一种限制宽带共享的接入驱动程序设计①

杨忠明

(广东石油化工学院 理学院，茂名 525000)

摘 要：针对目前主流的多种限制宽带共享的方法缺陷，设计了一个限制宽带共享的接入驱动程序。在接入用户的系统中安装一个底层的驱动程序，通过建立特殊的点对点通道方法把接入驱动绑定在用户系统中。该驱动不但限制了用户使用宽带路由器，也限制了用户卸载接入驱动开启代理服务器的行为。该驱动使用数据特征分析法甄别用户是否在使用代理服务器软件共享宽带，在实际工程应用中有一定的参考价值。

关键词：NDIS；宽带共享；驱动

Design of an Access Driver Program to Restrict Broadband Sharing

YANG Zhong-Ming

(Faculty of Science, Guangdong University of Petrochemical Technology, Maoming 525000, China)

Abstract: Contra-posing the deficiencies of many current mainstream methods which are restricted in sharing broadband, we design an access driver of restriction of Broadband Sharing. In the access-user's system, we install a low-level driver, through which to establish a special point to point channel method to bind the access drivers to the user's system. The driver does not only limit the user to use broadband router, it also limits the behavior that user to uninstall the access drivers to startup the proxy server. This drivers use the data property method to discriminate user who are using proxy server software to share broadband. These have some reference value in practical application.

Keywords: NDIS; broadband sharing; drive

1 引言

目前宽带网络中提供用户接入互联网的方式主要有固定 IP、DHCP、PPPoE 接入、802.1x 接入等，普遍存在宽带共享现象，如何有效打击宽带共享行为是目前宽带运营商研究的一个热点问题，已出现诸如 TLL(Time To Live)检测法、MAC(Medium/Media Access Control)地址检测法、拨号密码转换法、SNMP(Simple Network Management Protocol)服务检测法、代理服务器检测法等多种手段：

(1) MAC 地址检测法

通过检查宽带用户同一个 IP 地址的数据包，如果发现包含多个 MAC 地址，就判定用户共享上网，并发出相应的限制警告。可以通过克隆网卡 MAC 地址的方法实现突破限制。

(2) TTL 检测法

当一个数据包通过一级路由的时候，TTL 值会发生变化，宽带接入系统可通过检测 TTL 值的办法来限制用户使用路由器共享上网，但目前市面上已经出现一些宽带路由在数据包通过的时候不改变 TTL 值，使得这种方法受到很大的限制，只能针对老款路由器使用。

(3)“星空极速”软件[1]

有部分地区的宽带运营商给 ADSL 用户专门配备了一款名为“星空极速”的拨号软件，该软件内置一个密码协议转换器，将接入密码进行了加密换算。目前可使用软件计算密码或升级宽带路由补丁的方式突破限制。

(4) SNMP 服务检测[2]

① 基金项目:珠海市产学研项目(PC20082015);茂名市科技计划重点项目(20091007)
收稿时间:2010-08-06;收到修改稿时间:2010-09-14

使用 SNMP 服务的管理软件（如网络尖兵）来查看 ADSL 宽带用户连接情况，从而判断线路上是否有共享上网的电脑以及共享的电脑台数。面对这种检测手段，用户可以禁用 SNMP 服务，即关闭设备的 161 端口。

(5) 代理服务器检测[3]

通常检测代理服务器是使用特征检测法，比如著名的 CCPROXY 代理服务器软件就会在 HTTP(HyperText Transfer Protocol)的数据包中添加自己的特征字段，而且多个非法用户使用的操作系统不相同，不同的操作系统同样也会在 HTTP 的数据包中添加自己的特征字段。所以可以通过上述的方法来实现代理服务器的判断，但是这样的特征判断法存在一定的误差，而且随着代理服务器软件的快速更新，这些漏洞会很快被填补，无法实现长期有效的管理。

