

网络地址转换技术的应用与实现^{*}

徐 秀

(中国矿业大学计算机科学与技术学院, 江苏 徐州 221008)

摘 要: 随着互联网时代的到来, 很多的机关、企业、学校以至个人用户都希望在 Internet 上进行信息检索与查询等。但合法的 IP 地址对膨胀式 Internet 的发展已经不能满足要求。IP 地址短缺已成为一个十分突出的问题。本文介绍了怎么样利用 NAT 技术解决对 IP 地址紧张情况的处理, 并列出了在 Internet 上非常流行的网络操作系统 FreeBSD 上配置的实现。

关键词: 地址转换; IP 地址; 自由免费的 BSD 操作系统

中图分类号: TP393 **文献标识码:** A **文章编号:** 0529-6579 (2003) S2-0133-03

Internet 的飞速发展, 使网上丰富的资源产生了巨大的吸引力。访问 Internet, 已成为当今信息业最为迫切的需求。但连入 Internet 要受到 IP 地址的许多限制。

1 相关技术的分析

IP 地址负责惟一确定一台计算机在互联网的位置, 并找出通向它的路径后进行相互交换数据,

IP 协议为每个计算机都分配了一个惟一的 IP 地址。网络地址范围由表 1 所示。

这样划分是为了让 IP 地址同时满足要求不同的 IP 地址数量的网络及对 IP 地址数量的需要。IP 地址非常紧张, 虽然提出 IPV6 的标准可以扩展 IP 地址范围, 但目前仍不能完全得到网络的安全支持。这样, 就出现了当前所使用的另一种 IP 地址转换技术 NAT 来解决问题。

表 1 网 络地址范围
Tab 1 Range of Internet addresses

种类	网络地址范围	
A	1. 0. 0. 0 到 126. 0. 0. 0 有效	0. 0. 0. 0 和 127. 0. 0. 0 保留
B	128. 1. 0. 0 到 191. 254. 0. 0 有效	128. 0. 0. 0 和 191. 255. 0. 0 保留
C	192. 0. 1. 0 到 223. 255. 254. 0 有效	224. 0. 0. 0 和 239. 255. 255. 255 保留
D	240. 0. 0. 0 到 239. 255. 255. 255 用于广播	
E	240. 0. 0. 0 到 239. 255. 255. 254 有效	255. 255. 255. 255 用于广播

NAT 可以起到将内部私有地址转换为外部合法的全局地址的功能, 它使不具有合法 IP 地址的用户通过 NAT 访问到外部 Internet。具体的做法是将 IP 包内的地址域用合法的 IP 地址来替换。在建立内部网时可以用以下地址组用于主机。

Class A	10. 1. 1. 1 to 10. 254. 254. 254
Class B	172. 16. 1. 1 to 172. 31. 254. 254
Class C	192. 168. 1. 1 to 192. 168. 254. 254

在分配接口 IP 地址时接上设置: interface type slot/number。为接口设置 IP 地址: ip address ip -

address mask。设置 NAT 功能的路由至少要有有一个 inside, 一个 outside。inside 连接的网络用户, 使用的是内部 IP 地址 (非法 IP); outside 连接的是外部的网络, 使用电信部门分配的 IP 地址。Inside 和 outside 都可以是路由上的任意端口。NAT 路由器被放于内部网和 Internet 边界上, 并且在将数据包发送到外部网络前, 将数据包的地址转换为合法的 IP 地址。从而与 Internet 上的其他主机进行通讯。当多个内部主机共享一个合法的 IP 地址时, NAT 是通过端口多路复用来更改外部数据包的端口并进行端口映射来完成。

^{*} 收稿日期: 2003-04-08
作者简介: 徐秀 (1972 年生), 女, 硕士生; E-mail: xuxiu@cumt.edu.cn
(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2 NAT 的实现

NAT 主要应用环境之一是当用户不想让外部网络用户知道自己的网络内部结构时, 可通过 NAT 将内部网络与外部 Internet 隔离, 使外部用户不知道 NAT 设置的内部 IP 地址。另外一个应用环境是当一个用户申请的合法 Internet 的 IP 地址很多时, 通过 NAT 功能实现多个用户同时公用一个合法 IP 与外部 Internet 进行通信。

2.1 静态地址转换

它是将内部本地地址与内部合法地址进行一对一的转换, 且需要指定和哪个合法地址进行转换。如果内部网络有 E mail 服务器或 FTP 服务器等为外部用户提供服务, 则采用静态地址转换以方便外部用户使用这些服务。基本配置步骤如下:

(1) 在内部本地地址与内部合法地址之间建立静态地址转换。

(2) 指定连接网络的内部端口, 在端口上设置状态下输入。

(3) 指定连接外部网络的外部端口, 在端口设置状态下输入。以路由器 2501 的配置为例:

```
Ip nat inside source static 10.1.1.2 192.1.1.2
Interface Ethernet 0
Ip address 10.1.1.1 255.255.255.0
Ip nat inside
Interface serial 0
Ip address 192.1.1.1 255.255.255.0
Ip nat outside
No ip mroute-cache
Bandwidth 2000
No fair-queue
Interface serial 1
No ip address
Shut down
No ip classless
Ip route 0.0.0.0 0.0.0.0 serial 0
Line con 0
Line vty 0 4
Password cisco
End
Show ip nat statistics
Show ip nat translations
```

2.2 动态地址转换

它是将内部本地地址与内部合法地址一对一转换, 从内部合法地址池中动态选择一个未使用的地址来对内部本地地址进行转换。动态地址转换配置步骤如下:

