网络协议配置

目 录

第1 章 配置IP 寻址....4
1.1 IP 寻址任务列表....4
1.2 IP 寻址任务....4
1.2.1 在网络接口配置IP 地址....4
1.2.2 配置一个路由进程....6
1.2.3 配置广播报文处理....6
1.2.4 检测和维护IP 寻址....7
1.3 IP 寻址示例....8
第2 章 配置NAT....9
2.1 NAT 概述....9
2.1.1 NAT 应用....9
2.1.2 NAT 的优点....9
2.1.3 NAT 术语....10
2.1.4 NAT 规则匹配顺序....10
2.2 NAT 配置任务表....11
2.2.1 翻译内部源地址....11
2.2.2 内部全局地址的重载....13
2.2.3 翻译重叠地址....14
2.2.4 提供TCP 负载均衡....15
2.2.5 改变翻译超时及限制连接数目....16
2.2.6 监视和维护NAT....17
2.2.7 NAT 快速转发....17
2.2.8.NAT 日志配置....18
2.2.9.NAT 端口区域算法....18
2.3 NAT 配置示例....18
2.3.1 动态内部源转换示例....18
2.3.2 内部全局地址重载示例....19
2.3.3 转换重叠地址举例....19
2.3.4 TCP 负载分配示例....19
2.3.5 翻译H323 配置示例....20
2.3.6 网吧应用示例....21
2.3.7 快速NAT 应用示例....23
2.3.8 NAT 端口区域块算法示例....26
第3 章 配置DHCP....27
3.1 DHCP 概述....27
3.1.1 DHCP 应用....27
3.1.2 DHCP 的优点....27
3.1.3 DHCP 术语....27
3.2 配置DHCP Client....28

3.2.1 DHCP Client 配置任务列表 28
3.2.2 DHCP Client 配置任务 28
3.2.3 DHCP Client 配置示例 29
3.3 配置DHCP Server 30
3.3.1 DHCP 配置任务列表 30
3.3.2 DHCP 配置任务 30
3.3.3 DHCP Server 配置示例 30
3.3.4 dns-server 192.168.1.3 61.2.2.10 30
3.4 配置DHCP Relay 30
3.4.1 DHCP Relay 配置任务列表 30
3.4.2 DHCP Relay 配置任务 34
3.4.3 DHCP Relay 配置示例 34
第4 章 配置IP 服务 35
4.1 配置IP 服务 35
4.1.1 管理IP 连接 35
4.1.2 配置性能参数 38
4.1.3 在广域网上配置IP 39
4.1.4 检测和维护IP 网络 39
4.2 配置访问列表 40
4.2.1 过滤IP 报文 40
4.2.2 如果指定的访问列表不存在，所有的包允许通过扩展访问列表示例 42
4.2.3 交换芯片无法支持的ipacl 特性 43
4.2.4 配置 acl 特殊算法 43

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 1.0.0.0 to 126.0.0.0 127.0.0.0	保 留 可 用 保留
B	128.0.0.0 to 191.254.0.0 191.255.0.0	可用 保留
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	保 留 可 用 保留
D	224.0.0.0 to 239.255.255.255	多目广播地址

E	240.0.0.0 to 255.255.255.254 255.255.255.255	保留 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
ip address *ip-address mask*	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
ip address *ip-address mask* secondary	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
ip unnumbered *type number*	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。

1.2.3 配置广播报文处理

广播报文的目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
ipdirected-broadcast [*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
ip helper-address *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
ip forward-protocol udp [*port*]	指定哪些接口的 UDP 协议被转发。

1.2.4 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
clear arp-cache	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
show arp	显示 ARP 表中的内容。
show hosts	显示主机名-IP 地址映射缓存表。
show ip interface [*type number*]	显示接口状态。
show ip route [*protocol*]	显示路由表的当前状态。
ping {**host** | **address**}	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：