本文试图通过开发一个用户拨号接入的驱动程序，实现限制宽带共享的行为，能够用更有效的手段阻止宽带共享，且可在接入驱动程序实现更多的网络管理功能，如网络病毒控制、并发连接数限制等。开发接入驱动可利用 NDIS（Network Driver Interface Specification）中间驱动程序的架构，可以在网卡驱动程序和传输驱动程序之间插入一层自定义的处理函数，以实现限制宽带共享的效果。本文设计的接入驱动程序是以 NDIS 驱动的形式工作，在系统的驱动层运行，在网络用户的使用角度与以前使用标准 PPPoE 拨号系统上网没有任何区别，不需使用特殊的拨号接入软件。

2 接入驱动程序系统设计

2.1 系统框架设计

本文主要讨论基于 NDIS 的中间层驱动架构的一个接入驱动程序设计。NDIS 体系设计是遵循 OSI 七层模型的，但在具体划分层次的时候，并没有一一对应的层次结构。NDIS 定义了物理硬件，小端口驱动，协议驱动，传输驱动接口四个层次[4]。

接入驱动程序采用 DDK 中附带的示范代码 passthru 为编写的基础。passthru 是一个中间层过滤型的驱动程序，这个程序框架结构非常清晰规范，本文讨论的驱动程序也是一个中间层驱动程序，结构上有很大的共性。因此接入驱动程序的实现可在 passthru 源代码基础上修改增加，完成本文需要的驱动程序编写。接入驱动程序系统在 NDIS 架构中所处位置如图 1 所示。

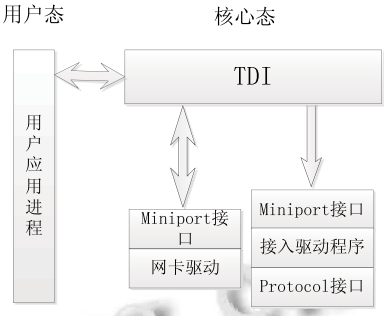

图 1　接入驱动程序系统位置图

NDIS 定义了操作系统网络传输模块的一个抽象环境，在这个环境中，各层驱动程序实体之间没有直接的通信机制，它们之间的交互全部由 NDIS（通过操作系统中的 NDIS Lib 或 NDIS Wrapper）提供统一例程和调用来实现。NDIS 负责上下层驱动程序之间服务原语和实际驱动程序相应调用入口之间的转换，分派消息通知。

NDIS 驱动程序一般是在主入口函数 DriverEntry 中根据驱动程序类型使用不同注册函数注册自己的输出函数集的入口。只要符合 NDIS 架构的设计原则，设计中并不需要知道其他驱动程序的入口，只需向 NDIS 注册私有的入口点即可，一般在主入口函数 DriverEntry 中根据驱动程序类型使用不同注册函数注册自己的输出函数集的入口。

对于发送出去的数据包处理，只要在 PassThru 中的 MiniportSend 和 MiniportSendPackets 中加入必要的操作代码，而对于接收的数据包时，则需要在 ProtocolReceive 和 ProtocolReceviePackets 中加入必要的操作代码。如此即实现了一个简单的包处理中间层驱动。

接入驱动程序即在这个包处理驱动上实现，可以添加一些以数据包为处理对象的网络行为控制功能，一切的实现均在底层运行，在网络用户的使用角度与以前使用标准 PPPoE 拨号系统上网没有任何区别。

2.2 数据发送与接收

接入驱动程序位于 NdisWan 下层，每次只接收一个 NDIS_WAN_PACKET 结构中仅包含一个 PPP 帧，所以不必考虑多包发送机制。而且接入驱动程序是作为 NIC 硬件驱动的协议来运行，以太网是属于无连接

类型，接入驱动程序仅需要实现无连接类型单包发送机制。

NDIS_PACKET 是整个 NDIS 体系的核心数据结构，所有流入流出的网络数据报文在 NDIS 中都将以 NDIS_PACKET 来表示。为了提供平台无关性，NDIS 中不少的函数都是 NDIS_PACKET 操作函数。为了实现源代码的平台无关性，一定要避免直接操纵 NDIS_PACKET 结构，而是要使用 NDIS 提供的操作函数来操作。

