数据包的截获与网络协议分析

蒋 波 李方军 郝 军

（中国工程物理研究院职工工学院，四川绵阳 621900）

摘 要：在网络测试、故障诊断及计算机网络教学实验中都需要从网上截获数据包并对其进行网络协议分析，作者通过实例介绍了用 Ethereal 从网上俘获数据包并对其进行 TCP/IP 协议研究的方法。

关键词：Winpcap；Ethereal；TCP/IP 协议；数据包

中图分类号：TP393 文献标识码：A 文章编号：1009-8135（2006）03-0026-02

1 引言

在数据包的截获方面，Winpcap 是一个可在 Windows 环境下运行的包俘获结构,它由三部分组成:一个数据包截获驱动程序、一个底层动态链接库(Packet.dll)和一个高层静态链接库(wpcap.lib)。它的核心部分是数据包俘获驱动程序,在 Windows NT/2000 系统中,它实现为一个内核驱动程序(packet.sys),在 Windows 95/98 系统中是一个虚拟设备驱动程序(packet.vxd),包俘获驱动程序通过 NDIS(Network Driver Interface Specification)同网络适配器的驱动程序进行通信,NDIS 是网络代码的一部分,它负责管理各种网络适配器以及在适配器和网络协议软件之间的通信。在库的高层是一个动态链接库(packet.dll)和一个静态链接库(wpcap.lib)，这两个库的作用是将俘获应用程序同包俘获驱动程序相隔离，屏蔽低层的实现细节，避免在程序中直接使用系统调用或 IOCTL 命令，为应用程序提供系统独立的高层接口（API 函数），从而在 Windows9x、Windows2000/XP 系统下,对驱动程序的系统调用都是相同的。

使用 Winpcap，我们可以编写出用于网络协议实验分析、故障诊断、网络安全和监视等各种应用程序，这方面的一个典型例子就是可在 Windows 系统下运行的 Ethereal，Ethereal 和 Winpcap 都可从网上下载，通过 Ethereal 我们可以从网上拦截数据包并对数据包进行网络协议分析，下面介绍一个分析实例。

2 数据包的截获与链路层协议分析

Ethereal 安装完成后，单击它的 Capture→Start 菜单，打开俘获选项对话框，在这些选项中比较重要的是设置混杂模式（Promiscuous mode）选项，选中这个选项使得网卡并不检验数据帧的目的地址，从而它可以截获网上的任何帧，其他选项可用默认设置，再单击 OK 按钮即可进行数据包截获，图 1 显示出了被截获的一个以太网数据帧。

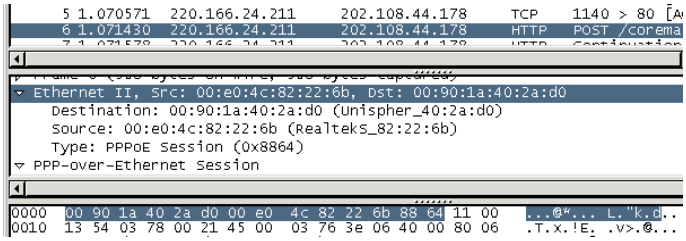

图 1 被截获的以太网数据帧

收稿日期：2005-11-18

作者简介：蒋 波（1963-），男，四川三台人,中国工程物理研究院职工工学院讲师。

截获的数据帧分别在 Ethereal 的包列表(Packet List)、包细节(Packet Details)和包字节(Packet Bytes)三个窗口中显示。图 1 依次显示了这三个窗口的部分内容，最上面的包列表窗口按俘获的顺序显示出帧的一般信息,如被俘获的时间、包的协议类型等。当应用层的数据通过网络协议栈（如 TCP/IP 协议栈）到达物理层传输时，各层协议都要在数据包上封装一个报头，而中间的包细节窗口就从低层到高层显示出数据包的各层协议信息，在下面的包字节窗口上，则以十六进制和 ASCII 码显示了被截获数据包的详细内容。

