 表项。

(3) HA 收到注册请求后，也做一系列和 FA 相似的有效性检查，如果注册请求是无效的，HA 就向 MN（或者 FA）发送一条注册应答，其中的 Code 域注明失败原因。如果注册请求有效，那么就更新 Binding 表，同时在路由表项中添加一条针对该 MN 家乡地址（即该 MN 的固定 IP 地址）且下一跳是 Mobile0 虚拟接口的路由表项，然后向 MN（或者 FA）发送注册应答，告知注册成功。当 MN 的转交地址是配置转交地址时则直接转向第 5 步。

(4) FA 收到注册应答后，同样要做一系列的有效性检查，如果是无效的，就产生一个包含适当的 Code 域的注册应答，并发送给 MN。如果注册应答是有效的，FA 就更新 Visitor 表，同时删除 Pending 表的相应表项，并将注册应答消息中继给 MN。

(5) MN 收到注册应答后，也需要进行有效性检查，如果应答有效，则检查 Code 域，确认是被接受还是被拒绝。如果被拒绝，则设法修正引起拒绝的错误，并尝试重新注册；如果注册被接受，则调整自己的路由表，以适应当前链路，然后就可以开始通信或继续先前的通信了。

(6) 注册成功后，HA 通过隧道向 MN 的转交地址传送数据包，或将从 MN 发出的包进行拆封（当使用反向隧道时）。另外，HA 还将发送免费 ARP 和代理 ARP 消息。当 MN 使用外地代理转交地址时，FA 对通过隧道发往 MN 的包进行拆封，或者将 MN 发出的包进行封装发往 HA（当使用反向隧道时）。当 MN 使用配置代理转交地址时，MN 对通过隧道到达 MN 的包进行拆封，或者将发出的包进行封装后发往 HA（当使用反向隧道时）。

另外，HA 还将发送免费 ARP 和代理 ARP 消息。MN 发送 ARP 请求时，HA 通过代理 ARP 将 ARP 请求中继给在外地网络的对端节点，并将获得的 MAC 地址回应给 MN。当移动到外地网络的节点注册成功后，HA 会发送免费 ARP 报文，以便 MN 更新 ARP 表项。

3. 数据包的选路

HA 收到发往 MN 的数据包，查找路由表项，如果下一跳是 Mobile0 接口，则 HA 对数据包进行封装后发往 MN 的转交地址。

当使用外地代理地址作为转交地址时，FA 是隧道的出口，对从隧道收到的数据包进行拆封，并发给 MN。当使用配置转交地址时，MN 是隧道的出口，同样需要对从隧道收到的数据包进行拆封。

在 MN 使用反向隧道和对端进行通信时，如果使用外地代理地址作为转交地址，那么 FA 就需要对 MN 发出的数据包进行封装并传送给 HA；如果使用配置转交地址，则 MN 要对发出的数据包进行封装并传送给 HA。HA 作为反向隧道的出口，对从反向隧道收到的数据包进行拆封，并通过正常路由发给通信对端。

4. 虚拟网络

如果家乡网络是一个虚拟网络，家乡网络在家乡代理上就没有一个实际的物理接口，也没有对应的物理链路发布代理公告消息。在这种情况下，该家乡网络上的移动终端总认为是在外地。虚拟网络允许本地路由器支持一个总是处于外地网络的移动终端。

5. 移动路由器

移动路由器是指路由器具有移动节点的功能，能够在移动代理之间移动，而且路由器所连接的静态网络也可以随路由器一起移动，因此，该静态网络也是移动网络。移动路由器同时能够提供外地代理的功能，为移动节点提供服务。例如，航行中的轮船，船上的局域网作为移动网络，通过一台移动路由器与 Internet 进行通信。

18.2 配置 MIP 总体策略

MIP 总体策略配置主要是指启动移动 IP 功能，只有设备启动了移动 IP 功能后，才能进行 HA 或者 FA 的相关配置。

18.2.1 配置 MIP 总体策略

表18-1 配置 MIP 总体策略

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
设置 PMTU（隧道 MTU）的更新策略	**mobile-ip tunnel path-mtu-discovery** [**age-timer** {*seconds* **| infinite**}]	可选 缺省情况下，不进行 PMTU 发现
打开 MIP 的 SNMP Trap 开关功能	**snmp-agent trap enable mobile-ip**	可选 缺省情况下，不启动 MIP 的 SNMP Trap 开关
显示 MIP 的全局信息	**display mobile-ip globals**	**display** 命令可以在任意视图下执行
显示 MIP 的所有计数器的统计信息	**display mobile-ip statistics**	

18.2.2 MIP 总体策略配置举例

1. 组网需求

在网络上设置两台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，另一台开启 FA 功能。有一台电脑作为 MN，MN 上安装了支持移动 IP 功能的相关软件，在通信过程中可以从家乡网络移动到外地网络。有一台电脑 CN 作为 MN 的对端节点，与 MN 进行通信。

2. 组网图

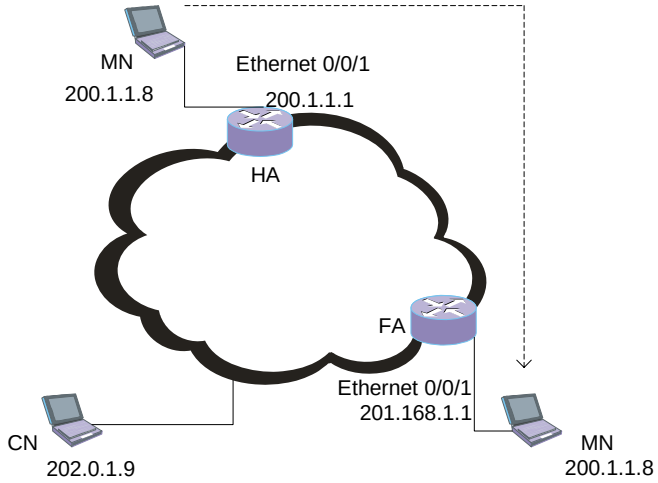


图18-2 MIP 总体策略配置组网图

3. 配置步骤

- 在 HA 上配置 MIP 的总体策略

在 HA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 HA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C] mobile-ip tunnel path-mtu-discovery
```

在 HA 上打开 SNMP Trap 开关（此项为可选配置）

