# 在VxWorks下实现NAT/NAPT的方法

■ 华北电力大学 刘燕华
■ 东方通信科技发展有限公司 林立志

摘 要 介绍NAT、NAPT的基本概念和工作原理；结合VxWorks的网络协议栈，描述一种利用VxWorks操作系统提供的钩子函数来开发实现NAT和NAPT的方法。

关键词 NAT NAPT 钩子函数 网络协议栈 截获 转换 校验和

## 引 言

近年来，随着Internet的迅猛发展，连入Internet的主机数量成倍增长。由于最初设计Internet的时候并没有考虑到需要支持这么大的规模，因而Internet使用的IPv4协议中IP地址的长度选择了32位，它可以使IP包的格式很好地对齐；但是，目前IP地址的短缺已经成为Internet面临的最大问题之一。

为了解决IP地址短缺的问题，人们提出了许多解决方案，以使Internet能够支撑到新一代IP协议IPv6的出台。在众多的解决方案中，网络地址转换NAT（Network Address Translation）技术提供了一种完全将私有网和公共网隔离的方法，从而得到了广泛的应用。

## 1 NAT技术

NAT技术的基本功能就是，用1个或几个IP地址来实现1个私有网中的所有主机和公共网中主机的IP通信。NAT技术可以为TCP、UDP以及ICMP数据包提供透明转发。

### 1.1 NAT工作原理

NAT的基本工作原理是，当私有网主机和公共网主机通信的IP包经过NAT网关时，将IP包中的源IP或目的IP在私有IP和NAT的公共IP之间进行转换。

如图1所示，NAT网关有2个网络端口，其中公共网络端口的IP地址是统一分配的公共IP，为202.204.65.2；私有网络端口的IP地址是保留地址，为192.168.1.1。私有网中的主机192.168.1.2向公共网中的主机166.111.80.200发送了1个IP包（Des = 166.111.80.200，Src = 192.168.1.2）。当IP包经过NAT网关时，NAT会将IP包的源IP转换为NAT的公共IP并转发到公共网，此时IP包（Des = 166.111.80.200，Src = 202.204.65.2）中已经不含任何私有网IP的信息。由于IP包的源IP已经被转换成NAT的公共IP，响应的IP包（Des = 202.204.65.2，Src = 166.111.80.200）将被发送到NAT。这时，NAT会将IP包的目的IP转换成私有网中主机的IP，然后将IP包（Des = 192.168.1.2，Src = 166.111.80.200）转发到私有网。对于通信双方而言，这种地址的转换过程是完全透明的。

### 1.2 NAPT技术

由于NAT实现的是私有IP和NAT的公共IP之间的转换，那么，私有网中同时与公共网进行通信的主机数量就受到NAT的公共IP地址数量的限制。为了克服这种限制，NAT被进一步扩展到在进行IP地址转换的同时进行Port的转换，这就是网络地址端口转换NAPT（Network Address Port Translation）技术。

NAPT与NAT的区别在于，NAPT不仅转换IP包中的IP地址，还对IP包中TCP和UDP的Port进

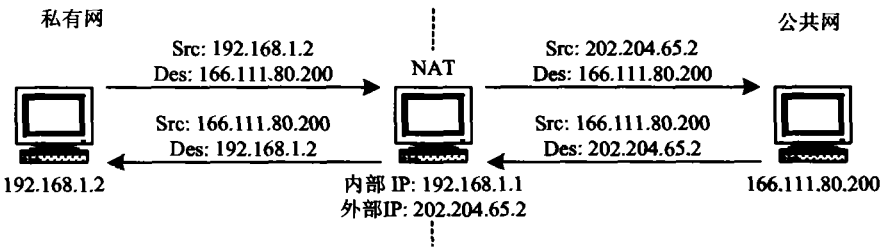


图1 NAT工作原理示意图

行转换。这使得多台私有网主机利用1个NAT公共IP就可以同时和公共网进行通信。

如图2所示，私有网主机192.168.1.2要访问公共网中的Http服务器166.111.80.200。首先，要建立TCP连接，假设分配的TCP Port是1010，发送了1个IP包（Des = 166.111.80.200:80，Src = 192.168.1.2:1010），当IP包经过NAT网关时，NAT会将IP包的源IP转换为NAT的公共IP，同时将源Port转换为NAT动态分配的1个Port。然后，转发到公共网，此时IP包（Des = 166.111.80.200:80，Src = 202.204.65.2:2010）已经不含任何私有网IP和Port的信息。由于IP包的源IP和源Port已经被转换成NAT的公共IP和Port，响应的IP包（Des = 202.204.65.2:，Src = 2010166.111.80.200:80）将被发送到NAT。这时NAT会将IP包的目的IP转换成私有网主机的IP，同时将目的Port转换为私有网主机的Port，然后将IP包（Des = 192.168.1.2:1010，Src = 166.111.80.200:80）转发到私有网。对于通信双方而言，这种IP地址和Port的转换是完全透明的。

