目 录

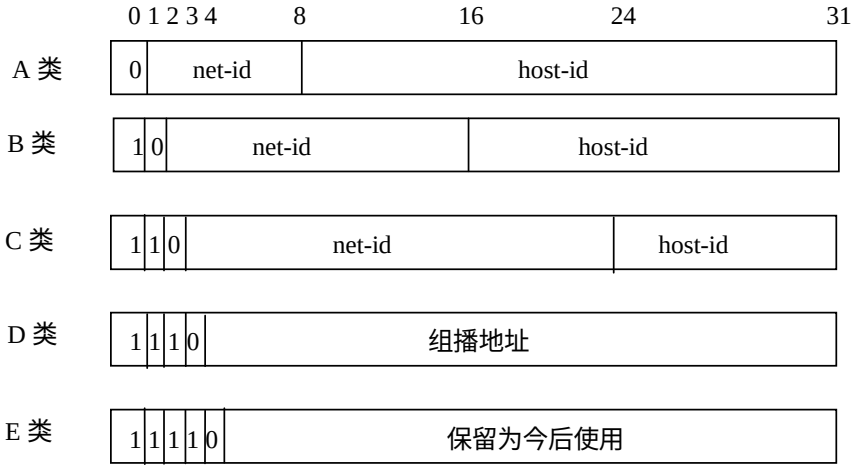
第1章 IP 地址配置

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	用户可用的 IP 网络范围	说明
A	0.0.0.0～ 127.255.255.255	1.0.0.0～ 126.0.0.0	全 0 的主机号码表示网络地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播； IP 地址 0.0.0.0 用于启动后不再使用的主机； 网络号码为 0 的 IP 地址表示当前网络，可以让机器引用自己的网络而不必知道其网络号； 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	128.0.0.0～ 191.254.0.0	全 0 的主机号码表示网络地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播。
C	192.0.0.0～ 223.255.255.255	192.0.0.0～ 223.255.254.0	全 0 的主机号码表示网络地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播。
D	224.0.0.0～ 239.255.255.255	无	D 类地址是一种组播地址。
E	240.0.0.0～ 247.255.255.255	无	保留今后使用。
其它地址	255.255.255.255	255.255.255.255	255.255.255.255 用于局域网广播地址。

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，子网的划分纯属本单位内部的事，在本单位以外是看不见划分的操作。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。

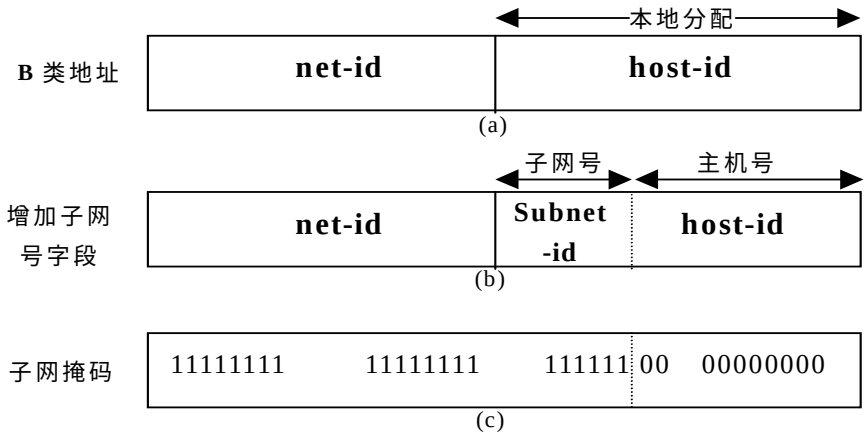


图1-2 IP 地址子网划分

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。

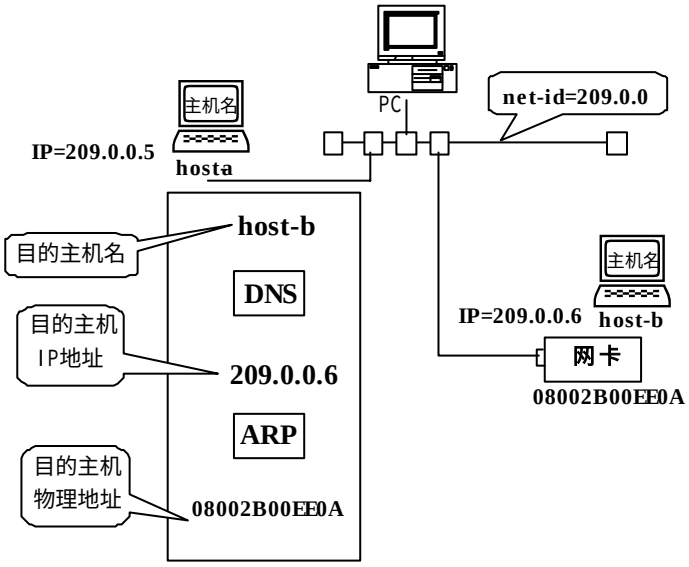


图1-3 主机名、IP 地址和物理地址之间的关系

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。

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（在本端路由器上配置 **ip address ppp-negotiate** 命令，在对端路由器上配置 **remote address** 命令），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**
配置为对端接口分配 IP 地址	**remote address** { *ip-address* | **pool** [*pool-number*] }
取消为对端接口分配 IP 地址	**undo remote address**

系统缺省为不允许接口 IP 地址的协商。

⚠ 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 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。

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 以及 Tunnel 的串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，在所有视图下执行 **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 IP 接口信息	**display ip interface** [*interface-type interface-number*]
显示 IP 接口摘要信息	**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，在所有视图下执行 **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*]]
显示路由器当前生效的配置参数	**display current-configuration**

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

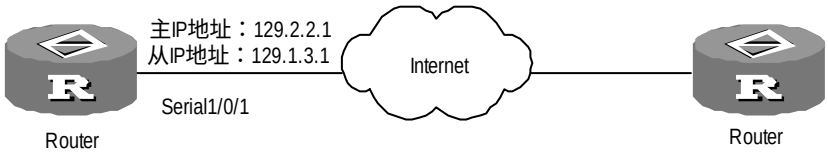


图1-4 为路由器接口配置主从 IP 地址

3. 配置步骤

配置路由器串口 Serial0/1 的主从 IP 地址。

```
[Quidway] interface serial 1/0/1
[Quidway-Serial1/0/1] ip address 129.2.2.1 255.255.255.0
[Quidway-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

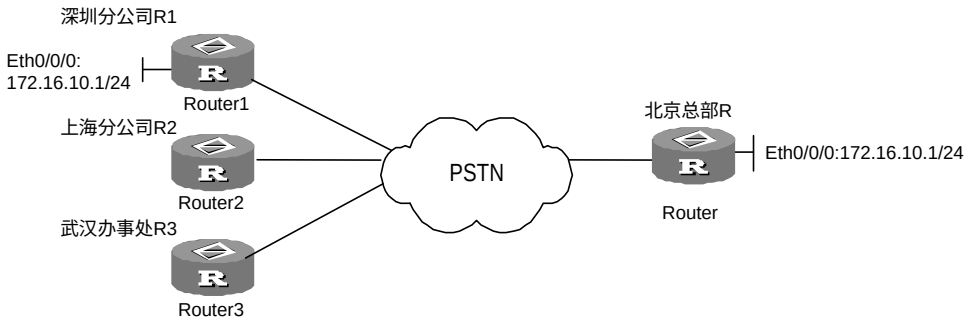


图1-5 某公司的网络拓扑图

3. 配置步骤

(1) 配置总部路由器 R

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

借用以太网的 IP 地址。

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

配置到深圳路由器 R1 以太网网段的路由。

```
[Quidway] 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。

```
[Quidway] 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

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

借用以太网的 IP 地址。

```
[Quidway-Serial2/0/0] ip address unnumbered ethernet 1/0/0
[Quidway-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：

```
[Quidway] 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。

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

4. 配置说明

上述配置只包含了与借用 IP 地址相关的配置。这里需要提请注意的是对于接口借用 IP 地址后路由的配置步骤。

在北京总部的路由器 R 上必须配置两条静态路由才能访问到深圳路由器 R1 的以太网上的主机。

第一条静态路由是到 R1 的以太网段的网段路由：下一跳为 R1 的串口的 IP 地址（或是借用的 IP 地址）。

ip route-static 172.16.20.0 255.255.255.0 172.16.20.1

第二条静态路由是到 R1 串口的接口路由，下一跳是 R 的串口。

ip route-static 172.16.20.1 255.255.255.255 serial0/0/0

加上这两条路由后，R 就能把访问 R1 以太网段的 IP 报文正确地转发给 R1。

同样，在 R1 上也要配置两条静态路由才能正确地访问到 R 的以太网网段。第一条静态路由是到 R 的以太网段的网段路由：下一跳为 R 的串口的 IP 地址（或是借用的 IP 地址）。

ip route-static 0.0.0.0 0.0.0.0 172.16.10.1

第二条静态路由是到 R 串口的接口路由，下一跳是 R1 的串口。

ip route-static 172.16.10.1 255.255.255.255 serial0/0

R2、R3 参照 R1 的配置即可。

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 IP 应用配置

2.1 地址解析协议（ARP）的配置

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 VRP 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 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。

2.1.5 ARP 显示和调试

在完成上述配置后，在所有视图下执行 **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。

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 ARP 进行调试。

表2-4 ARP 显示和调试

操作	命令
显示 ARP 映射表	**display arp** [**static** | **dynamic** | **all**]
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

请在以太网接口视图下进行下面配置。

表2-5 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 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 域名解析（DNS）的配置

2.4.1 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。

2.4.2 静态域名解析的配置

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2-6 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。

2.4.3 域名解析表显示和调试

表2-7 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**

2.5 DNS client 配置

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）。实际上，绝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，就向名字服务器发送查询报文，收到响应后再解析名字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。

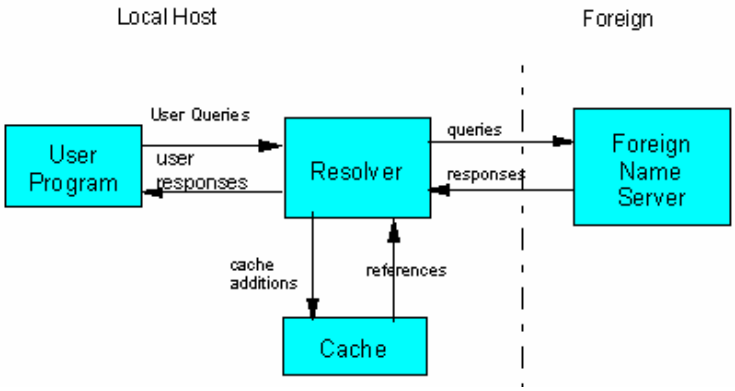


图2-1 DNS 系统组成框图

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（域名服务器端端口号为 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）。

2.5.1 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2-8 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2-9 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*]

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, huawei.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2-10 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 server** [*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。

2.5.2 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2-11 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**]
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2-12 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2-13 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。

2.5.3 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

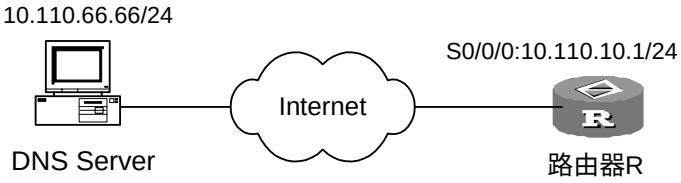


图2-2 使用 DNS Client 典型组网

3. 配置步骤

(1) 路由器配置

启动 DNS 域名解析功能。

```
[Router] dns resolve
```

配置 DNS 服务器 IP 地址。

```
[Router] dns server 10.110.66.66
```

配置 S0/0/0 的 IP 地址。

```
[Router] interface s 0/0/0
[Router-s0/0/0] ip address 10.110.10.1 255.255.255.0
```

配置到 DNS 服务器的静态路由。

