hh

计算机网络实验指导书

实验二：协议数据的捕获和解析

北京邮电大学计算机学院

2017 年 6 月

目　　录

实验二：协议数据的捕获和解析

1. 实验类别

协议分析验证型

2. 实验内容和实验目的

本次实验主要包含下列内容：

1）使用 Wireshark 软件捕获在使用 ping 命令时产生的 ICMP 消息；

2）分析网络层 IP 包头格式，理解各字段的作用，对于分段和校验和进行验证；

3）使用 Wireshark 软件捕获在使用 ARP 消息，分析其消息格式，理解其工作原理；

4）使用 Wireshark 捕获 DHCP 消息，分析其消息序列，理解 DHCP 的功能和操作原理；

5）使用 Wireshark 捕获 TCP 消息，分析 TCP 报文段头格式，理解连接建立和释放的原理，差错控制原理、序号和窗口管理的原理。

通过本实验学生可以深入理解分层体系结构，理解和掌握 TCP/IP 协议栈的代表协议——IP、TCP、UDP、ICMP、ARP 和 DHCP 协议的要点。

3. 实验学时

4 学时。

4. 实验组人数

每组 1 人，独立完成数据捕获工作、进行分析并撰写实验报告。

5. 实验设备环境

1 台装有 MS Windows 系列操作系统或 Mac OS 的计算机，能够连接到 Internet，并安装 Wireshark 软件。

6. 教学要点与学习难点

在课堂教学和教材中给出了 IP、TCP 和 UDP 协议的头部格式和工作原理，但是学生对于一些关键字段和主要原理缺乏感性认识，理解不足。同时，在教材中，对于 ICMP、ARP 和 DHCP 等协议仅仅进行了简单介绍。在本实验中，学生通过使用 Wireshark 软件来捕获网络上实际传输的数据，可以加深对于上述协议的要点的理解，例如 IP 分段、TCP 的连接管理、ICMP 的功能、ARP 的功能、DHCP 的功能等；同时对于教材中没有包含或阐述不够详细的内容，例如 IP 包头校验和的计算、TCP 的 MSS 概念、ICMP 的消息格式、ARP 的消息格式、DHCP 的消息格式及操作过程等，可以通过分析数据格式和协议流程进行自学和了解。

在本实验中，熟悉 Wireshark 软件并进行消息捕获的工作比较简单，实验的重点和难点在于协议的分析工作，例如 DHCP 消息的含义和操作过程，学生需要对所捕获到的 DHCP 消息的格式和序列进行分析，绘制出 DHCP 消息序列图，从而达到理解协议工作原理的目的。

7. 实验步骤

7.1 准备工作

1. 下载 Wireshark 软件并了解其功能和使用方法。
2. 确保计算机已经连接到网络。
3. 启动 Wireshark，设置捕获接口（Interface）为本机网卡，选中混杂模式（promiscuous mode）捕获选项，设置合适的捕获过滤器（Capture Filter）：
   - 对于 ping 命令，设置过滤器为 icmp
   - 对于 DHCP 消息，设置过滤器为 udp port 67
   - 对于 ARP 消息，设置过滤器为 arp
   - 对于通过网页浏览应用来捕获 TCP 消息，设置过滤器为 tcp port 80
4. 开始捕获。

7.2 数据捕获

7.2.1 捕获 ICMP 协议数据

1. 运行 ping 命令（例如：c> ping 192.168.0.1），远程主机地址可以是本机地址、网关路由器地址，也可以是域名（如 www.bupt.edu.cn）。将捕获到的数据保存为文件。
2. 使用 Windows 中 ping 命令的-l 选项（例如：c>ping -l 8000 192.168.0.1），生成大于 8000 字节的 IP 包并发送，捕获后分析其分段传输的包结构。

7.2.2 捕获 DHCP 协议数据

1. 使用 ipconfig 命令释放计算机的 IP 地址（c>ipconfig -release）；
2. 使用 ipconfig 命令重新申请 IP 地址（c>ipconfig -renew）。
   此时 wireshark 窗口中可以捕获到完整的 DHCP 地址分配的流程，将捕获到的数据保存为文件。