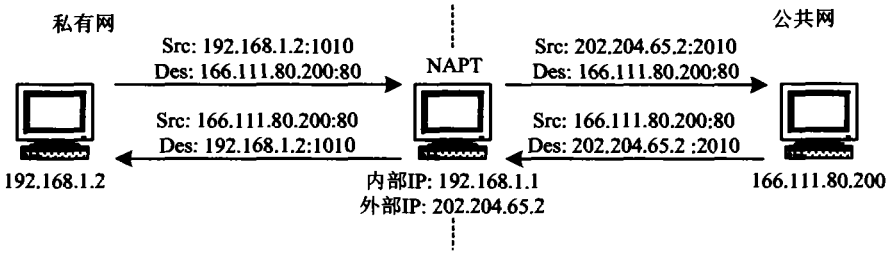


图2 NAPT工作原理示意图

## 2 VxWorks的网络协议栈

与VxWorks操作系统捆绑发行的标准网络协议栈，是一个与BSD4.4兼容、功能齐全并针对嵌入式应用作了大量优化的TCP/IP协议栈。该网络协议栈与VxWorks操作系统、开发工具、设备管理工具以及上层协议和应用可以集成在一起，有完整的路由功能并可以根据需要进行剪裁。VxWorks的网络协议栈的分层结构如图3所示。

VxWorks网络协议栈传输数据使用的内存，是在系统启动进行网络协议栈初始化的时候就申请下来的，并使用系统提供的netBufLib建立内存节点池来管理这些内存空间。网络协议栈传输数据所需的内存都是从这些内存节点池中申请，使用完毕后再释放。

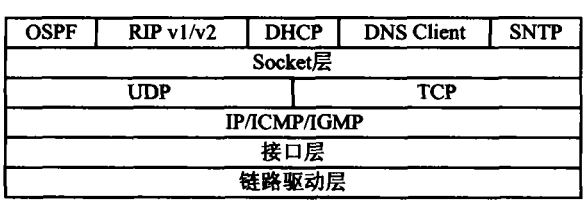


图3 VxWorks的网络协议栈

netBufLib通过3种数据结构处理网络协议栈传输的数据：mBlk、clBlk和Cluster。其中，Cluster保存的是实际的数据，mBlk和clBlk中保存的信息是用来管理Cluster中保存的数据的。为了满足传输不同大小数据的需要，Cluster是一些大小不同的内存块；缺省情况下，VxWorks网络协议栈创建了大小从64~2048字节的6个不同的内存节点池。

由于mBlk中保存的只是指向数据的指针，因此网络协议栈不同层之间的数据传输可以避免数据拷贝。此外，对于分布在多个Cluster中的数据，可以通过mBlk把它们链在一起，并且只需要传递链首的mBlk就可以了。VxWorks网络协议栈的“零拷贝”技术就是建立在这种机制的基础之上的。图4描述了2个提交给网络协议栈TCP层的包的数据结构。

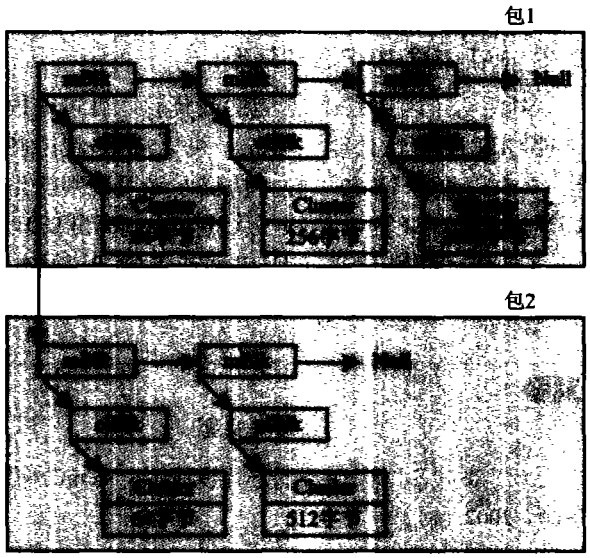


图4 提交到TCP层的2个包

在mBlk结构中，有2个指向其它mBlk的指针：1个指向同一个包的下一个mBlk；另一个指向下一个包的链首的mBlk。ClBlk指向的就是实际存储数据的Cluster。