```
[Router] ip route-static 10.110.66.66 s0/0/0
```

2.5.4 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。

2.6 URPF 配置

2.6.1 URPF 简介

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，甚至是以 root 权限来访问。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。

URPF 的处理流程如下：

(1) 如果报文的源地址在路由器的 FIB 表中存在

- 对于 **strict** 型检查，反向查找报文出接口，若其中至少有一个出接口和报文的入接口相匹配，则报文通过检查；否则报文将被 URPF 丢弃。
- 对于 **loose** 型检查，只要报文的源地址在路由器的 FIB 表中存在，报文就通过检查。

(2) 如果报文的源地址在路由器的 FIB 表中不存在，则检查缺省路由及 **allow-default** 参数

📖 说明：
缺省路由指收到报文的路由器上配置的缺省路由。

- 对于配置了缺省路由，但没有配置参数 **allow-default** 的情况，不管是 **strict** 型检查还是 **loose** 型检查，只要报文的源地址在路由器的 FIB 表中不存在，URPF 都将报文丢弃；
- 对于配置了缺省路由，同时又配置了参数 **allow-default** 的情况下，如果是 **strict** 检查，只要缺省路由的出接口与报文的入接口一致，则报文将通过 URPF 的检查，进行正常的转发；如果缺省路由的出接口和报文的入接口不一致，则报文将被 URPF 丢弃。如果是 **loose** 型检查，报文都将通过 URPF 的检查，进行正常的转发。

最后，当且仅当报文被 URPF 拒绝后，才去匹配 ACL 列表。如果被 ACL 允许通过，则报文继续进行正常的转发；如果被 ACL 拒绝，则报文被丢弃。

2.6.2 URPF 配置

请在接口视图下进行下列配置。

表2-14 使能或关闭 URPF 检查

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

缺省为关闭 URPF 检查。

2.6.3 URPF 的显示与调试

请在用户视图下进行下列配置。

表2-15 显示 URPF 的丢包情况

操作	命令
显示 URPF 的丢包情况	**debugging ip urpf discards** [**interface** *interface-type interface-num*]
禁止显示 URPF 的丢包情况	**undo debugging ip urpf discards** [**interface** *interface-type interface-num*]

第3章 UDP HELPER 配置

3.1 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，主要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。

3.2 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

3.2.1 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3-1 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。

3.2.2 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3-2 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3-3 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。

3.2.3 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3-4 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。

3.3 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3-5 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4章 BOOTP 客户端配置

4.1 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，报文最多能重传三次，重传三次之后还不成功就不再重传报文。

4.2 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

4.2.1 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4-1 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。

第5章 DHCP 配置

5.1 DHCP 简介

5.1.1 DHCP

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。

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。绝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。

5.1.2 DHCP 服务器

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。

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：

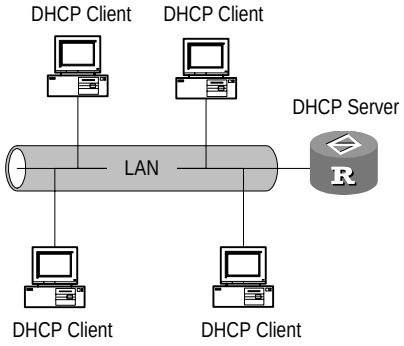


图5-1 DHCP 服务器典型组网应用

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。
- 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

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。

5.1.3 DHCP 中继

1. DHCP 中继的应用环境

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。

2. DHCP 中继的基本原理

下图是 DHCP 中继的典型应用示意图。

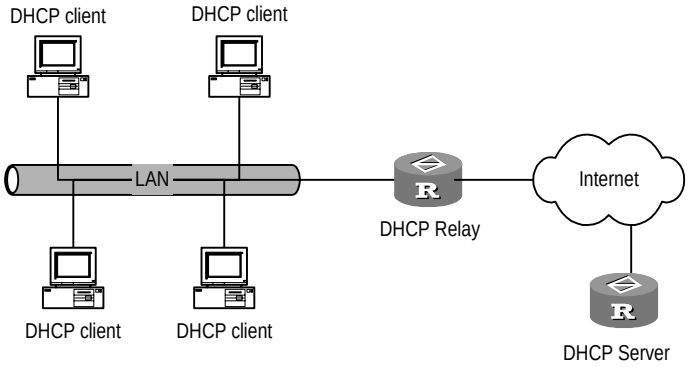


图5-2 DHCP 中继的典型组网应用

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。

可以认为 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。

5.2 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

5.2.1 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5-1 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。

5.2.2 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5-2 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。

5.3 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
- 配置 DHCP 数据保存到硬盘
- 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。

5.3.1 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）视图下进行下列配置。

表5-3 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**
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5-4 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** { **interface** *ethernet-subinterface-range* | **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** *ethernet-subinterface-range* | **all** }
恢复缺省设置	**undo dhcp select** { **interface** *ethernet-subinterface-range* | **all** }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。

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**。

5.3.2 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 服务器根据一定的算法选择合适的地址池，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，VRP 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5-5 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。

5.3.3 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 地址与某个 IP 地址绑定。当此 MAC 地址的客户端申请 DHCP 地址时，服务器根据客户端 MAC 地址寻找到对应的固定 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5-6 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	**static-bind mac-address** *mac-address*

操作	命令
删除静态绑定的客户端 MAC 地址	**undo static-bind mac-address**

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

📖 说明：

命令 **static-bind ip-address** 和 **static-bind mac-address** 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。

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5-7 配置接口地址池的静态地址绑定

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

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5-8 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。

5.3.4 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5-9 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。而在使用 **undo dhcp server forbidden-ip** 命令删除设置时，必须确保参数与原先配置的完全相同，即，不能仅删除原先配置的部分地址。

5.3.5 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5-10 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5-11 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5-12 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** *ethernet-subinterface-range* | **all** }
恢复缺省的 IP 地址租用有效期限	**undo dhcp server expired** { **interface** *ethernet-subinterface-range* | **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。

5.3.6 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5-13 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5-14 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5-15 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** *ethernet-subinterface-range* | **all** }
删除分配给 DHCP 客户端的域名	**undo dhcp server domain-name** *domain-name* { **interface** *ethernet-subinterface-range* | **all** }

缺省情况下，未配置分给 DHCP 客户端的域名。

5.3.7 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5-16 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5-17 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5-18 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** *ethernet-subinterface-range* | **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** *ethernet-subinterface-range* | **all** }

缺省情况下，未配置 DNS 服务器的 IP 地址。

5.3.8 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5-19 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5-20 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5-21 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** *ethernet-subinterface-range* | **all** }
删除 DHCP 客户端的 NetBIOS 服务器地址	**undo dhcp server nbns-list** { *ip-address* | **all** } { **interface** *ethernet-subinterface-range* | **all** }

缺省情况下，未配置 NetBIOS 服务器的 IP 地址。

5.3.9 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5-22 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5-23 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** }
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5-24 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** *ethernet-subinterface-range* | **all** }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	**undo dhcp server netbios-type** { **interface** *ethernet-subinterface-range* | **all** }

缺省情况下，客户端采用 h 类节点（**h-node**）。

5.3.10 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5-25 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5-26 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5-27 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** *ethernet-subinterface-range* | **all** }
删除 DHCP 自定义选项	**undo dhcp server option** *code* { **interface** *ethernet-subinterface-range* | **all** }

5.3.11 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5-28 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。

5.3.12 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5-29 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。

5.3.13 清除 DHCP 相关信息

在所有视图下执行 **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。

在所有视图下执行 **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。

在所有视图下执行 **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5-30 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**

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。

5.4 DHCP 客户端配置

5.4.1 DHCP 客户端简介

1. DHCP 介绍

(1) DHCP 的发展背景

随着网络规模的不断扩大、网络复杂度的不断提高，网络配置也变得越来越复杂，在计算机经常移动（如便携机或无线网络）和计算机的数量超过可分配的 IP 地址等情况下，原有针对静态主机配置的 BOOTP（Bootstrap Protocol）已经越来越不能满足实际需求。为方便用户快速地接入和退出网络、提高 IP 地址资源的利用率以及支持无盘网络工作站等应用，在 BOOTP 基础上，制定了动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）。

(2) DHCP 的应用场合

在以下场合通常利用 DHCP 服务来完成 IP 地址分配：

- 网络规模相对较大，手工配置需要很大的工作量，同时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 地址的数量，即无法给每个主机都分配一个固定的 IP 地址。比如，Internet 接入服务商即属于这种情况，大量用户必须通过 DHCP 服务动态获得自己的 IP 地址，而且并发用户的个数也有一定的限制。
- 网络中具有固定 IP 地址的主机比较少（比如各种服务器主机需要有固定的 IP 地址），而大部分主机没有固定的 IP 地址需求。

2. DHCP 客户端的基本原理

在典型的 DHCP 应用网络中，一般包含一台 DHCP 服务器和很多的客户端（如 PC 和便携机等），如下图所示：

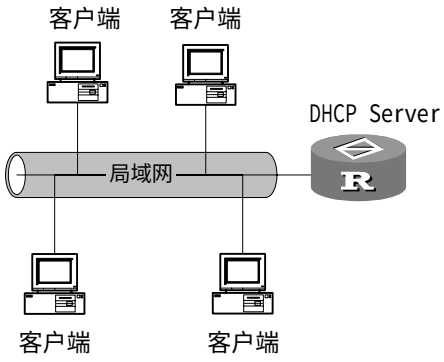


图5-3 DHCP 服务器典型组网应用

DHCP 客户端实际上是一接口级的概念，一主机若包含多个以太网接口，则该主机的每一以太网接口都可以配置成一独立的 DHCP 客户端。

路由器上实现的DHCP客户端特性,比主机上实现的DHCP客户端特性要简单一些。

为了获取并使用一个合法的动态 IP 地址，在不同的阶段，DHCP 客户端需要与服务器之间交互不同的信息，两者的交互包括以下几个过程：

(1) 地址分配过程

当 DHCP 客户端第一次登录网络时，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。DHCP 客户端以广播方式发送 DHCPDISCOVER 报文来寻找 DHCP 服务器，网络中每台安装了 TCP/IP 协议组件的主机都会接收到这种广播信息，但只有 DHCP 服务器才会作出响应。

- 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 DHCPDISCOVER 报文，从 IP 地址池中挑选一个尚未分配的 IP 地址分配给 DHCP 客户端，向该 DHCP 客户端发送包含出租 IP 地址和其它设置的 DHCPOFFER 报文。
- 选择阶段，即 DHCP 客户端选择某台 DHCP 服务器提供的 IP 地址的阶段。如果有多台 DHCP 服务器向该 DHCP 客户端发来 DHCPOFFER 报文，则 DHCP 客户端只接受第一个收到的 DHCPOFFER 报文，然后以广播方式向各 DHCP 服务器回应 DHCPREQUEST 报文，该信息中包含向所选定的 DHCP 服务器请求 IP 地址的内容。
- 确认阶段，即 DHCP 服务器确认所提供的 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户端回答的 DHCPREQUEST 报文之后，便向 DHCP 客户端发送包含它所提供的 IP 地址和其它设置的 DHCPACK 确认报文，告诉 DHCP 客户端可以使用它所提供的 IP 地址。然后 DHCP 客户端便将其 TCP/IP 协议组件与网卡绑定。除 DHCP 客户端选中的服务器外，其它 DHCP 服务器都将把本次未分配出的 IP 地址用于其他客户端的 IP 地址申请。

上述过程是完整的 DHCP 动态分配地址过程，路由器上的 DHCP 客户端特性完全遵照上述过程实现。

(2) 租约更新过程

DHCP 服务器向 DHCP 客户端分配的动态 IP 地址通常都有一定的租借有效期，期满后 DHCP 服务器会收回该 IP 地址。如果 DHCP 客户端想继续使用该地址，则需要更新 IP 租约（如延长 IP 地址租约）。

在实际使用中，DHCP 客户端在使用动态分配的 IP 地址 T1 时间（为更新定时器时长，取决于服务器上的配置，缺省为租约的 1/2）、在租约超时前会主动发起租约更新，向服务器发送 DHCPREQUEST，服务器若同意该更新请求，则回应 DHCPACK，客户端收到该应答后则会使用新的租约。

路由器上实现的 DHCP 客户端支持上述租约自动更新过程。对于用户 PC 机（DHCP 客户端），除了上述自动更新过程外，还可以使用 **ipconfig /renew** 命令或在图形界面下执行［winipcfg / 更新］进行强制租约更新。

(3) 重新绑定过程

即使租约更新过程失败，DHCP 客户端仍然可以继续使用动态获取的地址，并可以通过重新绑定过程来延长租约。

若 DHCP 客户端更新失败，DHCP 客户端在继续使用动态分配的 IP 地址（T2 - T1）时间（T2 为重新绑定定时器时长，取决于服务器上的配置，缺省为租约的 7/8）后，将发起重新绑定过程，向服务器发送 DHCPREQUEST，服务器若同意该更新请求，则回应 DHCPACK，客户端收到该应答后则会使用新的租约。

上述几个过程在下面的 DHCP 客户端状态迁移图有完整体现：

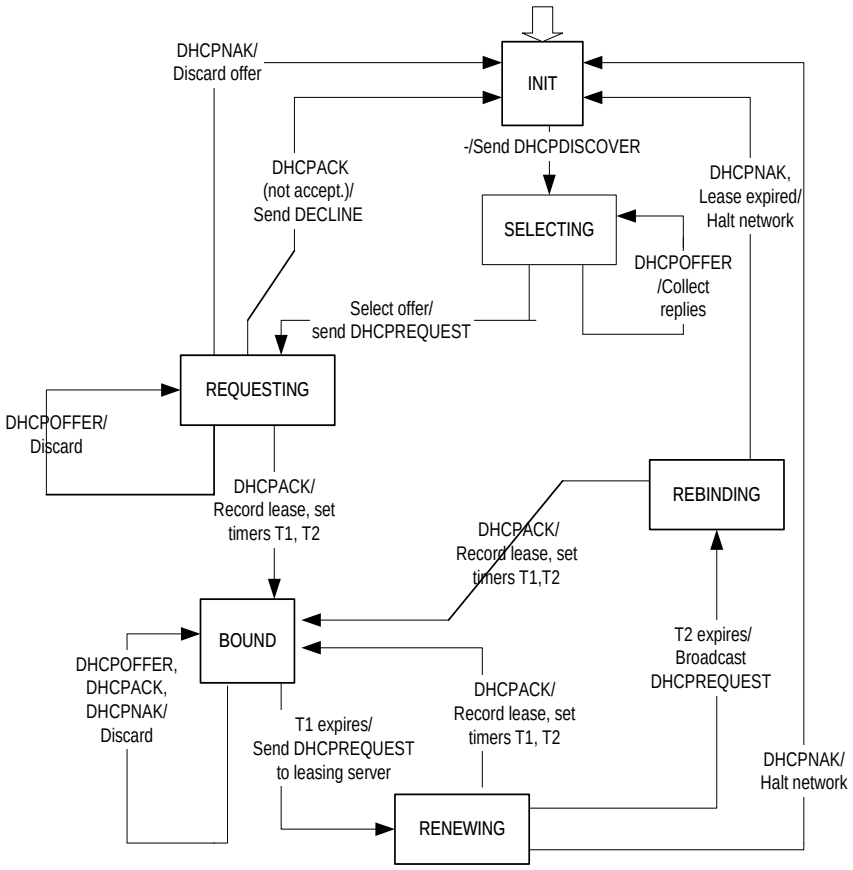


图5-4 DHCP 客户端状态迁移图

5.4.2 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：

- 配置以太网接口通过 DHCP 方式获取地址；

请在以太网接口（包括子接口）视图下进行下列配置。

表5-31 配置静态绑定的 IP 地址和 MAC 地址

操作	命令
启动 DHCP（Dynamic Host Configuration Protocol）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：

- 命令 **ip address dhcp-alloc** 与命令 **ip address** *ip-address* { *mask* | *mask-length* }不能同时配置在一个以太网接口下，两者只能取其一。
- 命令 **ip address dhcp-alloc** 不支持配置从地址。

5.5 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

5.5.1 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，请在接口视图下进行下列配置。

表5-32 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5-33 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** *ethernet-subinterface-range* | **all** }
恢复缺省设置	**undo dhcp select** { **interface** *ethernet-subinterface-range* | **all** }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。

📖 说明：

以太网子接口支持 DHCP Relay 时，只能是子接口对子接口，也就是说客户端也必须使用子接口（此时如果是 PC 作为客户端则无法得到 IP 地址）。

5.5.2 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 广播报文又被送到指定的外部 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5-34 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5-35 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** *ethernet-subinterface-range* | **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** *ethernet-subinterface-range* | **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 20 个外部 DHCP 服务器地址。

5.5.3 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5-36 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。

5.5.4 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5-37 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。

5.5.5 清除 DHCP 中继的统计信息

在所有视图下执行 **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5-38 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**

5.6 DHCP 显示和调试

在完成上述配置后，可在所有视图下执行 **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5-39 DHCP 服务器的显示和调试

操作	命令
查看 DHCP 地址池的可用地址信息	**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 数据库的存放路径和文件信息	**display dhcp server database**
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** }
打开 DHCP 服务器的调试开关	**debugging dhcp server { error | events | packets }**
关闭 DHCP 服务器的调试开关	**undo debugging dhcp server { events | packets | error }**
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5-40 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** *internace-name* | **all**]
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5-41 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**}
关闭 DHCP 客户端的调试开关	**undo debugging dhcp client { error| event | packet | all}**

5.7 DHCP 典型配置举例

5.7.1 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 huawei.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

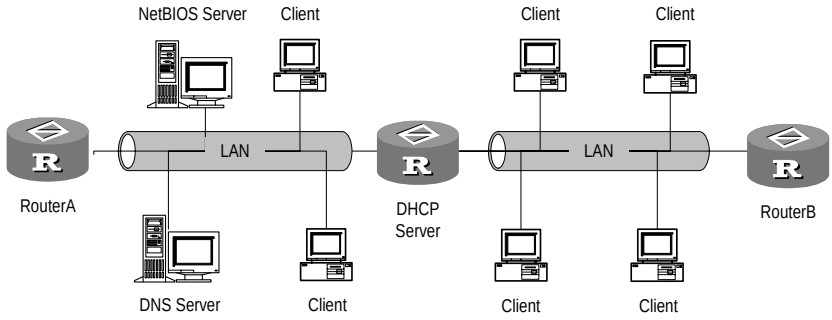


图5-5 DHCP 服务器与客户端在同一网络中

3. 配置步骤

启动 DHCP 服务。

```
[Quidway] dhcp enable
```

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

```
[Quidway] dhcp server forbidden-ip 10.1.1.2
[Quidway] dhcp server forbidden-ip 10.1.1.4
[Quidway] dhcp server forbidden-ip 10.1.1.126
[Quidway] 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）。

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

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）。

```
[Quidway] dhcp server ip-pool 1
[Quidway-dhcp-1] network 10.1.1.0 mask 255.255.255.128
[Quidway-dhcp-1] domain-name huawei.com
[Quidway-dhcp-1] gateway-list 10.1.1.126
[Quidway-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）。

```
[Quidway] dhcp server ip-pool 2
[Quidway-dhcp-2] network 10.10.1.128 mask 255.255.255.128
[Quidway-dhcp-2] expired day 5
[Quidway-dhcp-2] nbns-list 10.1.1.4
[Quidway-dhcp-2] gateway-list 10.1.1.254
```

5.7.2 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

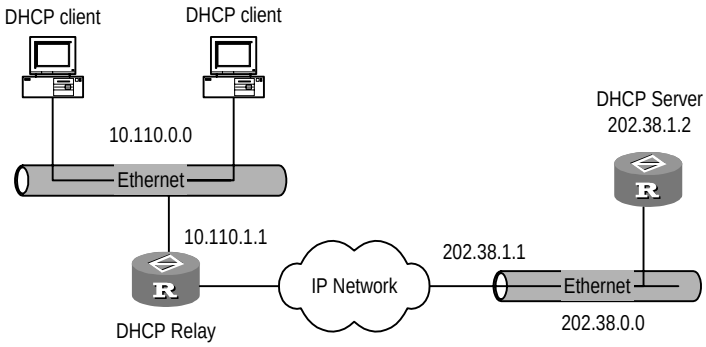


图5-6 DHCP 中继配置

3. 配置步骤

配置路由器：

使能 DHCP 服务

```
[Quidway] 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

```
[Quidway] interface ethernet 6/0/0
[Quidway-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

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

DHCP 服务器的配置略。

5.7.3 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 1760a 的上述两个以太口通过 DHCP 的方式获取地址。

(2) 组网图

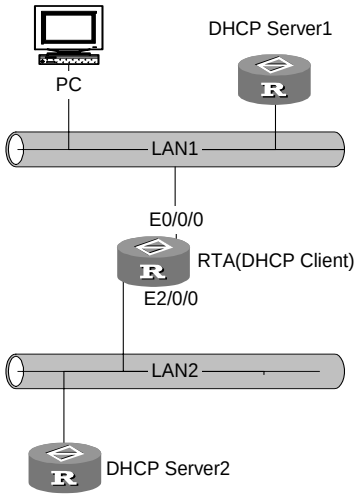


图5-7 主接口作 DHCP 客户端

(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。

```
[server1] dhcp enable
[server1] interface ethernet0/0
[server1-Ethernet0/0/0] ip address 169.254.0.1 16
[server1] dhcp server ip-pool 1
[server1-dhcp1] network 200.254.0.0 mask 255.255.0.0
```

配置 server2。

```
[server2] dhcp enable
[server2] interface ethernet0/0
[server2-Ethernet0/0/0] ip address 172.10.0.1 16
[server2] dhcp server ip-pool 2
[server2-dhcp2] network 172.10.0.0 mask 255.255.0.0
```

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

```
[client] interface ethernet0/0/0
[client-Ethernet0/0/0] ip address dhcp-alloc
```

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

```
[client] interface ethernet2/0/0
[client-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

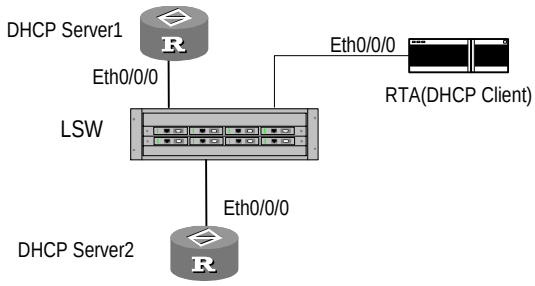


图5-8 子接口作 DHCP 客户端

(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

```
[client] interface ethernet0/0/0.1
[client-Ethernet0/0/0.1] vlan-type dot1q vid 10
[client-Ethernet0/0/0.1] ip addr dhcp-alloc
```

配置从 server1 获取地址的子接口

```
[client] interface ethernet0/0/0.2
[client-Ethernet0/0/0.2] vlan-type dot1q vid 20
[client-Ethernet0/0/0.2] ip addr dhcp-alloc
```

第6章 IP 性能配置

6.1 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6-1 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。

6.2 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6-2 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。

6.3 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6-3 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。

6.4 IP 性能显示和调试

在完成上述配置后，在所有视图下执行 **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6-4 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 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*]
过滤显示 FIB 信息	**display fib acl** *acl-number*

操作	命令
按照目的地址进行匹配显示 FIB 表项	**display fib** *dest-addr1* [*dest-mask2*] [**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 调试信息开关	**debugging ip packet**
打开 ICMP 调试信息开关	**debugging ip icmp**
打开 TCP 调试信息开关	**debugging tcp packet**
清除 IP 统计信息	**reset ip statistics**
打开 UDP 连接的调试信息	**debugging udp packet**
关闭 UDP 连接的调试信息	**undo debugging udp packet**
清除 TCP 流量统计信息	**reset tcp statistics**
显示系统当前所有的套接口信息	**display ip socket**
关闭 TCP 连接的调试开关	**undo debugging tcp packet**
打开 TCP 事件的调试开关	**debugging tcp event**
关闭 TCP 事件的调试开关	**undo debugging tcp event**
显示 UDP 流量统计信息	**display udp statistics**
清除 UDP 流量统计信息	**reset udp statistics**

6.5 快速转发配置

6.5.1 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，同时还为报文建立合适输出的 MAC 帧。建好后的 MAC 帧通过 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。

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、减少路由查找时间来提高 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。

VRP 实现的快速转发，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，提供快速转发的功能。
- 支持在配置了 ASPF 防火墙的情况下，提供快速转发的功能。
- 支持在配置了地址转换的情况下，提供快速转发的功能。
- 支持在配置了 GRE 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。

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，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。

6.5.2 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6-5 允许/禁止接口进行快速转发

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

缺省情况下，接口在入/出的双向上都使能快速转发。

⚠ 注意：

- 如果要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，该接口将不再发送 ICMP 重定向报文。
- 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，也就是说 **debugging ip packet** 不起作用了。

6.5.3 快速转发的显示和调试

表6-6 快速转发的显示和调试

操作	命令
显示快速转发表信息	**display ip fast-forwarding cache**
清除快速转发缓冲区中的内容	**reset ip fast-forwarding cache**

6.6 IP 性能配置排错

故障之一 :TCP 和 UDP 协议是建立在 IP 协议之上，保证 IP 可以提供数据报的传输，故障是 TCP 和 UDP 协议不能正常工作。

故障排除：这时，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：

```
[Quidway] info-center enable
[Quidway] quit
<Quidway> 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：

```
[Quidway] info-center enable
[Quidway] quit
<Quidway> 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7章 地址转换（NAT）的配置