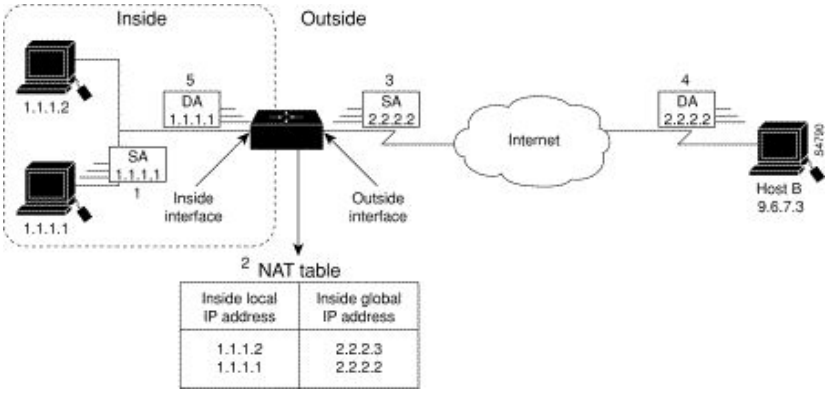


图 2-1 NAT 内部源地址转换

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

以上是最小配置。可以配置多个内部和外部接口。

2. 配置动态转换

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

注意：

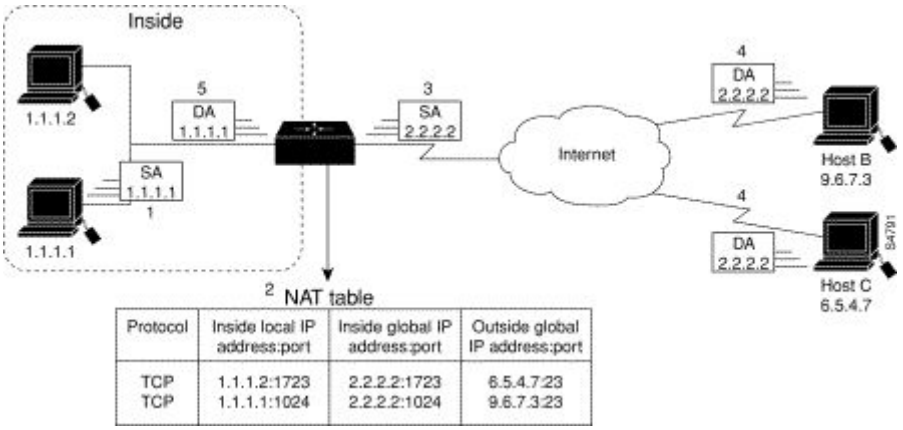
访问表必须只允许列那些可以被转换的地址（记住:在每一个访问表的结尾有一个隐含的“deny all”）太随意的访问表可能导致不可预期的结果。

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。



Protocol	Inside local IP address:port	Inside global IP address:port	Outside global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

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

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

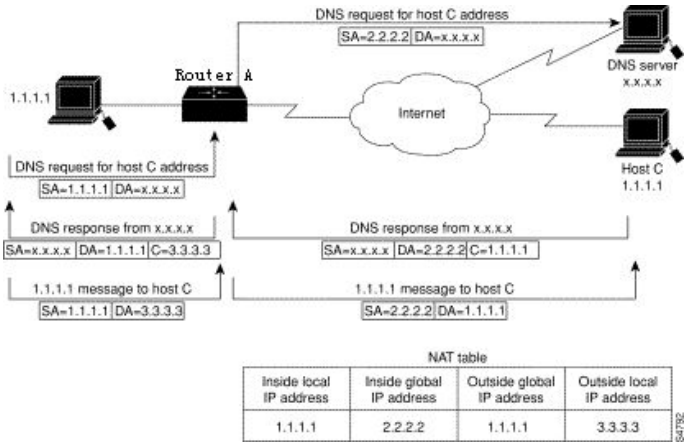


图 2-3 NAT翻译重叠地址的网络环境示意图

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 I P 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。