## 3 向VxWorks网络协议栈加入NAT

为了向VxWorks网络协议栈中加入NAT，必须实现2个基本操作：IP包的截获和IP包的处理。

### 3.1 VxWorks下IP包的截获

VxWorks网络协议栈在物理驱动层和IP层上分别提供了两类钩子函数：EtherHook和IpFilterHook。利用这两类钩子函数，可以实现对IP包的截获。

（1）EtherHook

EtherHook提供对以太帧的截获功能。它包括2个钩子函数：以太帧接收钩子函数EtherInputHook和以太帧发送钩子函数EtherOutputHook。它们分别用函数EtherInputHookAdd和EtherOutputHookAdd安装。安装了这些钩子函数后，每当有以太帧被接收到时，函数EtherInputHook就会在该以太帧被提交给上一层处理前被自动调用；每当有以太帧被发送时，函数EtherOutputHook会在该以太帧被发送前被自动调用。通过截获以太帧，可以达到截获IP包的目的。

（2）IpFilterHook

IpFilterHook提供对IP包的截获功能。它只对应1个钩子函数，用函数ipFilterHookAdd就可以完成IpFilterHook的安装。安装了IpFilterHook后，每当有IP包被接收到时，函数IpFilterHook就会被自动调用，从而实现对IP包的截获。

### 3.2 NAT过程中IP包的处理

利用钩子函数完成IP包的截获后，就可以根据需要对IP包进行处理。首先，可以从IP包中剥离出IP头，根据IP头中的“协议”域可以判断出是UDP包还是TCP包。然后，从IP包中剥离出UDP头或TCP头，利用IP头和UDP头或者TCP头中的相关信息，就可以根据需要进行IP地址和Port的转换处理。

NAT一般采用1个映射表来实现IP地址和Port的转换。对于截获到的IP包，通过比较IP包的目的IP、目的Port、源IP、源Port和NAT映射表中的相应表项，对IP包的目的IP、目的Port、源IP、源Port进行转换。

典型的NAT映射表如图5所示。

| NAT映射表项 | | | | | |
|---|---|---|---|---|---|
| Real Src IP | Real Src Port | Des IP | Des Port | NAT IP | NAT Port |

图5 NAT映射表示意图

（1）处理由内到外的IP包

由内到外的IP包指的是私有网主机通过NAT发送到公共网主机的IP包。它的源IP是私有IP，目的IP是公共IP。

当截获到1个由内到外的IP包时，NAT首先以IP包的源IP和源Port作为Real Src IP和Real Src Port的匹配条件，在映射表中进行搜索。如果找到1个对应的表项，就用表项的NAT IP和NAT Port替换IP包的源IP和源Port，而保持IP包的目的IP和目的Port不变。然后，重新计算TCP或UDP的校验和，就可把IP包归还给VxWorks网络协议栈。

如果在映射表中没有搜索到对应的表项，NAT就会向映射表中添加1个新的表项。该表项中的Real Src IP和Real Src Port用IP包的源IP和源Port来填充；NAT IP用NAT的公共IP填充，NAT Port用NAT分配的1个空闲Port填充。然后，根据新增加的表项，按照上面相同的步骤完成对IP包的处理。后续相同的IP包也都用这个表项来处理。

（2）处理由外到内的IP包

由外到内的IP包指的是从公共网通过NAT发送到私有网的IP包。它的源IP是公共IP，目的IP


参考文献

1 欧阳坚，等. 系统级芯片设计与SystemC. 微电子学，2002（6）

2 夏宇闻. Verilog基本知识（上、下）. 电子产品世界，2002（10A/B）

3 Synopsys. SystemC™ User's Guide(Version 2.0). 2002年White Paper

4 Synopsys. SystemC Reference Manual Release 2.0. 2001年White Paper

5 袁俊泉，等. Verilog HDL数字系统设计及其应用. 西安：西安电子科技大学出版社，2002

6 Co-Design. SuperlogV2—Powerful, Fast, Evolutionary Design & Verification Language. http://www.co-design.com

7 Co-Design. Evolving the Next Design Language.http://www.co-design.com

8 姜立东，等. VHDL语言程序设计及应用. 北京：北京邮电大学出版社，2001


（收稿日期：2003-02-20）

是NAT的公共IP。

当截获到1个由外到内的IP包时，NAT就以IP包的目的IP和目的Port作为NAT IP和NAT Port的匹配条件，在映射表中进行搜索。如果找到1个对应的表项，就用表项的Real Src IP和Real Src Port来替换IP包的目的IP和目的Port，而保持IP包的源IP和源Port不变。然后，重新计算TCP或UDP的校验和，就可把IP包归还给VxWorks网络协议栈。