7.1 地址转换（NAT）简介

7.1.1 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。

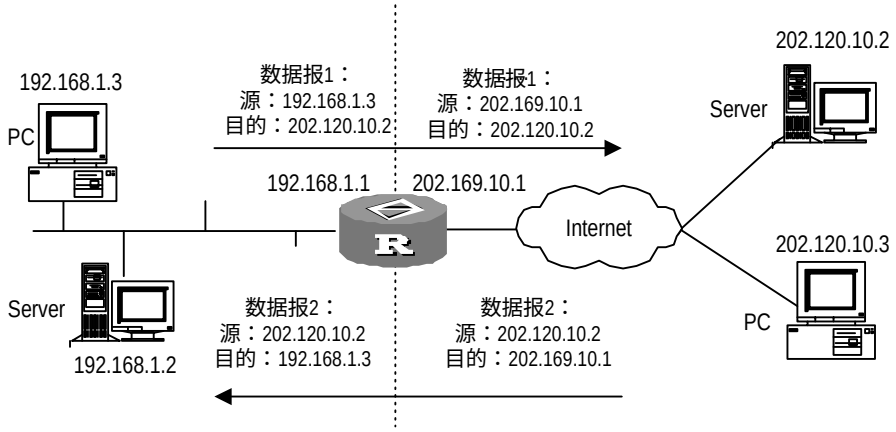


图7-1 地址转换的基本过程

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。

7.2 地址转换实现的功能

7.2.1 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。

Quidway 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。

7.2.2 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。

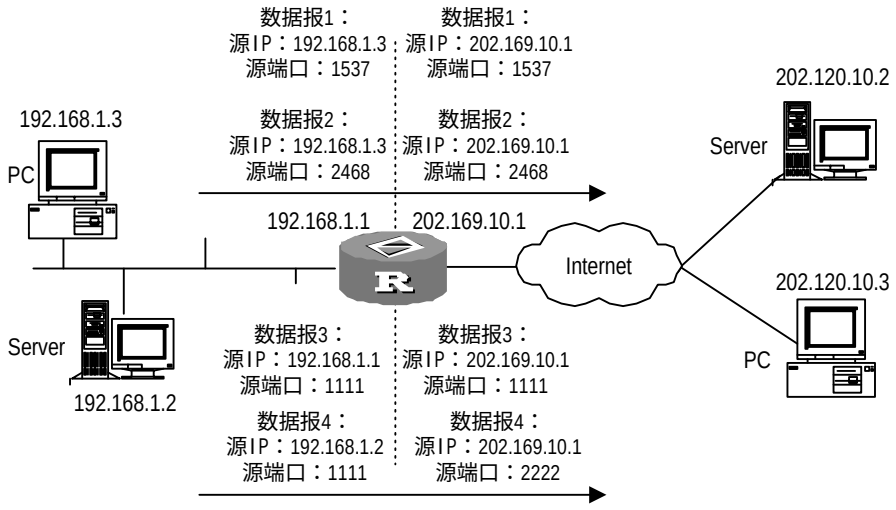


图7-2 NAPT 地址复用示意图

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。

7.2.3 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）。

Quidway 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。

7.2.4 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。

7.2.5 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 VRP 的 NAT ALG 支持 PPTP、DNS、FTP、ILS、NBT、SIP、H.323 等协议。

7.2.6 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，VRP 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。

VRP 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。

7.3 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）

7.3.1 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7-1 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。

7.3.2 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7-2 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*

当直接使用接口地址作为 NAT 转换后的公网地址时，若修改了接口地址应该首先使用 reset nat session 命令清除原 NAT 地址映射表项，然后再访问外部网络；否则就会出现原有 NAT 表项不能自动删除，也无法使用 **reset nat** 命令删除的情况。

2. 配置一对一地址转换

(1) 配置一对一地址转换

请在系统视图下进行下列配置。

表7-3 配置一对一地址转换

操作	命令
配置从内部地址到外部地址的一对一转换	**nat static** *ip-addr1 ip-addr2*
删除已经配置得 NAT 一对一转换	**undo nat static** *ip-addr1 ip-addr2*

(2) 使一对一转换在接口上生效

表7-4 使一对一转换在接口上生效

操作	命令
使已经配置的 NAT 一对一转换在接口上生效	**nat outbound static**

3. 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7-5 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**]

4. 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7-6 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*]

5. 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。

7.3.3 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。

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7-7 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*] **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* **inside** *host-addr1 host-addr2 host-port*
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*] **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* **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。

7.3.4 配置地址转换应用网关

请在系统视图下进行下面配置

表7-8 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** | **nbt** | **pptp** | **sip** }
禁用地址转换应用网关功能	**undo nat alg** { **dns** | **ftp** | **h323** | **ils** | **nbt** | **pptp** | **sip** }

缺省情况下，使能地址转换应用网关功能。

7.3.5 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7-9 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。

7.4 地址转换显示和调试

在完成上述配置后，在所有视图下执行 **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7-10 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*]}
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*] }
清除地址转换映射表	**reset nat**{ **log-entry** | **session slot** *slot-number* }

7.5 NAT 配置举例

7.5.1 典型 NAT 配置举例

1. 组网需求

如下图所示，一个公司通过 Quidway 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 Quidway 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

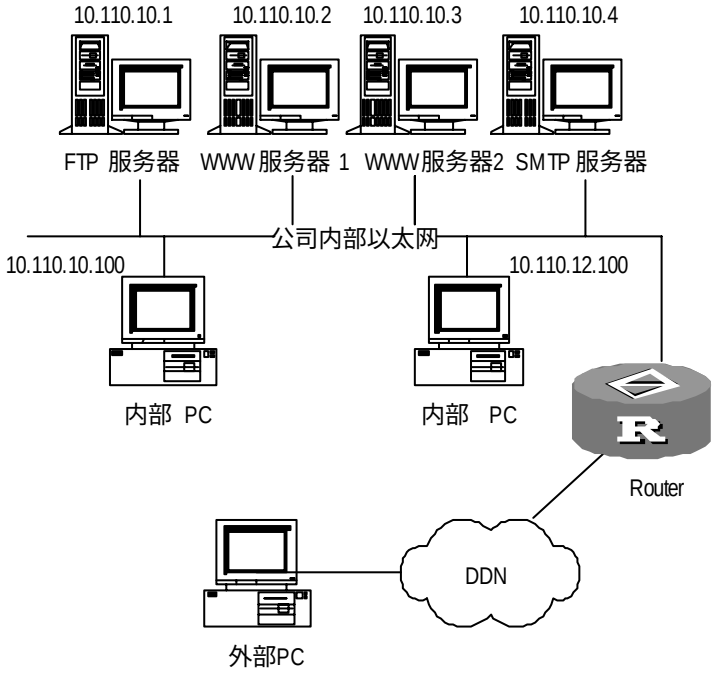


图7-3 地址转换配置案例组网图

3. 配置步骤

配置地址池和访问控制列表。

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

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

允许 10.110.10.0/24 网段地址转换。

```
[Quidway] interface Serial3/0/0
[Quidway-Serial3/0/0] nat outbound 2001 address-group 1
```

设置内部 ftp 服务器。

```
[Quidway-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。

```
[Quidway-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。

```
[Quidway-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。

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

7.5.2 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

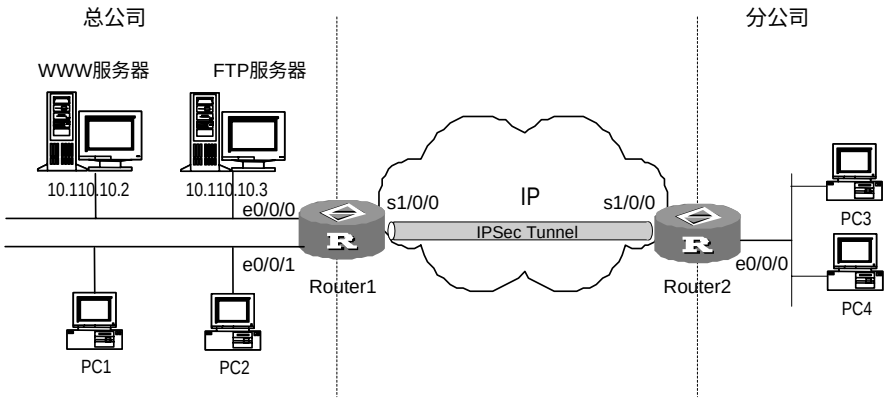


图7-4 内部服务器与 IPSec VPN 结合应用配置举例

3. 配置步骤

(1) 配置 Router1

配置以太网口 IP 地址。

```
[Quidway] interface ethernet 0/0/0
[Quidway-ethernet 0/0/0] ip address 10.110.10.1 255.255.255.0
[Quidway-ethernet 0/0/0] interface ethernet 0/0/1
[Quidway-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。

```
[Quidway] acl number 3001
[Quidway-acl-basic-3001] rule permit ip source 10.110.20.0 0.0.0.255
[Quidway-acl-basic-3001] rule permit ip source 10.110.30.0 0.0.0.255
[Quidway-acl-basic-3001] 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。

```
[Quidway-acl-basic-3001] acl number 3002
[Quidway-acl-basic-3002] rule permit ip source 10.110.10.0 0.0.0.255
[Quidway-acl-basic-3002] rule deny ip source 10.110.0.0 0.0.255.255
destination 10.110.30.0 0.0.0.255
[Quidway-acl-basic-3002] rule deny ip source any destination any
```

配置用于实现 IPSec 的访问控制列表。

```
[Quidway-acl-basic-3002] acl number 3003
[Quidway-acl-basic-3003] rule permit ip source 10.110.0.0 0.0.255.255
destination 10.110.30.0 0.0.0.255
[Quidway-acl-adv-3003] rule deny ip source any destination any
[Quidway-acl-adv-3003] quit
```

配置 Easy IP。

```
[Quidway] interface Serial1/0/0
```

```
[Quidway-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[Quidway-Serial1/0/0] nat outbound 3001
```

配置内部 ftp 及 www 内部服务器。

```
[Quidway-Serial1/0/0] nat server 3002 protocol tcp global 202.38.160.1 inside
10.110.10.3 ftp
[Quidway-Serial1/0/0] nat server 3002 protocol tcp global 202.38.160.1 inside
10.110.10.2 www
```

配置 IPSec。

```
[Quidway] ipsec proposal tran1
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
[Quidway-ipsec-proposal-tran1] transform esp
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
[Quidway-ipsec-proposal-tran1] quit
[Quidway] ipsec policy map1 10 manual
[Quidway-ipsec-policy-manual-map1-10] security acl 3003
[Quidway-ipsec-policy-manual-map1-10] proposal tran1
[Quidway-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
[Quidway-ipsec-policy-manual-map1-10] tunnel local 202.38.160.1
[Quidway-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[Quidway-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
[Quidway-ipsec-policy-manual-map1-10] sa string-key outbound esp
[Quidway-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[Quidway-ipsec-policy-manual-map1-10] quit
```

配置在串口上应用安全策略组。

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

配置到 Router2 以太网口的静态路由。

```
[Quidway] 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。

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

配置用于实现 IPSec 的访问控制列表。

```
[Quidway] acl number 3003
[Quidway-acl-basic-3003] rule permit ip source 10.110.30.0 0.0.0.255
destination 10.110.0.0 0.0.255.255
[Quidway-acl-adv-3003] rule deny ip source any destination any
```

配置 IPSec。

```
[Quidway] ipsec proposal tran1
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
[Quidway-ipsec-proposal-tran1] transform esp
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
[Quidway-ipsec-proposal-tran1] quit
[Quidway] ipsec policy use1 10 manual
[Quidway-ipsec-policyl-manual-use1-10] security acl 3003
[Quidway-ipsec-policyl-manual-use1-10] proposal tran1
[Quidway-ipsec-policyl-manual-use1-10] tunnel remote 202.38.160.1
[Quidway-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
[Quidway-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[Quidway-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
[Quidway-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[Quidway-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
[Quidway-ipsec-policyl-manual-use1-10] quit
```

配置串口地址并在串口上应用安全策略组。

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

配置到 Router1 以太网口的静态路由。

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

7.6 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8章 IP 单播策略路由配置

8.1 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。

目前为 **route-policy** 提供了两种 **if-match** 子句，分别为 **if-match packet-length** 和 **if-match acl**；有 5 种 **route-policy** 的 **apply** 子句：**apply ip-precedence**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**，5 个子句按配置顺序执行，直到不能继续为止。

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。

8.2 IP 单播策略路由的配置

IP 单播策略路由配置包括：

- 创建策略
- 定义 Route-policy 的 **if-match** 子句
- 定义 Route-policy 的 **apply** 子句
- 使能/禁止本地策略路由
- 使能/禁止接口策略路由

8.2.1 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8-1 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。

8.2.2 设置 Route-policy 的 if-match 子句

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。一条策略中可以包含多条 if-match 子句，多条 if-match 子句可以组合使用。

请在 **route-policy** 视图下进行下列配置。

表8-2 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 IP 地址匹配条件	**if-match acl** *acl-number*

缺省情况下，没有 if-match 子句被定义。

8.2.3 设置 Route-policy 的 apply 子句

请在 **route-policy** 视图下进行下列配置。

IP 策略路由提供五种 **apply** 子句：**apply ip-precedence**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。一条策略中可以包含多条 **apply** 子句，多条 **apply** 子句可以组合使用。

表8-3 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。

8.2.4 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8-4 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。

8.2.5 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8-5 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。

8.3 IP 单播策略路由显示和调试

在完成上述配置后，在所有视图下执行 **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8-6 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**

8.4 IP 单播策略路由典型配置举例

8.4.1 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

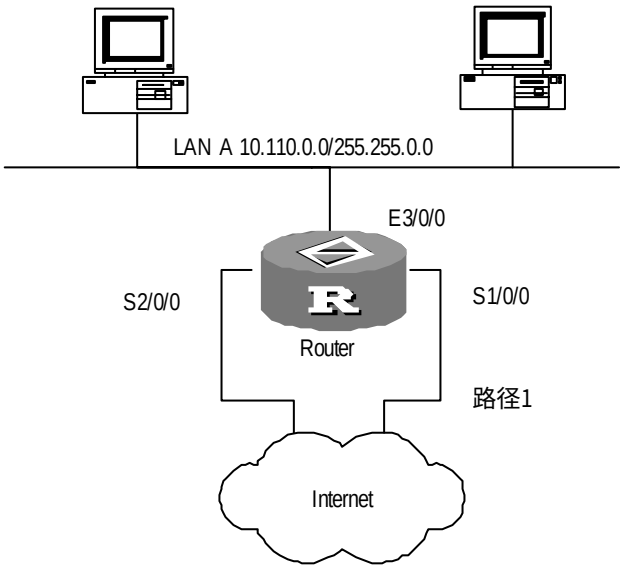


图8-1 配置基于源地址的策略路由组网图

3. 配置步骤

定义访问控制列表。

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

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

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

在以太网口上应用策略 aaa。

```
[Quidway] interface ethernet 3/0/0
[Quidway-Ethernet3/0/0] ip policy route-policy aaa
```

8.4.2 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

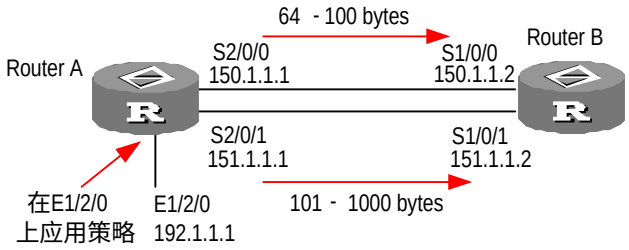


图8-2 配置基于报文大小的策略路由组网图

3. 配置步骤

配置路由器 Router A

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

配置路由器 Router B

```
[RouterB] interface serial 1/0/0
```

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

```
<RouterA> 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。

```
<RouterA> 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9章 IP 组播策略路由配置

9.1 IP 组播策略路由简介

9.1.1 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。

9.1.2 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。

9.1.3 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。

9.2 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

9.2.1 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9-1 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。

9.2.2 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9-2 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。

9.2.3 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9-3 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）。

9.2.4 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9-4 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。

9.3 IP 组播策略路由显示和调试

在完成上述配置后，在所有视图下执行 **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9-5 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10章 IPX 配置

10.1 IPX 协议简介

IPX（Internetwork Packet Exchange，网际报文交换）是 NetWare 的网络层协议，它在 Novell 的 NetWare 协议族中的位置类似于 IP 协议在 TCP/IP 中的位置，定义 Novell 网络的地址结构等内容。

IPX 协议是一个无连接的协议。虽然在 IPX 包中不仅包含数据，也包含目的地的 IPX 地址，但 IPX 并不确认包是否转发成功。包转发成功与否和连接控制等功能都由 IPX 的上层协议来提供。在 IPX 中，任何一个 IPX 包都被认为是一个独立的实体，与其它的 IPX 包没有任何逻辑上或顺序上的联系。

IPX 协议实现填地址、路由和转发信息包的功能。对于从上层产生的包，IPX 直接转发出去；对于用户数据包，IPX 会从路由信息表中查找正确的路径，将包转发出去。

📖 说明：

在 VRP 目前的实现中，只在集中式设备上提供对 IPX 特性的支持。

10.1.1 IPX 的地址结构

IPX 的地址结构与 IP 的地址结构不同，IPX 地址包括网络地址和节点地址两部分，形式为：网络号.节点值，即：network.node

网络地址表明站点所在的网络，长度为 4 个字节，用 8 个 16 进制数字表示，输入时，前导 0 可省略。节点地址标志网络中的一个节点，其结构与 MAC 地址相同，长度为 6 个字节，通常表示为用 “ - ” 分隔的三个两字节数，输入时，前导 0 不能省略。

例如，在 IPX 地址 bc.0-0cb-47 中，网络地址为 bc（更准确的写法是：000000bc），节点地址为 0-0cb-47（更准确的写法是：0000-00cb-0047）。

因此，IPX 地址也可以表示为 N.H-H-H，其中 N 是网络地址，H-H-H 是节点地址。

10.1.2 路由信息协议 RIP

IPX 使用 RIP 维护和发布动态路由信息。

路由器的主要功能是在网间转发包。当客户机在网间发送一个包时，它并不知道要到达目的地该经过什么样的路径，它只知道要把此包传到最近的路由器，再由下一台路由器继续转发。因此，路由器必须提供它可直接发给目的地或需要转发的网络

路由信息，以便接到一个包时，能找到下一正确站点，把包传递下去。这些路由信息可静态配置，也可动态收集。

RIP 是 Routing Information Protocol（路由信息协议）的简称。路由器通过 RIP 来创建和维护一个网间路由信息数据库（通常称为路由信息表，Router Information Table）。路由器启动后，RIP 与其他的 RIP 邻居交换路由信息，根据网络的变化情况维护路由信息表。

