

## 网络协议配置

# 目 录

|                           |    |
|---------------------------|----|
| 第 1 章 配置IP寻址.....         | 1  |
| 1.1 IP寻址任务列表.....         | 1  |
| 1.2 IP寻址任务.....           | 1  |
| 1.2.1 在网络接口配置IP地址 .....   | 1  |
| 1.2.2 配置地址解析.....         | 3  |
| 1.2.3 配置一个路由进程.....       | 5  |
| 1.2.4 配置广播报文处理.....       | 5  |
| 1.2.5 检测和维护IP寻址 .....     | 7  |
| 1.3 IP寻址示例.....           | 7  |
| 第 2 章 配置NAT.....          | 8  |
| 2.1 NAT概述.....            | 8  |
| 2.1.1 NAT应用.....          | 8  |
| 2.1.2 NAT的优点 .....        | 8  |
| 2.1.3 NAT术语.....          | 9  |
| 2.1.4 NAT规则匹配顺序.....      | 9  |
| 2.2 NAT配置任务表.....         | 9  |
| 2.2.1 翻译内部源地址 .....       | 10 |
| 2.2.2 内部全局地址的重载.....      | 12 |
| 2.2.3 翻译重叠地址.....         | 13 |
| 2.2.4 提供TCP负载均衡.....      | 14 |
| 2.2.5 改变翻译超时及限制连接数目 ..... | 15 |
| 2.2.6 监视和维护NAT .....      | 16 |
| 2.2.7 NAT快速转发.....        | 16 |
| 2.3 NAT配置示例 .....         | 17 |
| 2.3.1 动态内部源转换示例.....      | 17 |
| 2.3.2 内部全局地址重载示例 .....    | 17 |
| 2.3.3 转换重叠地址举例 .....      | 18 |
| 2.3.4 TCP负载分配示例.....      | 18 |
| 2.3.5 翻译H323 配置示例 .....   | 19 |
| 2.3.6 网吧应用示例.....         | 20 |
| 2.3.7 快速NAT应用示例 .....     | 22 |
| 第 3 章 配置DHCP.....         | 26 |
| 3.1 DHCP概述.....           | 26 |
| 3.1.1 DHCP应用 .....        | 26 |
| 3.1.2 DHCP的优点 .....       | 26 |
| 3.1.3 DHCP术语 .....        | 26 |

|                                              |    |
|----------------------------------------------|----|
| 3.2 配置DHCP Client .....                      | 27 |
| 3.2.1 DHCP Client配置任务列表.....                 | 27 |
| 3.2.2 DHCP Client配置任务 .....                  | 27 |
| 3.2.3 DHCP Client配置示例 .....                  | 28 |
| 3.3 配置DHCP Server.....                       | 29 |
| 3.3.1 DHCP 配置任务列表.....                       | 29 |
| 3.3.2 DHCP 配置任务 .....                        | 29 |
| 3.3.3 DHCP Server配置示例 .....                  | 32 |
| 3.3.4 dns-server 192.168.1.3 61.2.2.10 ..... | 32 |
| 3.4 配置DHCP Relay .....                       | 32 |
| 3.4.1 DHCP Relay配置任务列表.....                  | 32 |
| 3.4.2 DHCP Relay配置任务 .....                   | 33 |
| 3.4.3 DHCP Relay配置示例 .....                   | 33 |
| 第4章 配置DNS.....                               | 34 |
| 4.1 DNS概述 .....                              | 34 |
| 4.2 DNS应用 .....                              | 34 |
| 4.3 DNS术语 .....                              | 35 |
| 4.4 DNS Resolver的配置.....                     | 36 |
| 4.4.1 激活基于DNS的名称地址解析 .....                   | 36 |
| 4.4.2 指定域名服务器地址.....                         | 36 |
| 4.4.3 指定一个默认的域名.....                         | 37 |
| 4.4.4 定义域列表 .....                            | 37 |
| 4.4.5 映射主机名到IP地址.....                        | 38 |
| 4.4.6 设置DNS query的重发次数.....                  | 38 |
| 4.4.7 设置DNS query的超时重发的超时值 .....             | 38 |
| 4.4.8 从缓存里删除主机名称与地址映射项 .....                 | 39 |
| 4.4.9 指定主域名服务器的IP地址 .....                    | 39 |
| 4.4.10 设置DNS Resolver端的主机缓存数目上限.....         | 39 |
| 4.4.11 激活DNS Resolver端的代理服务器功能 .....         | 40 |
| 4.4.12 激活DNS Resolver端的动态更新功能 .....          | 40 |
| 4.4.13 设置周期性更新域名与地址绑定的超时值 .....              | 40 |
| 4.4.14 绑定主机IP地址和域名 .....                     | 40 |
| 4.4.15 花生壳客户端配置功能 .....                      | 41 |
| 4.4.16 软件模块信息显示功能与Debug显示功能需求 .....          | 43 |
| 4.5 DNS Resolver配置示例 .....                   | 43 |
| 第5章 配置IP服务.....                              | 45 |
| 5.1 配置IP服务 .....                             | 45 |
| 5.1.1 管理IP连接 .....                           | 45 |
| 5.1.2 配置性能参数.....                            | 49 |
| 5.1.3 在广域网上配置IP.....                         | 49 |
| 5.1.4 检测和维护IP网络 .....                        | 49 |

---

|                      |    |
|----------------------|----|
| 5.2 配置访问列表 .....     | 51 |
| 5.2.1 过滤IP报文 .....   | 51 |
| 5.2.2 扩展访问列表示例 ..... | 53 |

## 第1章 配置IP寻址

### 1.1 IP寻址任务列表

配置 IP 的一个基本和必需的要求就是要在路由器的网络接口上配置 IP 地址。这样才能激活这个接口，使它可以和其它系统用 IP 进行通信。同时还要确定 IP 网络掩码。

为了配置 IP 寻址功能，需要完成下列各项任务，其中第一项任务是必需的，其它都是可选的。

- 在网络接口配置 IP 地址
- 配置地址解析
- 配置一个路由进程
- 配置广播报文处理
- 检测和维护 IP 寻址

### 1.2 IP寻址任务

#### 1.2.1 在网络接口配置IP地址

IP 地址确定了IP报文可以发送到的目的地址。某些 IP地址是有特殊的意义而被保留的，不能作为主机地址或者是网络地址使用。表 1-1列出了IP地址的范围，以及保留地址和可以使用的IP地址。

表 1-1 IP 地址的范围

| 类别 | 地址或范围                        | 状态     |
|----|------------------------------|--------|
| A  | 0.0.0.0                      | 保留     |
|    | 1.0.0.0 to 126.0.0.0         | 可用     |
|    | 127.0.0.0                    | 保留     |
| B  | 128.0.0.0 to 191.254.0.0     | 可用     |
|    | 191.255.0.0                  | 保留     |
| C  | 192.0.0.0                    | 保留     |
|    | 192.0.1.0 to 223.255.254     | 可用     |
|    | 223.255.255.0                | 保留     |
| D  | 224.0.0.0 to 239.255.255.255 | 多目广播地址 |

|   |                              |    |
|---|------------------------------|----|
| E | 240.0.0.0 to 255.255.255.254 | 保留 |
|   | 255.255.255.255              | 广播 |

有关 IP 地址的正式描述在 RFC 1166 “Internet 数字”中。 如果希望得到可用的网络地址，和 Internet 服务提供商联系。

一个接口只能拥有一个主 IP 地址。要配置网络接口的主 IP 地址和网络掩码，在接口配置态使用下列命令：

| 命令                                       | 目的          |
|------------------------------------------|-------------|
| <b>ip address</b> <i>ip-address mask</i> | 配置接口的主IP地址。 |

掩码（mask）表示 IP 地址中的网络部分。

**注意：**

我们只支持按网络字节序从最高位开始连续置位的网络掩码。

其它附加、可选的 IP 寻址功能在下面介绍：

- 在网络接口配置多个 IP 地址
- 激活串口上的 IP 处理功能

## 1. 在网络接口配置多个IP地址

每个接口可以拥有多个 IP 地址，包括一个主 IP 地址和任意个从属 IP 地址。在以下几种情况下，需要配置从属 IP 地址：

当一个特定网段中没有足够的 IP 地址时。例如，某个逻辑子网中最多只有 254 个有效 IP 地址，但是需要在实际的物理网络中连接 300 台主机。在路由器或者是访问服务器上配置从属 IP 地址，可以使两个逻辑子网使用同一个物理子网。

许多较早期的网络是基于第二层网桥，而不是被划分成多个子网。正确使用从属 IP 地址可以把这样的网络改造成基于路由的多个子网。在网络中的路由器，通过配置的从属 IP 地址，可以了解同样连接在这个物理网络中的多个子网。

当一个网络的两个子网，被另一个网络在物理上分隔开。这时，可以把这个网络的地址作为从属 IP 地址，从而可以把一个逻辑网络中的两个在物理上被分隔开的网络在逻辑上连接在一起。

**注意：**

如果一个网段上的任意一台路由器配置了一个从属地址，则相同网段上的所有其它路由器也需要配置同样网段的从属 IP 地址。

在网络接口配置多个地址，在接口配置态使用下列命令：

| 命令 | 目的 |
|----|----|
|----|----|

|                                                    |
|----------------------------------------------------|
| <b>ip address</b> <i>ip-address mask secondary</i> |
|----------------------------------------------------|

|                  |
|------------------|
| 在网络接口上配置多个IP 地址。 |
|------------------|

**注意：**

IP 路由协议在发送路由更新信息时，可能会以不同的方式对待从属 IP 地址。

## 2. 激活串口上的IP处理功能

你可能希望一个串口或者是一个隧道接口可以不配置 IP 地址就具备 IP 处理功能。当这样的接口生成一个报文，例如路由更新报文时，它所使用的源地址是你所指定的该路由器的其它接口的有效 IP 地址，这样的接口被称为无编号（unnumbered）接口。路由器还使用被指定接口的 IP 地址来确定哪些路由进程在无编号接口上发送更新报文。下列是使用规则：

封装 HDLC，SLIP，PPP，LAPB 和帧中继的串口，还有隧道接口，都可以不配置 IP 地址就进行 IP 报文处理。但是对于封装帧中继的串口，该串口必须是一个点到点的子接口。对于封装 X.25 和 SMDS 的接口，不能使用这项功能。

这样的接口不能通过 Ping 来确定是否正常，因为该接口没有 IP 地址。可以使用 SNMP 来远程检测接口状态。

**注意：**

在不同主网之间的串行链路上使用这一配置，必须十分小心，任意运行在这条链路上的路由协议，都必须被配置成不广播任何有关子网的信息。

要在无编号串口上激活 IP 处理功能，在接口配置态使用下列命令：

| 命令                                      | 目的                           |
|-----------------------------------------|------------------------------|
| <b>ip unnumbered</b> <i>type number</i> | 在串口或者是隧道接口上不配置IP地址就激活IP处理功能。 |

上述命令中指定的接口，必须是这个路由器的其它某个拥有 IP 地址的接口，而不可以也是一个无编号接口。这个接口还必须是被激活的（在 **show interfaces** 命令的显示中接口是“up”的）。

本章最后“串口配置示例”显示如何配置串口。

### 1.2.2 配置地址解析

IP 实现允许在接口上控制 IP 地址解析和其它一些功能。下面介绍如何配置地址解析：

- 建立地址解析
- 映射主机名称到 IP 地址

## 1. 建立地址解析

一个 IP 设备可以同时有两个地址：本地地址（在本地网段或者是 LAN 唯一标识这台设备）和网络地址（表示设备所属的网络）。本地地址也就是通常所说的链路层地址，因为它是包含在链路层报文头部的，而且是由链路层设备读取、使用的。专业人员通常称之为 MAC 地址，因为链路层中的介质访问控制（MAC）子层是用来处理地址的。

例如，如果要与以太网上的一台设备通信，必须首先知道它的 48 比特 MAC 或者是本地数据链路层地址。从 IP 地址得到本地数据链路层地址的过程称为地址解析（ARP）。从本地链路层地址得到 IP 地址的过程称为反向地址解析（reverse address resolution）。

本系统使用两种形式的地址解析：地址解析协议（ARP）和代理 ARP（proxy ARP）。ARP 和代理 ARP 分别定义在 RFC 826 和 1027 中。

ARP 用于映射 IP 地址到介质或者说是 MAC 地址。已知 IP 地址，ARP 确定相应的 MAC 地址。一旦 MAC 地址被确定，IP 地址/MAC 地址的关系就被保存在 ARP 缓存中以便快速取得。然后 IP 报文就可以被封装在链路层报文中，被发送到网络上去。

设置地址解析包括下列任务：

- 定义一条静态 ARP 缓存
- 激活代理 ARP
- 端口 ARP 扫描

### (1) 定义一条静态 ARP 缓存

ARP 和其它的地址解析协议提供了在 IP 地址和介质地址之间的动态映射。由于大多数主机都支持动态地址解析，所以一般不需要配置静态的 ARP 缓存项。如果必须定义的话，可以在全局配置态定义，在 ARP 缓存中建立一个永久的表项。系统将使用这一表项把 32 比特的 IP 地址翻译成为 48 比特的硬件地址。另外，还可以指定路由器代替其它主机应答 ARP 请求。

动态 ARP 缓存不能超过 2000。

如果不希望 ARP 表项永久存在的话，可以设置 ARP 表项的生存时间。下面的两个表格列出了如何配置静态的 IP 地址/介质地址映射。

在全局配置态，使用下面的其中一条命令：

| 命令                                           | 目的                                |
|----------------------------------------------|-----------------------------------|
| <b>arp ip-address hardware-address</b>       | 在 ARP 缓存中全局地映射一个 IP 地址到介质地址。      |
| <b>arp ip-address hardware-address alias</b> | 指定路由器以自己的介质地址应答对指定 IP 地址的 ARP 请求。 |

在接口配置态使用下述命令：

| 命令                         | 目的                        |
|----------------------------|---------------------------|
| <b>arp timeout seconds</b> | 设置 ARP 缓存项在 ARP 缓存中的超时时间。 |