7.2.3 捕获 ARP 协议数据

采用与 7.2.2 相同的方法释放 IP 地址并重新申请，在 wireshark 窗口中可以捕获到 ARP 请求和响应消息，保存为文件。

7.2.4 捕获 TCP 协议数据

打开浏览器，输入一个页面内容较简单的网页的 URL，如 www.baidu.com；网页全部显示后关闭浏览器。

7.3 协议分析

运行 Wireshark 软件，打开所捕获的数据文件，完成下列分析工作：

1. IP 包头分析：对于采用 ping 命令-l 选项捕获的 ICMP 消息，对承载 ICMP 消息的 IP 包进行分析，记录包头各字段的值，对照讲义和教材分析各字段的功能，并对于分段进行验证；
2. ICMP 消息分析：记录并分析 ICMP 消息中分析各字段的功能；
3. DHCP 消息分析：针对一次地址分配过程（Transaction ID 相同的 4 个消息），分析其通信过程，

画出地址分配的消息序列图，并记录采用 DHCP 协议配置的各个参数。

4. ARP 消息分析：对照讲义理解 ARP 的操作过程，记录并分析消息中各字段的功能。
5. TCP 报头及消息分析：针对 TCP 连接建立、连接释放、数据和应答报文段，对照讲义和教材分析各字段的功能；针对一次完整的 TCP 通信过程，画出消息序列图，应包含连接建立、数据传送和连接释放阶段。

上述分析工作应在实验报告中进行详细描述，具体要求参见第 9 节。

7.4 撰写实验报告

按第 9 节的要求撰写实验报告，对于捕获到的数据进行认真分析，归纳各协议的工作原理和实现要点。

8. Wireshark 软件使用说明

本次实验使用的是 Wireshark 软件，其早期版本称为 Ethereal。Wireshark 是一个网络包分析工具，它可以捕获网络中传输的数据包，对于数据包进行解析，并显示包中各协议数据的详细内容，是目前最好的开源网络分析软件之一。Wireshark 可以应用在下列情形：

- 帮助网络管理员解决网络问题
- 帮助网络安全工程师检测安全隐患
- 帮助开发人员测试其开发的协议的执行情况
- 帮助学生学习网络协议

8.1 Wireshark 软件的安装

在 http://www.wireshark.org 下载 Wireshark 安装包并执行，安装选项可以选择默认配置。Wireshark 安装包中已包含 WinPcap，无需单独下载安装。

8.2 运行 Wireshark 并设置捕获条件

运行 Wireshark 软件，在启动页中选中活跃的网卡，如图 1 所示的无线网络连接，然后设置捕获过滤器（capture filter）条件，可以设置需要捕获的协议和端口号，例如捕获 DHCP 消息时，应设为：udp port 67。设置好后，双击活跃的网卡即开始捕获。

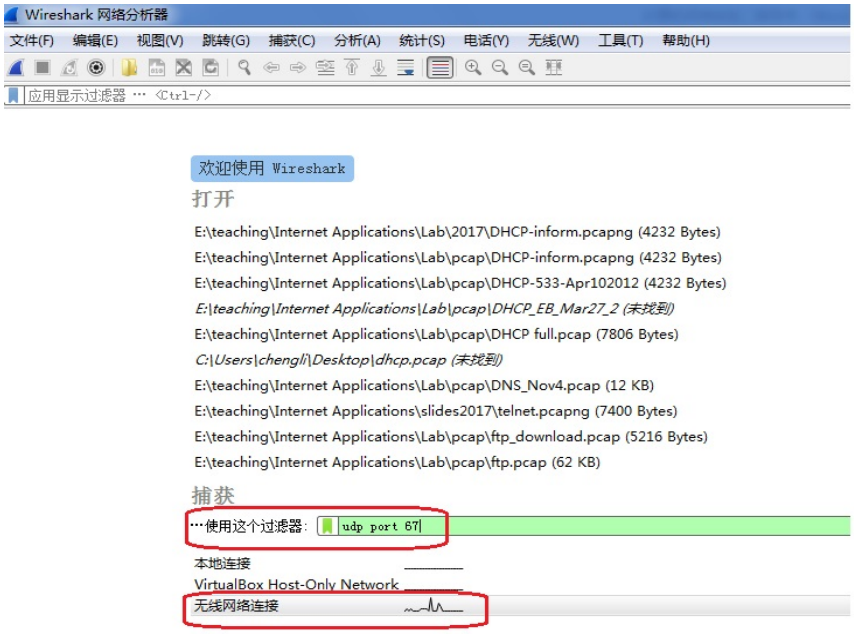

图 1 Wireshark 的捕获条件设置示例

8.3 解码分析

启动捕获之后，运行相应的网络通信程序，Wireshark 即可以捕获到网卡发送和接收到的符合捕获条件的数据，并在显示在如图 2 所示的主窗口中。

注：在显示过滤器中进行设置，可以只显示需要的消息，例如图 2 中，udp.port==67，表示只显示 DHCP 消息。Wireshark 的数据显示窗口分为 Packet List、Packet Detail 和 Packet Byte 三部分。