下图为 RIP 协议主要部件之间的关系示意图：

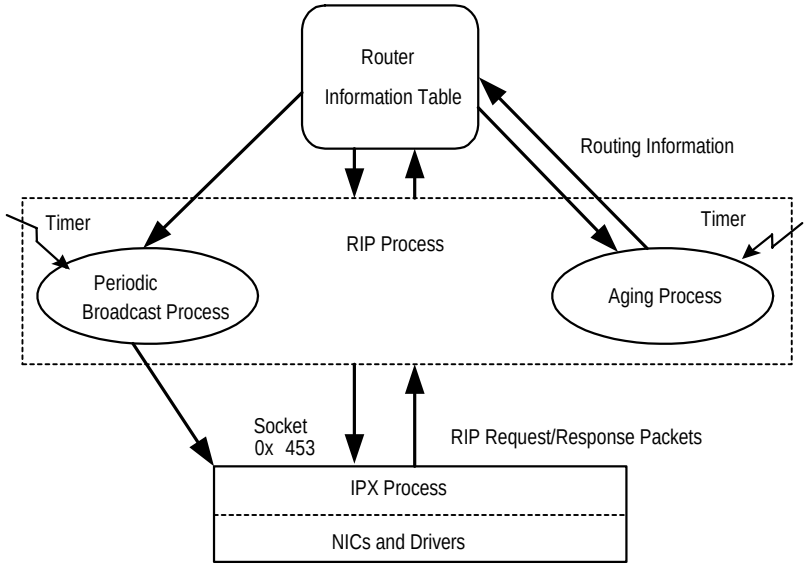


图10-1 RIP 主要部件间关系的示意图

本章中介绍的是 IPX 使用的 RIP，IP 环境下的 RIP 配置，请参考本手册的“ 路由协议 ”部分。

10.1.3 服务公告协议 SAP

SAP 是 Service Advertising Protocol（服务公告协议）的简称，用于发布服务器提供的服务类型和它们的地址。服务器启动时，通过 SAP 广播自己所提供的服务；服务器关闭时，通过 SAP 指示服务已经中止。

通过 SAP 协议，路由器创建和维护一个网间服务信息数据库（通常称为服务器信息表，Server Information Table）。它帮助客户了解网络所能提供的服务类型以及提供这些服务的服务器地址。这是一个很重要的作用，因为如果一个工作站不知道文件服务器的地址，它就不能建立同文件服务器的会话。

服务器在与它直接相连的网点上周期性广播它提供的服务类型和地址。这些服务器广播的信息不能直接被客户使用，而是由网络上路由器的 SAP 代理收集，并存入自己的服务器信息表。由于 SAP 动态更新服务器信息，所以客户总能得到最近的服务器的正确地址。

下图为 SAP 协议主要部件之间的关系示意图：

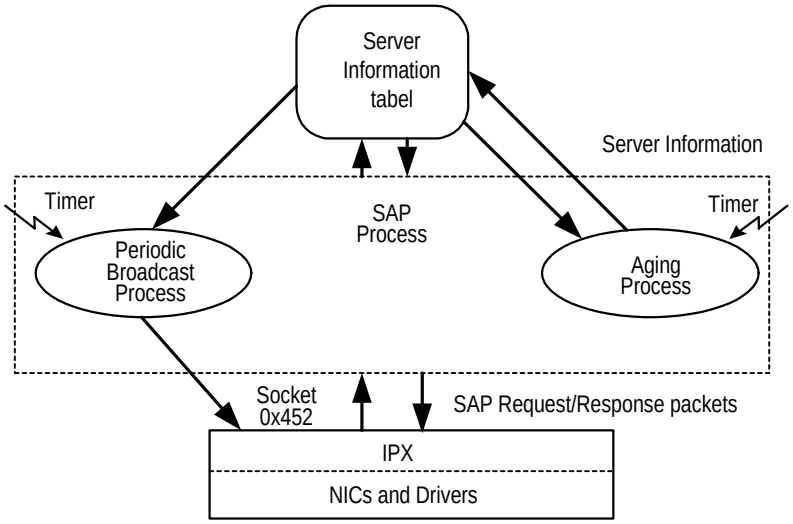


图10-2 SAP 主要部件间关系的示意图

SAP 定义了 3 种类型的数据包，包括服务请求、服务响应和定期更新，其工作原理如下：

1. NetWare 客户初始化

当一个 NetWare 客户正在初始化时，它需要定位一个服务器，以连接到其上。为达到这个目的，它发送一个 SAP 最近服务器（GNS）请求。这个请求是一个广播，至少有一个路由器或服务器能够给予响应。SAP 响应报文包含数据包类型、服务类型、服务器名称服务器地址等信息。

注意：因为 GNS 请求是一个广播，这意味着，客户仅仅能从本地 IPX 网络上的服务器和路由器得到响应。为可以定位其他网络上的服务器，IPX 路由器可以通过发送 RIP 请求来获得到其它网络服务器的路由。

2. SAP 定期更新

当一个服务器有服务需要进行通告时，它发送 SAP 广播，以列出服务名称、类型和 IPX 网络地址。IPX 路由器听到这些广播，并在服务信息数据库中加入被广播的服务。路由器定期向直接相连的网络广播这些数据库，所以通告可以在整个网络上传播。缺省情况下，这些广播每 60 秒钟发送一次。

10.2 IPX 配置

10.2.1 IPX 配置介绍

在 IPX 的配置中，为使用 IPX 特性而必须进行的配置有两项：

- 激活 IPX
- 使能 IPX 接口

IPX 支持静态路由配置。并且，在接口上使用 IPX 后，将自动启用动态路由协议 RIP。路由相关的配置包括：

- 配置 IPX 静态路由
- 配置 IPX 路由数限制
- 配置 IPX RIP 相关参数

IPX 的服务公告协议 SAP 随着 IPX 的使能而被使能，用户也可以根据实际需要配置 SAP 的其它参数或进行服务信息的配置。这部分的配置内容在：

- 配置 IPX SAP 相关参数

IPX 转发的相关配置还包括：

- 配置 IPX 的触发刷新特性
- 配置 IPX 的水平分割特性
- 配置 IPX 帧的封装格式
- 转发类型为 20 的 IPX 广播包

10.2.2 激活 IPX

请在系统视图下进行下列配置。

表10-1 激活 IPX

操作	命令
激活 IPX	**ipx enable** [**node** *node*]
关闭 IPX	**undo ipx enable**

缺省情况下，IPX 功能是关闭的。

node 关键字用于指定路由器的节点值，如果在这里没有配置 **node**，则路由器将使用它的第一个以太网接口的 MAC 地址路由器的节点值。

路由器串口、以太网口的节点值与路由器的节点值有如下关系：

- 在激活 IPX 功能时，如果没有指明路由器的节点值，则路由器将使用它的第一个以太网口的 MAC 地址作为其串口的节点值。
- 在激活 IPX 功能时，如果指明了路由器的节点值，则路由器将使用该节点值作为其串口的节点值。
- 而对于以太网口，则无论是否指明路由器的节点值，其节点值就是本身的 MAC 地址。

📖 说明：

如果路由器没有以太网接口，则会根据系统时钟产生一个随机的节点号。

10.2.3 使能 IPX 接口

当激活了路由器的 IPX 功能后，还必须对每一个独立的接口分配一个网络号，使 IPX 能在这个接口上运行。

请在接口视图下进行下列配置。

表10-2 使能 IPX 接口

操作	命令
使能 IPX 接口	**ipx network** *network-number*
删除 IPX 接口	**undo ipx network**

缺省情况下，IPX 启动后在所有接口上禁用。

如果删除 IPX 接口，则该接口的 IPX 配置和静态路由信息将会被删除。

10.2.4 配置 IPX 静态路由

请在系统视图下进行下列配置。

表10-3 配置 IPX 静态路由

操作	命令
配置 IPX 静态路由	**ipx route-static** *network* { *network.node* | *interface-type interface-num* } [**preference** *value*] [**tick** *ticks* **hop** *hops*]
删除 IPX 静态路由	**undo ipx route-static** { *network* [*network.node* | *interface-type interface-num*] | **all** }

目的网络号为-2（0xFFFFFFFE）的 IPX 静态路由是缺省路由。

在配置滴答数 tick 和跳数 hop 两个参数时，或者都配置，或者都不配置，不能只配置其中一个。一个滴答数是 1/18 秒。

在目前的实现中，出接口只能配置为封装 PPP 的接口。

10.2.5 配置 IPX 路由数限制

在 IPX 中，可以设置路由表中允许的到同一目的地址的最大动态路由数和等价路由数。这两项配置相互之间没有直接的联系，改变其中一项配置，不会影响另一项。

请在系统视图下进行下列配置。

1. 配置到同一目的地址的最大动态路由数

表10-4 配置到同一目的地址的最大动态路由数

操作	命令
配置到同一目的地址的最大动态路由数	**ipx route max-reserve-path** *paths*
恢复缺省设置	**undo ipx route max-reserve-path**

缺省情况下，到同一目的地址的最大动态路由数为 4。

当到同一目的地址的动态路由数达到设置的最大值时，新发现的动态路由将不被添加到路由表中，直接丢弃。如果新配置的值小于原先设定的值，不删除当前路由表中多出的路由，直到它们自行老化或被手工删除。

2. 配置到同一目的地址的等价路由数

表10-5 配置到同一目的地址的等价路由数

操作	命令
配置到同一目的地址的等价路由数	**ipx route load-balance-path** *paths*
恢复缺省设置	**undo ipx route load-balance-path**

缺省情况下，到同一目的地址的等价路由数为 1。

如果新配置的值小于当前激活的路由数，则系统将把超出的激活路由变为非激活状态；如果当前激活的路由数小于配置的等价路由数，并且当前还存在与这些激活路由等价的路由，则把这些路由变为激活状态，直到激活的路由数等于配置的等价路由数。

10.2.6 配置 IPX RIP 相关参数

在接口上使能了 IPX 后，系统将自动启用 RIP。用户也可以根据实际需求，进行下列 RIP 相关参数的配置：

- 配置 IPX RIP 的刷新周期
- 配置 IPX RIP 的老化周期
- 配置 IPX RIP 刷新报文的大小
- 配置接口发送 IPX 报文的延时
- 配置 IPX RIP 引入静态路由

1. 配置 IPX RIP 的刷新周期

路由器定期向外广播 RIP 刷新报文，用户可以配置 IPX 的 RIP 刷新周期。

请在系统视图下进行下列配置。

表10-6 配置 IPX RIP 的刷新周期

操作	命令
配置 IPX RIP 的刷新周期	**ipx rip timer update** *seconds*
恢复缺省设置	**undo ipx rip timer update**

缺省情况下，IPX RIP 的刷新周期为 60 秒。

2. 配置 IPX RIP 的老化周期

IPX RIP 的老化周期依赖于刷新周期，用户可以设置几个刷新周期为一个老化周期。

请在系统视图下进行下列配置。

表10-7 配置 IPX RIP 的老化周期

操作	命令
配置 IPX RIP 的老化周期	**ipx rip multiplier** *multiplier*
恢复缺省设置	**undo ipx rip multiplier**

缺省情况下，RIP 老化周期是刷新周期的 3 倍。即，如果一个路由表项在经过三个 RIP 刷新周期之后都没有得到更新，则它将从路由表中被删除，同时，与它相关联的动态服务信息表项也会从服务信息表中被删除。

3. 配置 IPX RIP 刷新报文的大小

请在接口视图下进行下列配置。

表10-8 配置 IPX RIP 刷新报文的大小

操作	命令
配置 IPX RIP 刷新报文的大小	**ipx rip mtu** *bytes*
恢复缺省设置	**undo ipx rip mtu**

缺省情况下，IPX RIP 的刷新报文最大为 432 字节。由于 IPX 报文头和 RIP 报文头共 32 字节，因此，一个刷新报文最多可以携带 50 个 8 字节的路由项。

4. 配置接口发送 IPX 报文的延时

在 IPX RIP 中，使用两个参数衡量到达目的网络的距离并进行选路，这两个参数是跳数（hops）和滴答数（ticks）。

滴答数表示延时，一个滴答数是 1/18 秒。延时量的大小代表接口转发 IPX 报文的快慢：延时大，表示接口转发 IPX 报文速度慢；延时小，表示接口转发 IPX 报文速度快。用户可以调节接口发送 IPX 报文的延时量。

请在接口视图下进行下列配置。

表10-9 配置接口发送 IPX 报文的延时

操作	命令
配置接口发送 IPX 报文的延时	**ipx tick** *ticks*
恢复缺省设置	**undo ipx tick**

缺省情况下，以太网接口的延时为 1 个滴答数，异步串口为 30 个滴答数，广域网口的延时是 6 个滴答数。滴答数（ticks）的取值范围为 0～30000。

5. 配置 IPX RIP 引入静态路由

通过路由引入，不同路由协议之间可以共享对方的路由信息。

请在系统视图下进行下列配置。

表10-10 配置 IPX RIP 引入静态路由

操作	命令
配置 IPX RIP 引入静态路由	**ipx rip import-route static**
取消 IPX RIP 引入的静态路由	**undo ipx rip import-route static**

缺省情况下，IPX RIP 不引入静态路由。

10.2.7 配置 IPX SAP 相关参数

IPX SAP 的配置包括：

- 激活/关闭 SAP
- 配置 IPX SAP 的刷新周期
- 配置 IPX SAP 的老化周期
- 配置 IPX SAP 刷新报文的大小
- 配置 IPX SAP 的 GNS 请求响应
- 配置 IPX 静态服务信息表项
- 配置服务信息存储队列的长度

1. 激活/关闭 SAP

在一个接口上，SAP 随着 IPX 的使能而被使能。如果需要手工控制 SAP 功能的启用，可以使用此配置。

请在接口视图下进行下列配置。

表10-11 激活/关闭 SAP

操作	命令
关闭 IPX SAP	**ipx sap disable**
激活 IPX SAP	**undo ipx sap disable**

2. 配置 IPX SAP 的刷新周期

在一个规模较大的网络中，一次 IPX SAP 广播可能会占用大量的带宽，而对于运行 PPP、X.25 和帧中继等协议的接口，其带宽是有限的，这时，改变 IPX SAP 刷新周期是减少带宽浪费的一种有效方法。

请在系统视图下进行下列配置。

表10-12 配置 IPX SAP 的刷新周期

操作	命令
配置 IPX SAP 的刷新周期	**ipx sap timer update** *seconds*
恢复缺省设置	**undo ipx sap timer update**

缺省情况下，IPX SAP 的刷新周期是 60 秒。

在配置时，应确保所有在网络上的服务器和路由器有同样的 SAP 刷新周期，否则的话，可能会导致路由器错误地认为一台仍在工作的服务器已失效。

3. 配置 IPX SAP 的老化周期

请在系统视图下进行下列配置。

表10-13 配置 IPX SAP 的老化周期

操作	命令
配置 IPX SAP 的老化周期	**ipx sap multiplier** *multiplier*
恢复缺省设置	**undo ipx sap multiplier**

缺省情况下，如果 IPX SAP 服务信息在 3 个刷新周期时间内没有得到更新，那么它将从服务信息表中被删除。

4. 配置 IPX SAP 刷新报文的大小

请在接口视图下进行下列配置。

表10-14 配置 IPX SAP 刷新报文的大小

操作	命令
配置 IPX SAP 刷新报文的大小	**ipx sap mtu** *bytes*
恢复缺省设置	**undo ipx sap mtu**

缺省情况下，IPX SAP 的刷新报文最大长度为 480 字节，即，一个 SAP 刷新报文中可以包含 7 个 64 字节的服务信息。

5. 配置 IPX SAP 的 GNS 请求响应方式

GNS（Get Nearest Server，请求最近的服务器）是一种 SAP 消息，由启用了 SAP 的 NetWare 客户端广播，NetWare 服务器以 Give Nearest Server 消息进行响应。

如果客户端所在的网段上存在 NetWare 服务器，将由此服务器进行响应；如果网段上不存在 NetWare 服务器，则由路由器来响应。

用户可设置路由器对 SAP GNS 请求的处理方式：

- 由路由器使用最近（nearest）的服务器信息进行响应；
- 由路由器通知它所知道的所有服务器轮流进行响应（Round-Robin 方式）；
- 设置路由器的某个接口上是否对 SAP GNS 请求进行响应。

请在系统视图下进行下列配置。

表10-15 配置路由器对 SAP GNS 请求的响应方式

操作	命令
以 Round-Robin 方式进行 GNS 请求响应	**ipx sap gns-load-balance**
使用最近的服务器信息进行 GNS 请求响应	**undo ipx sap gns-load-balance**

请在接口视图下进行下列配置。

表10-16 配置路由器接口对 SAP GNS 请求的响应方式

操作	命令
在当前接口上不对 GNS 请求进行响应	**ipx sap gns-disable-reply**
在当前接口上对 GNS 请求进行响应	**undo ipx sap gns-disable-reply**

缺省情况下，对于 SAP 的 GNS（Get Nearest Server）请求，路由器会通知知道的所有服务器轮流响应，以避免某个服务器负载过重。

6. 配置 IPX 静态服务信息表项

通常情况下，客户端只使用 NetWare 服务器通告的、并被路由器存储的服务，在特殊情况下，也可以指定客户端使用特定服务。

为了让客户端总能使用某个特定服务，可以手工将静态服务信息增加到服务信息表中。如果与静态服务信息相关联的路由失效或被删除，那么，这条静态服务信息将被禁止向外广播，直到路由器找到一条新的与此服务信息相关联的有效路由。

请在系统视图下进行下列配置。

表10-17 配置 IPX 静态服务信息表项

操作	命令
增加一条 IPX 静态服务信息表项	**ipx service** *service-type name network.node socket* **hop** *hopcount* **preference** *preference*
删除 IPX 静态服务信息表项	**undo ipx service** { { *service-type* [*name* [*network.node*]] [**preference** *preference*] } | **all** }

IPX 的服务信息与路由信息类似，具有优先级的概念，优先级的值越小，则服务信息的优先级越高。缺省情况下，静态服务信息的优先级为 60；动态服务信息的的优先级为 500。

7. 配置服务信息存储队列的长度

一种服务类型可以配置的最大动态服务信息数目可以通过命令进行调整。

请在系统视图下进行下列配置。

表10-18 配置服务信息存储队列的长度

操作	命令
配置服务信息存储队列的长度	**ipx sap max-reserve-servers** *length*
恢复缺省设置	**undo ipx sap max-reserve-servers**

缺省情况下，服务信息存储队列的长度为 2048。

需要说明的是，以上命令不限制静态服务信息的数目，只限制动态服务信息数目。如果用户配置的服务信息队列长度小于原来的长度，服务信息表中的表项不会被删除，如果同种服务类型的服务信息数目达到了配置的值，新的服务信息将不会被加入。

IPX 最多可以支持 10240 个服务信息，5120 种服务类型和 5120 条静态服务信息。

10.2.8 配置 IPX 的触发刷新特性

IPX 的 RIP 和 SAP 周期性地向外广播刷新报文，如果不希望路由器周期性发送广播报文，可以在接口上启用触发刷新特性，这样配置后，只有在路由或服务信息发生变化时，才向外发送刷新报文。

请在接口视图下进行下列配置。

表10-19 配置 IPX 的触发刷新特性

操作	命令
在接口上启用触发刷新特性	**ipx update-change-only**
在接口上关闭触发刷新特性	**undo ipx update-change-only**