要显示特定接口的 ARP 超时时间，使用 **show interfaces** 命令。使用 **show arp** 命令来检查 ARP 缓存中的内容。使用 **clear arp-cache** 命令清除 ARP 缓存中所有的表项。

## (2) 激活代理 ARP

系统使用代理 ARP（RFC 1027 定义）帮助没有相应路由的主机得到位于其它网络上的主机的介质地址。例如，当路由器收到一个 ARP 请求，如果路由器发现它所请求的主机和发出 ARP 请求的主机不连在路由器的同一个接口上，而且路由器所有到目的主机的路由都是通过其他接口，而不是收到 ARP 请求的接口，则它将发出一个代理 ARP 应答，回答自己的本地链路层地址。那台主机就会把报文发送给路由器，然后由路由器把它转发到目的主机。代理 ARP 功能缺省是被激活的。

要激活代理 ARP，在接口配置态使用下列命令：

| 命令                  | 目的           |
|---------------------|--------------|
| <b>ip proxy-arp</b> | 在接口上激活代理ARP。 |

## (3) 端口 ARP 扫描

为了简便地获取全网段的静态 ARP 配置，在端口上配置 ARP 扫描，并把扫描到的动态表项都保存为静态表项。扫描时，向端口配置的 IP 地址所在网段全网段发送 ARP 请求，对网段中的每个地址，得到的第一次应答有效，保存为静态表项，后续得到的应答都视为有修改静态表项的企图。该功能在一定程度上可防止病毒 ARP 欺骗引起的以太网不通的问题。

要启用 ARP 扫描，在接口配置态使用下列命令：

| 命令              | 目的           |
|-----------------|--------------|
| <b>arp scan</b> | 在接口上配置ARP扫描。 |

## 2. 映射主机名称到IP地址

任一 IP 地址都可以有一个主机名称与之对应。系统保存了一个可以被 **telnet**, **ping** 等命令使用的主机名到地址的映射缓存。

要指定主机名到地址的映射，在全局配置态使用下列命令：

| 命令                          | 目的             |
|-----------------------------|----------------|
| <b>ip host name address</b> | 静态地映射主机名到IP地址。 |

### 1.2.3 配置一个路由进程

配置到这里，用户可以根据各自网络的需要配置一个或者多个路由协议。路由协议提供有关互联网络的拓扑结构信息。配置 IP 路由协议，例如 **BGP**, **RIP**, **OSPF** 在后面的文档中介绍。

### 1.2.4 配置广播报文处理

广播报文的地址是某个物理网络上的所有主机。网络主机通过特殊的地址识别广播报文。某些协议频繁使用广播报文，其中包括一些重要的 **Internet** 协议。控制广播报文是

IP 网络管理员的一项基本工作。系统支持定向广播，也就是到特定网络的广播。系统不支持到一个网络中所有子网的广播。

某些早期的 IP 实现使用的不是现在的广播地址标准，它们使用全“0”而不是全“1”表示广播地址。因此，系统可以同时识别和接收这两种形式的报文。

- 允许从定向广播到物理广播的翻译
- 转发 UDP 广播报文和协议

## 1. 允许从定向广播到物理广播的翻译

缺省情况下，IP 定向广播报文都将被丢弃，而不被转发。丢弃 IP 定向广播报文使路由器不易受到“拒绝服务”类型的攻击。

用户可以在定向广播转成物理广播的接口上激活 IP 定向广播的转发功能。如果这一转发功能被激活，所有到这个接口所在网络的定向广播报文都将被转发到这个接口，然后作为物理广播报文发送。

用户可以指定一个访问表来控制广播报文的转发。当指定了访问表以后，只有被访问表允许的 IP 报文才可以从定向广播转变到物理广播。

如果要激活 IP 定向广播的转发，在接口配置态使用下列命令：

| 命令                                             | 目的                     |
|------------------------------------------------|------------------------|
| <b>ipdirected-broadcast</b> [access-list-name] | 在一个接口上允许从定向广播到物理广播的翻译。 |

## 2. 转发UDP广播报文和协议

有时，网络主机使用 UDP 广播报文确定地址，配置和名称等信息。如果该主机所在的网络上没有相应的服务器，而一般情况下这些 UDP 报文又不会被转发，则主机无法得到这些信息。为解决这个问题，用户可以在相应的接口上配置把某些类型的广播报文转发到一个帮助地址。一个接口可以配置多个帮助地址。

用户可以指定一个 UDP 目的端口来控制哪些 UDP 报文将被转发。目前，系统缺省转发目的端口是 NetBIOS 名字服务（端口 137）的 UDP 报文。

如果要允许转发并指定目的地址，在接口配置态使用下列命令：

| 命令                               | 目的                  |
|----------------------------------|---------------------|
| <b>ip helper-address</b> address | 允许转发UDP广播报文并指定目的地址。 |

如果要指定转发哪些协议，在全局配置态使用下列命令：

| 命令                                    | 目的               |
|---------------------------------------|------------------|
| <b>ip forward-protocol udp</b> [port] | 指定哪些接口的UDP协议被转发。 |

### 1.2.5 检测和维护IP寻址

要检测和维护网络，执行下列操作：

- 清除缓存，列表和数据库
- 显示系统和网络统计数据

#### 1. 清除缓存，列表和数据库

用户可以清除某个缓存、列表和数据库中的所有内容。当你认为某个缓存、列表或者数据库中的内容无效时，就需要清除它。

下表中的操作与清除缓存、列表和数据库有关，在管理态使用下列命令：

| 命令                     | 目的          |
|------------------------|-------------|
| <b>clear arp-cache</b> | 清除IP ARP缓存。 |

#### 2. 显示系统和网络统计数据

系统可以显示特定的统计数据，如 IP 路由表，缓存和数据库。这些信息可以帮助确定系统资源使用情况，从而解决网络问题。系统还可以显示端点的可到达性以及发出报文在网络中的行进路线。

这些操作都列在下面的表中。这些命令的具体使用方法，请参见“IP 寻径命令”一章。在管理态使用下列命令：

| 命令                                     | 目的               |
|----------------------------------------|------------------|
| <b>show arp</b>                        | 显示ARP表中的内容。      |
| <b>show hosts</b>                      | 显示主机名-IP地址映射缓存表。 |
| <b>show ip interface [type number]</b> | 显示接口状态。          |
| <b>show ip route [protocol]</b>        | 显示路由表的当前状态。      |
| <b>ping {host   address}</b>           | 测试网络端点的可到达性。     |

### 1.3 IP寻址示例

在下面的例子中，串口（serial 1/0）使用了 ethernet1/1 的地址。

```
interface ethernet 1/1
ip address 202.96.2.3 255.255.255.0
interface Serial 1/0
ip unnumbered ethernet 1/1
```

## 第2章 配置NAT

Internet 面临的两个关键问题是 IP 地址空间的缺乏和路由的度量。网络地址翻译(NAT) 是一种允许一个组织的 IP 网络从外部看上去使用不同的 IP 地址空间而不是它实际使用的地址空间的特性。这样, 通过将这些地址转换到全局可路由的地址空间, NAT 允许一个具有非全局可路由地址的组织连接到 Internet。NAT 也允许一个更好的重编码策略, 为组织机构更改服务提供商或自动编码到 CIDR 块。NAT 也在 RFC 1631 中讲述。

### 2.1 NAT概述

#### 2.1.1 NAT应用

NAT 的应用主要有以下几种:

- 需要连接到 Internet 网上, 但是并非所有主机都有唯一的全局 IP 地址。NAT 使得使用非注册的 IP 地址的私有 IP 互联网络能够连接到互联网上。NAT 一般在单连接域 (即内部网络)上和公共网络(即 Internet) 的边界路由器上配置。在发送报文到外部网络之前, NAT 将内部本地地址转换到全局唯一的 IP 地址。
- 必须改变内部地址。可以通过使用 NAT 完成地址的转换, 而无须改变它们, 因为那将费时太多。
- 要实现基本的 TCP 传输负载均衡。可以通过使用 TCP 负载分布特性将单个全局 IP 地址映射到多个本地 IP 地址。
- 作为连接问题的解决方案, 只有在单连接的域中相对少的主机同时与域外通信时, NAT 有实用价值。此时, 只有在需要和外部通信时, 内部少量主机的 IP 才被转换成全局唯一的 IP 地址。当不再使用时这些地址又可以被重新使用。

#### 2.1.2 NAT的优点

NAT 的一个明显的优点是, 在不需要改变主机或路由器的情况下可以进行配置。如上所述, 如果在单连接域中的大量主机与域外通信, NAT 可能是不实用的。并且, 某些使用嵌入式 IP 地址的应用, 也不适用于 NAT 设备来进行翻译。这些应用可能不会透明地工作或者完全 (不经翻译的) 通过一个 NAT 设备。NAT 也隐藏主机的标识, 这可能是一个优点, 也可能是一个缺点。

配置了 NAT 的 router 将至少有一个内部接口和一个外部接口。在一个典型的环境中, NAT 配置于单连接域和骨干域之间的出口 router。当一个报文离开该域时, NAT 将本地有效源地址转换到全局唯一地址。当报文进入到该域时, NAT 将这个全局唯一目的地址转换到本地地址。如果存在多个出口点, 每一个 NAT 必须有相同的转换表。如果地址用完了, 软件不能分配一个地址, 那么它就丢弃该报文, 并发出一个主机不可达的 ICMP 报文。

配置了 NAT 的路由器不应该向外公布本地网络。然而, NAT 从外部收到的路由信息可以像通常那样在单域中公告。

### 2.1.3 NAT术语

如前所述，术语 **inside** 是指某一组织机构所拥有的和必须进行转换的那些网络。在这个域中，主机将会有有一个地址空间中的地址，而在域外，配置 **NAT** 时，它们会在另一个地址空间中拥有地址。第一个地址空间指的是局部地址空间，而第二个地址空间是全局地址空间。

类似地，**outside** 是指单连接网络所连接的那些网络，一般不在一个组织的控制内。就像在后面将要讨论的那样，外部网络中的主机地址也可以/需要翻译为某个地址并且可能有局部地址和全局地址。

总之，**NAT** 使用以下定义：

内部局部地址——在内部网络上一个主机分配到的 **IP** 地址。这个地址可能不是网络信息中心(NIC)或服务提供商所分配的合法 **IP** 地址。

内部全局地址——一个合法的 **IP** 地址(由 **NIC** 或服务供应商分配)，向外部网络描述一个或多个本地 **IP** 地址。

外部局部地址——出现在内部网络的一个外部主机的 **IP** 地址。不一定是合法地址，它可以在内部网络中从可路由的地址空间进行分配。

外部全局地址——主机的拥有者在外部网络上分配给主机的 **IP** 地址。该地址可以从全局可路由地址或网络空间进行分配。

### 2.1.4 NAT规则匹配顺序

**NAT** 在翻译报文时，首先要匹配已配置的 **NAT** 规则。**NAT** 的规则主要有三大类型：内部源地址映射、外部源地址映射和内部目的地址映射，每一个大类型下又有子类型。下面以内部源地址映射为例，介绍 **NAT** 匹配规则子类型的顺序如下：

- (1) 静态 **TCP/UDP** 端口映射规则。
- (2) 静态单个地址映射规则。
- (3) 静态网段映射规则。
- (4) 动态 **POOL** 地址映射规则。
- (5) **PAT** 映射规则。

对于同一大类型下的相同子类的规则，对于三大规则类型之间，则按添加的先后顺序匹配。在 **show running** 时，**NAT** 规则的显示顺序和实际匹配的顺序一样。

## 2.2 NAT配置任务表

在配置任何 **NAT** 翻译之前，必须知道内部局部地址范围和内部全局地址范围。下一节将显示如何使用 **NAT** 执行以下可选任务：

- 翻译内部源地址
- 内部全局地址的重载
- 翻译重叠地址
- 提供 TCP 负载均衡
- 改变翻译超时及限制连接数目
- 监视和维护 NAT

## 2.2.1 翻译内部源地址

与网络外部通信时，使用这个特性将自己的 IP 地址翻译到全局唯一的 IP 地址。可按以下方式配置静态或动态内部源地址翻译：

静态翻译在内部本地地址和内部全局地址之间建立一对一的映射。当一个内部主机必须被一个固定的外部地址访问时，静态转换是有用的。

动态翻译在一个内部本地地址和外部地址池之间建立一种映射。

下图表明一个路由器，它将一个网络内的源地址转换到网络外的源地址：

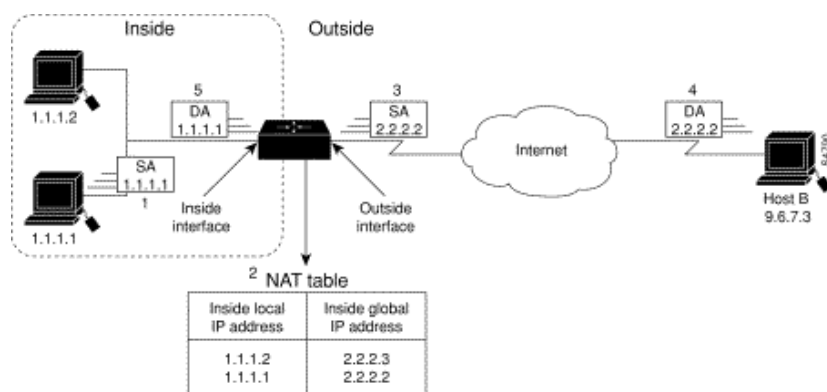


图 2-1 NAT 内部源地址转换

以下步骤描述了内部源地址翻译，如上图所示。

- (1) 主机 1.1.1.1 的用户建立一个到主机 B 的连接。
- (2) 路由器接收的来自主机 1.1.1.1 的第一个数据包使路由器检查它的 NAT 表。  
如果已配置一个静态翻译项，路由器转到第(3)步。  
如果没有翻译项存在，路由器决定源地址(SA) 1.1.1.1 必须动态翻译，然后从动态地址池选择一个合法的、全局地址，最终产生一个翻译项。该类型项称做简单项。
- (3) 路由器用转换项的全局地址替换主机 1.1.1.1 的内部本地源地址，并且转发该报文。
- (4) 主机 B 通过使用内部全局 IP 目的地址(DA)2.2.2.2 接收报文并响应主机 1.1.1.1。