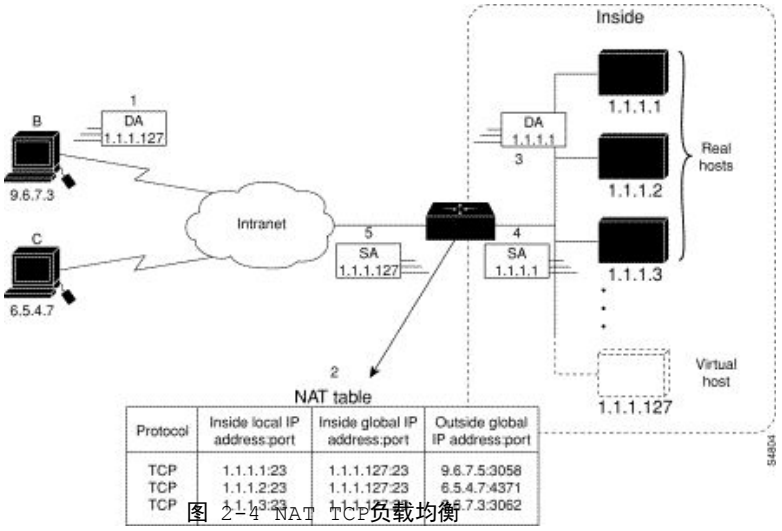


图 2-4 NAT TCP负载均衡

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
ip nat pool name start-ip end-ip netmask	定义一个包含真实主机的地址池。
ip access-list standard access-list-name **permit** source [source-mask]	定义允许虚拟主机地址的一个访问表。
ip nat inside destination list access-list-name **pool** name	建立动态内部目标转换，确定在前一步定义的访问表。
interface type number	指定内部接口。
ip nat inside	把接口标记为连接到内网部的。
interface type number	指定外部接口。
ip nat outside	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
ip nat translation timeout *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
ip nat translation udp-timeout *seconds*	改变 UDP 超时值(缺省值 5 分钟)。
ip nat translation dns-timeout *seconds*	改变 DNS 超时值(缺省值 1 分钟)。
ip nat translation tcp-timeout *seconds*	改变 TCP 超时值(缺省值 1 小时)。
ip nat translation icmp-timeout *seconds*	设置 ICMP 的 NAT 超时时间(缺省值是 60 秒)。
ip nat translation syn-timeout *seconds*	设置 TCP SYN 状态的 NAT 超时时间(缺省值是 60 秒)。
ip nat translation finrst-timeout *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

ip nat translation max-entries *numbers*	设置 NAT 的最大翻译条目数(缺省值是 4000)。
ip nat translation max-entries host A.B.C.D *numbers*	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。
ip nat translation max-entries host any *numbers*	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
clear ip nat translation *	从 NAT 转换表中清除所有动态地址转换项。
clear ip nat translation inside *local-ip global-ip* [outside *local-ip global-ip*]	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。
clear ip nat translation outside *local-ip global-ip*	清除包含外部翻译的简单的动态翻译项。
clear ip nat translation inside *local-ip local-port global-ip global-port* [**outside** *local-ip local-port global-ip global-port*]	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
show ip nat translations [**host** *A.B.C.D* | **tcp** | **udp** | **icmp**][**verbose**]	显示活动翻译。
show ip nat statistics	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：

A 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。

A 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。

A 不支持IP NAT OUTSIDE SOURCE 规则

A 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”。

2.2.8 NAT 日志配置

Nat 条目创建时，会用 syslog 记录新建条目的记录。

ip nat log { translations syslog | event syslog }

使用说明：

A 使用 translations，那么会记录 nat 表项的相关信息。

A 使用 event，那么会记录 nat 过程中，nat 表项的各种事件。譬如，最大表项数等。

注：如果使用了 syslog 方式记录 nat 一些条目，会一定程度上影响设备性能。

2.2.9 NAT 端口区域块算法

PAT 方式下，条目创建时，根据配置对于特定的内网主机采用特定的源端口进行翻译。

ip nat inside source list acl-name interface interface-name fixed-srcport x.x.x.x y.y.y.y base-port total-ports