缺省情况下，接口上不启用触发刷新特性。

10.2.9 配置 IPX 的水平分割特性

水平分割（Split Horizon）是避免产生路由环的一种方法，是指从一个接口接收到的路由信息不能再从这个接口发送出去。在某些情况下，必须禁用水平分割以保证正确的路由信息传递。建议只在必要时才禁用水平分割。另外，禁止水平分割对点到点连接的链路不起作用。

请在接口视图下进行下列配置。

表10-20 配置 IPX 的水平分割特性

操作	命令
允许水平分割	**ipx split-horizon**
禁止水平分割	**undo ipx split-horizon**

缺省情况下，接口上允许水平分割。

10.2.10 配置 IPX 帧的封装格式

在广域网类型的接口上，IPX 帧目前只支持 PPP 封装。在以太网接口上，可以通过命令改变 IPX 帧的封装格式。

请在以太网接口视图下进行下列配置。

表10-21 配置 IPX 帧的封装格式

操作	命令
配置 IPX 帧封装格式为 Ethernet_802.2	**ipx encapsulation dot2**
配置 IPX 帧封装格式为 Ethernet_802.3	**ipx encapsulation dot3**
配置 IPX 帧封装格式为 Ethernet_II	**ipx encapsulation ethernet-2**
配置 IPX 帧封装格式为 Ethernet_SNAP	**ipx encapsulation snap**
恢复缺省设置	**undo ipx encapsulation**

缺省情况下，以太网接口的 IPX 帧封装格式为 Ethernet_802.3（**dot3**）。

10.2.11 转发类型为 20 的 IPX 广播包

Novell NetWare 定义了一种类型为 20 的 IPX 报文，用于 NetBIOS（Network Basic Input/Output System）。缺省情况下，这种类型为 20 的广播包会被路由器丢弃，但用户可以通过配置命令，允许将类型为 20 的广播包发送至其它网段上。

请在接口视图下进行下列配置。

表10-22 转发类型为 20 的 IPX 广播包

操作	命令
允许转发类型为 20 的广播包	**ipx netbios-propagation**
禁止转发类型为 20 的广播包	**undo ipx netbios-propagation**

10.3 IPX 显示和调试

1. IPX 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 IPX 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 IPX 进行调试。

表10-23 IPX 显示和调试

操作	命令
查看 IPX 的接口状态和接口参数	**display ipx interface** [*interface-type interface-num*]
查看接收和传送包类型及数量	**display ipx statistics**
查看 IPX 服务信息表	**display ipx service-table** [[**type** *service-type* | **name** *name* | **network** *network* | **order** { **network** | **type** }] | [**inactive**]] [**verbose**]
查看 IPX 激活路由信息	**display ipx routing-table**
查看 IPX 详细路由信息，包括激活和非激活	**display ipx routing-table verbose**
查看 IPX 路由统计信息	**display ipx routing-table statistics**
查看指定目的网络号的 IPX 激活路由信息	**display ipx routing-table** *network*
查看指定目的网络号的 IPX 路由详细信息，包括激活和非激活	**display ipx routing-table** *network* **verbose**
查看指定目的类型的 IPX 路由信息	**display ipx routing-table protocol** { **default** | **direct** | **rip** | **static** } [**inactive**]
查看指定目的类型的 IPX 路由详细信息，包括激活和非激活	**display ipx routing-table protocol** { **default** | **direct** | **rip** | **static** } **verbose**

操作	命令
打开 IPX SAP 报文和事件调试信息的开关	**debugging ipx sap** [**packet** [**verbose**] | **event**]
关闭 IPX SAP 调试开关	**undo debugging ipx sap** [**packet** [**verbose**] | **event**]
打开 IPX 报文调试开关	**debugging ipx packet** [*interface-type interface-num*]
关闭 IPX 报文调试开关	**undo debugging ipx packet** [*interface-type interface-num*]
打开 IPX ping 调试开关	**debugging ipx ping**
关闭 IPX ping 调试开关	**undo debugging ipx ping**
打开 IPX RIP 调试开关	**debugging ipx rip** { **packet** [**verbose**] | **event** }
关闭 IPX RIP 调试开关	**undo debugging ipx rip** { **packet** [**verbose**] | **event** }
打开 IPXRM 模块的路由刷新调试开关	**debugging ipx rtpro-flash**
打开 IPXRM 模块的接口变化调试开关	**debugging ipx rtpro-interface**
打开 IPXRM 模块的路由变化调试开关	**debugging ipx rtpro-routing**

2. 清除 IPX 统计信息

请在用户视图下进行下列配置。

表10-24 清除 IPX 统计信息

操作	命令
清除 IPX 统计信息	**reset ipx statistics**
清除指定类型 IPX 路由的路由记数统计信息	**reset ipx routing-table statistics**

3. 检查主机可达性及网络可达性

可在所有视图下进行下列操作。

表10-25 检查主机可达性及网络可达性

操作	命令
检查主机可达性及网络可达性	**ping ipx** *network.node* [**-c** *count*] [**-t** *timeout*] [**-s** *size*]

10.4 IPX 典型配置举例

10.4.1 通过 IPX 网络提供文件服务和目录服务

1. 组网需求

路由器 RouterA 与 RouterB 的串口通过 IPX 网络相连。RouterA 的以太网接口节点地址是 00e0-fc01-0000，RouterB 的以太网接口节点地址是 00e0-fc01-0001。

服务器上安装 Netware4.1，网络号为 2。包的封装格式为 Ethernet_II。客户端是 PC 机，网络号为 3，包的封装格式为 SNAP，服务器提供文件服务和目录服务。客户通过 IPX 网络访问这些服务。服务器的节点值为 0000-0c91-f61f。

2. 组网图

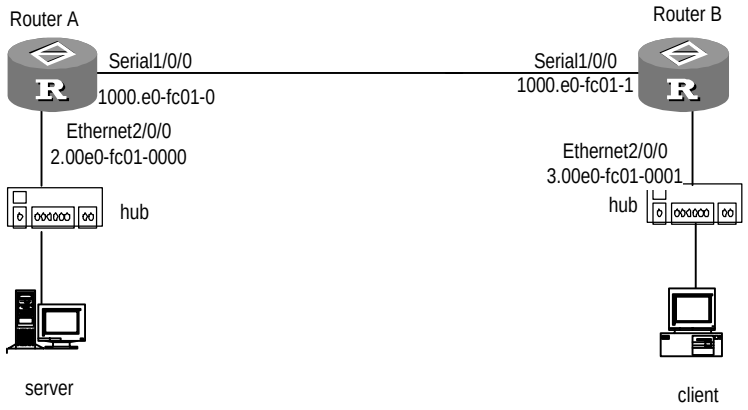


图10-3 IPX 配置组网图

3. 配置步骤

(1) 配置 RouterA

激活 IPX。

```
[Quidway] ipx enable
```

在接口 Ethernet2/0/0 上激活 IPX，网络号为 2。

```
[Quidway] interface ethernet 2/0/0
[Quidway-Ethernet2/0/0] ipx network 2
```

设置以太网口上包的封装格式为 Ethernet_II。

```
[Quidway-Ethernet2/0/0] ipx encapsulation ethernet-2
[Quidway-Ethernet2/0/0] quit
```

在接口 Serial1/0/0 上激活 IPX，网络号为 1000。

```
[Quidway] interface serial 1/0/0
[Quidway-Serial1/0/0] ipx network 1000
```

```
[Quidway-Serial1/0/0] quit
```

(2) 配置 RouterB

激活 IPX。

```
[Quidway] ipx enable
```

在接口 Ethernet2/0/0 上激活 IPX，网络号为 3。

```
[Quidway] interface ethernet 2/0/0
[Quidway-Ethernet2/0/0] ipx network 3
```

设置以太网口上包的封装格式为 Ethernet_SNAP。

```
[Quidway-Ethernet2/0/0] ipx encapsulation snap
[Quidway-Ethernet2/0/0] quit
```

在接口 Serial1/0/0 上激活 IPX，网络号为 1000。

```
[Quidway] interface serial 1/0/0
[Quidway-Serial1/0/0] ipx network 1000
[Quidway-Serial1/0/0] quit
```

配置一条关于 Server 文件服务的信息。

```
[Quidway] ipx service 4 server 2.0000-0c91-f61f 451 hop 2
```

配置一条关于 Server 目录服务的信息。

```
[Quidway] ipx service 26B tree 2.0000-0c91-f61f 5 hop 2
[Quidway] ipx service 278 tree 2.0000-0c91-f61f 4006 hop 2
```

说明：IPX 接口配置了 **ipx network** 命令就自动启动了 **RIP** 和 **SAP** 功能，故本例中不再配置路由协议了。

10.5 IPX 故障诊断与排除

1. IPX 核心层故障诊断与排除

故障之一：在 PPP 链路上，IPX 协议不能进入 UP 状态

故障排除：

- 检查链路两端配置的网络号是否一致，如果不一致，请重新配置。
- 检查链路两端的节点号是否不同，如果相同，请重新配置。

故障之二：Ping 不通目的地址

故障排除：

- 检查 Ping 命令的目的地址是否正确。
- 使用 **display ipx interface** 命令检查路由器的接口配置，相连接口的网络号和 IPX 帧封装格式必须相同，否则不能 Ping 通。

- 使用**display ipx routing-table**命令查看路由信息，检查目的网络号是否可达。
- 使用 **debugging ipx packet** 命令打开 IPX 报文调试开关，根据显示的 IPX 报文接收、发送、转发和丢弃的详细信息定位错误。

故障之三：报文被丢弃

故障排除：

- 如果 IPX 报文调试信息显示报文被丢弃，并提示“ Packet size is greater than interface MTU! ”，则说明发送报文的大小超过了接口能发送的最大报文长度。请使用 **display interface** 命令检查接口的 MTU，使用 **display ipx interface** 命令检查 RIP 和 SAP 的报文长度，如果 RIP 或 SAP 的报文长度大于接口的 MTU，则 RIP 或 SAP 报文无法从此接口发送出去。

故障之四：路由器收不到 SAP 报文

故障排除：

- 使用 **display ipx interface** 命令检查接收接口的配置，如果该接口上 SAP 被禁止了，那么从该接口受到的 SAP 报文就会被丢弃。

故障之五：类型为 20 的 IPX 报文不能被传送至其它网段

故障排除：

- 使用 **display ipx interface** 命令检查接收和发送接口上是否使能了类型为 20 的 IPX 报文的转发功能，如果未使能，则无法转发。
- 使用 **debugging ipx packet** 命令打开 IPX 报文调试开关，如果调试信息显示类型为20的报文被丢弃，并提示‘ Transport Control field of IPX type-20 packet >= 8! ”，这是因为类型为 20 的 IPX 报文只能被转发 8 次，如果已经转发了 8 次，则不再继续转发。

2. IPX RIP 故障诊断与排除

故障之一：不能从对端路由器学到路由。

故障排除：

- 使用命令 **debugging ipx rip packet verbose** 打开 IPX RIP 调试开关，查看是否有含有路由的 RIP 报文从对端路由器发送过来，如果没有，则表示两台路由器底层连接有问题。
- 如果对端路由器发送来了含有路由信息的 RIP 报文，使用命令 **debugging ipx rip event** 查看是否这条路由被添加到路由表里，如果没有，则表示向路由表中添加路由时发生错误。

故障之二：配置了一条静态路由后，引入静态路由到 IPX RIP 中，但没有静态路由发送出去。

故障排除:

- 首先使用命令 **display ipx routing-table** 查看静态路由是否已经配置。
- 如果在路由表中没有看到所配的静态路由，再使用命令 **display ipx routing-table verbose** 查看是否有这样一条非激活路由（inactive）。如果存在，进一步检查它为什么处于 inactive 状态，当此路由成为激活状态后，就可以作为 RIP 路由发布出去了。
- 如果在路由表中看到了所配的静态路由，继续检查它的跳数，如果跳数大于或等于 15，那么发不出去属于正常现象。

📖 说明：

RIP 引入的静态路由是激活的静态路由，非激活的静态路由不会被引入，更不会被发送出去。静态路由中有一类特殊的路由是缺省路由，如果想把缺省路由引入 RIP，同样使用命令 ipx rip import-route static，但正确引入的前提是此缺省路由必须是激活的。

对于跳数为 15 的路由的处理：

路由器在收到一条跳数 hop 为 15 的路由后，将以不可达属性将这条路由向外发一次。因为 RIP 认为可达的最大跳数为 15，跳数 16 或大于 16 的都是不可达路由，当收到一条 hop 为 15 的路由时，如果向外发送，应该将跳数加 1，变成 hop＝16，即不可达路由，这种路由对于对端而言是没有实际意义的，因此 RIP 只以不可达属性发送一次这种路由。

需要注意的是：对于引入的静态路由，处理也是一样的。由于在引入静态路由的命令 **ipx rip import-route static** 中不能配置 hop，原静态路由的 hop 将作为引入的 RIP 路由的 hop，如果引入了 hop＝15 的静态路由，就会导致 RIP 将这条路由以 hop＝16 发送一次之后不再发送。

3. IPX SAP 故障诊断与排除

故障之一：不能向服务信息表添加静态服务信息。

故障排除：

- 使用命令 **display ipx service-table inactive**，查看服务信息是否在非激活服务信息表中，如果是，表示没有到这个服务器的活跃路由。

故障之二：服务信息表里没有服务信息项。

故障排除：

- 使用命令 **display ipx service-table inactive**，查看服务信息是否在非激活服务信息表中，如果是，表示没有到这个服务器的活跃路由。
- 使用命令 **display ipx interface** 检查接口是否处于 UP 状态，SAP 是否已经激活。
- 使用命令 **display ipx routing-table**，确认到此服务器的活跃路由跳数小于 15。
- 还有一个可能的原因是系统没有足够的内存来添加这个服务信息项到服务信息表中，用户可以尝试添加静态服务信息项。

故障之三：服务信息表中没有新的动态服务信息项。

故障排除：

- 使用命令 **debugging ipx packet** 和 **debugging ipx sap packet verbose** 查看是否收到相关的报文。如果没有，表示底层网络连接存在问题。
- IPX 关闭：在系统视图下执行命令 **ipx enable** 来打开 IPX。
- 没有配置 IPX 接口：通过命令 **display ipx interface** 确保在相关的接口配置了 IPX。
- SAP 关闭：在相关接口使用命令 **undo ipx sap disable** 把 SAP 激活。
- SAP 的服务信息项超出了限制：SAP 的服务信息项是否已经超出了限制，IPX 支持 10240 个服务信息项，5120 个服务类型。
- 接口 MTU 不匹配：SAP 配置的 MTU 应小于或等于物理层 MTU。

故障之四：接口没有收到刷新报文。

故障排除：

- 使用命令 **debugging ipx packet** 和 **debugging ipx sap packet verbose** 查看报文内容。每一个收发的报文都会通过调试信息显示出来。如果没有看到相关的报文，表示底层的网络连接存在问题。
- 使用命令 **display ipx interface** 查看接口是否启用了 SAP。
- 查看到该服务器的路由，确保到这个服务器的活跃路由跳数小于 16。
- 使用命令 **display current-configuration** 查看刷新时间间隔是否太长。
- 使用命令 **display current-configuration** 查看接口是否设置了触发刷新，采用触发刷新的接口不会周期性广播刷新报文。

故障之五：接口没有发送刷新报文。

故障排除：

- SAP 的 MTU 大于物理层 MTU：使用命令 **debugging ipx packet** 和 **debugging ipx sap packet verbose** 查看报文内容。如果报文在调试信息中显示出来了，那么很可能是 SAP 的 MTU 大于接口 MTU，被底层丢弃。
- 使用命令 **display current-configuration** 查看接口是否设置了触发刷新，采用触发刷新的接口不会周期性广播刷新报文。
- 如果 SAP 报文没有从这个接口上发出去，检查是否所有的服务信息都是从该接口上学到的。可能是由于水平分割才使得没有服务信息从这个接口发出。

故障之六：SAP 不响应 GNS 请求。

故障排除：

- 使用命令 **debugging ipx packet sap** 检查路由器是否收到了 GNS 请求报文。
- 查看接收报文的接口是否使能了 SAP。
- 使用命令 **display ipx interface** 查看接收接口是否配置了不响应 GNS 请求。如果是，执行命令 **undo ipx sap gns-disable-reply** 来使能响应 GNS 请求。
- 使用命令 **display ipx service-table** 查看服务信息表里面是否有符合该请求的类型服务信息，如果没有，SAP 就不会做出响应。
- 如果服务信息表里面有符合该请求类型的服务信息，但 SAP 没有做出响应，就要看这个服务信息是不是从接收请求报文的接口学来的，如果是这种情况，SAP 也不会做出响应。

故障之七：对 GNS 请求，SAP 没有以 Round-Robin 方式响应。

故障排除：

- 使用命令 **display current-configuration** 查看是否配置了轮流响应方式。
- 如果 SAP 配置了以轮流方式响应 GNS 请求，查看对请求的服务类型是否有多个等价的服务信息。对于 SAP，只有当这些服务信息的 RIP 延时、RIP 跳数、SAP 跳数和 SAP 优先级都相同，才认为是等价的服务信息。

4. IPX 路由管理故障诊断与排错

故障之一：路由器没有配置动态路由协议，接口的物理状态和链路层协议状态均已处于 UP，但 IPX 报文不能正常转发。

故障排除：

- 使用 **display ipx routing-table protocol static** 命令查看是否正确配置了相应的静态路由。
- 使用 **display ipx routing-table** 命令查看静态路由是否已经生效。查看是否在非 PPP 接口上未指定下一跳地址或指定的下一跳地址不正确。

故障之二：相邻路由器发出了路由，本地路由器也收到了这条路由，但在本路由器上使用命令 **display ipx routing-table verbose** 看不到这条路由。

故障排除：

- 使用命令 **display current-configuration** 查看是否配置了每个目的网络号下的最大动态路由数目，对应的命令是 **ipx route max-reserve-path**，如果没有配置，则使用的是缺省值 4。
- 使用命令 **display ipx routing-table verbose** 查看该目的网络号下面已经存在的动态路由数目（目前动态路由只有 RIP 路由）。
- 如果当前系统中该目的网络号下的动态路由数目已经达到配置的最大值，新收到的路由将无法加入路由表，解决的方法是使用命令 **ipx route max-reserve-path** 把动态路由数目最大值调大一些。

第11章 DLSw 配置

11.1 DLSw 简介

数据链路交换协议（Data Link Switching）简称 DLSw，是 Advanced Peer-to-Peer Networking（APPN）Implementers Workshop（AIW）研制用来实现通过 TCP/IP 承载 SNA（System Network Architecture，系统网络结构体系）的一种方法。SNA 是 IBM 在 70 年代推出的与 OSI 参考模型完全对应的网络协议。要实现 SNA 协议跨广域网传输，解决方案之一就是 DLSw 技术。