- (5) 路由器收到内部全局 IP 地址的报文时，它将内部全局地址作为一个关键字执行 NAT 表的查询。然后将地址翻译到主机 1.1.1.1 的内部本地地址，并向主机 1.1.1.1 转发报文。

主机 1.1.1.1 接收该报文并继续会话。路由器为每一个报文执行第(2)步到第(5)步。

## 1. 配置静态转换

为了配置静态内部源地址转换，在全局配置方式下执行下列命令：

| 命令                                                           | 目的                        |
|--------------------------------------------------------------|---------------------------|
| <b>ip nat inside source static</b> <i>local-ip global-ip</i> | 在内部局部地址和内部全局地址之间建立一个静态转换。 |
| <b>interface</b> <i>type number</i>                          | 指定内部接口。                   |
| <b>ip nat inside</b>                                         | 将接口标记为连接到内部网的。            |
| <b>interface</b> <i>type number</i>                          | 指定外部接口。                   |
| <b>ip nat outside</b>                                        | 将接口标记为连接到外部网的。            |

以上是配置静态转换。可以配置多个内部和外部接口。

## 2. 配置动态转换

为了配置动态内部源地址翻译，在全局配置方式下执行下列命令：

| 命令                                                                                                    | 目的                      |
|-------------------------------------------------------------------------------------------------------|-------------------------|
| <b>ip nat pool</b> <i>name start-ip end-ip netmask</i>                                                | 按需要定义一个将要分配的地址池。        |
| <b>ip access-list standard</b> <i>access-list-name</i><br><b>permit source</b> [ <i>source-mask</i> ] | 定义一个标准的访问列表，允许哪些地址可以转换。 |
| <b>ip nat inside source list</b> <i>access-list-name</i><br><b>pool</b> <i>name</i>                   | 建立动态源地址转换，指定前一步定义的访问列表。 |
| <b>interface</b> <i>type number</i>                                                                   | 指定内部接口。                 |
| <b>ip nat inside</b>                                                                                  | 将接口标记为连接到内部网的。          |
| <b>interface</b> <i>type number</i>                                                                   | 指定外部接口。                 |
| <b>ip nat outside</b>                                                                                 | 将接口标记为连接到外部网的。          |

**注意：**

访问表必须只允许列那些可以被转换的地址（记住：在每一个访问表的结尾有一个隐含的“deny all”）。太随意的访问表可能导致不可预期的结果。

关于动态内部源地址转换的示例，请参阅本章后面的“动态内部源地址转换举例”一节。

## 2.2.2 内部全局地址的重载

通过允许路由器为多个局部地址使用一个全局地址，可以在内部全局地址池中保存地址。当配置了重载后，路由器从较高级的协议(例如 TCP 或 UDP 端口号)中保持足够的信息，将这个全局地址转换回到正确的局部地址。当多个本地地址映射到一个全局地址时，每一个内部主机的 TCP 或 UDP 端口号用于在诸多本地地址之间区分。

图 2-2 说明了当一个内部全局地址代表多个内部局部地址时的 NAT 操作。TCP 端口号充当区分者。

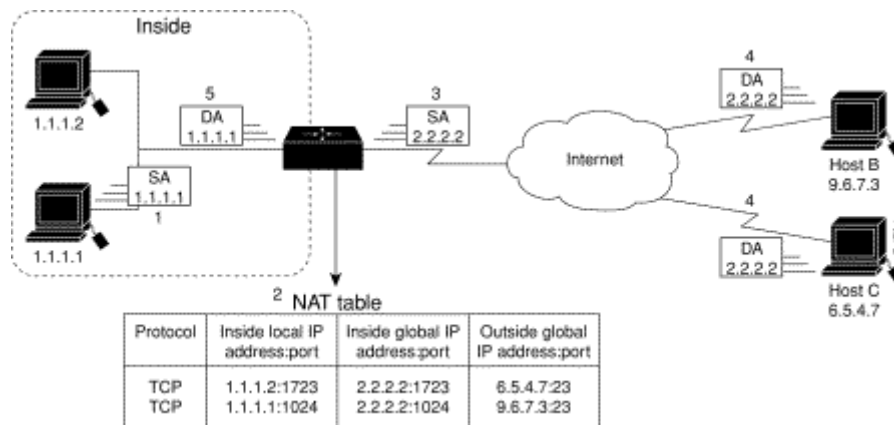


图 2-2 内部全局地址重载时的 NAT 操作

路由器在重载的内部全局地址中执行以下过程所示。主机 B 和主机 C 都认为它们正在与地址为 2.2.2.2 的一个主机会话。而实际上它们正在与不同的主机会话，端口号是区分标识。实际上，使用多个不同的端口号可以使多个内部主机共享一个内部全局 IP 地址。

- (1) 主机 1.1.1.1 的用户发出指令连接到主机 B。
  - (2) 路由器接收来自主机 1.1.1.1 的第一个报文，引起路由器检查它的 NAT 表。
- 如果没有转换项存在，那么路由器决定地址 1.1.1.1 必须进行翻译，并建立一个内部局部地址 1.1.1.1 到合法全局地址的翻译。如果重载起作用，就会启动另一个翻译，路由器从那个翻译中重新使用全局地址，并保存能够转换回来的足够信息。这种项称做扩展项。
- (3) 路由器用所选择的全局地址替换内部局部源地址 1.1.1.1，并转发该数据包。
  - (4) 主机 B 接收该数据包并通过使用内部全局 IP 地址 2.2.2.2 响应主机 1.1.1.1。
  - (5) 路由器用内部全局 IP 地址接收该报文时，它使用协议、内部全局地址和端口，外部地址和端口作为关键字搜索 NAT 表。然后，它转换该地址到内部局部地址 1.1.1.1，并转发该报文到主机 1.1.1.1。
  - (6) 主机 1.1.1.1 接收该报文并继续对话。路由器为每一个报文执行第(2)到第(5)步。

为配置内部全局地址的重载，在全局配置方式下执行下列命令：

| 命令 | 目的 |
|----|----|
|----|----|

|                                                                             |                         |
|-----------------------------------------------------------------------------|-------------------------|
| <b>ip nat pool name start-ip end-ip netmask</b>                             | 按需要定义一个将要分配的全局地址池。      |
| <b>ip access-list standard access-list-name permit source [source-mask]</b> | 定义一个标准访问列表。             |
| <b>ip nat inside source list access-list-name pool name overload</b>        | 建立动态源地址转换，确定在前一步定义的访问表。 |
| <b>interface type number</b>                                                | 指定内部接口                  |
| <b>ip nat inside</b>                                                        | 将接口标记为连接到内部网的。          |
| <b>interface type number</b>                                                | 指定外部接口。                 |
| <b>ip nat outside</b>                                                       | 将接口标记为连接到外部网的。          |

注意：

访问表必须只允许列出那些将要被转换的地址（请记住在每一个访问表的结尾有一个隐含的“deny all”）。太随意的访问表可能导致不可预期的结果。

关于内部全局地址重载的示例，请参阅本章后面的“内部全局地址重载”示例一节。

### 2.2.3 翻译重叠地址

当一个内部本地地址与所想连接的外部地址相同时，就发生了地址重叠。图 2-3显示了 NAT如何翻译重叠地址的网络环境。

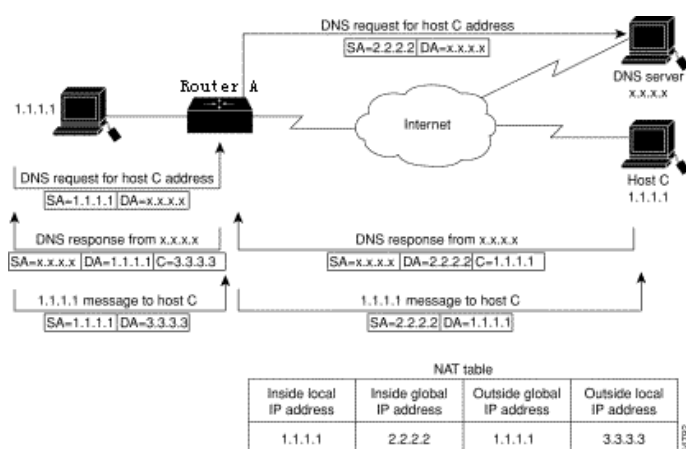


图 2-3 NAT 翻译重叠地址的网络环境示意图

当翻译重叠地址的时候，路由器执行以下步骤：

- (1) 主机 1.1.1.1 的用户用域名发出指令连接到主机 C，从 DNS 服务器请求域名到地址的检查。
- (2) DNS 服务器有回应，把主机 C 的地址 1.1.1.1 返回。路由器截取 DNS 应答报文，并从外部本地地址池中选择一个外部本地地址代替源地址，此处是将源地址 1.1.1.1 替换为 3.3.3.3。

- (3) 路由器建立地址转换映射表，内部本地地址和内部全局地址互相映射，外部全局地址和外部本地地址互相映射。
- (4) 主机 1.1.1.1 向主机 C 发送的报文，目的 IP 地址就是外部本地地址 3.3.3.3。
- (5) 而当路由器 A 收到目的为外部本地地址的报文时，就把本地地址转换为全局地址。
- (6) 主机 C 接收数据包并继续会话。

## 2.2.4 提供TCP负载均衡

另一种使用NAT的方式是与Internet地址无关的。你的机构可能有多个主机必须与一个频繁使用的主机通信。使用NAT，在内部网上建立一个虚拟主机用于在那些真实主机中协调负载均衡。匹配一个访问列表的目的地地址用循环地址池中的地址替换。分配是在一个循环中完成的，且只当打开了一个从外部到内部的新连接时。非TCP的通信不用经过翻译(除非其他翻译有效)。图 2-4说明了这个特性。

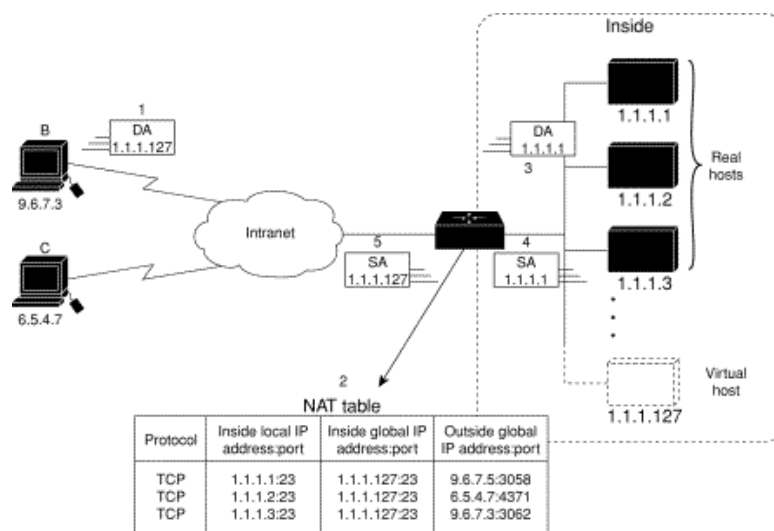


图 2-4 NAT TCP 负载均衡

当翻译循环地址时，路由器执行以下步骤：

- (1) 在主机 B(9.6.7.3)上的用户发出指令连接到 1.1.1.127 上的虚拟主机。
- (2) 路由器接收连接请求并建立一个新的翻译项，为内部本地 IP 地址分配下一个主机 (1.1.1.1)。
- (3) 路由器用所选的实际主机地址替换目标地址并转发该报文。
- (4) 主机 1.1.1.1 接收报文并且响应。
- (5) 路由器接收该报文，并使用内部本地地址和端口号以及外部地址和端口号作为关键字检查 NAT 表。路由器然后转换源地址到虚拟主机地址并且转发该报文。
- (6) 下一个连接请求将引起路由器为内部本地地址分配 1.1.1.2。为了配置目标地址转换，在全局配置方式下执行下列命令。这些命令允许映射一个虚拟主机到多个真实

主机。每一个与虚拟主机打开的新的 TCP 会话都将转换成与不同的真实主机的会话。

| 命令                                                                                    | 目的                       |
|---------------------------------------------------------------------------------------|--------------------------|
| <b>ip nat pool</b> name start-ip end-ip netmask                                       | 定义一个包含真实主机的地址池。          |
| <b>ip access-list standard</b> access-list-name<br><b>permit</b> source [source-mask] | 定义允许虚拟主机地址的一个访问表。        |
| <b>ip nat inside destination list</b><br>access-list-name <b>pool</b> name            | 建立动态内部目标转换，确定在前一步定义的访问表。 |
| <b>interface</b> type number                                                          | 指定内部接口。                  |
| <b>ip nat inside</b>                                                                  | 把接口标记为连接到内网部的。           |
| <b>interface</b> type number                                                          | 指定外部接口。                  |
| <b>ip nat outside</b>                                                                 | 把接口标记为连接到外部网的。           |

注意：

访问表必须只允许列出那些可以被转换的地址（记住：在每一个访问表的结尾有一个隐含的“deny all”）。太随意的访问表可能导致不可预期的结果。

有关循环转换的示例可参看本章末尾的“TCP 负载分配举例”。

## 2.2.5 改变翻译超时及限制连接数目

缺省时，在经过一段时间的空闲后，动态地址翻译会超时。如果需要可以改变超时的缺省值。当重载没有配置时，在 1 小时后简单的翻译项就会超时。为了改变这个值，在全局配置方式下执行下列命令：

| 命令                                        | 目的                  |
|-------------------------------------------|---------------------|
| <b>ip nat translation timeout</b> seconds | 改变不使用重载的动态地址翻译的超时值。 |

如果配置了重载，就会对翻译超时有一个较好的控制，因为每一项包含了更多的内容。在扩展项中改变超时，在全局配置方式下执行下面一条或多条命令：

| 命令                                               | 目的                            |
|--------------------------------------------------|-------------------------------|
| <b>ip nat translation udp-timeout</b> seconds    | 改变UDP超时值(缺省值5分钟)。             |
| <b>ip nat translation dns-timeout</b> seconds    | 改变DNS超时值(缺省值1分钟)。             |
| <b>ip nat translation tcp-timeout</b> seconds    | 改变TCP超时值(缺省值1小时)。             |
| <b>ip nat translation icmp-timeout</b> seconds   | 设置ICMP的NAT超时时间(缺省值是60秒)。      |
| <b>ip nat translation syn-timeout</b> seconds    | 设置TCP SYN状态的NAT超时时间（缺省值是60秒）。 |
| <b>ip nat translation finrst-timeout</b> seconds | 改变TCP FIN or RST超时值(缺省值1分钟)。  |