```
[H3C] snmp-agent trap enable mobile-ip
```

- 在 FA 上配置 MIP 的总体策略

在 FA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 FA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C] mobile-ip tunnel path-mtu-discovery
```

在 FA 上打开 SNMP Trap 开关（此项为可选配置）

```
[H3C] snmp-agent trap enable mobile-ip
```

18.3 配置 HA

18.3.1 配置准备

当设备提供家乡代理（HA）服务时，需要进行 HA 的相关配置，只有启动了 MIP 功能且没有启动移动路由器（MR）服务，才能进行 HA 配置。

18.3.2 配置 HA

表18-2 配置 HA

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
启动 HA 功能	**mobile-ip home-agent** [**care-of-acl** *number*] [**ha-virtual-net** *ip-address*] [**lifetime** *seconds*] [**replay** *seconds*] [**reverse-tunnel** { **off** | **mandatory** }] [**roam-acl** *number*]	必选
配置 MN 的策略	请参见“18.5 配置MN”	必选
配置 MIP 安全联合	请参见“18.7 配置MIP的安全策略”	必选
定义一个虚拟网络	**mobile-ip virtual-network** *ip-address* { *mask* | *mask-length* } [**ha-address** *ip-address*]	可选 如果在启动 HA 功能时支持虚拟网络，则必须定义该虚拟网络
显示 MIP 绑定表信息	**display mobile-ip binding** [*ip-address* | **brief**]	**display** 命令可以在任意视图下执行
删除绑定表中的某条绑定信息	**reset mobile-ip binding** [*ip-address* | **interface ethernet** *interface-number*]	请在用户视图下执行该命令

18.3.3 HA 配置举例

1. 组网需求

组网需求同 1.2.2。现在要求只允许 IP 地址为 200.1.1.8 的 MN 进行漫游，可以漫游到的 FA 为 201.168.1.1。

2. 配置步骤

增加两个 ACL，2000 用作 **roam-acl**，用来指定那些 MN 可以进行移动；2001 用作 **care-of-acl**，指定节点可以漫游到那些 FA。

```
<H3C> system-view
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 200.1.1.8 0.0.0.0
[H3C-acl-basic-2000] quit
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 201.168.1.1 0.0.0.0
[H3C-acl-basic-2001] quit
```

启动 HA 功能。

```
[H3C] mobile-ip home-agent care-of-acl 2001 roam-acl 2000
```

18.4 配置 FA

18.4.1 配置准备

当设备提供外地代理（FA）服务时，需要进行 FA 的相关配置，只有启动了 MIP 功能后才能进行 FA 配置。

18.4.2 配置 FA

表18-3 配置 FA

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
启动 FA 功能	**mobile-ip foreign-agent** { **care-of ethernet** *interface-number* **| pending** *seconds* }	必选
进入以太网接口视图	**interface ethernet** *interface-number*	-
在接口上启动 FA 服务	**mobile-ip foreign-agent service** [**home-acl** *acl*] [**registration-required**] [**restrict** *number*] [**reverse-tunnel** [**mandatory**]]	必选
启动 MIP 前缀扩展	**mobile-ip prefix-length**	可选 缺省情况下，不启动该功能
配置注册生存时间	**mobile-ip registration-lifetime** *seconds*	可选 缺省情况下，注册生存时间为 3600 秒
配置 MIP 安全联合	请参见“18.7 配置MIP的安全策略”	可选

操作	命令	说明
显示 MIP 访问者信息	**display mobile-ip visitor** [**pending**] [*ip-address* **| brief**]	**display** 命令可以在任意视图下执行
显示 MIP 接口信息	**display mobile-ip interface** [**ethernet** *interface-number*]	**display** 命令可以在任意视图下执行
清除 FA 上的 visitor 和/或 pending 表的信息	**reset mobile-ip visitor** [**pending**] [*ip-address* **| interface ethernet** *interface-number*]	请在用户视图下执行该命令

18.4.3 FA 配置举例

1. 组网需求

组网需求同 1.2.2。

2. 配置步骤

在 FA 上启动 FA 功能，配置转交接口。

```
<H3C> system-view
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

在 FA 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

在 FA 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

18.5 配置 MN

18.5.1 配置准备

当设备提供家乡代理（HA）服务时，需要设置相关的移动节点（MN）的信息，这些 MN 是以该设备作为家乡代理的。只有启动了 HA 功能后才能进行 MN 的配置。

当 MN 是移动路由器（MR）时，用户还可以对针对 MR 进行某些配置，以保证 HA 可以支持该 MR 以及该 MR 连接的移动网络。

18.5.2 配置 MN

表18-4 配置 MN

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
配置 MN 的属性	**mobile-ip node** *low-addr* [*up-addr*] { **interface ethernet** *name* **| virtual-network** *ip-address mask*} [**lifetime** *lifetime*]	必选
当 MN 为 MR 时，配置该 MR 在 HA 上的编号，并且进入 HA-MR 视图	**mobile-ip home-agent mobile-router** *number*	可选 如果 MN 是移动路由器并且需要在 HA 上支持该 MR 连接的移动网络，需要进行该配置
配置移动路由器的 IP 地址	**ip address** *ip-address*	可选 如果 MN 是移动路由器并且需要在 HA 上支持该 MR 连接的移动网络，需要进行该配置
配置该 MR 连接的移动网络	**mobile-network** *ip-address* {*mask* | *mask-length* }	可选 如果 MN 是移动路由器并且需要在 HA 上支持该 MR 连接的移动网络，需要进行该配置
显示移动节点相关信息	**display mobile-ip node** [*ip-address* **| interface ethernet** *interface-number* **| virtual-network** *ip-address* **| brief**]	**display** 命令可以在任意视图下执行
清空移动节点的统计信息	**reset mobile-ip node-statistics** [*ip-address*]	请在用户视图下执行该命令

18.5.3 MN 配置举例

1. 组网需求

组网需求同 1.2.2。

2. 配置步骤

在 HA 上设置 MN 的属性，设置 IP 地址范围为 200.1.1.2 到 200.1.2.10 之间的 MN 都属于接口 ethernet 0/0/1。