(1) 在全局设置模式下, 定义内部合法地址

池。

(2) 在全局设置模式下, 定义内部地址动态地址转换。

(3) 在全局设置模式下, 将内部本地地址与指定的内部合法地址池进行地址转换。

(4) 指定与内部网络相连的内部端口在端口设置状态下。

(5) 指定与外部网络相连的外部端口。

```
Ip nat pool aaa 192.1.1.2 192.1.1.10 netmask 255.255.255.0
```

```
Ip nat inside source list 1 pool aaa
Interface Ethernet 1
Ip address 10.1.1.1 255.255.255.0
Ip nat inside
Interface serial 0
Ip address 192.1.1.1 255.255.255.0
Ip nat outside
```

2.3 复用动态地址转换

它是首先进行动态地址转换, 允许多个内部本地地址共用一个内部合法地址, 它只适用申请到少量 IP 地址, 但却经常同时有多于合法地址个数的用户上外部网络的情况。复用动态地址转换配置步骤如下:

(1) 在全局设置模式下, 定义内部合法地址池。

(2) 在全局设置模式下, 允许内部地址进行动态地址转换。

(3) 在全局设置模式下, 设置内部本地地址与合法 IP 地址建立复用动态地址转换。

(4) 端口设置状态下, 指定与内部网络相连的内部端口。

(5) 端口设置状态下, 指定与外部网络相连的外部端口。

```
Ip nat pool bbb 192.1.1.1 192.1.1.1 netmask 255.255.255.0
```

```
Ip nat inside source list 1 pool bbb overload
Interface Ethernet 0
Ip address 10.1.1.1 255.255.255.0
Ip nat inside
Interface serial 0
Ip address 192.1.1.1 255.255.255.0
Ip nat outside
No ip mroute-cache
Bandwidth 2000
No fair-queue
Interface serial 1
No ip address
Shut down
```

```
No ip classless
Ip route 0.0.0.0 0.0.0.0 serial
Access-list 1 permit 10.1.1.0 0.0.0.255
```

3 例举 NAT 的具体应用技术

NAT 的实现可以通过路由器或防火墙等硬件形式来完成，也可以通过网络操作系统等软件形式实现，本例以软件技术来说明 NAT 在具体网络环境中的实现。

FreeBSD 是运行在 intel 平台上可以自由使用的 UNIX 网络操作系统。它支持多个使用者同时使用 FreeBSD，共享系统的磁盘、外设、处理器等系统资源。同时也支持全面的 TCP/IP 协议。可以用作 internet /intranet 的服务器。提供 NFS，FTP，E mail，WWW 路由和防火墙的能力。开发者们通过 FreeBSD 在 Internet 彼此相互联系。在 FreeBSD 系统中用户级 PPP 提供 alias 功能。使用 alias 参数启动 PPP 将所有来自其他网络介面的数据包中的源 IP 地址改变为 tun 0 网络界面的 IP，转发到 PPP 且连接上去来实现 NAT 功能。内核通过一个特定的 diver 类型的端口将需要转换的数据包交给 Natd，而 Natd 转换之后再发送回内核，由内核再进行转发。

设置 Natd 需要以下的步骤：首先设置好包过滤支持，包括内核中的 ipfirewall 和 rc.conf 中的 gateway enable 参数设置。然后为 Natd 指定一个 divert 端口。用于接收和发送从内核转发过来的包。这需要在 /etc/services 中增加一个 divert 端口设置 (natd 8668/divert)。

最后将所有的数据包发送给相应的 divert 端口 natd，由监听这个端口的守护进程 natd 接收并转换。以下是使用 ipfw 指令 divert，通过 divert 规定的端口 natd 进行地址转换：

```
#/sbin/ipfw f flash
```

```
#/sbin/ipfw add divert natd all from any to any via fxpo
#/sbin/ipfw add pass all from any to any
alias-address 202.102.245.60
Deny incoming yes
Unregistered only yes
Same poros yes
Use sockets yes
```

其中 Deny incoming 用于拒绝向 alias address 发起的所有连接请求，保护网络内部安全。它和 -redirect port 参数结合，控制提供的网络服务。Unregistered only 用于只对 RFC1918 定义的内部网址进行地址转换，是为防止出现错误设置影响正常的路由设置。Same poros 选择与原数据包相同的端口，来保证与端口相关的服务。Use sockets 是允许 Natd 查出 FTP、IRC 连接的数据内部，以设置正确的端口。在设置好文件之后，就可以启动 Natd 了。

4 结 语

NAT 的功能就是在一个网络内部，根据需要可以随意自定义的 IP 地址。在网络内部，各计算机间通过内部的 IP 地址进行通讯。当内部计算机要与外部的 Internet 网络进行通讯时，有 NAT 功能的设备负责将其内部 IP 地址转换为合法 IP 地址进行通信。从而达到了与 Internet 的互联。

参考文献:

[1] 陈庆章. 用 NAT 实现 IP 地址的平稳转移[J] . 计算机工程, 2002, 6: 23— 25.
[2] <http://202.119.199.89/freebsd/index.htm> [EB/OL] . 2003— 01.
[3] <http://www.zdnet.com.cn/developer/category/web/service/dotnet/> [EB/OL] . 2003— 03.
[4] <http://www.ccidnet.com.cn/> [EB/OL] . 2003— 03.
[5] <http://linkwan.com/gb/routertech/router/> [EB/OL] . 2003— 03

Application and Achievement of NAT

XU Xiu

(Department of Computer Science and Technology, China University of Mining, Xuzhou 221008, China)

Abstract: Come in with internet, too many institutions, establishments, schools, up to personal customers are hoping proceed information retrieval and query in internet. But IP addresss of weii formed cannot gratify demand of inflate development in internet. Run short of the IP addresss has already become ever so much a problem. This text introduce how to make use of the IP address, and lists allocation of FrssBSD in internet.

Key words: NAT; IP address; FreeBSD