使用说明：

对于[x.x.x.x, y.y.y.y]区间内的主机，平均依次分配从 base-port 开始的共 total-ports 个端口，每个主机获得的是连续端口号。

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-208 171.69.233.208 171.69.233.223 255.2555.255.240
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 Virtual-tunnel1
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
!
ip route default Virtual-tunnel1
!
vpdn enable
!
vpdn-group1
request-dialin
port Virtual-tunnel1
protocol pppoe
pppoe bind Ethernet0/1
!
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 ouside destination static interface Virtual-tunnel1 192.168.20.100
ip nat inside source static tcp 192.168.20.120 80 dialer1 80
ip nat inside source list nat interface interface Virtual-tunnel1
!
```

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 ouside 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
!
```

2.3.8 NAT 端口区域块算法示例

配置如下：

```
interface GigaEthernet0/0
 ip address 172.16.20.64 255.255.255.0
 ip nat outside
!
interface GigaEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
ip access-list extended acl_nat
 permit ip any any
!
ip nat inside source list acl_nat interface GigaEthernet0/0 fixed-srcport 10.0.0
.2 10.0.0.21 1025 60
!
```

上述配置功能，即为[10.0.0.2, 10.0.0.21]这 20 个主机，每个分配 3 个端口号供 PAT 翻译使用，10.0.0.2 获得的是[1025, 1027]，10.0.0.3 获得的是[1028, 1030]，...，10.0.0.21 获得的是[1082, 1084]，当来自 10.0.0.2:20001 的报文经 PAT 翻译之后，源地址:源端口翻译为 172.16.20.64:x（其中 x 为[1025, 1027]区间的任一值）

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 最主要的一项功能是分配接口上的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，同时在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
ip address dhcp	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
ip dhcp-server *ip-address*	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
ip dhcp client minlease *seconds*	指定最小可接受的租用时间 。
ip dhcp client retransmit *count*	指定协议报文的重传次数 。
ip dhcp client select *seconds*	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
show dhcp server	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
show dhcp lease	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
ip dhcpd enable	打开 DHCP Server 服务。
no ip dhcpd enable	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
ip dhcpd ping packets *pkgs*	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
ip dhcpd ping timeout *timeout*	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
ip dhcpd abandon-time *time*	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
ip dhcpd write-time *time*	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
Ip dhcpd pool *name*	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
network ip-addr netsubnet	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
range *low-addr high-addr*	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
default-router *ip-addr …*	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
dns-server *ip-addr* ...	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
domain-name *name*	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
lease {*days* [*hours*][*minutes*] | *infinite* }	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
netbios-name-server *ip-addr*...	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
host *ip-addr netmask*	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
hardware-address *hardware-address{ type}*	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
client-identifier *unique-identifier*	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
client-name *name*	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
show ip dhcpd binding	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
show ip dhcpd statistic	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
show ip dhcpd pool	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
clear ip dhcpd binding {*ip-addr*|*}	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
clear ip dhcpd statistic	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
clear ip dhcpd abandoned	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IP 服务

4.1 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。

4.1.1 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
ip unreachables	发送 ICMP 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
ip redirects	允许发送 ICMP 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
ip mask-reply	发送 ICMP 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。源主机会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
ip mtu *bytes*	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
ip source-route	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
ip route-cache	允许路由缓存（使用路由缓存转发 IP 报文）
no ip route-cache	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
ip route-cache same-interface	允许发送接口与接受接口相同的 IP 报文进行 路由缓存。

4.1.2 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
ip tcp synwait-time *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
ip tcp window-size *bytes*	设置 TCP 窗口尺寸。