DLSw 的工作原理下图所示：

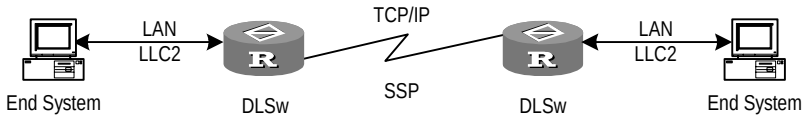


图11-1 DLSw 原理示意图

从上图可以看出，运行 DLSw 的路由器将本地 SNA 设备的 LLC2 格式的帧转换成可封装在 TCP 报文中的 SSP（Switch-to-Switch Protocol，交换机到交换机协议）帧，通过 TCP 通道跨越广域网送达远端，在远端将 SSP 帧再转换成相应的 LLC2 的帧，发送给对端 SNA 设备。可见 DLSw 使得本地的终接设备以为远端的设备和自己处于同一个网络上。但 DLSw 同透明桥不同，它不是将原来的 LLC2 协议帧直接透传到对端，而是转换成 SSP 协议帧来完成将原有数据在 TCP 报文中的封装。它具有本地应答机制，因此，可以减少不必要的数据传输（确认帧和保持活跃帧），并且解决了数据链路控制超时的问题。

利用 DLSw 技术，还可以实现 SDLC（Synchronous Data Link Control，同步数据链路控制）链路协议的跨 TCP/IP 传输。方法是先将 SDLC 格式的报文转换成 LLC2（Logical Link Control，type 2，第二类逻辑链路控制）格式的报文，再通过 DLSw 和远端互联。这样 DLSw 还支持 LAN 与 SDLC 之间不同的介质互联。

11.2 DLSw 的配置

DLSw 的配置包括：

(1) 以太网环境下 DLSw 的配置

基本配置：

- 使能网桥及桥组

- 使能/暂停 DLSw 的运行
- 创建 DLSw 本地对等体
- 创建 DLSw 远端对等体
- 配置连接 DLSw 的桥组
- 配置将以太网接口加入桥组

可选配置：

- 配置 DLSw 定时器参数
- 配置 LLC2 提前应答窗口
- 配置 LLC2 本地应答窗口
- 配置 LLC2 发送报文队列长度
- 配置 LLC2 的模值
- 配置 LLC2 重传次数
- 配置 LLC2 本地应答延迟时间
- 配置 LLC2 本地应答时间
- 配置 LLC2 的 BUSY 状态时间
- 配置 LLC2 的 P/F 等待时间
- 配置 LLC2 的 REJ 状态时间
- 配置路由器可达信息

(2) SDLC 环境下 DLSw 的配置

基本配置：

- 使能网桥及桥组
- 使能/暂停 DLSw 的运行
- 配置接口封装的链路层协议为 SDLC
- 配置 SDLC 对等体
- 配置连接 DLSw 的桥组
- 将封装成 SDLC 的同步串口加入桥组
- 配置 SDLC 角色
- 配置 SDLC 地址
- 配置 SDLC 的 XID（PU2.0 设备必配）
- 配置 SDLC 虚 MAC 地址

可选配置：

- 配置同步串口的波特率
- 配置同步串口的编码方式

- 配置同步串口空闲时间编码方式
- 配置 SDLC 发送报文队列长度
- 配置 SDLC 本地应答窗口
- 配置 SDLC 的模值
- 配置 SDLC 最大帧长度
- 配置 SDLC 的重传次数
- 配置 SDLC 转换 LLC2 的 SAP 地址
- 配置 SDLC 的数据双向传输模式
- 配置 SDLC 的轮循时间间隔
- 配置 SDLC 主站应答等待时间
- 配置 SDLC 从站应答等待时间
- 配置路由器可达信息

11.2.1 使能网桥及桥组

请在系统视图下进行下列配置。

表11-1 使能/禁用网桥

操作	命令
使能网桥	**bridge enable**
禁用网桥	**undo bridge enable**

表11-2 配置网桥组

操作	命令
使能网桥组	**bridge** *bridge-set* **enable**
删除网桥组	**undo bridge** *bridge-set* **enable**

详细说明请参见链路层协议的网桥部分。

11.2.2 创建 DLSw 本地对等体

建立 TCP 通道是建立 DLSw 连接的关键一步。为建立 TCP 通道，需要明确建立 TCP 连接的双方的 IP 地址。通过配置本地对等体为建立 TCP 连接指定了本端的 IP 地址。配置了本命令后，才能够接受远端路由器发起的建立 TCP 连接的请求。一个路由器只能有一个本地对等体。

请在系统视图下进行下列配置。

表11-3 创建 DLSw 本地对等体

操作	命令
创建 DLSw 本地对等体	**dlsw local** *ip-address* [**init-window** *init-window-size*] [**keepalive** *keepalive-interval*] [**max-frame** *max-frame-size*] [**max-window** *max-window-size*] [**permit-dynamic**]
删除 DLSw 本地对等体或恢复参数的缺省值	**undo dlsw local** *ip-address* [**init-window**] [**keepalive**] [**max-frame**] [**max-window**] [**permit-dynamic**]

配置 DLSw 首先要配置 **dlsw local**，然后才能配置其他命令。其中，IP 地址是必须的，配置的 IP 地址必须是可达的本机的 IP 地址。对于命令 **undo dlsw local** 只接 **local** *ip-address* 时，用来删除本地对等体。如果接其它参数则表示恢复指定参数的缺省值。

11.2.3 创建 DLSw 远端对等体

配置了本地对等体后，需要配置远端对等体以建立 TCP 通道。本命令指定了远端路由器用来建立 TCP 连接的 IP 地址。配置了本命令后，路由器会不断尝试去与远端的路由器建立 TCP 连接。一个路由器可以有多个远端对等体，通过配置多个远端对等体可以和多个远端路由器建立 TCP 通道。

请在系统视图下进行下列配置。

表11-4 创建 DLSw 远端对等体

操作	命令
创建 DLSw 远端对等体	**dlsw remote** *ip-address* [**backup** *backup-address*] [**dmac** *mac-address*] [**dmac-list** *acl-number*] [**priority** *priority*] [**keepalive** *keepalive-interval*] [**max-frame** *max-frame-size*] [**max-queue** *max-queue-length*] [**linger** *minutes*]
删除 DLSw 远端对等体	**undo dlsw remote** *ip-address*

其中 IP 地址是必须的，配置的 IP 地址必须是可达的远端 DLSw 路由器的 IP 地址。

11.2.4 配置连接 DLSw 的桥组

DLSw 技术是在桥技术上发展起来的。桥组是桥进行转发的单位，我们可以把多个不同的以太口配置在同一个桥组里，这样它们之间就可以转发报文。为了把指定桥组的报文通过TCP连接转发到远端，就需要本命令将一个本地桥组连接到DLSw上，即这个本地桥组的报文可以通过 TCP 通道被送到远端。可以多次使用本命令把多个桥组和 DLSw 连接起来，使它们都能参加通过 TCP 通道的转发。

注意：配置本命令前务必先使能桥及桥组。

请在系统视图下进行下列配置。

表11-5 配置连接 DLSw 的桥组

操作	命令
配置连接 DLSw 的桥组	**dlsw bridge-set** *bridge-set-number*
取消配置连接 DLSw 的桥组	**undo dlsw bridge-set** *bridge-set-number*

缺省情况下，未配置任何连接 DLSw 的桥组。

11.2.5 配置 DLSw 定时器参数

通过配置 DLSw 协议定时器，可以修改 DLSw 建立虚电路时的各种定时器的值。

请在系统视图下进行下列配置。

表11-6 配置 DLSw 协议定时器

操作	命令
配置 DLSw 定时器参数	**dlsw timer** { **connected** | **explorer-wait** | **local-pending** | **remote-pending** | **cache** | **explorer** } *seconds*
恢复 DLSw 定时器各参数的缺省值	**undo dlsw timer** { **connected** | **explorer-wait** | **local-pending** | **remote-pending** | **cache** | **explorer** }

缺省情况下，**connected** *seconds* 为 300 秒；**explorer-wait** *seconds* 为 30 秒；**local-pending** *seconds* 为 30 秒；**remote-pending** *seconds* 为 30 秒；**cache** *seconds* 为 120 秒；**explorer** *seconds* 为 30 秒。

建议用户在一般情况下不要随便修改配置 DLSw 定时器参数。

11.2.6 配置使能/暂停 DLSw 的运行

请在系统视图下进行下列配置。

表11-7 配置暂停 DLSw 的运行

操作	命令
使能 DLSw 的运行	**dlsw enable**
暂停 DLSw 的运行	**undo dlsw enable**

缺省情况下，使能 DLSw 的运行。

在使用本命令后，系统将释放所有的动态资源，但保留原有的配置。

11.2.7 配置将以太网接口加入桥组

为了将一个以太口加入桥组，需要使用本命令，确定需要加入哪个桥组。本命令和上一操作配合使用，就可以把一个以太口上的 LLC2 报文转发到 TCP 通道上，传送给远端对等体。

请在以太网接口视图下进行下列配置。

表11-8 将以太网接口加入桥组

操作	命令
将以太网接口加入桥组	**bridge-set** *bridge-set-number*
取消将以太网接口加入的桥组	**undo bridge-set** *bridge-set-number*

缺省情况下，未将任何以太网接口加入桥组。其中 *bridge-set-number* 为桥组号。为了使这个接口能够参加 DLSw 转发，本命令应该和上一操作配合使用，即指定相同的桥组号。

11.2.8 配置 LLC2 提前应答窗口

LLC2 提前应答窗口是指未发确认帧前可接收的最大信息帧数，即在收到第 n 个报文时就提前给对方发应答报文。

请在以太网接口视图下进行下列配置。

表11-9 配置 LLC2 提前应答窗口

操作	命令
配置 LLC2 提前应答窗口	**llc2 max-ack** *length*
恢复 LLC2 提前应答窗口长度的缺省值	**undo llc2 max-ack**

缺省情况下，LLC2 提前应答窗口长度为 3。

11.2.9 配置 LLC2 本地应答窗口

本地发送报文到对方后，将等待对方返回确认帧，在接受到对方响应帧之前，本地可连续发送报文的最大数目，就是 LLC2 本地应答窗口。

请在以太网接口视图下进行下列配置。

表11-10 配置 LLC2 本地应答窗口

操作	命令
配置 LLC2 本地应答窗口	**llc2 receive-window** *length*
恢复 LLC2 本地应答窗口长度的缺省值	**undo llc2 receive-window**

缺省情况下，LLC2 本地应答窗口的长度为 7。

11.2.10 配置 LLC2 发送报文队列长度

请在以太网接口视图下进行下列配置。

表11-11 配置 LLC2 发送报文队列长度

操作	命令
配置 LLC2 发送报文队列长度	**llc2 max-send-queue** *length*
恢复默认值	**undo llc2 max-send-queue**

缺省情况下，LLC2 发送报文队列长度为 50。

11.2.11 配置 LLC2 的模值

LLC2 和 X25 协议一样采用了模方式对信息报文进行编号，模值为 8 或 128。以太网一般使用模 128。

请在以太网接口视图下进行下列配置。

表11-12 配置 LLC2 的模值

操作	命令
配置 LLC2 的模值	**llc2 modulo** *n*
恢复 LLC2 模值的缺省值	**undo llc2 modulo**

缺省情况下，LLC2 的模值为 128。

11.2.12 配置 LLC2 重传次数

LLC2 重传次数是指在未收到对端发来的确认帧前重发信息帧的次数。

请在以太网接口视图下进行下列配置。

表11-13 配置 LLC2 重传次数

操作	命令
配置 LLC2 重传次数	**llc2 max-transmission** *retries*
恢复 LLC2 重传次数的缺省值	**undo llc2 max-transmission**

缺省情况下，LLC2 重传次数为 3 次。

11.2.13 配置 LLC2 本地应答延迟时间

SNA 在以太网上传输的是 LLC2 报文。通过配置 LLC2 相关命令可以修改 LLC2 的一些工作参数。

LLC2 本地应答延时时间是指当收到一个 LLC2 数据报文时，延时应答的最大等待时间。

请在以太网接口视图下进行下列配置。

表11-14 配置 LLC2 本地应答延迟时间

操作	命令
配置 LLC2 本地应答延迟时间	**llc2 timer ack-delay** *mseconds*
恢复 LLC2 本地应答延迟时间的缺省值	**undo llc2 timer ack-delay**

缺省情况下，LLC2 本地应答延迟时间为 100ms。

11.2.14 配置 LLC2 本地应答时间

LLC2本地应答时间是指发出一个LLC2数据报文后，等待对方应答的最大等待时间。

请在以太网接口视图下进行下列配置。

表11-15 配置 LLC2 本地应答时间

操作	命令
配置 LLC2 本地应答时间	**llc2 timer ack** *mseconds*
恢复 LLC2 本地应答时间时间的缺省值	**undo llc2 timer ack**

缺省情况下，LLC2 的本地应答时间为 200ms。

11.2.15 配置 LLC2 的 BUSY 状态时间

LLC2 的 BUSY 状态时间是指重新轮循一个忙站点之前的等待时间。

请在以太网接口视图下进行下列配置。

表11-16 配置 LLC2 的 BUSY 状态时间

操作	命令
配置 LLC2 的 BUSY 状态时间	**llc2 timer busy** *mseconds*
恢复 LLC2 的 BUSY 状态时间的缺省值	**undo llc2 timer busy**

缺省情况下，LLC2 的 BUSY 状态时间为 300ms。

11.2.16 配置 LLC2 的 P/F 等待时间

LLC2 的 P/F 等待时间是指发送 P 帧后等待确认帧的时间。

请在以太网接口视图下进行下列配置。

表11-17 配置 LLC2 的 P/F 等待时间

操作	命令
配置 LLC2 的 P/F 等待时间	**llc2 timer poll** *mseconds*
恢复 LLC2 的 P/F 等待时间的缺省值	**undo llc2 timer poll**

缺省情况下，LLC2 的 P/F 等待时间为 5000ms。

11.2.17 配置 LLC2 的 REJ 状态时间

LLC2 的 REJ 状态时间是指发送拒绝帧后等待确认帧的时间。

请在以太网接口视图下进行下列配置。

表11-18 配置 LLC2 的 REJ 状态时间

操作	命令
配置 LLC2 的 REJ 状态时间	**llc2 timer reject** *mseconds*
恢复 LLC2 的 REJ 状态时间的缺省值	**undo llc2 timer reject**

缺省情况下，LLC2 的 REJ 状态时间为 500ms。

11.2.18 配置接口封装的链路层协议为 SDLC

SDLC 是相对 SNA 而言一种链路层协议，其工作原理和 HDLC 十分相似。为了使 DLSw 能正常工作，需要将同步串口链路层的封装协议改为 SDLC。

请在同步串口视图下进行下列配置。

表11-19 配置接口封装的链路层协议为 SDLC

操作	命令
配置接口封装的链路层协议为 SDLC	**link-protocol sdlc**

缺省情况下，同步串口封装的链路层协议为 PPP。

需要注意的是：由于 SDLC 链路协议不能用来承载 IP 协议，所以在封装 SDLC 之前应该先去掉该接口上所有和 IP 相关的配置，如删除接口 IP 地址等。

11.2.19 将封装成 SDLC 的同步串口加入桥组

为了使封装了 SDLC 的接口能参加 DLSw 转发，需要用本命令将 SDLC 接口加入一个桥组。不同的是以太网口上的桥组参加本地转发，而在 SDLC 上配置的桥组只参加 DLSw 的转发，即其上的数据都会被转发到 TCP 通道上去。

请在同步串口视图下进行下列配置。

表11-20 将同步串口加入桥组

操作	命令
将同步串口加入桥组	**bridge-set** *bridge-set-number*
取消将同步串口加入的桥组	**undo bridge-set** *bridge-set-number*

11.2.20 配置同步串口的波特率

以上命令都是配置 DLSw 的一些基本命令。在实际环境中，SNA 设备种类繁多，差别很大。下面一些命令就是一些经常要用到的调整参数，以兼容各种不同的设备。

请在同步串口视图下进行下列配置。

表11-21 配置同步串口的波特率

操作	命令
配置同步串口的波特率	**baudrate** *baudrate*
恢复同步串口的波特率的缺省值	**undo baudrate**

缺省情况下，同步串口的波特率为 64000pbs，SNA 设备的串口波特率为 9600bps。

11.2.21 配置同步串口的编码方式

同步串口上有 NRZI 和 NRZ 两种编码格式。缺省情况下，使用 NRZ 的编码格式，一些 SNA 设备的串口编码方式为 NRZI 编码。所以需要根据所接设备使用的编码方式改变路由器的编码。

请在同步串口视图下进行下列配置。

表11-22 配置同步串口的编码方式

操作	命令
配置同步串口的 NRZI 编码方式	**code nrzi**
取消同步串口的 NRZI 编码方式	**undo code**

缺省情况下，同步串口采用 NRZ 编码方式。

11.2.22 配置同步串口空闲时间编码方式

Quidway 系列路由器的 SDLC 串口在空闲时间一般用“ 7E ”标识，而有的 SDLC 设备在空闲时间采用全“ 1 ”高电平工作做状态。为了更好的兼容这种设备，需要改变路由器的空闲状态的编码方式。

请在同步串口视图下进行下列配置。

表11-23 配置同步串口口空闲时间编码方式

操作	命令
配置同步串口空闲时间的编码方式	**idle-mark**
恢复同步串口空闲时间的缺省的编码方式。	**undo idle-mark**

同步串口空闲时间的编码方式一般不需要修改。有时连接 AS/400 时需要配置此命令，改变空闲状态的编码方式以加快 AS/400 的轮循速度。

11.2.23 配置 SDLC 角色

和 HDLC 所不同的是，SDLC 是一种非平衡模式的链路层协议，就是说，建立连接的两端设备地位是不平等的，分主从的。其中一方起主导作用，控制整个连接过程，成为主站，角色就是 **primary**；另外一方被动的接受控制，成为从站，角色就是 **secondary**。因此，我们需要为封装了 SDLC 协议的接口配置角色。

请在同步串口视图下进行下列配置。

表11-24 配置 SDLC 角色

操作	命令
配置 SDLC 角色	**sdlc status** { **primary**	**secondary** }
取消 SDLC 角色	**undo sdlc status**{ **primary**	**secondary** }

配置 SDLC 角色时应根据与本路由器相连的 SDLC 设备的角色决定。本接口连接的 SDLC 设备为 **primary** 时，就将本接口设置为 **secondary** ；连接的设备是 **secondary** 时，就将本接口设置为 **primary**。一般中心的 IBM 大型机都是 **primary**；终端设备，包括 Unix 主机和 ATM 提款机都是 **secondary**。