```
<H3C> system-view
[H3C] mobile-ip node 200.1.1.2 200.1.2.10 interface ethernet 0/0/1
```

如果 200.1.1.9 的 MN 为移动路由器，其连接的移动网络是 201.1.3.0，则需要进行下面的配置。

```
[H3C] mobile-ip home-agent mobile-router 1
[H3C-HA-MobileRouter] ip addresss 200.1.1.9
[H3C-HA-MobileRouter] mobile-network 201.1.3.0 255.255.255.0
```

18.6 配置 MR

18.6.1 配置准备

当设备提供移动路由器服务时，需要进行移动路由器的相关配置。只有启动了 MIP 功能且没有启动 HA 服务，才能进行移动路由器的配置。

18.6.2 配置 MR

表18-5 配置 MR

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
启动 MR 功能，进入 MR 视图	**mobile-ip mobile-router**	必选
配置 MR 的家乡地址	**ip address** *ip-address* { *mask* | *mask-length* }	必选
配置 MR 的家乡代理	**home-agent ip-address** *ip-address*	必选
进入相应的接口视图	**interface** *interface-type interface-number*	-
配置接口的漫游功能	**mobile-ip mobile-router roam** [**priority** *value*]	必选
退回到系统视图	**quit**	-
配置 MR 所支持的移动网络	**mobile-network** { *interface-type interface-number* | *ip-address* { *mask* | *mask-length* } }	可选 如果 HA 也支持 MR，并且配置了 MR 所支持的移动网络，则 HA 会添加相应的 MR 支持的移动网络的路由，这样移动路由器所连接的移动网络才能够正常通信
配置 MR 的注册生命时间	**register lifetime** *value*	可选 缺省情况下，MR 的注册生命期为 36000s
配置 MR 的注册重传参数	**register retransmit** { **initial** *initial-time* **| maximum** *max-time* **| retry** *number* }	可选 缺省情况下，初始时间间隔 **initial** 为 1 秒，最大时间间隔 **maximum** 为 128 秒，最大重传次数 **retry** 为 5

操作	命令	说明
配置反向隧道功能	**reverse-tunnel enable**	可选 缺省情况下，没有配置反向隧道功能
配置同时绑定功能	**simultaneous-bindings enable**	可选 缺省情况下，没有配置同时绑定功能
配置报文封装类型	**encapsulation gre**	可选 缺省情况下，报文封装类型为 IP in IP
进入相应的接口视图	**interface** *interface-type interface-number*	-
配置代理请求参数	**mobile-ip mobile-router solicit** { **interval** *value* | **retransmit** { **initial** *value* | **maximum** *value* | **retry** *value* } }	可选 缺省情况下，接口的周期性发送代理请求的时间间隔 *interval-time* 为 600 秒，代理请求重传初始间隔 *initial-time* 为 1000ms。，代理请求重传最大时间间隔 *max-time* 为 4000ms，代理请求重传最大次数 *number* 为 5
配置 MR 只能使用配置转交地址进行注册以及注册时使用的默认网关	**mobile-ip mobile-router ccoa only** **mobile-ip mobile-router ccoa gateway** *ip-address*	可选 缺省情况下，接口没有配置只使用配置转交地址进行注册，也没有配置默认网关地址
显示移动路由器相关配置信息	**display mobile-ip mobile-router**	**display** 命令可以在任意视图下执行

18.6.3 MR 配置举例

1. 组网需求

在网络上设置三台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，一台开启 FA 功能，另一台开启 MR 功能。MR 在外地网络时可以与通信对端 CN 进行通信。

2. 组网图

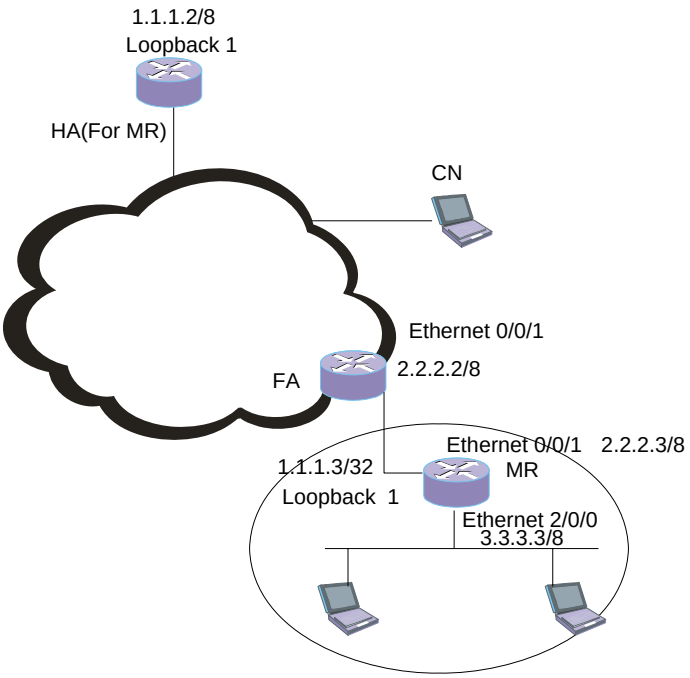


图18-3 MR 配置组网图

3. 配置步骤

在 MR 上启动 MIP 功能