我们先分析网络协议的数据链路层，它一般采用以太网的 IEEE802.3 标准。其中数据部分包括了更高层的协议内容，由于前导码被网络硬件用于接收信号的同步，因此 Ethereal 已从数据帧中去掉了前导码，在图 1 的包细节窗口中，显示出帧的头部信息，可以读出这个帧的目的物理地址为 00:90:1a:40:2a:d0,源物理地址为 00:e0:4c:82:22:6b。帧类型是 0x8864，它表示 PPPOE 会话，在 ADSL 宽带网接入中，数据链路层通常要包括这种在以太网上的点到点协议（PPPOE）。包字节窗口中紧跟着高亮显示的帧头部就是帧的数据区和 CRC 校验码，图 1 并未显示帧数据区的全部。

3 网络层协议的分析

网络层协议在 TCP/IP 中包括网间互联协议（IP）、消息控制协议（ICMP）、路由信息协议（RIP）等，它要实现地址解析及路由管理等功能，由 IP 协议中的数据报格式可以分析出版本号为 4，即这个数据报为 IPv4，报头长度 20 字节，服务类型 00 表示是普通数据包，数据报总长度 886 字节，标识为 0x3e06，当数据报需要分片传送时，这个域用来指出接收到的数据片属于哪一个数据报,标志 04 表示该报文不分片，片偏移为 0，生存时间 128，协议域 06 表示上层协议是 TCP，头部校验和 0xcce3 表示正确，源 IP 地址是 220.166.24.211，目的 IP 地址为 202.108.44.178，包字节窗口中的数据区显示了上层协议的 TCP 段内容。

4 传输层协议的分析

TCP/IP 的传输层协议包括用户数据报协议（UDP）、传输控制协议（TCP）等，TCP 要在 IP 服务上提供可靠的、面向连接的字节流传输，它是以数据段（segment）的形式交换数据，忽略选项后的数据段格式

从包细节窗口可看出，TCP 源端口号 1140，目的端口号 80，其中 80 是 HTTP 协议的保留端口号，在包字节窗口中显示出序列号的实际值是 0x000af00b，但它等于本次连接的初始序号加上报文第一个字节在整个数据流中的序号，因此包细节窗口显示了相对于建立连接的初始握手序列号的相对值 1，图中的下一序列号 847 就意味着数据区长度是 846 字节。同理确认号的相对值也为 1，头部长度 20 字节，标志位 0x0018 指示 ACK 标志为 1，表明确认号有效，PSH 为 1 表示接收方将数据不做缓存，将接收到的数据立即传输给应用层。窗口字段指示发送方想要接收的最大字节数为 8484，这个域用于进行流量控制，校验和 0x1168 表明正确。协议头部以后显示了本层协议的数据区。

5 应用层协议的分析

TCP/IP 的应用层协议通常包括文件传输协议(FTP)、简单邮件传输协议（SMTP）、超文本传输协议（HTTP）等等，使用 Ethereal 也可方便地对它们进行分析，例如对于 HTTP 协议，可查看客户端的 GET、POST 等请求方法、请求头内容、请求数据，服务器端应答的状态行、响应头、响应数据等，具体分析方法与上面类似，这里不再重复。

参考文献：

[1]Douglas E Comer.Computer Networks and Internets with Internet Applications[M].北京：电子工业出版社，2004.

[2]Ethereal 文档资料[DB/OL]. http://www.ethereal.com

（责任编辑：冯天祥）

The Capturing Of Data Packets And The AnalyzingOf Network Protocol

JIANG Bo LI Fang-jun HAO Jun

(Technical college，China Engineering Physics Research University，Mianyang，621900)

Abstract：Network testing、fault analyzing and computer network teaching experiments all must capture data packets from network and analyze the network protocol. using Ethereal, by a specific example the author introduce the way of capturing data packet from network and researching its TCP/IP network protocol.

Key words：Winpcap; Ethereal; TCP/IP Protocol; Data Packet