4.1.3 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。

4.1.4 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
clear tcp statistics	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
clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}	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

show ip access-lists *name*	显示某个或所有访问列表的内容。
show ip cache [*prefix mask*] [*type number*]	显示用于快速交换 IP 报文的路由缓存。
show ip sockets	显示路由器所有 socket 的信息。
show ip traffic	显示 IP 协议统计数据。
show tcp	显示所有的 TCP 连接状态信息。
show tcp brief	显示简要的 TCP 连接状态信息。
show tcp statistics	显示 TCP 统计数据。
show tcp tcb	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
debug arp	显示地址解析协议（ARP）的交互信息。
debug ip icmp	显示 Internet 控制信息协议（ICMP）的交互信息。
debug ip raw	显示收到的和发送的 Internet 协议（IP）报文信息。
debug ip packet	显示 Internet 协议（IP）的交互信息。
debug ip tcp	显示传输控制协议（TCP）的交互信息。
debug ip udp	显示用户数据报协议（UDP）的交互信息。

4.2 配置访问列表

4.2.1 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
ip access-list standard *name*	使用名字定义一个标准的 IP 访问列表。
deny {*source [source-mask]* | any}[log] **orpermit** {*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过。
exit	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
ip access-list extended *name*	使用名字定义一个扩展的 IP 访问列表。
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [precedence *precedence*] [tos *tos*] [established] [log]{deny | permit} *protocol* 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过。(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.

在接口配置态使用以下命令:

命令	目的
ip access-group *name*	将访问列表应用到接口。

对于标准的访问列表，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。

4.2.2 如果指定的访问列表不存在，所有的包允许通过扩展访问列表示例

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
```

4.2.3 交换芯片无法支持的ipacl 特性

由于某些端口由交换芯片直接控制， 使用在这些端口上的 acl 会通过硬件来做记录和判断. 而硬件的记录和判断能力不如软件来的全面， 所以有些acl 属性是无法被支持的.
以下列出不被支持的acl 属性:
standard access list 中的不被支持属性有**:**

1. log:

example: permit any log

2. 用range 表示的ip 地址范围

example: permit src_range 1.1.1.1 1.1.1.100

extended access list 中的不被支持属性有**:**

1. 匹配端口的acl

example: permit ip interface fastEthernet 0/1 interface ethernet 1/0

2. 用range 表示的ip 地址范围 (包括源地值和目的地址)

example: permit ip src_range 1.1.1.1 1.1.1.10 dst_range 2.1.1.1 2.1.1.100

3. acl 生效的时间范围设定

example: permit ip any any time-range timer_name

4. 报文优先级的限定设置

example: permit ip any any precedence 3

5. 各类大小比较限定符, 如lt, gt, neq

example: permit udp any gt 100 any lt 200

6. 对tcp 的状态限定

example: permit tcp any any established

如果将有不支持属性的 **acl** 应用到交换芯片端口上**,** 系统将给出错误提示**,** 提示用户更改

acl 设定**.**

比如:

ip access-list extended ext

permit ip any any time-range timer_name

端口上配置:

ip access-group ext

系统会打印: IPACL: hardware acl does not support ipacl timer-range

4.2.4 配置 acl 特殊算法

在普通的扩展访问里表配置后增加 massive 关键字, 即对该访问列表表项进行特殊算法处理, 加快查表速度.

加速后, 规则数量将基本不影响查询性能, 但规则数量和复杂度的增加将大幅增加内存消耗.

ip access-list extended *** massive

为了平衡性能和内存消耗, 增加了一个命令

ip access-list table-limit ***

原来一个 acl 表默认转换成一个算法表, 配了这条命令后, 规定每个算法表的规则数量上限, 从而使得一个 acl 表可以转换成多个小的算法表, 内存消耗将会大幅下降, 但由于要查多个表, 性能也会下降. 但相对于内存消耗的下降, 还是很有实际意义的