```
[H3C] mobile-ip
```

在 MR 上启动 MR 功能

```
[H3C] mobile-ip mobile-router
```

在 MR 上配置 MR 的家乡地址

```
[H3C-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

在 MR 上配置 MR 的家乡代理

```
[H3C-MobileRouter] home-agent ip-address 1.1.1.2
```

在 MR 上配置移动网络

```
[H3C-MobileRouter] mobile-network ethernet 2/0/0
```

或者

```
[H3C-MobileRouter] mobile-network 3.3.3.3 255.0.0.0
```

在 loopback 口下配置 IP 地址，该 IP 地址为移动路由器的家乡地址。

```
[H3C] interface LoopBack1
[H3C-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

在以太口配置漫游功能

```
[H3C] interface Ethernet2/0/0
[H3C-Ethernet2/0/0] ip address 3.3.3.3 255.0.0.0
[H3C-Ethernet2/0/0] mobile-ip mobile-router roam
```

18.7 配置 MIP 的安全策略

18.7.1 配置准备

设置移动主机、家乡代理和外地代理间的移动安全联合，在移动节点注册的过程中使用安全联合以增强安全性。

- 当设备提供家乡代理（HA）服务时，必须配置 MN 与 HA 之间（即 **host**）的安全联合。同时，还可以选择配置 FA 与 HA 之间（即 **foreign-agent**）的安全联合。
- 当设备提供家乡代理（FA）服务时，可以选择配置 MN 与 FA 之间（即 **visitor**）的安全联合以及 HA 与 FA 之间（即 **home-agent**）的安全联合。
- 只有启动了 MIP 功能后才能进行 MIP 安全策略的配置。
- 当设备提供移动路由器（MR）服务时，必须配置 MR 与 HA 之间的安全联合。同时还可以选择配置 MR 与 FA 之间的安全联合。

18.7.2 配置 MIP 的安全策略

表18-6 配置 MIP 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
配置 MIP 的安全联合	**mobile-ip secure** { **home-agent** { **host** | **foreign-agent** } | **foreign-agent** { **visitor** | **home-agent** } | **mobile-router** { **home-agent** | **foreign-agnet** } } *low-addr* [*up-addr*] **spi** *spi* **key** *string*	必选 当设备提供 HA 服务时，必须配置 HA 与 MN 之间的安全联合。 当设备提供 MR 服务时，必须配置 MR 与 HA 间的安全联合。 其余类型的安全联合均为可选配置。
显示移动代理所记录的移动节点违反安全联合的相关信息	**display mobile-ip violation** [*ip-address*]	**display** 命令可以在任意视图下执行

操作	命令	说明
显示 MIP 的安全联合信息	**display mobile-ip secure**{ **home-agent** { **host** | **foreign-agent** } | **foreign-agent** { **visitor** | **home-agent** } | **mobile-router** { **home-agent** | **foreign-agnet** } } [*ip-address*]	**display** 命令可以在任意视图下执行

📖 说明：

配置HA与MR的安全联合功能，需要首先在HA指明MR的地址，相关配置请参考 18.5.2 配置MN

18.7.3 MIP 配置举例

1. 组网需求

组网需求同 18.6.3 。

2. 配置步骤

在 HA 上设置 HA-MN 的安全联合。

```
<H3C> system-view
[H3C] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

在 MR 上设置 MR-HA 的安全联合

```
<H3C> system-view
[H3C] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

在 HA 上设置 HA-FA 的安全联合（此项为可选配置）。

```
<H3C> system-view
[H3C] mobile-ip secure home-agent foreign-agent 2.2.2.2 spi 123 key abc
```

在 FA 上设置 FA-MN 的安全联合（此项为可选配置）。

```
<H3C> system-view
[H3C] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

在 FA 上设置 FA-HA 的安全联合（此项为可选配置）。

```
<H3C> system-view
[H3C] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

在 MR 上设置 MR-FA 的安全联合。