如果在映射表中没有搜索到对应的表项，则对IP包不作任何处理，直接归还给VxWorks网络协议栈。

（3）NAT映射表的配置

作为NAT完成IP包中IP和Port转换的依据，NAT映射表的管理关系到NAT的功能和性能。NAT映射表的配置可以分为2部分：静态配置部分和动态配置部分。

静态配置部分主要用于NAT IP、NAT Port和私有IP、私有Port的映射关系可以预见的应用，例如UDP通信和TCP Server运行在私有网中某个主机等情况。NAT映射表静态配置部分可以在NAT运行前根据规划直接完成配置。

动态配置部分主要用于NAT IP、NAT Port和私有IP、私有Port的映射关系不可预见的应用，例如在私有网中某个主机上运行TCP Client来与公共网中某个主机上的TCP Server建立连接进行通信。在这种情况下，私有网主机使用的Port是动态分配的。为了实现需要NAT IP、NAT Port和私有IP、私有Port的转换，必须动态配置NAT映射表。相对于静态配置部分而言，动态配置部分的数据结构、数据组织和搜索算法的设计和实现的难度要大得多，关键是要实现一个高效的搜索算法。

**参考文献**

1 WindRiver. VxWorks Network Programmer's Guide

2 Uyless Black. TCP/IP & Related Protocols(Second Edition)

3 Comer Douglas E. 用TCP/IP进行网际互连. 第3版. 林瑶等译. 北京：电子工业出版社，2000

（收稿日期：2003-03-06）

# 风河公司推出风河汽车信息娱乐平台

近日，嵌入式软件和服务知名厂商风河系统公司宣布推出风河汽车信息娱乐平台（PLATFORM CI），这是一个行业市场整合嵌入式平台，可作为开发汽车信息娱乐和远程信息处理设备的软件基础。汽车信息娱乐平台为原始设备制造厂家和一级供应商提供了一个汽车行业市场嵌入式平台，它预先整合了风河VxWorks，并具有开发工具、多媒体应用程序界面和连接协议。使用汽车信息娱乐平台，制造商就具备了开发非常可靠的汽车信息娱乐产品的所有基础。

汽车信息娱乐平台的主要特性包括：

* 操作系统、嵌入式开发工具和汽车硬件支持：汽车信息娱乐平台依赖于最先进的汽车信息娱乐处理器和芯片组所采用的VxWorks 实时操作系统、嵌入式开发工具和硬件升级工具的支持。

* 汽车连接性：汽车信息娱乐平台为与其它汽车内设设备、消费电子产品和网络基础设备相连接的设备提供驱动和协议。也提供对CAN、MOST、USB和802.11支持。

* 多媒体支持：汽车信息娱乐平台包括WIND ML（风河多媒体图书馆），可为图形用户界面和多媒体功能提供支持。

* 服务和培训：汽车信息娱乐平台可赠送积分，灵活换取服务和培训。汽车信息娱乐平台也包括一个可定制的WIND SPRINT安装和入门培训服务。即在客户的公司现场用两天的时间来帮助客户尽快起动项目，并在现场环境下培训用户使用汽车信息娱乐平台。

* 伙伴技术：为保证拥有全面的整合技术，风河公司与世界领先企业进行了例如开放服务网关组织规范（OSGi）、语言识别及合成、IDB-1394网络、蓝牙、浏览器和电子邮件技术的合作。

风河系统中国区总经理韩青先生说："随着消费者对交通工具的服务和功能性的需求迅速增长，生产汽车信息娱乐设备的原始设备生产厂商和一级供应商面临着越来越激烈的竞争和因设备复杂性的增加而带来的众多开发挑战问题。通过在风河汽车信息娱乐平台上进行标准化生产，原始设备生产厂商和一级供应商可完全依赖已经验证的集成技术和汽车专业知识，以便使他们的开发人员能够专注于有竞争力的增值技术，从而满足客户的需求。"

有机构预测，在2006年至2010年之间，全球将有超过1.05亿采用远程信息处理技术的汽车投入使用。如果要为驾驶员和乘客提供广泛的服务，并保证所生产的设备能被消费者接受的话，汽车信息娱乐和远程信息处理设备开发商必须使用一种已经验证的集成软件。通过在类似汽车信息娱乐平台的软件平台上进行标准化生产，原始设备制造厂家和一级供应商可以有效地避免初始开发环节，而专注于他们的主营业务——开发最新、最有创意及物美价廉的设备。