限制 NAT 的连接数目主要有三种方式，在全局配置方式下执行下列命令可以实现这三种方式：

| 命令                                                                | 目的                                                       |
|-------------------------------------------------------------------|----------------------------------------------------------|
| <b>ip nat translation max-entries</b> <i>numbers</i>              | 设置NAT的最大翻译条目数(缺省值是4000)。                                 |
| <b>ip nat translation max-entries host</b> A.B.C.D <i>numbers</i> | 针对指定的内部IP地址, 限制该IP地址能建立NAT连接表项的最大数目, 无缺省值。               |
| <b>ip nat translation max-entries host any</b> <i>numbers</i>     | 针对所有的内部IP地址, 限制单个IP地址能建立NAT连接表项的最大数目, 缺省值与max-entries相同。 |

## 2.2.6 监视和维护NAT

缺省时, 动态地址翻译将按 NAT 转换表所规定的时间超时。可以在超时前, 通过在管理态方式下执行下列命令清除超时项:

| 命令                                                                                                                                                   | 目的                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>clear ip nat translation *</b>                                                                                                                    | 从NAT转换表中清除所有动态地址转换项。                 |
| <b>clear ip nat translation inside</b> <i>local-ip global-ip</i> [ <i>outside local-ip global-ip</i> ]                                               | 清除一个包含内部翻译, 或者既有内部翻译也有外部翻译的简单的动态翻译项。 |
| <b>clear ip nat translation outside</b> <i>local-ip global-ip</i>                                                                                    | 清除包含外部翻译的简单的动态翻译项。                   |
| <b>clear ip nat translation inside</b> <i>local-ip local-port global-ip global-port</i> [ <i>outside local-ip local-port global-ip global-port</i> ] | 清除扩展动态翻译条目。                          |

在管理态方式下通过执行下列任一条命令, 可以显示转换信息:

| 命令                                                                                            | 目的      |
|-----------------------------------------------------------------------------------------------|---------|
| <b>show ip nat translations</b> [ <i>host A.B.C.D   tcp   udp   icmp</i> ] [ <i>verbose</i> ] | 显示活动翻译。 |
| <b>show ip nat statistics</b>                                                                 | 显示翻译统计。 |

## 2.2.7 NAT快速转发

为提高 IP NAT 的转发性能, 使用 **ip fastnat ito1** 全局配置命令, 开启 ip fast nat 处理流程。该命令的 NO 形式可以恢复正常的 IP NAT 处理流程。

**ip fastnat 1to1 outside** {*interface-type number*} [**backup-outside** {*interface-type number*}] **inside** {*interface-type number*} [**privateservices**] [**extend**]

同时, 使用 **ip fastaccess deny** 端口配置命令, 开启快速访问控制功能, 该命令只能基于传输层 TCP/UDP/ICMP 控制 IP 流。该命令的 NO 形式删除该项访问限制。

**ip fastaccess deny** {*tcp | udp | icmp*} {*port number*}

使用说明:

为提高 IPNAT 转发性能, 简化了很多处理过程, 必然也限制了使用范围:

- 只支持一对一转发，也就是说，在同一时间，报文只能从一个标记为 NAT inside 的接口进入，然后从一个标记 NAT outside 的接口转发出去。
- 支持一个备份端口，只有主线路 down 掉后，报文才能自动从备份线路转发。
- 不支持 IP NAT OUTSIDE SOURCE 规则
- 由于 ip fastaccess 只能基于传输层限制报文转发，如果需要基于 IP 地址限制，则需要用到一般访问列表。

有关快速 NAT 的配置示例可参看本章末尾的“快速 NAT 应用举例”。

## 2.3 NAT配置示例

**建议：**如果需要使用访问列表限制内网用户，如果使用到动态 NAT 规则，则强烈建议利用 NAT 所用的访问列表。特别对于那些需要定义非常多规则的访问列表，这样可以显著提高性能。

### 2.3.1 动态内部源转换示例

以下例子将匹配了访问列表 a1 的所有源地址(192.168.1.0/24) 转换到 NET-208 池中的一个地址。池中地址范围是：171.69.233.208 到 171.69.233.233。

```
ip nat pool net-208 171.69.233.208 171.69.233.233 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface serial1/0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet1/1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
!
```

### 2.3.2 内部全局地址重载示例

下面示例建立了一个名为 NET-208 的地址池。该池包含了从 171.69.233.208 到 171.69.233.233 的地址。访问表 a1 允许源地址从 192.168.1.0 到 192.168.1.255 的数据包。如果没有转换，那么匹配访问表 a1 的包转换到池中的一个地址。路由器允许多个本地地址(从 192.168.1.0 到 192.168.1.255)使用相同的全局地址。路由器保留端口号以区分各个连接。

```
ip nat pool net-208 171.69.233.208 171.69.233.233 255.255.255.240
```

```

ip nat inside source list a1 pool net-208 overload
!
interface serial1/0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet1/1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
!

```

### 2.3.3 转换重叠地址举例

在下面例子中，局部网络中的地址正被 Internet 上的其他人合法地使用。访问那个外部网络需要额外的转换。**net-10** 池是一个外部本地 IP 地址池。语句 **ip nat outside source list 1 pool net-10** 将来自外部重叠网络的主机地址转换到池中的地址。

```

ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208
ip nat outside source list a1 pool net-10
!
interface serial1/0
ip address 171.69.232.192 255.255.255.240
ip nat outside
!
interface ethernet1/1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
!

```

### 2.3.4 TCP负载分配示例

以下例子的目的是定义一个虚拟地址，在一组真实主机中到该地址的连接是分布的。该池定义了真实主机的地址。访问表定义了虚拟地址。来自串口 **1/0**（外部接口）的目的地址与访问列表匹配的 **TCP** 包将翻译成池中的地址。

```

ip nat pool real-hosts 192.168.15.2 192.168.15.15 255.255.255.240
ip nat inside destination list a2 pool real-hosts
!
interface serial1/0

```

```

ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet1/1
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
ip access-list standard a2
permit 192.168.15.1 255.255.255.0

```

### 2.3.5 翻译H323 配置示例

建立 Intranet，在 Intranet 中有若干 H323 网关；内部网与外界联系 IP 网关使用本公司路由器，在网关上运行 H323 NAT 程序。Gatekeeper 放置在内部网中，接受外部网网关的注册。

```

interface FastEthernet1/0
ip address 218.1.119.98 255.255.255.248
ip nat outside
!
interface FastEthernet2/0
ip address 192.168.1.6 255.255.0.0
ip nat inside
!
ip route default 218.1.119.97
!
ip access-list standard nat
permit 192.168.0.0 255.255.0.0
!
ip nat inside source static tcp 192.168.1.11 1720 218.1.119.98 1720
ip nat inside source static udp 192.168.1.10 1718 218.1.119.98 1718
ip nat inside source static udp 192.168.1.10 1719 218.1.119.98 1719
ip nat inside source list nat interface FastEthernet1/0

```

说明：

- (1) 只要 GK 和 GW 在内部网，上述 NAT 规则是必须的，其中 1720 端口主要用来映射 H225 消息；1718 端口映射 GK discovery 消息；1719 映射 RAS 消息；PAT 规则映射 H245 消息和媒体流。
- (2) 如果内部网有多个 GW 和一个 GK，则可以分配 30000—31000 端口给 H323，如下配置：

```

ip nat inside source static udp 192.168.1.10 1718 218.1.119.98 1718
ip nat inside source static udp 192.168.1.10 1719 218.1.119.98 1719
GW1 :
ip nat inside source static tcp 192.168.1.11 1720 218.1.119.98 30000
GW2 :

```

```

ip nat inside source static tcp 192.168.1.12 1720 218.1.119.98 30001
GW3 :
ip nat inside source static tcp 192.168.1.15 1720 218.1.119.98 30002
...

```

## 2.3.6 网吧应用示例

### 1. 动态IP地址

以 ADSL 接入为例，路由器通过以太网接口 **Ethernet0/0** 与内部多个主机连接，而通过接口 **Ethernet0/1** 跟 ADSL Modem 连接。跟 Access Server 建立 PPP 连接，利用 NAT 实现多个主机（192.168.20.0 网段）同时上网的功能以及架设内部私服和 WEB 服务。

配置如下：

```

interface Dialer1
ip address negotiated
no ip directed-broadcast
ppp pap sent-username 8888 888
ip nat outside
ip nat mss
!
interface Ethernet0/0
ip address 192.168.20.1 255.255.255.0
no ip directed-broadcast
ip nat inside
!
interface Ethernet0/1
no ip address
no ip directed-broadcast
pppoe-client Dialer1
!
ip route default Dialer1
!
ip access-list standard nat
permit 192.168.0.0 255.255.255.0
!
ip nat translation dns-timeout 30
ip nat translation icmp-timeout 30
ip nat translation max-entries host any 200
ip nat outside destination static dialer1 192.168.20.100
ip nat inside source static tcp 192.168.20.120 80 dialer1 80
ip nat inside source list nat interface dialer1
!

```

说明：

命令 `ip nat translation max-entries all 200` 限制所有主机能够发起的 NAT 动态翻译表项的最大数目为 200。如果连接路由器是终端用户，此值较为合适；如果不是终端用户，如交换机，则需根据实际应用环境而定。

## 2. 静态IP地址

以以太网接入为例，路由器通过以太网接口 **Ethernet0/0** 与内部多个主机连接，上行接口为 **Ethernet0/1**。利用 NAT 实现多个主机（192.168.20.0 网段）同时上网的功能以及架设内部私服和 WEB 服务。

配置如下：

```
interface Ethernet0/0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Ethernet0/1
 ip address 218.1.119.101 255.255.255.248
 no ip directed-broadcast
 ip nat outside
!
ip route default 218.1.119.97
!
ip access-list standard nat
 permit 192.168.0.0 255.255.255.0
!
ip nat translation dns-timeout 30
ip nat translation icmp-timeout 30
ip nat translation max-entries host any 200
ip nat outside destination static 218.1.119.101 192.168.20.100
ip nat inside source static tcp 192.168.20.120 80 218.1.119.101 80
ip nat inside source list nat interface Ethernet0/1
!
```

说明：

命令 `ip nat translation max-entries host any 200` 限制所有主机能够发起的 NAT 动态翻译表项的最大数目为 200。如果连接路由器是终端用户，此值较为合适；如果不是终端用户，如交换机，则需根据实际应用环境而定。

## 2.3.7 快速NAT应用示例

### 1. 一般应用

配置如下：

Current configuration:

```
!
ip fastnat 1to1 outside FastEthernet0/1 inside FastEthernet0/0
!
interface FastEthernet0/0
 ip address 10.4.3.252 255.255.255.0
/*****快速访问列表*****/
 ip fastaccess deny tcp 420
 ip fastaccess deny tcp 9604
 ip fastaccess deny tcp 113
 ip fastaccess deny tcp 667
 ip fastaccess deny tcp 3067
 ip fastaccess deny tcp 5554
 ip fastaccess deny tcp 9996
 ip fastaccess deny tcp 1068
 ip fastaccess deny tcp 2745
 ip fastaccess deny tcp 135
 ip fastaccess deny tcp 3333
 ip fastaccess deny udp 4444
 ip fastaccess deny tcp 445
 ip fastaccess deny tcp 139
 ip fastaccess deny tcp 593
 ip fastaccess deny udp 135
 ip fastaccess deny udp 137
 ip fastaccess deny udp 138
 ip fastaccess deny udp 139
 ip fastaccess deny tcp 137
 ip fastaccess deny tcp 138
/*****/
 ip nat inside
!
interface FastEthernet0/1
 ip address 218.75.102.190 255.255.255.252
 ip nat outside
!
ip route default 218.75.102.189 10
!
ip access-list standard aaa
 permit 10.4.3.0 255.255.255.0
deny 172.16.0.0 255.0.0.0
```

```

deny 192.168.0.0 255.0.0.0
!
ip nat inside source list aaa interface FastEthernet0/1
!

```

## 2. 备份线路应用

配置如下：

Current configuration:

```

!
ip fastnat 1to1 outside FastEthernet0/1 backup-outside dialer1 inside FastEthernet0/0
!
interface Dialer1
 ip address negotiated
 no ip directed-broadcast
 ppp pap sent-username jhkd3293600 3293600
 ip nat outside
 ip nat mss
!
interface FastEthernet0/0
 ip address 10.4.3.252 255.255.255.0
/*****快速访问列表*****/
 ip fastaccess deny tcp 420
 ip fastaccess deny tcp 9604
 ip fastaccess deny tcp 113
 ip fastaccess deny tcp 667
 ip fastaccess deny tcp 3067
 ip fastaccess deny tcp 5554
 ip fastaccess deny tcp 9996
 ip fastaccess deny tcp 1068
 ip fastaccess deny tcp 2745
 ip fastaccess deny tcp 135
 ip fastaccess deny tcp 3333
 ip fastaccess deny udp 4444
 ip fastaccess deny tcp 445
 ip fastaccess deny tcp 139
 ip fastaccess deny tcp 593
 ip fastaccess deny udp 135
 ip fastaccess deny udp 137
 ip fastaccess deny udp 138
 ip fastaccess deny udp 139
 ip fastaccess deny tcp 137
 ip fastaccess deny tcp 138
/*****
 ip nat inside
!

```

```

interface FastEthernet0/1
  ip address 218.75.102.190 255.255.255.252
ip nat outside
!
interface Ethernet1/0
  no ip address
  no ip directed-broadcast
  duplex half
  pppoe-client Dialer 1
!
ip route default 218.75.102.189 10      /*主线路*/
ip route default Dialer1 90            /*备份线路*/
!
ip access-list standard aaa
permit 10.4.3.0 255.255.255.0
deny 172.16.0.0 255.0.0.0
deny 192.168.0.0 255.0.0.0
!
ip nat inside source list aaa interface FastEthernet0/1
ip nat inside source list aaa interface Dialer1
!