缺省情况下，设备没有角色。

11.2.24 配置 SDLC 虚 MAC 地址

DLSw 最初是为 LLC2 类型的协议设计的，通过 MAC 地址建立虚电路的映射关系。因此，为了让 SDLC 报文也能参加转发，就必须为 SDLC 虚电路指定 MAC 地址。

本命令指定了接口上的虚 MAC 地址，为 SDLC 报文转化成 LLC2 报文时提供了源 MAC 地址。

请在同步串口视图下进行下列配置。

表11-25 配置 SDLC 虚 MAC 地址

操作	命令
配置 SDLC 虚拟 MAC 地址	**sdlc mac-map local** *mac-address*
取消 SDLC 虚拟 MAC 地址	**undo sdlc mac-map local**

缺省情况下，SDLC 无虚拟 MAC 地址。

注意：MAC 地址的第六个字节应设置为 0x00。系统会用这个虚拟 MAC 地址的前 5 个 Byte 和 SDLC 地址复合成一个新的 MAC 地址，用于转换 LLC2 协议时构成本地的 MAC 地址。

11.2.25 配置 SDLC 地址

SDLC 协议允许在一条 SDLC 物理链路上跑多条虚电路，一端连接主站，一端连接从站。为了区分每一条虚电路，需要指定每条虚电路的 SDLC 地址。由于 SDLC 是非平衡模式的，通过共享器或 SDLC 交换机，一个主设备可以和多个从设备相连，并且是唯一的；但从设备之间是不能建立连接的。所以，只需标明从设备的地址，就能保证同一组 SDLC 设备之间的正常通讯。本命令为虚电路指定了 SDLC 地址，这个地址在一个物理接口上是唯一的。我们在同步串口上的配置 SDLC 地址实际上就是 SDLC 从站的地址。

请在同步串口视图下进行下列配置。

表11-26 配置 SDLC 地址

操作	命令
配置 SDLC 地址	**sdlc controller** *sdlc-address*
取消配置的 SDLC 地址	**undo sdlc controller** *sdlc-address*

SDLC 地址范围是 0x01～0xFE。一台路由器上的 SDLC 地址只在一个物理接口上有效，就是说，不同接口上配置的 SDLC 地址可以是相同的。

11.2.26 配置 SDLC 对等体

本命令是为一个 SDLC 虚电路指定一个对端的 MAC 地址，用于在做 SDLC 到 LLC2 转换时提供目的 MAC 地址。在设置 DLSw 时，一个 SDLC 地址应配置一个对应的对等体，对等体的 MAC 地址应是远端 SNA 设备的 MAC 地址（以太网和 Token-Ring 等设备的物理地址），或由 SDLC 复合的对端 MAC 地址。

请在同步串口视图下进行下列配置。

表11-27 配置 SDLC 对等体

操作	命令
配置 SDLC 对等体	**sdlc mac-map remote** *mac-addr sdlc-addr*
取消 SDLC 对等体	**undo sdlc mac-map remote** *mac-addr sdlc-addr*

需要注意的是 Token-Ring 和以太网的字位序的差别，配置 Token-Ring 时，可直接按设备标配的地址配置；而配置以太网时，应将每一个 Byte 都倒过来如：对标配为 00e0.fc03.a548 的以太网 MAC 地址，应配置为 0007.3fc0.5a12。

缺省情况下，同步串口无对等体。

11.2.27 配置 SDLC 的 XID

XID 在 SNA 中用于标识一个设备的身份。在配置 SDLC 连接时，需要注意所连接的 SNA 设备的类型。一般有 PU2.0 和 PU2.1 两种设备。PU2.1 的设备自己已经配置了 XID，可以通过交换 XID 来表明彼此的身份；而 PU2.0 的设备不交换 XID，也就没有 XID。所以，PU2.1 类型的设备不用配置本命令，而对于 PU2.0 的设备，我们需要用本命令为它指定一个 XID。

请在同步串口视图下进行下列配置。

表11-28 配置 SDLC 的 XID

操作	命令
配置 SDLC 的 XID	**sdlc xid** *sdlc-address xid-number*
取消配置的 SDLC 的 XID	**undo sdlc xid** *sdlc-address*

缺省情况下，同步串口未配置 SDLC 的 XID。

11.2.28 配置 SDLC 发送报文队列长度

请在同步串口视图下进行下列配置。

表11-29 配置 SDLC 发送报文队列长度

操作	命令
配置 SDLC 发送报文队列长度	**sdlc max-send-queue** *length*
恢复 SDLC 发送报文队列长度的缺省值	**undo sdlc max-send-queue**

缺省情况下，SDLC 发送报文队列长度为 50。

11.2.29 配置 SDLC 本地应答窗口

SDLC 本地应答窗口是指在接受到对方响应包之前，本端能够连续发送的报文的最大数目。

请在同步串口视图下进行下列配置。

表11-30 配置 SDLC 本地应答窗口

操作	命令
配置 SDLC 本地应答窗口	**sdlc window** *length*
恢复默认值	**undo sdlc window**

缺省情况下，SDLC 本地应答窗口的长度为 7。

11.2.30 配置 SDLC 的模值

SDLC 和 X25 协议一样采用了模方式对信息报文进行编号，模值为 8 或 128。SDLC 一般使用模 8。

请在同步串口视图下进行下列配置。

表11-31 配置 SDLC 的模值

操作	命令
配置 SDLC 的模值	**sdlc modulo** *n*
恢复 SDLC 的模值的缺省值	**undo sdlc modulo**

缺省情况下，SDLC 的模值为 8。

11.2.31 配置 SDLC 最大帧长度

SDLC 最大帧长度指能够发送的最大报文的字节数，不包括校验位和起停位。

请在同步串口视图下进行下列配置。

表11-32 配置 SDLC 最大帧长度

操作	命令
配置 SDLC 可发送最大帧长度	**sdlc max-pdu** *n*
恢复 SDLC 可发送最大帧长度的缺省值	**undo sdlc max-pdu**

缺省情况下，SDLC 可发送最大帧长度为 265 个字节。

一些 PU2.0 设备的可发送最大帧长度为 265，IBM AS/400 一般为 521。通常情况下，可发送最大帧长度的值应该与所连接的 SDLC 设备配置成相同的。

11.2.32 配置 SDLC 的重传次数

SDLC 的重传次数是指在未收到对端确认包前的重传次数。

请在同步串口视图下进行下列配置。

表11-33 配置 SDLC 的重传次数

操作	命令
配置 SDLC 的重传次数	**sdlc max-transmission** *retries*
恢复 SDLC 重传次数的缺省值	**undo sdlc max-transmission**

缺省情况下，SDLC 重传次数为 20 次。

11.2.33 配置 SDLC 转换 LLC2 的 SAP 地址

在把 SDLC 报文转换成 LLC2 报文时，除了需要 MAC 地址外，还需要 SAP（Service Access Point）地址。

请在同步串口视图下进行下列配置。

表11-34 配置 SDLC 转换 LLC2 的 SAP 地址

操作	命令
配置 SDLC 转换 LLC2 的 SAP 地址	**sdlc sap-map** { **local** *lsap* | **remote** *dsap* } *sdlc-addr*
恢复 SDLC 转换 LLC2 的缺省 SAP 地址	**undo sdlc sap-map** { **local** *lsap* | **remote** *dsap* } *sdlc-addr*

缺省情况下，lsap 和 dsap 都是 04。

11.2.34 配置 SDLC 的数据双向传输模式

本命令使封装 SDLC 协议的同步串口工作在双向数据同时传输模式。即 SDLC 主站在接收数据的同时可以向从站发送数据。

请在同步串口视图下进行下列配置。

表11-35 配置 SDLC 数据双向传输模式

操作	命令
配置 SDLC 数据双向传输模式	**sdlc simultaneous**
取消 SDLC 数据双向传输模式	**undo sdlc simultaneous**

缺省情况下为双向交换（alternate）传输模式。一般情况下不用配置本命令。

11.2.35 配置 SDLC 的轮循时间间隔

SDLC 轮循时间间隔指 SDLC 主站轮循两个 SDLC 节点之间的等待时间间隔。

请在同步串口视图下进行下列配置。

表11-36 配置 SDLC 的轮循时间间隔

操作	命令
配置 SDLC 的轮循时间间隔	**sdlc timer poll** *mseconds*
恢复 SDLC 轮循时间间隔缺省值	**undo sdlc timer poll**

缺省情况下，SDLC 轮循时间间隔为 1000ms。

11.2.36 配置 SDLC 主站应答等待时间

主站应答等待时间是指主站发送信息帧后等待从站应答的时间。

请在同步串口视图下进行下列配置。

表11-37 配置 SDLC 的应答等待时间

操作	命令
配置 SDLC 的应答等待时间	**sdlc timer ack** *mseconds*
恢复 SDLC 主站应答等待时间的缺省值	**undo sdlc timer ack**

缺省情况下，配置 SDLC 主站应答等待时间为 3000ms。

11.2.37 配置 SDLC 从站应答等待时间

从站应答等待时间是指从站发送信息帧后等待主站应答的时间。

请在同步串口视图下进行下列配置。

表11-38 配置 SDLC 的控制帧应答等待时间

操作	命令
配置 SDLC 的控制帧应答等待时间	**sdlc timer lifetime** *mseconds*
恢复 SDLC 从站应答等待时间 T2 缺省值	**undo sdlc timer lifetime**

缺省情况下，SDLC 从站应答等待时间为 500ms。

11.2.38 配置路由器本地或远端可达信息

为了减少路由器发送报文前的探询过程，在网络拓扑比较稳定的情况下，可以在路由器上手工配置本地和远端可达信息。

表11-39 配置路由器本地或远端可达信息

操作	命令
配置路由器本地可达的 MAC 地址和 SAP 地址	**dlsw reachable**
取消前面配置的可达信息	**undo dlsw reachable**
配置路由器远端可达信息	**dlsw reachable-cache**
取消前面配置的可达信息	**undo dlsw reachable-cache**

11.3 DLSw 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 DLSw 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 DLSw 进行调试。

表11-40 DLSw 显示和调试

操作	命令
显示接口桥组信息	**display dlsw bridge-entry** [*interface-type interface-number*]
显示性能交换信息	**display dlsw information** [**local**] [*ip-address*]
显示虚电路信息	**display dlsw circuits** [*circuit-Id*] [**verbose**]
显示远端对等体信息	**display dlsw remote** [*ip-address*]
显示 DLSw 的可达信息列表	**display dlsw reachable-cache**
显示 LLC2 的统计信息	**display llc2**
清除虚电路信息	**reset dlsw circuits** [*circuit-id*]
清除接口桥组信息	**reset dlsw bridge-entry**
清除 DLSw 的可达信息列表	**reset dlsw reachable-cache**
打开 DLSw 调试信息开关	**debugging dlsw** { **circuit** [*correlator*] | **tcp** [*ip-address*] | **reachable-cache** }
关闭 DLSw 调试信息开关	**undo debugging dlsw** { **circuit** [*correlator*] | **tcp** [*ip-address*] | **reachable-cache** }
打开 LLC2 调试信息开关	**debugging llc2 circuit** [*correlator*]
关闭 LLC2 调试信息开关	**undo debugging llc2 circuit** [*correlator*]
打开 SDLC 调试信息开关	**debugging sdlc** { **all** | **event** | **packet** }
关闭 SDLC 调试信息开关	**undo debugging sdlc** { **all** | **event** | **packet** }

11.4 DLSw 典型配置案例

11.4.1 LAN—LAN 的 DLSw 配置

1. 组网需求

采用 LAN—LAN 方式工作。IP 跨越广域网，将两个运行 SNA 的 LAN 连接起来。

2. 组网图

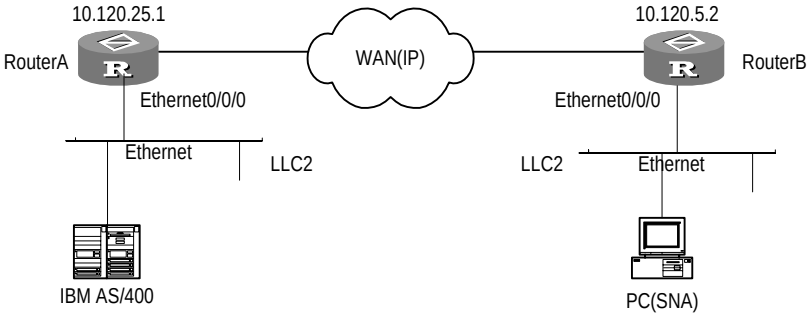


图11-2 LAN—LAN 的 DLSw 配置组网图

3. 配置步骤

路由器 A 的配置：

```
[Quidway] bridge enable
[Quidway] bridge 5 enable
[Quidway] dlsw local 10.120.25.1
[Quidway] dlsw remote 10.120.5.2
[Quidway] dlsw bridge-set 5
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] bridge-set 5
```

路由器 B 的配置：

```
[Quidway] bridge enable
[Quidway] bridge 7 enable
[Quidway] dlsw local 10.120.5.2
[Quidway] dlsw remote 10.120.25.1
[Quidway] dlsw bridge-set 7
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] bridge-set 7
```

这样两个跨越 WAN 的 LAN 就被连接起来。注意这里没有将 IP 相关的命令写出来，配置 DLSw 首先要保证配置的 local 和 remote 之间的 IP 地址可以 **ping** 通，以下均同。

11.4.2 SDLC—SDLC 的 DLSw 配置

1. 组网需求

采用 SDLC—SDLC 工作方式，将两个跨越 WAN 的 SDLC 就被连接起来。

2. 组网图

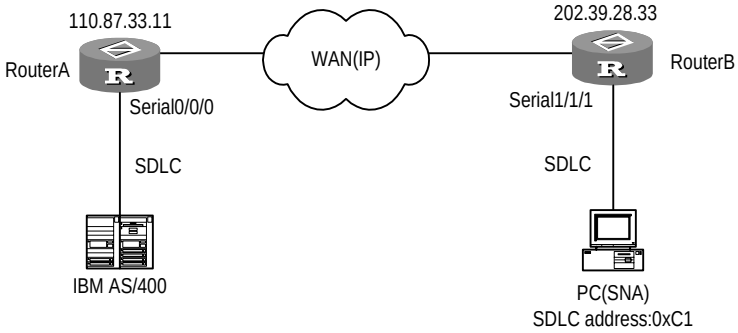


图11-3 SDLC—SDLC 的 DLSw 配置的组网图

3. 配置步骤

路由器 A 的配置：

```
[Quidway] bridge enable
[Quidway] bridge 1 enable
[Quidway] dlsw local 110.87.33.11
[Quidway] dlsw remote 202.39.28.33
[Quidway] dlsw bridge-set 1
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sdlc
[Quidway-Serial0/0/0] baudrate 9600
[Quidway-Serial0/0/0] code nrzi
[Quidway-Serial0/0/0] sdlc status secondary
[Quidway-Serial0/0/0] sdlc mac-map local 0000-1111-0000
[Quidway-Serial0/0/0] sdlc controller c1
[Quidway-Serial0/0/0] sdlc mac-map remote 0000-2222-00c1 c1
[Quidway-Serial0/0/0] bridge-set 1
```

路由器 B 的配置：

```
[Quidway] bridge enable
[Quidway] bridge 1 enable
[Quidway] dlsw local 202.39.28.33
[Quidway] dlsw remote 110.87.33.11
[Quidway] dlsw bridge-set 1
[Quidway] interface serial 1/1/1
[Quidway-Serial1/1/1] link-protocol sdlc
```

```
[Quidway-Serial1/1/1] baudrate 9600
[Quidway-Serial1/1/1] code nrzi
[Quidway-Serial1/1/1] sdlc status primary
[Quidway-Serial1/1/1] sdlc mac-map local 0000-2222-0000
[Quidway-Serial1/1/1] sdlc controller c1
[Quidway-Serial1/1/1] sdlc mac-map remote 0000-1111-00c1 c1
[Quidway-Serial1/1/1] bridge-set 1
```

这样两个跨越 WAN 的 SDLC 就被连接起来。

11.4.3 SDLC—LAN 远端介质转换 DLSw 的配置

1. 组网需求

本例是一个典型的 SDLC—LAN 的 DLSw 转换配置，SDLC 带多点支持。其中所接节点 C1、C2 为 PU2.0 类型节点(ATM)，C3 为 PU2.1 类型节点(OS2)；与多路复用器连接的端口采用 NRZ 编码，连接 PC3 的端口采用 NRZI 编码。

2. 组网图

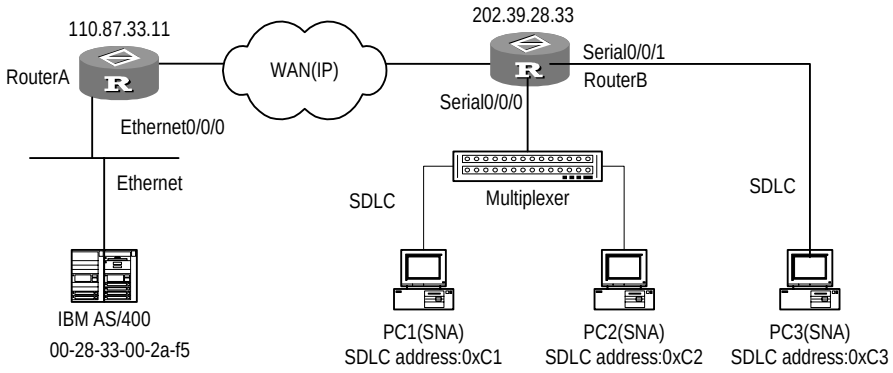


图11-4 SDLC—LAN 的配置图

3. 配置步骤

路由器 A 的配置：

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

路由器 B 的配置：

```
[Quidway] bridge enable
[Quidway] bridge 1 enable
```

```
[Quidway] dlsw local 202.39.28.33
[Quidway] dlsw remote 110.87.33.11
[Quidway] dlsw bridge-set 1
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol sdlc
[Quidway-Serial0/0/0] baudrate 9600
[Quidway-Serial0/0/0] sdlc status primary
[Quidway-Serial0/0/0] sdlc mac-map local 0000-1234-5600
[Quidway-Serial0/0/0] sdlc controller c1
[Quidway-Serial0/0/0] sdlc xid c1 03e00001
[Quidway-Serial0/0/0] sdlc mac-map remote 0014-cc00-54af c1
[Quidway-Serial0/0/0] sdlc controller c2
[Quidway-Serial0/0/0] sdlc xid c2 03e00002
[Quidway-Serial0/0/0] sdlc mac-map remote 0014-cc00-54af c2
[Quidway-Serial0/0/0] bridge-set 1
[Quidway-Serial0/0/0] interface serial 0/0/1
[Quidway-Serial 0/0/1] link-protocol sdlc
[Quidway-Serial 0/0/1] baudrate 9600
[Quidway-Serial 0/0/1] code nrzi
[Quidway-Serial 0/0/1] sdlc status primary
[Quidway-Serial 0/0/1] sdlc mac-map local 0000-2222-0000
[Quidway-Serial 0/0/1] sdlc controller c3
[Quidway-Serial 0/0/1] sdlc mac-map remote 0014-cc00-54af c3
[Quidway-Serial 0/0/1] bridge-set 1
[Quidway-Serial 0/0/1] quit
```