```
<H3C> system-view
[H3C] mobile-ip secure mobile-router foreign-agent  2.2.2.2 spi 123 key abc
```

18.8 配置 IRDP

18.8.1 配置准备

当在设备上启动了 FA 或 HA 服务后，FA 或 HA 并不周期性地发布代理公告报文，只有接到 MN 的代理请求报文后才会发送代理公告报文。通过设置 IRDP（ICMP Router Discovery Protocol，ICMP 路由发现协议）的相关属性，FA 或者 HA 会通过 IRDP 协议在各自的本地网络上周期性地广播代理公告消息，以声明自己的存在。

只有启动了 MIP 功能后才能进行 IRDP 相关属性的配置。

18.8.2 配置 IRDP

表18-7 配置 IRDP

操作	命令	说明
进入系统视图	**system-view**	-
启动 MIP 功能	**mobile-ip**	必选
设置路由发现协议相关参数	**mobile-ip irdp** [**lifetime** *seconds*] [**max-interval** *seconds*] [**min-interval** *seconds*] [**multicast**]	必选
显示路由发现协议相关信息	**display mobile-ip irdp**	**display** 命令可以在任意视图下执行

18.9 MIP 配置显示和维护

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

在用户视图下执行 **reset** 命令可以清除相应的统计信息。

表18-8 MIP 配置显示和维护

操作	命令	说明
显示 MIP 的全局信息	**display mobile-ip globals**	**display** 命令可以在任意视图下执行
显示MIP的所有计数器的统计信息	**display mobile-ip statistics**	
显示 MIP 访问者信息	**display mobile-ip visitor** [**pending**] [*address* **|** **brief**]	
显示 MIP 接口信息	**display mobile-ip interface** [**ethernet** *interface-number*]	
显示在 MIP 中违反安全的信息	**display mobile-ip violation** [*address*]	
显示 MIP 的安全联合信息	**display mobile-ip secure** { **home-agent** { **host |** **foreign-agent** } **|** **foreign-agent** { **visitor |** **home-agent** **} |** **mobile-router** { **home-agent |** **foreign-agnet** } } [*address*]	
显示路由发现协议相关信息	**display mobile-ip irdp**	
显示移动路由器相关信息	**display mobile-ip mobile-router** [**agent |** **registration | statistics**]	
清空MIP所有计数器的统计信息	**reset mobile-ip statistics**	用户视图下执行
清空移动路由器的相关信息	**reset mobile-ip mobile-router** { **agent** [*agent-address*] **|** **registration** [*reg-address*] **|** **statistics** }	用户视图下执行

18.10 典型组网案例

18.10.1 家乡网络为正常网络的典型组网

1. 组网需求

在网络上设置两台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，另一台开启 FA 功能。有一台电脑作为 MN，可以从家乡网络移动到外地网络。有一台电脑作为对端节点 CN，与 MN 通信。

2. 组网图

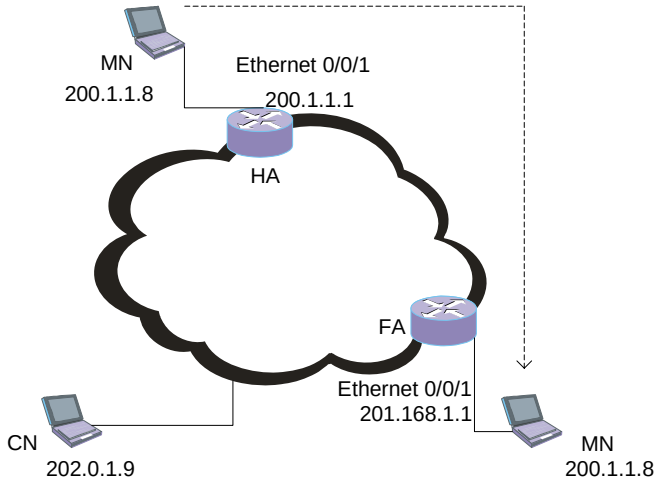


图18-4 家乡网络为正常网络 MIP 组网图

3. 配置步骤

(1) HA 的配置过程如下：

- 配置 MIP 的总体策略

在 HA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 HA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

在 HA 上打开 SNMP Trap 开关（此项为可选配置）

```
[H3C] snmp-agent trap enable mobile-ip
```

- 配置 HA 的策略

在 HA 上启动 HA 功能。

```
[H3C] mobile-ip home-agent
```

- 配置 MN 的策略

在 HA 上设置 MN 的属性。

```
[H3C] mobile-ip node 200.1.1.2  200.1.1.10 interface ethernet 0/0/1
```

- 配置 MIP 的安全策略

在 HA 上设置 HA-MN 的安全联合。

```
[H3C] mobile-ip secure home-agent host 200.1.1.2  200.1.1.10 spi 123 key abc
```

在 HA 上设置 HA-FA 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 201.168.1.1 spi 123 key abc
```

(2) FA 的配置过程如下

- 配置 MIP 的总体策略

在 FA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 FA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

在 FA 上打开 SNMP Trap 开关（此项为可选配置）

```
[H3C] snmp-agent trap enable mobile-ip
```

- 配置 MIP 的安全策略（注意，安全策略配置为可选配置）

在 FA 上设置 FA-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 200.1.1.2  200.1.1.10 spi 123 key
abc
```

在 FA 上设置 FA-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agent home-agent 200.1.1.1 spi 123 key abc
```

- 配置 FA 的策略

在 FA 上启动 FA 功能，配置转交接口为 Ethernet 0/0/1。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

在 FA 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

在 FA 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- 配置 MIP 的路由公告策略（此项为可选配置）

在 FA 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C-Ethernet0/0/1] mobile-ip irdp
```

18.10.2 家乡网络为虚拟网络的典型组网

1. 组网需求

在网络上设置三台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，另两台开启 FA 功能。有一台电脑作为 MN，其家乡网络为虚拟网络，一直在外地移动。

有一台电脑 CN 作为对端节点，与 MN 通信。在配置了虚拟网络后，属于该网络的 MN 永远在漫游。

2. 组网图

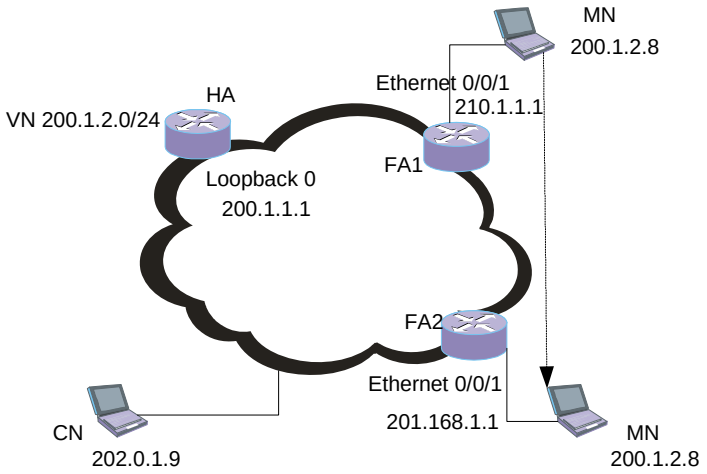


图18-5 家乡网络为虚拟网络 MIP 组网图

3. 配置步骤

(1) HA 的配置过程如下：

- 配置 MIP 的总体策略

在 HA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 HA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 HA 的策略

在 HA 上启动 HA 功能，指定虚拟网络的 HA 地址。