```

### 3. 私服应用

配置如下：

Current configuration:

```

ip fastnat 1to1 outside FastEthernet0/1 inside FastEthernet0/0 privateservices
!
interface FastEthernet0/0
  ip address 10.4.3.252 255.255.255.0
/*****快速访问列表*****/
ip fastaccess deny tcp 420
ip fastaccess deny tcp 9604
ip fastaccess deny tcp 113
ip fastaccess deny tcp 667
ip fastaccess deny tcp 3067
ip fastaccess deny tcp 5554
ip fastaccess deny tcp 9996
ip fastaccess deny tcp 1068
ip fastaccess deny tcp 2745
ip fastaccess deny tcp 135
ip fastaccess deny tcp 3333
ip fastaccess deny udp 4444
ip fastaccess deny tcp 445
ip fastaccess deny tcp 139

```

```
ip fastaccess deny tcp 593
ip fastaccess deny udp 135
ip fastaccess deny udp 137
ip fastaccess deny udp 138
ip fastaccess deny udp 139
ip fastaccess deny tcp 137
ip fastaccess deny tcp 138
/*****/
ip nat inside
!
interface FastEthernet0/1
 ip address 218.75.102.190 255.255.255.252
ip nat outside
!
ip route default 218.75.102.189 10
!
ip access-list standard aaa
 permit 10.4.3.0 255.255.255.0
deny 172.16.0.0 255.0.0.0
deny 192.168.0.0 255.0.0.0
!
ip nat service privateservice
ip nat outside destination static tcp 218.75.102.190 5631 10.4.3.250 5631
ip nat outside destination static udp 218.75.102.190 5632 10.4.3.250 5632
ip nat outside destination static udp 218.75.102.190 6040 10.4.3.250 6040
ip nat inside source list aaa interface FastEthernet0/1
!
```

## 第3章 配置DHCP

### 3.1 DHCP概述

DHCP (*Dynamic Host Configuration Protocol*) 协议为 Internet 上的主机提供了部分网络配置参数。DHCP 在 RFC 2131 中讲述。路由器上 DHCP 最主要的一项是分配接口上的 IP 地址。DHCP 协议支持三种机制的 IP 地址分配机制：

- 自动分配 —— DHCP 服务器自动分配一个永久性的 IP 地址给某一客户端使用
- 动态分配 —— DHCP 服务器分配一个 IP 地址给某一客户端使用一定的时间，或者直到该客户主动放弃该地址的使用权
- 手工分配 —— DHCP 服务器管理员手工指定一个 IP 地址且通过 DHCP 协议传送给客户端使用

#### 3.1.1 DHCP应用

DHCP 有几种应用。当存在以下需求时，可以使用 DHCP 协议：

- 如果需要为某一个以太网接口分配 IP 地址、网段及相关资源（如相应的网关），可以通过配置 DHCP 客户端来实现。
- 当路由器上有一个接口通过 PPP 和对端 A 设备相连，而另外有一个接口能够访问到 DHCP 时，可以通过 DHCP 协议，从 DHCP 服务器上获得一个 IP 地址并且通过 IPCP 给 A 设备分配该 IP 地址。

#### 3.1.2 DHCP的优点

在路由器当前软件版本中，支持 DHCP 客户端的功能，只有在以太网接口上支持该 DHCP 客户端功能，同时所有类型接口上支持 DHCP 协议报文的处理。该功能的使用可以提供以下优点：

- 减少配置时间
- 减少配置错误
- 通过 DHCP 服务器集中控制路由器部分接口的 IP 地址

#### 3.1.3 DHCP术语

DHCP 协议本身是基于 Server/Client 结构的，所以在 DHCP 运行环境中，存在 DHCP-Server 和 DHCP-Client：

- **DHCP-Server** —— 用来发放、收回 DHCP 协议所涉及资源（如 IP 地址、租用时间等）的设备
- **DHCP-Client** —— 从 DHCP-Server 处获取 IP 地址等信息，并且用于本地系统的设备

如上所述，对于 DHCP 信息动态分配的过程中，存在租用时间的概念：

- **租用时间** —— 某个 IP 地址资源从分配开始计时的一段有效期，在该段时间之后，相应的 IP 地址资源将被 DHCP-Server 收回，若要继续使用，DHCP-Client 需要重新申请。

## 3.2 配置DHCP Client

### 3.2.1 DHCP Client配置任务列表

- 为以太网接口获取一个 IP 地址
- 指定 DHCP-Server 地址
- 配置 DHCP 协议参数
- 为 PPP 交互过程从 DHCP 服务器获取一个 IP 地址
- 监视 DHCP

### 3.2.2 DHCP Client配置任务

#### 1. 为以太网接口获取一个IP地址

通过 DHCP 协议为路由器上的以太网接口获取一个 IP 地址，在以太网接口执行下列命令：

| 命令                     | 说明                        |
|------------------------|---------------------------|
| <b>ip address dhcp</b> | 指定通过DHCP协议来配置该以太网接口的IP地址。 |

#### 2. 指定DHCP-Server地址

如果已知某些 DHCP-Server 地址，可以在路由器上指定这些 Server 的地址以减少协议处理的交互和时间，在全局配置状态下，执行下列命令：

| 命令                               | 说明              |
|----------------------------------|-----------------|
| <b>ip dhcp-server ip-address</b> | 指定DHCP服务器的IP地址。 |

当进行“为以太网接口获取一个 IP 地址”时该命令为可选命令。

### 3. 配置DHCP协议参数

可以根据需要，调整 DHCP 协议交互时的参数，在全局配置方式下执行下列命令：

| 命令                                     | 说明              |
|----------------------------------------|-----------------|
| <b>ip dhcp client minlease seconds</b> | 指定最小可接受的租用时间 。  |
| <b>ip dhcp client retransmit count</b> | 指定协议报文的重传次数 。   |
| <b>ip dhcp client select seconds</b>   | 指定SELECT的处理时间 。 |

当进行“为以太网接口获取一个 IP 地址”时以上命令为可选命令。

### 4. 为PPP交互过程从DHCP服务器获取一个IP地址

关于该种方案的示例，请参阅相关的“PPP 配置”章节。

### 5. 监视DHCP

可以查看路由器当前发现的 DHCP-Server（包括手工指定的）的相关信息，在管理态下执行下列命令：

| 命令                      | 说明                   |
|-------------------------|----------------------|
| <b>show dhcp server</b> | 显示路由器所知DHCP服务器的相关信息。 |

可以查看路由器当前使用 IP 地址的相关信息，在管理态下执行下列命令：

| 命令                     | 说明                       |
|------------------------|--------------------------|
| <b>show dhcp lease</b> | 显示路由器当前所使用的IP地址资源及其相关信息。 |

另外，如果采用 DHCP 协议为一个以太网接口分配一个 IP 地址，也可以通过“show interface”命令来查看该以太网口所需的 IP 地址是否成功获得。

#### 3.2.3 DHCP Client配置示例

##### 1. 为以太网接口获取一个IP地址示例

以下例子将为 Ethernet1/1 接口通过 DHCP 协议分配一个 IP 地址。

```
!
interface Ethernet1/1
 ip address dhcp
```

## 3.3 配置DHCP Server

### 3.3.1 DHCP 配置任务列表

- 打开 DHCP Server 服务
- 配置 ICMP 检测参数
- 配置保存 database 参数
- 配置 DHCP Server 地址池
- 配置 DHCP Server 地址池参数
- 监视 DHCP Server
- 清除 DHCP Server 信息

### 3.3.2 DHCP 配置任务

#### 1. 打开DHCP Server服务

打开 DHCP Server 服务，为 DHCP Client 分配 IP 地址等参数，在全局配置态下执行下列命令（此时，DHCP 服务器也支持 relay 操作，对于自身不能分配的地址请求，配置了 ip helper-address 的端口将转发 DHCP 请求）：

| 命令                        | 说明               |
|---------------------------|------------------|
| <b>ip dhcpd enable</b>    | 打开DHCP Server服务。 |
| <b>no ip dhcpd enable</b> | 关闭DHCP Server服务。 |

#### 2. 配置ICMP检测参数

可以根据需要，调整 Server 进行地址检测时，发送的 ICMP 报文的参数：

配置发送 ICMP 报文个数，在全局配置状态下，执行下列命令：

| 命令                                       | 说明                  |
|------------------------------------------|---------------------|
| <b>ip dhcpd ping packets <i>pkgs</i></b> | 指定地址检测是发送ICMP报文的个数。 |

配置等待 ICMP 报文响应的超时时间，在全局配置状态下，执行下列命令：

| 命令                                          | 说明                 |
|---------------------------------------------|--------------------|
| <b>ip dhcpd ping timeout <i>timeout</i></b> | 指定等待ICMP报文响应的超时时间。 |

### 3. 配置清除abandoned标志的参数

配置每隔多长时间清除一次 **abandoned** 标志(dhcp 服务器在分配地址的时候, 如果发现该地址已经被使用, 为了提高分配的效率, 就将此地址置为 **abandon** 标志, 在以后的分配过程中不在探测此地址, 直至 **abandon** 标志被清除), 在全局配置状态下, 执行下列命令:

| 命令                                       | 说明                         |
|------------------------------------------|----------------------------|
| <b>ip dhcpd abandon-time</b> <i>time</i> | 指定每隔多长时间清除一次abandoned 标志 。 |

### 4. 配置保存database的参数

配置每隔多长时间将地址分配信息保存到 **agent database** 中, 在全局配置状态下, 执行下列命令:

| 命令                                     | 说明                                  |
|----------------------------------------|-------------------------------------|
| <b>ip dhcpd write-time</b> <i>time</i> | 指定每隔多长时间将地址分配信息保存到agent database 中。 |

### 5. 配置DHCP Server地址池

添加 DHCP Server 地址池, 在全局配置态下执行下列命令:

| 命令                               | 说明                                 |
|----------------------------------|------------------------------------|
| <b>ip dhcpd pool</b> <i>name</i> | 添加添加DHCP Server地址池, 并进入DHCP地址池配置态。 |

### 6. 配置DHCP Server地址池参数

在 DHCP 地址池配置态下, 可以执行以下命令来配置相关参数

用户可以使用以下命令来配置用于自动分配的地址池的网络地址:

| 命令                                      | 说明                 |
|-----------------------------------------|--------------------|
| <b>network</b> <i>ip-addr netsubnet</i> | 配置用于自动分配的地址池的网络地址。 |

用户可以使用此命令来配置用于自动分配的地址区域:

| 命令                                     | 说明              |
|----------------------------------------|-----------------|
| <b>range</b> <i>low-addr high-addr</i> | 配置用于自动分配的地址区域 。 |

用户可以使用此命令来配置分配给客户机的缺省路由:

| 命令                                       | 说明             |
|------------------------------------------|----------------|
| <b>default-router</b> <i>ip-addr ...</i> | 配置分配给客户机的缺省路由。 |

用户可以使用此命令来配置分配给客户机的 DNS 服务器地址:

| 命令                                   | 说明                 |
|--------------------------------------|--------------------|
| <b>dns-server</b> <i>ip-addr ...</i> | 配置分配给客户机的DNS服务器地址。 |

用户可以使用此命令来配置分配给客户机的域名：

| 命令                             | 说明           |
|--------------------------------|--------------|
| <b>domain-name</b> <i>name</i> | 配置分配给客户机的域名。 |

用户可以使用此命令来配置分配给客户机的地址的时间期限：

| 命令                                                              | 说明                |
|-----------------------------------------------------------------|-------------------|
| <b>lease</b> { <i>days [hours][minutes]</i>   <i>infinite</i> } | 配置分配给客户机的地址的时间期限。 |

用户可以使用此命令来配置分配给客户机的 netbios 名字服务器地址：

| 命令                                           | 说明                       |
|----------------------------------------------|--------------------------|
| <b>netbios-name-server</b> <i>ip-addr...</i> | 配置分配给客户机的netbios名字服务器地址。 |

用户可以使用此命令来配置用于手动分配的地址池的主机地址：

| 命令                                 | 说明                 |
|------------------------------------|--------------------|
| <b>host</b> <i>ip-addr netmask</i> | 配置用于手动分配的地址池的主机地址。 |

用户可以使用此命令来配置用于匹配客户机的硬件地址：

| 命令                                                        | 说明              |
|-----------------------------------------------------------|-----------------|
| <b>hardware-address</b><br><i>hardware-address{ type}</i> | 配置用于匹配客户机的硬件地址。 |

用户可以使用此命令来配置用于匹配客户机的客户端 ID：

| 命令                                                | 说明               |
|---------------------------------------------------|------------------|
| <b>client-identifier</b> <i>unique-identifier</i> | 配置用于匹配客户机的客户端ID。 |

用户可以使用此命令来配置用于手动分配给客户机的主机名：

| 命令                             | 说明                |
|--------------------------------|-------------------|
| <b>client-name</b> <i>name</i> | 配置用于手动分配给客户机的主机名。 |

## 7. 监视DHCP Server

查看 DHCP Server 当前的地址分配信息，在管理态下执行下列命令：

| 命令                           | 说明                      |
|------------------------------|-------------------------|
| <b>show ip dhcpd binding</b> | 显示DHCP Server当前的地址分配信息。 |

查看 DHCP Server 当前的报文统计信息，在管理态下执行下列命令：

| 命令                             | 说明                    |
|--------------------------------|-----------------------|
| <b>show ip dhcpd statistic</b> | 显示DHCP Server当前的统计信息。 |

查看 DHCP Server 地址池的统计信息，在管理态下执行下列命令：

| 命令                        | 说明                     |
|---------------------------|------------------------|
| <b>show ip dhcpd pool</b> | 显示DHCP Server地址池的统计信息。 |

## 8. 清除DHCP Server信息

删除 DHCP Server 当前的地址分配信息，在管理态下执行下列命令：

| 命令                                         | 说明           |
|--------------------------------------------|--------------|
| <b>clear ip dhcpd binding {ip-addr[*]}</b> | 删除指定的地址分配信息。 |