具体的数据发送与接收流程如图 2，图 3 所示。

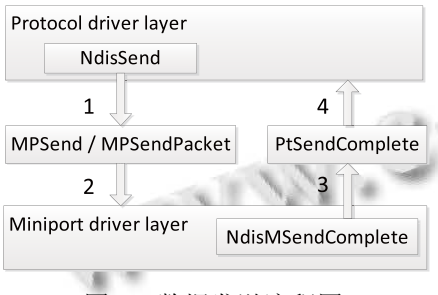

图 2 数据发送流程图

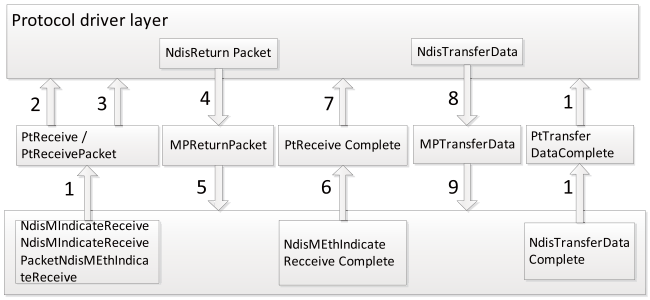

图 3 数据接收流程图

3 限制宽带共享的模块设计

3.1 点对点通信的特殊通道设计

为了与标准 PPPOE 协议区分开来，接入驱动程序的以太网帧类型 type 由标准的类型代码 0x8864/0x8863 改为 0xxxxx/0xxxxx，可保证用户无法通过简单修改 PPPOE 拨号软件发送数据包的类型取代本接入驱动，简单绕开驱动的过滤机制，Session_ID 采用了加密的方法。同时本方法也达到了限制用户使用宽带路由器共享上网行为的效果。以太帧结构优化如图 4 所示。

通过接入驱动程序可实现一条专用的点对点通道，该通道以 PPPoE 协议为框架，对其进行特殊化后，可限定用户必须使用本驱动。并且在驱动中对共享上网的行为进行了限制，实现了具有特殊意义的点对点通道，对网络的安全管理有很大的帮助，且保护了运营商的投资，杜绝共享上网的盗用网络资源的行为。

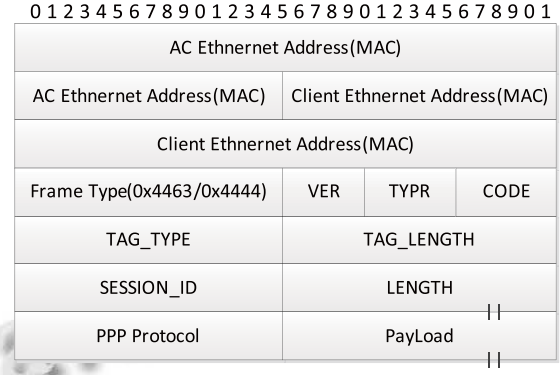

图 4 接入驱动程序的以太网帧结构

3.2 限制宽带共享的设计

代理服务器可为区域内用户提供共享上网的业务，其主要数据特征有两类：

(1) 转发远程用户机的请求，如 HTTP 代理即转发 HTTP 协议相关的一些命令等。对此类特征只需拦截用户机发送到代理服务器的第一个请求即可，HTTP 第一请求的固定格式为：GET URL HTTP/1.0 Accept image/gif 等。

处理方法：监控局域网内的用户机发送的数据，查找匹配特征“GET”及查找匹配特征“HTTP/1.0”，若两种特征同时存在的请求，即抛弃该相应的数据包。当请求命令无法发送的时候，用户机即无法通过代理服务器共享宽带。

(2) 代理服务器一般采用固定端口为用户机提供服务，代理服务器进程具有某端口接受大量的内网用户机的流量且有大量的流量到外网的流量特征，那么可在接入驱动程序监控本机进程与端口的数据通信情况进行分析判断，核心算法步骤如下。