```
[H3C] mobile-ip home-agent ha-virtual-net 200.1.2.1
```

在 HA 上定义逻辑接口并为该接口配置 IP 地址。

```
[H3C] interface loopback 0
[H3C-loopback0] ip address 200.1.2.1 255.255.255.0
```

定义虚拟网络，为此虚拟网络指明其 HA 的地址为已经配置的环回地址。

```
[H3C-loopback0] quit
[H3C] mobile-ip virtual-network 200.1.2.0 24 ha-address 200.1.2.1
```

- 配置 MN 的策略

在 HA 上设置 MN 的属性。

```
[H3C] mobile-ip node 200.1.2.2  200.1.2.10 virtual-network 200.1.2.0 24
```

- 配置 MIP 的安全策略

在 HA 上设置 Host-MN 的安全联合。

```
[H3C] mobile-ip secure home-agent host 200.1.2.2  200.1.2.10 spi 123 key abc
```

在 HA 上设置 HA-FA1 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 210.1.1.1 spi 123 key abc
```

在 HA 上设置 HA-FA2 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 201.168.1.1 spi 123 key abc
```

(2) FA1 的配置过程如下：

- 配置 MIP 的总体策略

在 FA1 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

#在 FA1 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 MIP 的安全策略（注意，安全策略为可选配置）

在 FA1 上设置 FA1-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 200.1.2.2  200.1.2.10 spi 123 key
abc
```

在 FA1 上设置 FA1-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agent home-agent 200.1.1.1 spi 123 key abc
```

- 配置 FA 的策略

在 FA1 上启动 FA 功能，配置转交接口。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA1 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

在 FA1 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

在 FA1 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- 配置 MIP 的路由公告策略（注意：此项为可选配置）

在 FA1 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C-Ethernet0/0/1] mobile-ip irdp
```

(3) FA2 的配置过程如下：

- 配置 MIP 的总体策略

在 FA2 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 FA2 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 MIP 的安全策略（注意，安全策略为可选配置）

在 FA2 上设置 FA2-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 200.1.1.2  200.1.2.10 spi 123 key abc
```

在 FA2 上设置 FA2-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agnet home-agent 200.1.1.1 spi 123 key abc
```

- 配置 FA 的策略

在 FA2 上启动 FA 功能，配置转交接口。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA2 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C] interface Ethernet0/0/1
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

#在 FA2 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

在 FA2 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 38000
```

- 配置 MIP 的路由公告策略（注意：此项为可选配置）

在 FA2 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C-Ethernet0/0/1] mobile-ip irdp
```

18.10.3 移动路由器的典型组网 1（MR 使用的外地代理转交地址）

1. 组网需求

网络上有四台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，两台开启 FA 功能，另一台开启 MR 功能。开启 MR 功能的路由器可以在 FA1 和 FA2 之间进行漫游，并且使用固定的 IP 地址 1.1.1.3 与网络上的其他设备进行通信。MR 使用外地代理转交地址与网络上的通信对端 CN 进行通信。

2. 组网图

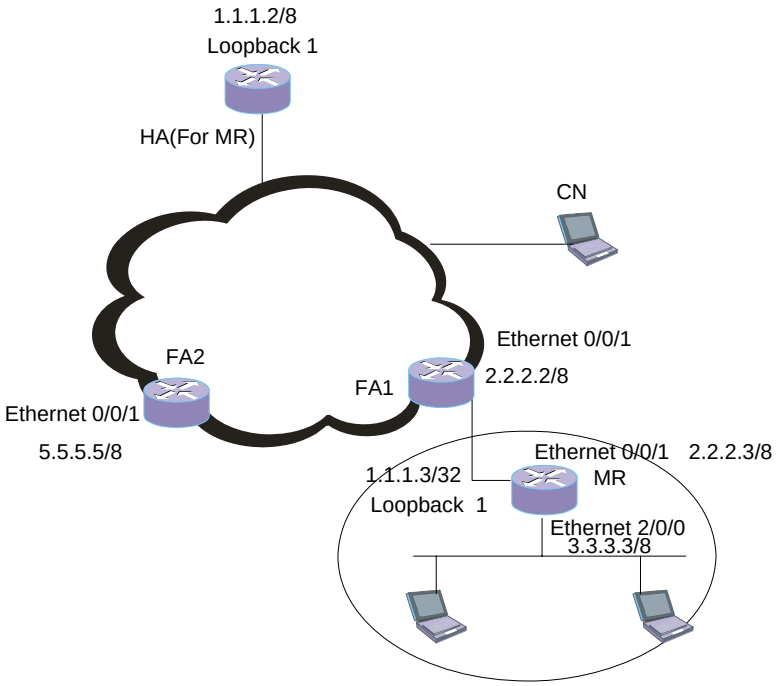


图18-6 移动路由器的典型组网 1（MR 使用的外地代理转交地址）

3. 配置步骤

(1) HA 的配置过程如下：

- 配置 MIP 的总体策略

在 HA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 HA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 HA 的策略

在 HA 上启动 HA 功能，指定虚拟网络的 HA 地址。

```
[H3C] mobile-ip home-agent
```

在 HA 上配置虚拟网络

```
[H3C] mobile-ip virtual-network 1.0.0.0 255.0.0.0
```

在 HA 上定义逻辑接口并为该接口配置 IP 地址。

```
[H3C] interface loopback 0
[H3C-loopback0] ip address 1.1.1.2 255.255.255.255
```