删除 DHCP Server 当前的报文统计信息，在管理态下执行下列命令：

| 命令                              | 说明                    |
|---------------------------------|-----------------------|
| <b>clear ip dhcpd statistic</b> | 删除DHCP Server当前的统计信息。 |

清除所有已设置的 abandoned 标志，在管理态下执行下列命令：

| 命令                              | 说明             |
|---------------------------------|----------------|
| <b>clear ip dhcpd abandoned</b> | 清除abandoned标志。 |

### 3.3.3 DHCP Server配置示例

以下例子将 ICMP 检测包的超时时间设为 200ms，配置一个名为 1 的地址池，并打开 DHCP Server 服务。

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
network 192.168.20.0 255.255.255.0
range 192.168.20.211 192.168.20.215
domain-name my315
default-router 192.168.20.1
```

### 3.3.4 dns-server 192.168.1.3 61.2.2.10

```
netbios-name-server 192.168.20.1
lease 1 12 0
!
ip dhcpd enable
```

## 3.4 配置DHCP Relay

### 3.4.1 DHCP Relay配置任务列表

- 启动 DHCP Relay 服务

- 关闭 DHCP Relay 服务
- 配置 DHCP Relay 参数

### 3.4.2 DHCP Relay配置任务

#### 1. 启动DHCP Relay服务

在路由器上，若需使用 DHCP Relay 功能，请先启动 DHCP Server 服务，请参见“打开 DHCP Server 服务”。

#### 2. 关闭DHCP Relay服务

在路由器上，若需停止 DHCP Relay 功能，请关闭 DHCP Server 服务，请参见“关闭 DHCP Server 服务”

#### 3. 配置DHCP Relay参数

可以根据需要，调整 relay 的目标地址，DHCP 协议报文的 Relay 功能受到“转发 UDP 广播报文”相同的控制，请参见“转发 UDP 广播报文”的命令 `ip forward-protocol udp`。

### 3.4.3 DHCP Relay配置示例

以下例子打开 DHCP Relay 服务，将从 Ethernet1/1 中收到的 DHCP-Request 报文 relay 到 10.1.1.1，同时把到达 192.168.20.1 的 DHCP-Reply 报文从 Ethernet1/1 再发送出去。

```
interface Ethernet1/1
 ip address 192.168.20.1 255.255.255.0
 ip help-address 10.1.1.1
!
ip dhcpd enable
```

## 第4章 配置DNS

### 4.1 DNS概述

DNS 是域名系统 (Domain Name System) 的缩写，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、有关电子邮件的选路信息以及其它与主机有关的信息。

DNS 命名用于 TCP/IP 网络，如 Internet，用来通过用户友好的名称定位计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与此名称相关的其他信息，如 IP 地址。

在 DNS 系统中，DNS Resolver 相当于 DNS Server 的客户端。应用程序通过 DNS Resolver 访问 DNS Server 获得相关信息，这些信息中最基本的是：根据主机名获得 IP 地址和根据 IP 地址获得主机名。

Dynamic DNS Resolver 主要用在动态 IP 地址环境中，Dynamic DNS Resolver 能自动的向可以注册的 DNS Server 注册 Host/address 等信息，当 IP 地址变化后，能自动的向 DNS Server 发送更新消息，使 DNS Server 自动更新域名数据库。

花生壳动态主机注册协议提供一种将域名和动态 IP 地址绑定的方法，允许客户机将自己的 IP 地址提交给服务器，并选择希望注册的域名记录，服务器确认客户机拥有该域名的权限，并修改 DNS 相应记录，在客户机在线的情况下维持这些动态注册的域名，并且在客户机离线自动删除动态注册的余名。该协议分两部分：管理协议和更新协议，前者提供账号申请、修改、登录以及域名注册、申请、修改的功能。后者完成动态注册的更新和在线状态监测。

### 4.2 DNS应用

DNS 有着广泛的应用：

1. 为 ping、telnet 和 traceroute 等提供从主机名到主机地址的解析
2. 为 telnet 提供从主机地址到主机名的解析。Traceroute 在解析路由上每一跳的 IP 地址的同时，还解析对应地址的域名。
3. 当客户端的 IP 地址更新后，自动到具有动态域名服务的 DNS 服务器上更新 IP 地址

*DNS resolver 在路由器中的位置见图1：*

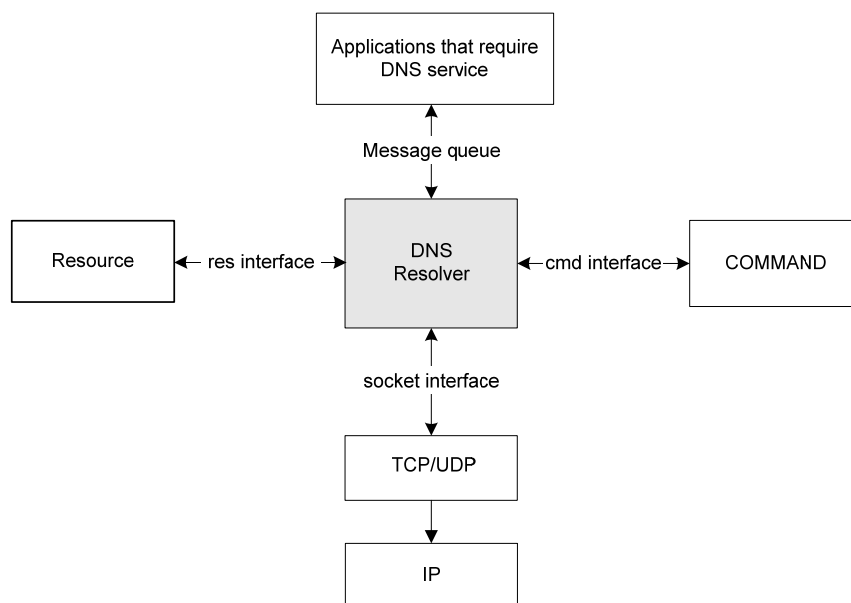


图 1 DNS resolver 在路由器中的位置

## 4.3 DNS术语

**DNS 资源记录（RR）：**

每个 DNS 数据库都由资源记录构成。一般来说，资源记录包含与特定主机有关的信息，如 IP 地址、主机的所有者或者提供服务的类型。

**起始授权机构（SOA）：**

此记录指定区域的起点。它所包含的信息有区域名、区域管理员电子邮件地址，以及指示辅 DNS 服务器如何更新区域数据文件的设置等。

**常用的资源记录类型：**

**A（地址）** 此记录列出特定主机名的 IP 地址。这是名称解析的重要记录。

**CNAME（标准名称）** 此记录指定标准主机名的别名。

**MX（邮件交换器）** 此记录列出了负责接收发到域中的电子邮件的主机。

**NS（名称服务器）** 此记录指定负责给定区域的名称服务器。

**PTR（指针查询）** 此记录列出特定 IP 地址的主机名

**DNS 区域（zone）：**

通常，DNS 数据库可分成不同的相关资源记录集，其中的每个记录集称为区域。区域可以包含整个域、部分域或只是一个或几个子域的资源记录。在域中划分多个区域的主要目的是为了简化 DNS 的管理任务，即委派一组权威名称服务器来管理每个区域。采用这样的分布式结构，当域名称空间不断扩展时，各个域的管理员可以有效地管理各自的

子域。区域和域是很难分辨的。区域是域的子集。可以将它看作域名称空间的某个分支（或子树）。

权威名称服务器（authoritative name server）：

管理某个区域（或记录集）的 DNS 服务器称为该区域的权威名称服务器。每个名称服务器可以是一个或多个区域的权威名称服务器。

主服务器（primary server）和辅服务器（slave server）：

为保证服务的高可用性，DNS 要求使用多台名称服务器冗余支持每个区域。某个区域的资源记录通过手动或自动方式更新到单个主名称服务器（称为主 DNS 服务器）上。主 DNS 服务器可以是一个或几个区域的权威名称服务器。其它冗余名称服务器（称为辅 DNS 服务器）用作同一区域中主服务器的备份服务器，以防主服务器无法访问或宕机。辅 DNS 服务器定期与主 DNS 服务器通讯，确保它的区域信息保持最新。如果不是最新信息，辅 DNS 服务器就会从主服务器获取最新区域数据文件的副本。这种将区域文件复制到多台名称服务器的过程称为区域交换。

## 4.4 DNS Resolver的配置

本模块实现了 DNS 协议的客户端程序，并通过对 DNS 报文的转发实现了 DNS 代理服务器功能，但这并不是真正的 DNS 服务器功能。DNS 协议的服务器端功能不在本模块涉及范围内。

### 4.4.1 激活基于DNS的名称地址解析

激活基于 DNS 的名称地址解析就是使其能进行 DNS 查询。本模块缺省是已经激活了基于 DNS 的名称地址解析。

在全局配置态使用以下命令：

| 命令                         | 目的               |
|----------------------------|------------------|
| <b>ip domain lookup</b>    | 激活基于 DNS 的名称地址解析 |
| <b>no ip domain lookup</b> | 取消基于 DNS 的名称地址解析 |

### 4.4.2 指定域名服务器地址

可以指定多个域名服务器，但最多只能指定六个。先指定的服务器将优先查询，若查询不到主机才去查找后一个服务器。

在全局配置态使用以下命令：

| 命令                                                            | 目的              |
|---------------------------------------------------------------|-----------------|
| <b>ip domain name-server address</b> <i>ip-address</i>        | 设置指定的域名服务器      |
| <b>ip domain name-server dhcp</b>                             | 使用dhcp指定域名服务器   |
| <b>ip domain name-server ppp</b>                              | 使用ppp指定域名服务器    |
| <b>no ip domain name-server ppp</b>                           | 取消由ppp指定的域名服务器  |
| <b>no ip domain name-server dhcp</b>                          | 取消由dhcp指定的域名服务器 |
| <b>no ip domain name-server address</b> [ <i>ip-address</i> ] | 删除指定的域名服务器      |

注：

**no ip domain name-server** 表示删除所有的域名服务器。

#### 4.4.3 指定一个默认的域名

通过指定一个默认的域名来完整不完全的主机名称，只有当没有域名列表时，默认的域名才会被使用。

在全局配置态使用以下命令：

| 命令                                | 目的        |
|-----------------------------------|-----------|
| <b>ip domain name</b> <i>name</i> | 指定一个默认的域名 |
| <b>no ip domain name</b>          | 删除一个默认的域名 |

#### 4.4.4 定义域列表

resolver 利用配置的列表里的域名来完整不完全的主机名称，resolver 在解析域名时会依次尝试列表里的域名，直到找到相应的主机或域名列表搜索完毕。如果存在一个 domain list，则默认的域名不会使用。

在全局配置态使用以下命令：

| 命令                                       | 目的       |
|------------------------------------------|----------|
| <b>ip domain list</b> <i>name</i>        | 指定一个域名列表 |
| <b>no ip domain list</b> [ <i>name</i> ] | 删除一个域名列表 |

注：

**no ip domain list** *name* 表示删除域名 *name*；

**no ip domain list** 表示删除域名列表中所有的域名。

#### 4.4.5 映射主机名到IP地址

任一 IP 地址都可以有一个主机名称与之对应，同一主机名称可以对应多个 IP 地址。系统保存了一个可以被 **telnet**，**ping** 等命令使用的主机名到地址的映射缓存。

要指定主机名到地址的映射，在全局配置态使用下列命令：

| 命令                                               | 目的              |
|--------------------------------------------------|-----------------|
| <b>ip host name name address1[address2, ...]</b> | 静态地映射主机名到IP地址   |
| <b>no ip host name name [address1, ...]</b>      | 删除静态地映射主机名到IP地址 |

例：如下映射主机 djh 与多个 IP 地址对应

```
router_config# ip host name djh 172.16.20.209
```

```
router_config# ip host name djh 172.16.20.210
```

或：

```
router_config# ip host name djh 172.16.20.209 172.16.20.210
```

删除时也可删除一个或多个 IP 地址，还可删除主机

```
router_config# no ip host name djh 172.16.20.209          /*将删除 djh 的一个IP 地址*/
```

```
router_config# no ip host name djh 172.16.20.209 172.16.20.210
```

/\*将删除 djh 的二个 IP 地址\*/