当一个新的数据包到达，则启动以下步骤：

第一步：检查该数据包对应的通信端口是否在监控记录表中存在，如存在跳到第 3 步；

第二步：添加一个新的通信端口至监控记录表中；

第三步：在监控记录表中更新通信端口的通信量数据；

第四步：查找通信量最大的前三个端口对应的应用程序，查找监控记录表中其是否同时存在内网与外

网两种流量；

第五步：对疑似代理服务器的进程对应的内网通信端口进行流量阻断，禁止该进程与内网用户通信。

除了使用代理服务器软件，还可使用 Windows 系统自带的 Internet 共享程序（简称 ICS）进行共享上网。ICS 使用两个网络之间路由 TCP/IP 数据包的网络地址转换 (NAT) 技术。ICS 连接内部网络（通常在小型家庭本地区域网络）和外部网络（通常 Internet）。ICS 将关联到内部网络上的特定 Internet 协议（IP）地址的 TCP/UDP 端口号。在表中会记录到 IP 地址关联的端口号。

根据 ICS 的工作原理分析，可根据数据包中的 IP 地址判断系统是否开启了 ICS 服务。开启了 ICS 服务后，通常会出现一个内网向外网请求的数据包（目标地址是外部网络 IP，源地址是内部网络 IP）及会出现对应的一个回复请求的数据包（目标地址是内部网络 IP，源地址是外部网络 IP，其 IP 与请求数据包一一对应）。若在接入驱动中捕抓到以上特征的数据包，即视为该系统启动了 ICS 服务，中断该系统的上网业务。

4 小结

目前研究限制宽带共享是一个热点问题，本文分析了目前限制宽带共享的一些主流技术手段的技术方法及其缺陷，提出了设计一种在接入用户端实现接入驱动程序的方法进行限制带宽共享。该接入驱动程序基于 NDIS 架构进行开发，以 Microsoft 提供的标准 NDIS 框架 passthru 为基础，添加自定义的处理函数进行包分析与过滤。接入驱动通过修改以太网帧类型 type 的内容实现与服务器的加密点对点特殊通道，可保证用户无法绕开驱动的过滤机制，也达到了限制用户使用宽带路由器共享上网行为的效果。在驱动处采用数据特征分析方法可对用户系统中运行的程序进行分析，甄别是否代理服务器，从而实现限制用户机使用代理服务器提供宽带共享，在实际工程应用中有一定的参考价值。

参考文献

1 方徐.星空极速破解面面观.微型计算机,2007,11:150−150.

2 安志锋.破解网络尖兵初探.电脑知识与技术,2006,8:101−102.

3 崔建,钱杰,张蓓.校园网中代理服务器和 NAT 设备的监控与防范.大连理工大学学报,2005,10:90−94.

4 李晓莺,曾启铭.NDIS 网络驱动程序的研究与实现.计算机应用,2002,22(4):60−61.

（上接第 240 页）

3 结论

作为企业来讲，通过过程改进提高成熟度从而降低项目成本并获得最大利润是 CMMI 实施的最终目标。组织级定义的高成熟度的过程是否是稳定的，或者说是否适合本企业项目的执行，需要量化管理的判断。量化管理需要数据统计的支撑，我们利用工具和 CMMI 模型相结合，帮助企业得到准确的统计数据，不断加强量化管理的水平，从而帮助企业不断改进过程、提升过程稳定性。

参考文献

1 Florac WA, Careton AD.任爱华,刘又诚译.度量软件过程—用于软件过程改进的统计过程控制.北京：北京航空航天大学出版社,2002.4-11,29−33,59−68.

2 Pressman RS.梅宏译.软件工程——实践者的研究方法.第 5 版.北京:机械工业出版社,2003.38−45,67−72.

3 Maxwell KD.张丽萍,梁金昆译.软件管理的应用统计学.北京:清华大学出版社,2006.95−129.

4 Fleming Q, Koppelman J.张斌,陈洁译.挣值项目管理.第 3 版.北京:电子工业出版社,2007.12−24,64−75,142−155.

5 Fenton NE, Pfleeger SL.杨海燕,赵巍,张力,等译.软件度量.第 2 版.北京:机械工业出版社,2004.11−15,118−140.

6 Budd CI, Budd CS.广联达软件股份有限公司译.挣值项目管理实践指南.北京:电子工业出版社,2008.30−32.

7 Webb A. Using Earned Value: A Project Manager Guide. Gower Publishing Company, 2003. 21−40, 85−100.