若本地及远端网络比较稳定，可以增加下面的配置，以减少探询过程。

```
[Quidway] dlsw reachable mac-exclusivity
[Quidway] dlsw reachable-cache 0014-cc00-54af remote 110.87.33.11
```

需要注意的是：在配置路由器 B 时，**sdlc mac-map remote** 和 **dlsw reachable-cache** 的 MAC 地址就是 AS/400 的网卡的 MAC 地址，不过由于以太网和 Token-Ring 上的字位顺序相反，所以配置的 MAC 地址应反转配置。如果对端的是 Token-Ring，则不必反转配置。对于配置在主机通道一侧的虚 MAC 地址也不必反转。上例中 c1、c2 为 PU2.0 类型设备，c3 为 PU2.1 类型设备。

11.4.4 DLSw 支持 VLAN 配置举例

1. 组网需求

LSW 的端口 ethernet0/0/0 与 IBM 主机相连，端口 ethernet0/0/1 与 RouterA 相连。ethernet0/0/0 加入 VLAN1，ethernet0/0/1 设置为 Trunk 模式并许可 ethernet0/0/0 的 VLAN1 通过；RouterA 配置子接口并将该子接口加入 VLAN1，则 IBM 主机与 RouterA 仍可以正常通信。

此时，由于有 VLAN 的作用，IBM 主机与 RouterA 之间的报文不会被交换机随意广播，可以提高通讯的安全性。

2. 组网图

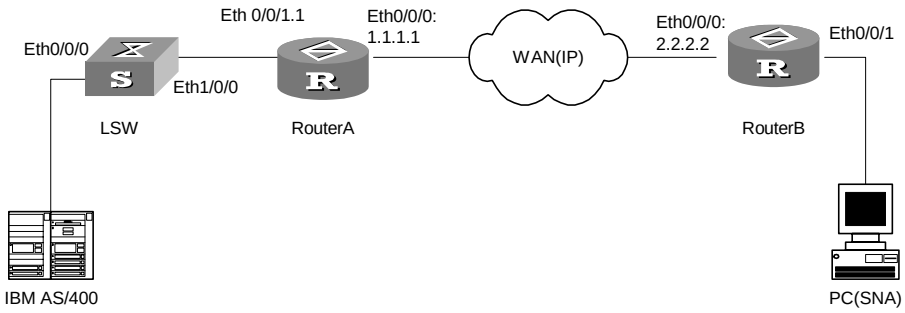


图11-5 DLSw 支持 VLAN 配置举例

3. 配置步骤

(1) 配置 RouterA

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] dlsw enable
[RouterA] dlsw local 1.1.1.1
[RouterA] dlsw remote 1.1.1.2
[RouterA] dlsw bridge 1
[RouterA] interface ethernet 0/0/1.1
[RouterA-Ethernet0/0/1.1] vlan dot1q vid 1
[RouterA-Ethernet0/0/1.1] bridge 1
[RouterA-Ethernet0/0/1.1] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] ip address 1.1.1.1 255.255.0.0
[RouterA-Ethernet0/0/0] quit
[RouterA] ip route-static 2.2.2.2 16 ethernet 0/0/0
```

(2) 配置 RouterB

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] dlsw enable
[RouterB] dlsw local 1.1.1.1
[RouterB] dlsw remote 1.1.1.2
[RouterB] dlsw bridge 1
[RouterB] interface ethernet 0/0/1
[RouterB-Ethernet0/0/1] bridge 1
[RouterB-Ethernet0/0/1] ip address 2.2.2.2 255.255.0.0
[RouterA-Ethernet0/0/0] quit
[RouterA] ip route-static 1.1.1.1 16 ethernet 0/0/0
```

(3) 配置 LSW

创建 VLAN1 并进入其视图并加入端口 Ethernet0/0/0。

```
[Quidway] vlan 1
[Quidway-vlan1] port ethernet0/0/0
[Quidway-vlan1] quit
```

配置 ethernet1/0/0 为 trunk 口，并允许 VLAN1 通过。

```
[Quidway] interface ethernet1/0/0
[Quidway-Ethernet1/0/0] port link-type trunk
[Quidway-Ethernet1/0/0] port trunk permit vlan 1
```

11.5 DLSw 故障的诊断与排除

DLSw 的正常通讯需要参与通讯的两个 SNA 设备和两台运行 DLSw 的路由器之间能够很好的配合，任何两点之间配合有问题都可能导致连接失败。

故障之一 :无法建立 TCP 通道，**dispaly dlsw remote** 时显示状态是 DISCONNECT

建立 TCP 连接是 DLSw 连接成功的第一步。如果不能建立 TCP 连接，是两个路由器之间的问题，一般是 IP 路由配置有问题。可以用带源地址的 **ping** 命令检查 remote 的 IP 地址是否是可达的，也可使用 **display ip routing-table** 检查是否有到达该网段的路由。当双方都建立了正确的路由后，就能够建立 TCP 连接。

故障之二：无法正确建立 circuit，**display dlsw circuit** 时，虚电路无法达到 CONNECTED 状态

不能建立 circuit 的原因有很多。首先要确保到对端的 TCP 通道建立成功。当 TCP 连接能够成功建立，而无法建立 circuit 时，一般是路由器和 SNA 设备之间配合有问题，主要是 SDLC 配置有问题。

首先打开 SDLC 调试开关，观察 SDLC 接口是否能够正常的收发报文，通过 **display interface** 命令可以观察接口上收发报文的情况。如果不能正确的收发报文，一般是接口的编码方式、波特率或时钟配置有问题。一般可以通过修改路由器的接口配置参数或调整 SDLC 设备的配置参数解决。

如果报文收发正确，检查 PU 类型的配置是否正确。可以用 **sdlc xid** 命令来配置 XID，改变对 PU 类型的设置。

如果报文收发正确，就用 **display dlsw circuit verbose** 命令检查，看虚电路能否进入 CIRCUIT_EST 状态。如果一直不能达到 CIRCUIT_EST，说明配置的虚 MAC 地址和 remote 配合有问题。一般可以通过修改 sdlc mac-map remote 等配置参数解决。

如果 circuit 可以达到 CIRCUIT_EST 状态，但不能达到 CONNECTED 状态，说明路由器的 SDLC 的配置和 SNA 设备之间的配置不匹配，检查两端的 SDLC 设备的

配置和路由器的配置，如 SNA 设备的 XID 是否配置正确（PU2.1），路由器的 XID 配置是否正确（PU2.0）。如果配置没有问题，检查 SDLC 主设备一端（如 AS/400 或 S390）的 SDLC 线路是否激活。有时需要手工激活 SDLC 线路才能通讯。

第12章 QLLC 配置

12.1.1 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。）

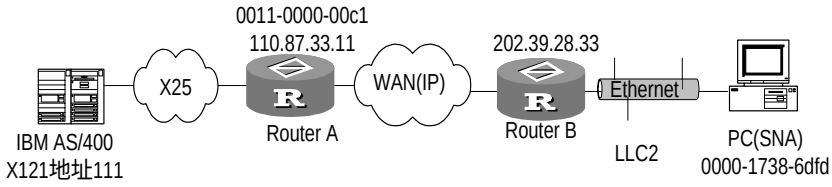


图12-1 QLLC 典型组网图

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。

12.1.2 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12-1 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。

12.1.3 QLLC 的显示和调试

请在用户视图下进行下来操作。

表12-2 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 }**

12.1.4 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

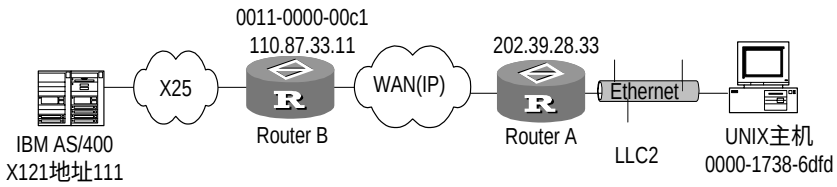


图12-2 QLLC 典型配置组网图

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

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

(2) 路由器 B 的配置

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

第13章 SOT 配置

13.1 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 13-1所示：

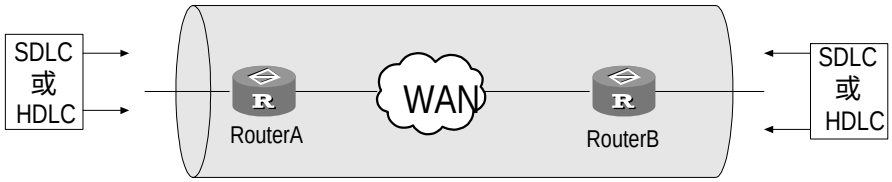


图13-1 Simple SOT Mode

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 13-2所示：

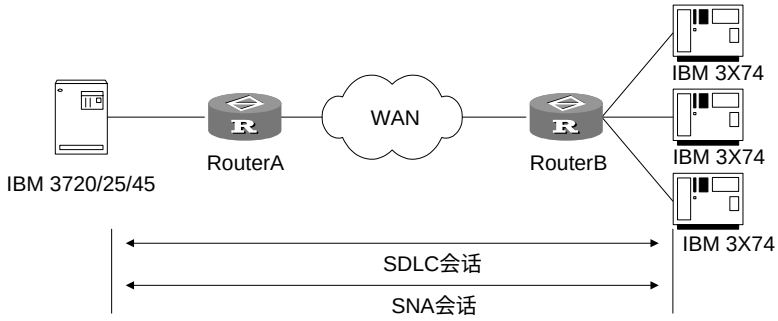


图13-2 SDLC Pass Through Mode

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 13-3所示：

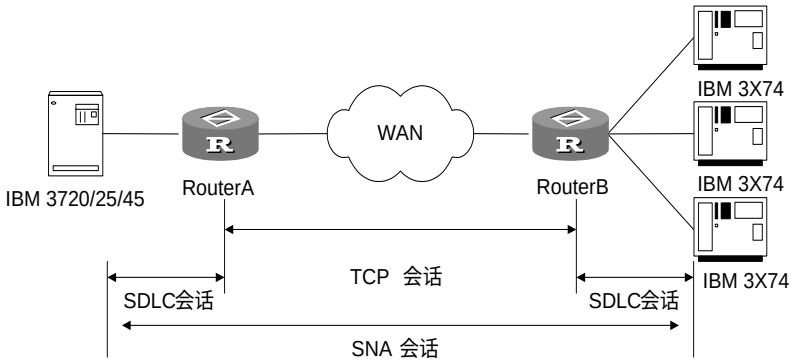


图13-3 SOT local acknowledgment mode

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。

13.2 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

13.2.1 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13-1 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。

13.2.2 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13-2 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13-3 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*

13.2.3 封装 SOT 协议

请在同步串口视图下进行下列配置。

表13-4 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**

13.2.4 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13-5 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*

13.2.5 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13-6 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。

13.2.6 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13-7 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。

13.2.7 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13-8 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13-9 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13-10 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13-11 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13-12 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。

13.3 SOT 的显示和调试

请在所有视图下使用下面命令。

表13-13 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**

13.4 SOT 典型配置举例

13.4.1 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

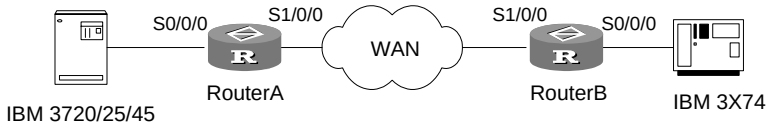


图13-4 SOT 基本模式典型配置举例

3. 配置步骤

(1) 路由器 A

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.1 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.1
[Router] sot group-set 8 simple
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 8
[Router-Serial0/0/0] sot send all tcp 1.0.0.2
[Router-Serial0/0/0] interface serial1/0/0
[Router-Serial1/0/0] ip address 100.1.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 200.2.1.1 serial 1/0/0
```

(2) 路由器 B

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.2 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.2
```

```
[Router] sot group-set 8 simple
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 8
[Router-Serial0/0/0] sot send all tcp 1.0.0.1
[Router-Serial0/0/0] interface serial1/0/0
[Router-Serial1/0/0] ip address 200.2.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 100.1.1.1 serial 1/0/0
```

13.4.2 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

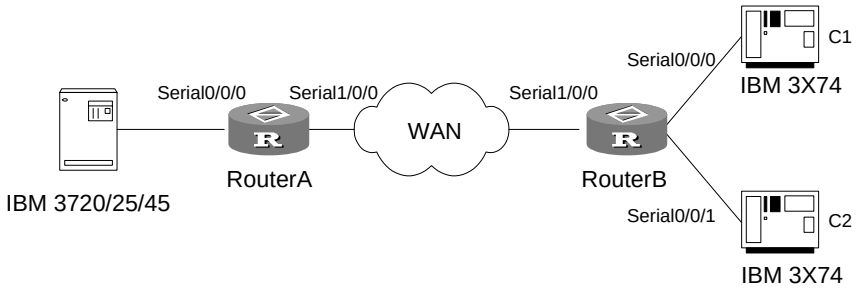


图13-5 SOT 穿透模式典型配置举例

3. 配置步骤

(1) 路由器 A

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.1 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.1
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc controller c1
[Router-Serial0/0/0] sot send address c1 tcp 1.0.0.2
[Router-Serial0/0/0] sot sdlc controller c2
```

```
[Router-Serial0/0/0] sot send address c2 tcp 1.0.0.2
[Router-Serial0/0/0] interface serial1/0/0
[Router-Serial1/0/0] ip address 100.1.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 200.2.1.1 serial 1/0/0
```

(2) 路由器 B

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.2 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.2
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc controller c1
[Router-Serial0/0/0] sot send address c1 tcp 1.0.0.1
[Router-Serial0/0/0] interface serial0/0/1
[Router-Serial0/0/1] link-protocol sot
[Router-Serial0/0/1] sot gather 1
[Router-Serial0/0/1] sot sdlc controller c2
[Router-Serial0/0/1] sot send address c2 tcp 1.0.0.1
[Router-Serial0/0/1] interface serial1/0/0
[Router-Serial1/0/0] ip address 200.2.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 100.1.1.1 serial 1/0/0
```

13.4.3 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

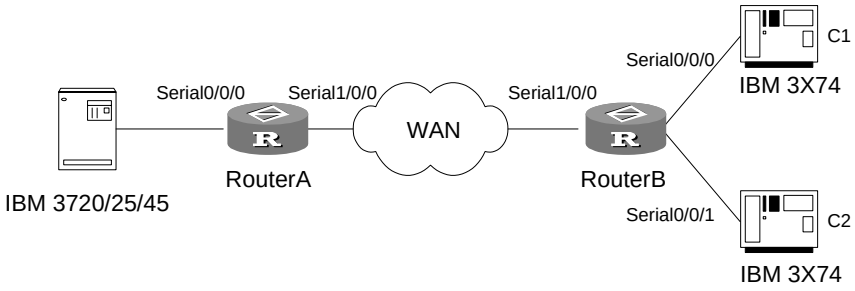


图13-6 SOT 穿透模式下的广播发送方式配置举例

3. 配置步骤

(1) 路由器 A

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.1 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.1
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc-status secondary
[Router-Serial0/0/0] sot sdlc broadcast
[Router-Serial0/0/0] sot send address ff tcp 1.0.0.2
[Router-Serial0/0/0] interface serial1/0/0
[Router-Serial1/0/0] ip address 100.1.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 200.2.1.1 serial 1/0/0
```

(2) 路由器 B

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.2 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.2
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc-status secondary
[Router-Serial0/0/0] sot sdlc broadcast
[Router-Serial0/0/0] sot send address ff tcp 1.0.0.1
[Router-Serial0/0/0] interface serial0/0/1
[Router-Serial0/0/1] link-protocol sot
```

```
[Router-Serial0/0/1] sot gather 1
[Router-Serial0/0/1] sot sdlc-status secondary
[Router-Serial0/0/1] sot sdlc broadcast
[Router-Serial0/0/1] sot send address ff tcp 1.0.0.1
[Router-Serial0/0/1] interface serial1/0/0
[Router-Serial1/0/0] ip address 200.2.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 100.1.1.1 serial 1/0/0
```

13.4.4 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

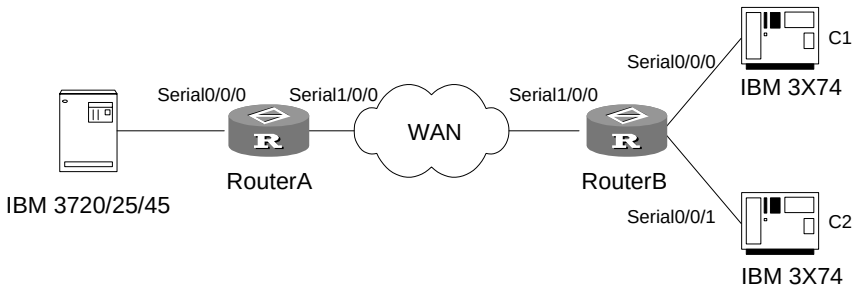


图13-7 SOT 本地应答模式的配置举例

3. 配置步骤

(1) 路由器 A

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.1 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.1
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc-status secondary
[Router-Serial0/0/0] sot sdlc controller c1
[Router-Serial0/0/0] sot send address c1 tcp 1.0.0.2 local
[Router-Serial0/0/0] sot sdlc controller c2
```

```
[Router-Serial0/0/0] sot send address c2 tcp 1.0.0.2 local
[Router-Serial0/0/1] interface serial1/0/0
[Router-Serial1/0/0] ip address 200.2.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 100.1.1.1 serial 1/0/0
```

(2) 路由器 B

```
[Router] interface loopback 0
[Router-LoopBack0] ip address 1.0.0.2 24
[Router-LoopBack0] quit
[Router] sot peer 1.0.0.2
[Router] sot group-set 1 sdlc
[Router] interface serial0/0/0
[Router-Serial0/0/0] link-protocol sot
[Router-Serial0/0/0] sot gather 1
[Router-Serial0/0/0] sot sdlc-status primary
[Router-Serial0/0/0] sot sdlc controller c1
[Router-Serial0/0/0] sot send address c1 tcp 1.0.0.1 local
[Router-Serial0/0/0] interface s0/0/1
[Router-Serial0/0/1] link-protocol sot
[Router-Serial0/0/1] sot gather 1
[Router-Serial0/0/1] sot sdlc-status primary
[Router-Serial0/0/1] sot sdlc controller c2
[Router-Serial0/0/1] sot send address c2 tcp 1.0.0.1 local
[Router-Serial0/0/1] interface serial1/0/0
[Router-Serial1/0/0] ip address 200.2.1.1 16
[Router-Serial1/0/0] quit
[Router] ip route-static 100.1.1.1 serial 1/0/0
```