```
router_config# no ip host name djh                        /*将删除 djh 主机*/
```

#### 4.4.6 设置DNS query的重发次数

当发送失败或未接收到服务器的应答信息要重新发送，重发次数不得大于设置的重发次数。缺省时，重发次数是 3（次）。如果需要可以改变缺省值

在全局配置态使用以下命令：

| 命令                           | 目的       |
|------------------------------|----------|
| <b>ip domain retry count</b> | 指定重发次数   |
| <b>no ip domain retry</b>    | 恢复默认重发次数 |

#### 4.4.7 设置DNS query的超时重发的超时值

当与 DNS Server 端的交互失败时，可以重试。缺省时，超时重发的超时值是 2（seconds）。如果需要可以改变超时值。

在全局配置态使用以下命令：

| 命令                                      | 目的           |
|-----------------------------------------|--------------|
| <b>ip domain timeout</b> <i>seconds</i> | 指定超时重发的超时值   |
| <b>no ip domain timeout</b>             | 恢复默认超时重发的超时值 |

#### 4.4.8 从缓存里删除主机名称与地址映射项

查询过的主机将置于 **resolve** 缓存中，可以从缓存里删除一个或者全部主机名称与地址映射项，该命令不删除静态配置的主机名称与地址映射项

在管理态使用以下命令：

| 命令                               | 目的         |
|----------------------------------|------------|
| <b>clear ip host</b> <i>name</i> | 删除缓存中的一个主机 |
| <b>clear ip host *</b>           | 删除缓存中的全部主机 |

#### 4.4.9 指定主域名服务器的IP地址

只能配置一个主域名服务器，如果配置多个，后面配置的将覆盖前面的。

在全局配置态使用以下命令：

| 命令                                             | 目的       |
|------------------------------------------------|----------|
| <b>ip domain primary-server</b> <i>address</i> | 指定主域名服务器 |
| <b>no ip domain primary-server</b>             | 删除主域名服务器 |

#### 4.4.10 设置DNS Resolver端的主机缓存数目上限

指定缓存中的主机数目上限，如果多次配置，后面的配置将覆盖前面的配置。缺省时不对此数目作任何限制。

在全局配置态下使用以下命令：

| 命令                                        | 目的                  |
|-------------------------------------------|---------------------|
| <b>ip domain host limit</b> <i>number</i> | 设置缓存中的主机数目上限为number |
| <b>no ip host limit</b>                   | 取消对缓存中主机数目上限的限制     |

#### 4.4.11 激活DNS Resolver端的代理服务器功能

一般情况下不需要开启此功能，因此可以用该命令的 **no** 形式关闭此功能。缺省情况下，此功能是关闭的。

在全局配置态下使用以下命令：

| 命令                               | 目的           |
|----------------------------------|--------------|
| <b>ip domain proxy enable</b>    | 激活DNS代理服务器功能 |
| <b>no ip domain proxy enable</b> | 关闭DNS代理服务器功能 |

#### 4.4.12 激活DNS Resolver端的动态更新功能

对于拥有静态 IP 地址的路由器，一般不需要动态 DNS 功能，可以用该命令的 **no** 形式关闭。默认情况下，该功能是关闭的。

在全局态使用以下命令：

| 命令                                 | 目的       |
|------------------------------------|----------|
| <b>ip domain dynamic enable</b>    | 激活动态更新功能 |
| <b>no ip domain dynamic enable</b> | 关闭动态更新功能 |

#### 4.4.13 设置周期性更新域名与地址绑定的超时值

在全局态使用以下命令：

| 命令                                             | 目的                 |
|------------------------------------------------|--------------------|
| <b>ip domain dynamic period</b> <i>seconds</i> | 设置周期性更新域名与地址绑定的超时值 |
| <b>no ip domain dynamic period</b>             | 恢复默认的超时值           |

#### 4.4.14 绑定主机IP地址和域名

该命令暂时不支持将该端口下的次级 IP 地址绑定到该域名下

当执行此命令后，任何时候该端口下的 IP 地址发生变化便可自动向主服务器更新域名到 IP 地址的映射，即动态域名更新。

通常，以下情况要进行更新操作：

- a. 当路由器启动时，应该立即启动 **update** 模块注册。

- b. 时钟引发。
- c. 当通过命令绑定了新的域名地址对，则引发 **update** 子模块注册，当通过命令删除已有的域名地址对，则引发 **update** 子模块注销。
- d. 当绑定的域名和地址对中，任何一方发生改变，则引发 **update** 子模块。
- e. 当绑定的域名和地址对中，IP 地址所在端口被删除或者被 **shutdown** 时。

首先在全局配置态使用以下命令进入动态 DNS 配置态：

| 命令                           | 目的         |
|------------------------------|------------|
| <b>ip domain ddns update</b> | 进入动态DNS配置态 |

注：在动态 DNS 配置态下使用 **exit** 命令能够退回到全局配置态。

在动态 DNS 配置态下：

| 命令                                       | 目的                                                         |
|------------------------------------------|------------------------------------------------------------|
| <b>bind name interface number</b>        | 绑定该端口下的主IP地址和域名name<br>(注：同一个端口只能绑定一个域名，第二次绑定的域名将覆盖第一次绑定的) |
| <b>bind name interface number singly</b> | 绑定该端口下的主IP地址和域名name，并删除primary-server上的所有其他域名为name的主机      |
| <b>no bind name interface number</b>     | 删除域名和该端口IP地址的映射                                            |
| <b>bind name ip_addr</b>                 | 绑定IP地址和域名name<br>(注：同一域名可以对应多个IP，域名可以跟端口的域名相同)             |
| <b>bind name ip_addr singly</b>          | 绑定IP地址和域名name，并删除primary-server上的所有其他域名为name的主机            |
| <b>no bind name ip_addr</b>              | 删除域名和IP地址的映射                                               |
| <b>no bind name</b>                      | 删除此域名的所有信息                                                 |

注意：对于动态更新命令，在路由器重启后会自动在主域名服务器上进行一次注册，但是若相应端口还没有 UP 的话，与域名服务器的通信将不会成功，也就是重新注册未成功。为了保证更新在端口已经 UP 后进行，本模块设置在第一次注册时重试次数和超时值均大一些，因此对于 **retry** 和 **timeout** 的配置要在 30 秒钟以后配置才能生效。

另外，当使用端口的绑定时，若在某个时候端口 IP 地址的改变使得该路由器与主域名服务器暂时不能正常通信而过一会又可以通信，这时可以增加重发次数和加大超时值来延迟时间以便当与主域名服务器恢复正常通信时能够成功的更新。

#### 4.4.15 花生壳客户端配置功能

DNS Resolver 模块内嵌的花生壳客户端模块实现了花生壳动态主机注册协议的客户端程序，花生壳服务器端功能不在本模块涉及范围内。

首先在全局配置态使用以下命令创建一个花生壳客户端配置实例，即进入花生壳客户端配置态，命令如下：

| 命令                                       | 目的                    |
|------------------------------------------|-----------------------|
| <b>ip domain ddns peanuthull name</b>    | 创建一个名为name的花生壳客户端配置实例 |
| <b>no ip domain ddns peanuthull name</b> | 删除名为name的花生壳客户端配置实例   |

注：在同一台路由器设备上可同时配置多个花生壳客户端配置实例，模块没有对此数目设置限制。不同的配置实例之间只要具有不同的实例名即可。

在花生壳客户端配置态下使用以下命令对配置实例进行配置：

| 命令                           | 目的                                              |
|------------------------------|-------------------------------------------------|
| <b>enable</b>                | 激活花生壳客户端的地址解析功能，激活后系统自动查找服务器并注册                 |
| <b>no enable</b>             | 取消花生壳客户端的地址解析功能                                 |
| <b>server name</b>           | 指定花生壳服务器名，只能指定一个，后来设置的服务器名将覆盖之前设置的并自动向新的服务器重新连接 |
| <b>no server</b>             | 删除花生壳服务器名                                       |
| <b>domain name</b>           | 指定一个默认的域名，此域名之前已在花生壳网站上申请过。                     |
| <b>no domain</b>             | 删除一个默认的域名                                       |
| <b>port num</b>              | 指定连接的服务器端口号                                     |
| <b>no port</b>               | 删除配置的端口号                                        |
| <b>username name</b>         | 设置用户名                                           |
| <b>no username</b>           | 删除配置的用户名                                        |
| <b>pssword password</b>      | 设置密码                                            |
| <b>no password</b>           | 删除配置的密码                                         |
| <b>bind interface number</b> | 绑定接口number                                      |
| <b>bind ip_addr</b>          | 绑定IP地址ip_addr                                   |

注：一个配置实例中可以使用 **domain** 命令配置最多 6 个注册域名，若未指定任何域名，则系统自行选择一个已经注册过的域名。接口下可能存在多个 **ip**，系统自行选择主 **ip** 地址。接口没有 **ip** 地址时花生壳客户端无法启动，当接口被分配 **ip** 或者 **ip** 发生变化，花生壳客户端会重新注册。

#### 4.4.16 软件模块信息显示功能与Debug显示功能需求

系统可以显示特定的统计数据，如默认的域名、与域名有关的一些特性、缓存里的域名地址表项以及 Resolve 运行时的一些参数和动作。这些信息可以帮助确定系统资源使用情况，从而解决网络问题。

在管理态使用以下命令

| 命令                          | 目的                                                          |
|-----------------------------|-------------------------------------------------------------|
| <b>show ip hosts</b>        | 显示默认域名、域名列表、域名服务器信息以及主机名-IP地址映射缓存表                          |
| <b>show ip hosts detail</b> | 除了显示上述内容之外，还显示非阻塞调用DNS模块的上层应用的有关信息，如消息ID（或回调函数地址）、提前通知的时间等。 |
| <b>show ip domain</b>       | 显示设置的域名服务器列表                                                |
| <b>show ip peanuthull</b>   | 显示设置的花生壳客户端配置实例信息                                           |
| <b>debug ip domain</b>      | 显示本模块的debug信息                                               |

### 4.5 DNS Resolver配置示例

以下将配置 DNS Resolver，使其能从域名服务器上进行域名查询和动态更新。

在全局配置态下，最小配置：

```
!
ip domain name-server 192.168.1.3
ip domain dynamic enable
ip domain primary-server 172.16.20.212
ip domain bind www.bind1.edu.cn interface e1/1
ip domain ddns peanuthull aaa
    server hph016.oray.net
    username bdtest
    password bdtest
    port 5050
    bind interface f0/2
    enable!
!
```

在全局配置态下，非最小配置：