为虚拟网络指明其 HA 的地址为已经配置的环回地址。

```
[H3C-loopback0] quit
[H3C] mobile-ip virtual-network 1.0.0.0 8 ha-address 1.1.1.2
```

- 配置 MN 的策略

在 HA 上设置 MN 的属性。

```
[H3C] mobile-ip node 1.1.1.3 virtual-network 1.0.0.0 255.0.0.0
```

- 配置 HA 上的移动路由器及该移动路由器对应的移动网络。

```
[H3C] mobile-ip home-agent mobile-router 1
[H3C-HA-MobileRouter1] ip address 1.1.1.3
[H3C-HA-MobileRouter1] mobile-network 3.0.0.0 255.0.0.0
[H3C-HA-MobileRouter1] quit
```

- 配置 MIP 的安全策略

在 HA 上设置 Host-MN 的安全联合。

```
[H3C] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

在 HA 上设置 HA-FA1 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 2.2.2.2 spi 123 key abc
```

在 HA 上设置 HA-FA2 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 5.5.5.5 spi 123 key abc
```

(2) FA1 的配置过程如下：

- 配置 MIP 的总体策略

在 FA1 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 FA1 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 MIP 的安全策略（注意，安全策略为可选配置）

在 FA1 上设置 FA1-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

在 FA1 上设置 FA1-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- 配置 FA 的策略

在 FA1 上启动 FA 功能，配置转交接口。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA1 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C] interface Ethernet0/0/1
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

在 FA1 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

在 FA1 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- 配置 MIP 的路由公告策略（注意：此项为可选配置）

在 FA1 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C-Ethernet0/0/1] mobile-ip irdp
```

(3) FA2 的配置过程如下：

- 配置 MIP 的总体策略

在 FA2 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

#在 FA2 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 MIP 的安全策略（注意，安全策略为可选配置）

在 FA2 上设置 FA2-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

在 FA2 上设置 FA2-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- 配置 FA 的策略

在 FA2 上启动 FA 功能，配置转交接口。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA2 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

在 FA2 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

#在 FA2 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- 配置 MIP 的路由公告策略（注意：此项为可选配置）

在 FA2 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C-Ethernet0/0/1] mobile-ip irdp
```

(4) MR 的配置过程如下：

在 MR 上启动 MIP 功能。

```
<H3C> system-view
[H3C] mobile-ip
```

在 MR 上启动 MR 功能。

```
[H3C] mobile-ip mobile-router
```

在 MR 上配置 MR 的家乡地址。

```
[H3C-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

在 MR 上配置 MR 的家乡代理。

```
[H3C-MobileRouter] home-agent ip-address 1.1.1.2
```

在 MR 上配置移动网络。

```
[H3C-MobileRouter] mobile-network ethernet 2/0/0
```

或者

```
[H3C-MobileRouter] mobile-network 3.0.0.0 255.0.0.0
```

在 loopback 口下配置 IP 地址，该 IP 地址为移动路由器的家乡地址。

```
[H3C-MobileRouter] quit
[H3C] interface loopback 1
[H3C-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

配置漫游功能。

```
[H3C-LoopBack1] quit
[H3C] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] ip address 2.2.2.3 255.0.0.0
[H3C-Ethernet0/0/1] mobile-ip mobile-router roam
```

配置代理请求参数（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip mobile-router solicit interval 30
```

配置 MR 与 HA 的安全联合。

```
[H3C-Ethernet0/0/1] quit
[H3C] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

配置 MR 与 FA1 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure mobile-router foreign-agent 2.2.2.2 spi 123 key abc
```

配置 MR 与 FA2 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure mobile-router foreign-agent 5.5.5.5 spi 123 key abc
```

18.10.4 移动路由器的典型组网 2（MR 使用配置转交地址）

1. 组网需求

在网络上设置四台 AR46 路由器，都开启 MIP 功能，其中一台开启 HA 功能，一台开启 FA 功能，一台开启 MR 功能，一台作为普通路由器。开启 MR 功能的路由器

可以在 FA1 和普通路由器之间进行漫游，并且使用固定的 IP 地址 1.1.1.3 与网络上的其他设备进行通信。当 MR 进行漫游时，使用通过 DHCP 获取的配置转交地址与网络上的通信对端 CN 进行通信。

2. 组网图

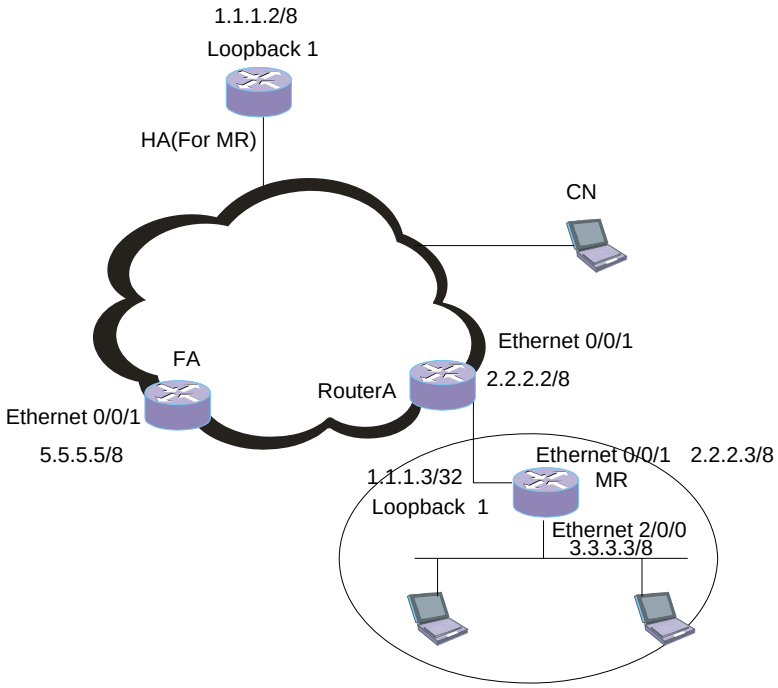


图18-7 移动路由器组网图 2（MR 使用配置转交地址）

3. 配置步骤

(1) HA 的配置过程如下：

- 配置 MIP 的总体策略

在 HA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 HA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 HA 的策略

在 HA 上启动 HA 功能，指定虚拟网络的 HA 地址。