```
!  
ip domain name aaa.com.cn  
ip domain list com.cn  
ip domain list edu.cn  
ip host name djh 172.16.20.209 10.0.0.90  
ip host limit 2500  
ip domain proxy enable  
ip domain name-server 192.168.1.3  
ip domain name-server 172.16.20.212  
ip domain timeout 3  
ip domain retry 2  
ip domain dynamic enable  
ip domain primary-server 172.16.20.212  
ip domain dynamic period 7200  
ip domain ddns update  
    bind www.test.edu.cn 202.10.10.56  
    bind www.bind1.edu.cn interface e1/1  
    bind djh.edu.cn 202.10.10.45 singly  
    bind right.edu.cn interface loopback100 singly  
!  
ip domain ddns peanuthull aaa  
    server hph016.oray.net  
    username bdtest  
    password bdtest  
    port 5050  
    bind interface f0/2  
    enable  
!
```

## 第5章 配置IP服务

### 5.1 配置IP服务

本章介绍如何配置 IP 可选服务。如果要了解本章提到的 IP 服务命令的详细使用方法，请参阅“IP 服务命令”章节。

以配置下列 IP 的可选服务：

- 管理 IP 连接
- 配置性能参数
- 在广域网上配置 IP
- 检测和维护 IP 网络

这些操作并不是必需的，而是根据网络需要进行的。

#### 5.1.1 管理IP连接

IP 提供了一系列的服务来控制和管理 IP 连接。大多数这样的服务是由 ICMP 提供的。ICMP 报文一般是在路由器或者是访问服务器发现 IP 报头错误时发给主机或者是其它路由器的。ICMP 主要由 RFC 792 定义。

要管理 IP 连接的不同方面，执行下列相关操作：

- 发送 ICMP 不可到达报文
- 发送 ICMP 重定向报文
- 发送 ICMP 掩码应答报文
- 支持路径 MTU 发现
- 设置 IP 最大发送单元（MTU）
- 允许 IP 源路由
- 允许 IP 路由缓存
- 允许同一接口上的 IP 路由缓存

## 1. 发送ICMP不可到达报文

如果系统收到一个报文，但是发现无法把它送到目的地，例如没有相应的路由，它将发送一个 **ICMP** 主机不可到达报文给源主机。系统的这一功能是缺省打开的。

如果这一功能被关闭的话，用户可以在接口配置态使用下列命令打开这一功能：

| 命令                    | 目的                        |
|-----------------------|---------------------------|
| <b>ip unreachable</b> | 发送 <b>ICMP</b> 不可到达报文的功能。 |

## 2. 发送ICMP重定向报文

有时，主机所选择的路由不是最佳的，因此收到报文的路由器发现，根据路由表要把这个报文从收到它的接口再次发送出去，转发到和发送主机在同一个网段上的另一台路由器。在这种情况下，路由器会通知源主机把到这一目的地址的报文直接发送到另一台路由器，而不必再经过本机。重定向报文要求源主机以报文中建议的更加直接的路由取代原来的路由。很多主机操作系统会在路由表中添加一条主机路由。但是，路由器更信任根据路由协议得到的信息，所以不会根据这条信息添加主机路由。

这一功能是缺省打开的。但是，如果在这个接口上配置了热备份路由器协议，则这项功能将被自动关闭。如果热备份路由器协议配置被取消，这一功能不会被自动打开。

如果这一功能被关闭，可以在接口配置态使用下列命令打开发送 **ICMP** 重定向报文功能：

| 命令                  | 目的                      |
|---------------------|-------------------------|
| <b>ip redirects</b> | 允许发送 <b>ICMP</b> 重定向报文。 |

## 3. 发送ICMP掩码应答报文

有时主机必须了解网络掩码，为了得到这一信息，主机可以发送 **ICMP** 掩码请求报文。路由器如果能确定这台主机的掩码，将回应 **ICMP** 掩码应答报文。缺省情况下，路由器会发送 **ICMP** 掩码应答报文。

如果要求发送 **ICMP** 掩码请求报文，在接口配置态使用下列命令：

| 命令                   | 目的                     |
|----------------------|------------------------|
| <b>ip mask-reply</b> | 发送 <b>ICMP</b> 掩码应答报文。 |

## 4. 支持路径MTU发现

系统支持 **RFC 1191** 定义的 **IP** 路径 **MTU** 发现机制。**IP** 路径 **MTU** 发现使主机可以动态发现和适应不同路径的最大发送单元（**MTU**）长度。有时，路由器发现收到的 **IP** 报文长度大于报文转发接口上设置的 **MTU**，需要把 **IP** 报文分片，但是该 **IP** 报文的“不分片”位被置位，报文不允许被分片，所以报文只能被丢弃。这时，路由器会发送 **ICMP** 报文通知源主机转发失败的原因，以及转发接口上的 **MTU**。源主机减小发往这个目的地址的报文的长度，以适应这条路径的最小 **MTU**。

如果路径中的一条链路断开，将导致报文采用其它路径，它的最小 MTU 可能和原来的路径不同。这时，路由器会通知源主机新路径的 MTU。在可能的情况下，应该尽量采用路径中最小的 MTU 封装 IP 报文，这样，既避免分片，又发送尽可能少的报文，从而提高通信效率。

相应的主机必须支持 IP 路径 MTU 发现，它才会根据路由器通知的 MTU 值调整发送的 IP 报文的长度，避免在转发过程中分片。

## 5. 设置IP最大发送单元（MTU）

所有的接口都有一个缺省的 IP 最大发送单元（MTU），也就是允许发送的最大 IP 报文长度。如果 IP 报文长度超过这个值的话，路由器就会对报文进行分片。

改变接口的 MTU 值将会影响接口的 IP MTU 值。如果 IP MTU 与 MTU 相等的话，改变 MTU，IP MTU 将自动调整到和新的 MTU 值相同。但是，改变 IP MTU 不会影响 MTU。IP MTU 不能大于当前接口上配置的 MTU。连接在同一物理介质上的所有设备必须具有相同的协议 MTU，才能正常通信。

要设置特定接口上的 IP MTU，在接口配置态使用下列命令：

| 命令                  | 目的           |
|---------------------|--------------|
| <b>ip mtu bytes</b> | 设置接口的IP MTU。 |

## 6. 允许IP源路由

路由器检查每个报文的 IP 报头选项，它支持 RFC 791 定义的 IP 报头选项：严格源路由、松弛源路由、记录路由和时戳。如果发现选项错误，将发送 ICMP 参数问题报文给源主机并丢弃报文。如果在源路由过程中发现错误，将发送 ICMP 不可到达（源路由失败）报文给源主机。

IP 允许源主机指定报文通过 IP 网络的路由，这称为源路由，可以在 IP 报头选项的源路由选项中指定。路由器必须根据该选项转发 IP 报文，或者出于安全考虑丢弃这类报文，并发送 ICMP 不可到达（源路由失败）报文给源主机。路由器缺省支持源路由。

如果 IP 源路由功能被关闭的话，可以在全局配置态使用下列命令允许 IP 源路由：

| 命令                     | 目的       |
|------------------------|----------|
| <b>ip source-route</b> | 允许IP源路由。 |

## 7. 允许IP路由缓存

IP 路由缓存使用路由缓存转发 IP 报文。当转发第一个到某目的地址的报文时，系统查找路由表，根据路由转发报文。然后，这条路由将被保存在路由缓存中，以后到该主机的报文，系统就直接根据缓存中的路由转发，不再查询路由表。系统不对 ICMP 报文和广播报文生成路由缓存，因为这些报文一般不会持续发送。如果缓存不被使用，将很快被超时删去。

路由缓存可能不适合从高速介质向低速链路（64k 或更低）转发时使用，因为它会加快转发速度，导致报文更快地积压到低速接口上，更多的报文被丢弃。这种情况下，应该在

低速接口上禁止 IP 路由缓存。系统将根据源地址/目的地址进行负载均衡。如果存在多条网络路由，路由缓存 保证同一源地址/目的地址的报文采用同一路由，而不同源地址/目的地址的转发报文可以分别从多条路由发送，从而均衡负载。 <![endif]>

要允许或者禁止路由缓存，在接口配置态使用下列 command:

| 命令                       | 目的                     |
|--------------------------|------------------------|
| <b>ip route-cache</b>    | 允许路由缓存（使用路由缓存转发IP报文）。  |
| <b>no ip route-cache</b> | 禁止路由缓存，系统将对每个报文进行负载均衡。 |

## 8. 允许同一接口上的IP路由缓存

用户可以在允许同一接口上的 IP 路由缓存，即接受接口和发送接口相同。通常情况下，建议不要开启这一功能，因为这和 **router** 的重定向功能冲突。如果用户有一个不完全连接的网络，例如 **FR**，可以在 **FR** 接口开启这项功能。例如 **routerA**, **B**, **C** 共同构成一个 **FR** 网络，但只有 **A—B** 和 **B—C** 之间存在物理链路，**A** 和 **C** 的通信必须由 **B** 中转：**A—B—C**，**B** 从接口的一个 **DLCI** 收到 **A** 的报文，然后又从同一接口经另一个 **DLCI** 发送到 **C**。

要允许同一接口的 IP 路由缓存，在接口配置态使用下列 command:

| 命令                                   | 目的                        |
|--------------------------------------|---------------------------|
| <b>ip route-cache same-interface</b> | 允许发送接口与接受接口相同的IP报文进行路由缓存。 |

## 9. 开启keepalive保活探测功能

用户可以对目的地址的设备进行保活探测，一旦目的地址没有响应，则该端口的状态变为 **down**，不能收发报文。被探测设备一旦有数据包发送到该端口，则端口状态变为 **up**。经常用于备份线路切换。用户可以通过命令 **ip-keepalive period** 来配置保活探测数据包发送的间隔时间，默认为 5 秒。

要允许开启 **keepalive** 保活探测功能，在接口配置态使用下列 command:

| 命令                                                           | 目的                |
|--------------------------------------------------------------|-------------------|
| <b>ip-keepalive address [dest address] [nexthop address]</b> | 开启keepalive保活探测功能 |

## 10. 开启keepalive dns保活探测功能

用户可以对 **dns** 服务器发送 **DNS** 请求进行保活探测，一旦 **dns** 服务器没有响应，则该端口的状态变为 **down**，不能收发报文。被探测服务器一旦有 **DNS** 回应报文发送到该端口，则端口状态变为 **up**。经常用于备份线路切换。用户可以通过命令 **ip-keepalive-dns period** 来配置保活探测数据包发送的间隔时间，默认为 10 秒。

要允许开启 **keepalive dns** 保活探测功能，在接口配置态使用下列 command:

| 命令                                                               | 目的                     |
|------------------------------------------------------------------|------------------------|
| <b>ip-keepalive-dns</b> address [dest address] [nexthop address] | 开启keepalive-dns 保活探测功能 |

### 5.1.2 配置性能参数

要调节 IP 性能，执行下列操作。

- 设置 TCP 连接等待时间
- 设置 TCP 窗口尺寸

#### 1. 设置TCP连接等待时间

当路由器进行 TCP 连接时，如果在 TCP 连接等待时间之后连接还没有建立，路由器将认为连接失败，并把这一结果返回给上层应用程序。用户可以设置 TCP 连接等待时间，系统的缺省值是 75 秒。这项配置与路由器转接的 TCP 连接无关，只与路由器本机建立的 TCP 连接有关。

要设置 TCP 连接等待时间，在全局配置态使用下列命令：

| 命令                                 | 目的           |
|------------------------------------|--------------|
| <b>ip tcp synwait-time</b> seconds | 设置TCP连接等待时间。 |

#### 2. 设置TCP窗口尺寸

缺省的 TCP 窗口尺寸是 2000 字节。如果要改变缺省的窗口尺寸，在全局配置态使用下列命令：

| 命令                              | 目的         |
|---------------------------------|------------|
| <b>ip tcp window-size</b> bytes | 设置TCP窗口尺寸。 |

### 5.1.3 在广域网上配置IP

用户可以在 X.25，帧中继和 PPP 网络上配置 IP 网络。如果要在这些广域网络上配置 IP，例如配置地址映射等，参见相关文档。

### 5.1.4 检测和维护IP网络

要检测和维护网络，执行下列操作：

- 清除缓存，列表和数据库
- 清除 TCP 连接

- 显示系统和网络统计数据
- 显示调试信息

### 1. 清除缓存，列表和数据库

用户可以清除某个缓存、列表或者是数据库中的所有内容。如果认为某个缓存、列表或是数据库中的数据不正确，则需要清除它。

使用下列命令进行清除：

| 命令                          | 目的         |
|-----------------------------|------------|
| <b>clear tcp statistics</b> | 清除TCP统计数据。 |

### 2. 清除TCP连接

如果要关闭某个 TCP 连接，使用下列命令：

| 命令                                                                          | 目的                                         |
|-----------------------------------------------------------------------------|--------------------------------------------|
| <b>clear tcp {local host-name port remote host-name port   tcb address}</b> | 清除指定的TCP连接。(TCB为TCP控制块：TCP Control Block)。 |

### 3. 显示系统和网络统计数据

系统可以显示缓存、列表和数据库中的内容。这些信息可以帮助了解系统资源使用情况，解决网络问题。

可以在管理态使用下列命令。这些命令的具体使用方法，参见“IP 服务命令”章节。

| 命令                                               | 目的                 |
|--------------------------------------------------|--------------------|
| <b>show ip access-lists name</b>                 | 显示某个或所有访问列表的内容。    |
| <b>show ip cache [prefix mask] [type number]</b> | 显示用于快速交换IP报文的路由缓存。 |
| <b>show ip sockets</b>                           | 显示路由器所有socket的信息。  |
| <b>show ip traffic</b>                           | 显示IP协议统计数据。        |
| <b>show tcp</b>                                  | 显示所有的TCP连接状态信息。    |
| <b>show tcp brief</b>                            | 显示简要的TCP连接状态信息。    |
| <b>show tcp statistics</b>                       | 显示TCP统计数据。         |
| <b>show tcp tcb</b>                              | 显示特定的TCP连接的状态信息。   |

### 4. 显示调试信息

当网络出现问题时，可以用 **debug** 命令要求系统显示调试信息。

可以在管理态使用下列命令。这些命令的具体使用方法，参见“IP 服务命令”章节。

| 命令                     | 目的                           |
|------------------------|------------------------------|
| <b>debug arp</b>       | 显示地址解析协议（ARP）的交互信息。          |
| <b>debug ip icmp</b>   | 显示Internet控制信息协议（ICMP）的交互信息。 |
| <b>debug ip raw</b>    | 显示收到的和发送的Internet协议（IP）报文信息。 |
| <b>debug ip packet</b> | 显示Internet协议（IP）的交互信息。       |
| <b>debug ip tcp</b>    | 显示传输控制协议（TCP）的交互信息。          |
| <b>debug ip udp</b>    | 显示用户数据报协议（UDP）的交互信息。         |

## 5.2 配置访问列表

### 5.2.1 过滤IP报文

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的用户或设备限制网络使用。为了从交叉指定的接口中使包有效或无效，本公司路由器提供了访问列表。可以用以下方式使用访问列表：

- 控制在接口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容

本节概括了如何建立 IP 访问列表以及如何应用它们。

IP 访问列表是应用 IP 地址的允许和禁止条件的有序集合。本公司路由器的 ROS 软件在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。

在使用访问列表中有以下两个步骤：

- (1) 通过指定访问列表名及访问条件，建立访问列表。
- (2) 将访问列表应用到接口。

#### 1. 建立标准的和扩展的IP访问列表

用一个字符串建立 IP 访问列表。

**注意：**

标准的访问列表和扩展的访问列表不能用相同的名字。

为了建立标准的访问列表，在全局配置态执行下列命令：

| 命令                                                                                                  | 目的                                        |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------|
| <b>ip access-list standard name</b>                                                                 | 使用名字定义一个标准的IP访问列表。                        |
| <b>deny</b> {source [source-mask]   any}[log]<br><b>or permit</b> {source [source-mask]   any}[log] | 在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通。 |
| <b>exit</b>                                                                                         | 退出访问列表配置模式。                               |

为建立扩展的访问列表，在全局配置态执行下列命令：

| 命令                                                                                                                                                                                         | 目的                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>ip access-list extended name</b>                                                                                                                                                        | 使用名字定义一个扩展的IP访问列表。                                                                  |
| { <b>deny</b>   <b>permit</b> } protocol source<br>source-mask destination destination-mask<br>[precedence precedence] [tos tos]<br>[established] [log]{deny   permit} protocol<br>any any | 在扩展访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通。(precedence表示IP包优先级，TOS表示Type of Service)。 |
| Exit                                                                                                                                                                                       | 退出访问列表配置模式。                                                                         |

在初始建立访问列表后，任何后续的增加部分(可能从终端键入)都放入表的尾部。换句话说，你不能从指定的访问列表选择增加访问列表命令行。但是，你可以使用 **no permit** 和 **no deny** 命令从名字访问列表中删除项。

**注意：**

当建立访问列表时，记住缺省时访问列表的结尾包含隐含的 **deny** 语句。进一步讲，标准的访问列表，如果从相关的 IP 主机地址访问列表指定中省略了掩码，那么 255.255.255.255 就假定是掩码。

在建立了访问列表后，必须将它应用到线路或接口上。如下一节“将访问列表应用到接口”所描述。

## 2. 将访问列表应用到接口

当建立了访问列表后，可以将它应用到一个或多个接口上，可以应用到进或出这两种情况。

在接口配置态使用以下命令：

| 命令                                     | 目的          |
|----------------------------------------|-------------|
| <b>ip access-group name {in   out}</b> | 将访问列表应用到接口。 |

访问列表既可用在出接口也可用在入接口。对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展的访问列表，该路由器也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。如果访问表不允许该地址，该软件放弃包并返回一个 **ICMP** 主机不可到达报文。

对于标准的出口访问表，在接收和路由一个包到控制接口以后，软件对照访问列表检查包的源地址。对于扩展的访问表，路由器还检查接收端访问表。如果访问表允许该软件就

传送这个包。如果访问列表不允许该地址，软件放弃这个包并返回一个 **ICMP** 主机不可达报文。

如果指定的访问列表不存在，所有的包允许通过。

### 5.2.2 扩展访问列表示例

在以下例子中,第一行允许任何新到的 **TCP** 与大于 **1023** 的目标端口连接。第二行允许新来的 **TCP** 与主机 **130.2.1.2** 的 **SMTP** 端口连接。

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface ethernet 1/0
ip access-group aaa in
```

另一个使用扩展访问列表的例子,假定有一个连接到 **Internet** 的网络,你希望在以太网上的任何主机都能够建立 **TCP** 连接到任何 **Internet** 上的主机。但是,并不希望 **Internet** 上主机能够建立 **TCP** 连接到以太网上的主机,除非是到邮件主机的 **SMTP** 端口。

**SMTP** 使用连接的一端上的 **TCP** 端口 **25** 和另一端的随机端口号。在连接期间,使用同样的两个端口号。来自 **Internet** 的邮件包将有一个端口号为 **25** 的目标端口。出站包将有一个反向的端口号。事实上,在路由器后面的安全系统总是会接收连接在端口 **25** 上的邮件,这也正是能够单独控制入站服务和出站服务的原因。访问列表既可以配置成出站服务又可以配置成入站服务。

以下例子中,以太网是一个带有地址 **130.20.0.0** 的 **B** 类网络,邮件主机的地址是 **130.20.1.2**。关键字 **established** 只用于 **TCP** 协议,表示一个建立的连接。如果 **TCP** 数据报有 **ACK** 或者 **RST** 位设置,匹配就会出现,表示该包属于一个现存的连接。

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface ethernet 1/0
ip access-group aaa in
```