```
[H3C] mobile-ip home-agent
```

在 HA 上配置虚拟网络

```
[H3C] mobile-ip virtual-network 1.0.0.0 255.0.0.0
```

在 HA 上定义逻辑接口并为该接口配置 IP 地址。

```
[H3C] interface loopback 0
[H3C-loopback0] ip address 1.1.1.2 255.255.255.255
```

#为虚拟网络指明其 HA 的地址为已经配置的环回地址。

```
[H3C-loopback0] quit
[H3C] mobile-ip virtual-network 1.0.0.0 8 ha-address 1.1.1.2
```

- 配置 MN 的策略

在 HA 上设置 MN 的属性。

```
[H3C] mobile-ip node 1.1.1.3 virtual-network 1.0.0.0 255.0.0.0
```

- 配置 HA 上的移动路由器及该移动路由器对应的移动网络。

```
[H3C] mobile-ip home-agent mobile-router 1
[H3C-HA-MobileRouter1] ip address 1.1.1.3
[H3C-HA-MobileRouter1] mobile-network 3.0.0.0 255.0.0.0
```

- 配置 MIP 的安全策略

在 HA 上设置 Host-MN 的安全联合。

```
[H3C] mobile-ip secure home-agent host 1.1.1.3 spi 123 key abc
```

在 HA 上设置 HA-FA 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure home-agent foreign-agent 5.5.5.5 spi 123 key abc
```

(2) RouterA 的配置过程如下：

设置 DHCP 服务端的 IP 地址池及网关。

```
<H3C> system-view
[H3C] dhcp server ip-pool abc
[H3C-abc] network 2.0.0.0 mask 255.0.0.0
[H3C-abc] gateway-list 2.2.2.2
```

配置接口 Ethernet0/0/1 的 IP 地址。

```
[H3C-Ethernet0/0/1] ip address 2.2.2.2 255.0.0.0
```

(3) FA 的配置过程如下：

- 配置 MIP 的总体策略

在 FA 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 FA 上设置 PMTU 的更新策略（此项为可选配置）

```
[H3C]mobile-ip tunnel path-mtu-discovery
```

- 配置 MIP 的安全策略（注意，安全策略为可选配置）

在 FA 上设置 FA-Visitor 的安全联合。

```
[H3C] mobile-ip secure foreign-agent visitor 1.1.1.3 spi 123 key abc
```

在 FA 上设置 FA-HA 的安全联合。

```
[H3C] mobile-ip secure foreign-agent home-agent 1.1.1.2 spi 123 key abc
```

- 配置 FA 的策略

在 FA 上启动外地代理的功能，配置转交接口。

```
[H3C] mobile-ip foreign-agent care-of ethernet 0/0/1
```

在 FA 的 Ethernet 0/0/1 接口上启动 FA 服务。

```
[H3C-Ethernet0/0/1] mobile-ip foreign-agent service
```

#在 FA 的 Ethernet 0/0/1 接口上启动前缀扩展（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip prefix-length
```

#在 FA 的 Ethernet 0/0/1 接口上设置注册生存时间（此项为可选配置）。

```
[H3C-Ethernet0/0/1] mobile-ip registration-lifetime 1600
```

- 配置 MIP 的路由公告策略（注意：此项为可选配置）

在 FA 的 Ethernet 0/0/1 接口上启动路由公告。

```
[H3C] ethernet 0/0/1
[H3C-Ethernet0/0/1] mobile-ip irdp
```

在 FA 上启动 DHCP 服务，设置 DHCP 服务端的 IP 地址池及网关。

```
[H3C] dhcp ser ip-pool abc
[H3C-abc] network 5.0.0.0 mask 255.0.0.0
[H3C-abc] gateway-list 5.5.5.5
```

(4) MR 的配置过程如下：

在 MR 上启动 MIP 功能

```
<H3C> system-view
[H3C] mobile-ip
```

在 MR 上启动 MR 功能

```
[H3C] mobile-ip mobile-router
```

在 MR 上配置 MR 的家乡地址

```
[H3C-MobileRouter] ip address 1.1.1.3 255.0.0.0
```

在 MR 上配置 MR 的家乡代理

```
[H3C-MobileRouter] home-agent ip-address 1.1.1.2
```

在 loopback 口下配置 IP 地址，该 IP 地址为移动路由器的家乡地址。

```
[H3C-MobileRouter] quit
[H3C] interface loopback 1
[H3C-LoopBack1] ip address 1.1.1.3 255.255.255.255
```

配置漫游功能

```
[H3C-Ethernet0/0/0] ip address dhcp-alloc
[H3C-Ethernet0/0/0] mobile-ip mobile-router roam
```

配置代理请求参数（此项为可选配置）。

```
[H3C-Ethernet0/0/0] mobile-ip mobile-router solicit interval 30
```

配置 MR 与 HA 的安全联合

```
[H3C] mobile-ip secure mobile-router home-agent 1.1.1.2 spi 123 key abc
```

配置 MR 与 FA 的安全联合（此项为可选配置）。

```
[H3C] mobile-ip secure mobile-router foreign-agent 5.5.5.5 spi 123 key abc
```