1. PacketList：显示所捕获到的所有数据包，每行显示一个数据包。如果选中一行，在下面的 Packet Detail 和 Packet Byte 窗口中显示对应的详细信息。

默认情况下，PacketList 显示包括下面各列：

No. ：表示包的序号

Time：表示包的时间戳

Source：显示包的源 IP 地址。

Destination：显示包的目的 IP 地址。

Protocal：显示包内数据的协议类型

Info：包内容的附加信息，例如对于 UDP 数据报，将包含源/目的端口号、数据包长度、校验和等信息。

2. PacketDetail：显示在 PacketList 窗口中所选中的数据包解析后的详细信息，包括每个协议字段的含义及其值。PacketList 窗口中的显示是从数据链路层开始，每层协议显示一行概要信息，包括协议的源地址和目的地址。如图 2 示例的 UDP 消息，概要信息分别显示了以太网帧地址、IP 包地址和 UDP 数据报端口号。

每层协议的细节信息是以树状方式组织的，可以展开，如图 2 示例，对 DHCP 的协议消息进行了展开，可以看到每个协议字段的名字、值和补充信息。

3. Packet Byte：以十六进制的方式在 PacketList 和 PacketDetail 窗口中所选中的部分对应的数据值。该窗口分为 3 部分，左侧分栏显示选中数据在整个帧中的偏移量，中间分栏显示 16 进制的对应值，右侧分栏显示对应的 ASCII 字符值。如图 2 所示，在 PacketDetail 窗口中选中了 DHCP Discover 消息的 Message

Type 字段，其值为 1，长度为 1 字节，对应的十六进制值为 01。

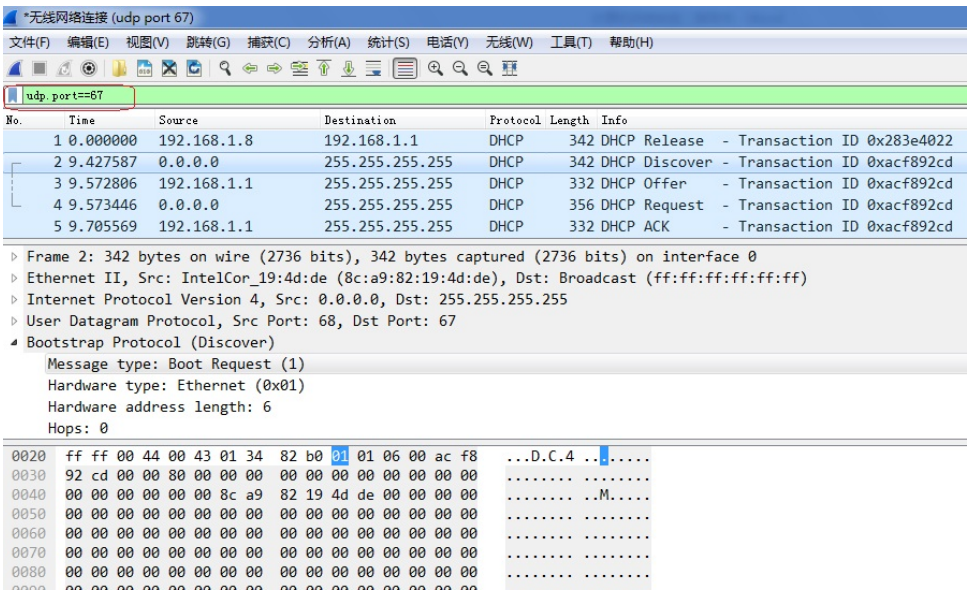

图 2 Wireshark 主窗口示例

关于 Wireshark 的详细功能和具体使用说明，请参照 Wireshark 用户手册。

9. 实验报告要求

本节描述了应提交实验报告的内容提纲和每项具体要求。实验完成后，应以电子版方式提交实验报告。

9.1 实验内容和实验步骤描述

描述本次实验的任务、内容、实验环境和实验步骤。

9.2 IP 协议分析

1）对于所捕获并选中的 IP 包，找出包头各字段，参照下表示例的格式记录在实验报告中：

字　段	报　文（16 进制）	内　　容
包头长度	45	包头长 20 字节
服务类型	00	正常时延，正常吞吐量，正常可靠性
总长度	004e	数据分组长 78 字节
标识	b46c	标识为 46188
标志	00	MF=0,DF=0 允许分片，此片为最后一片
片偏移	00	偏移量为 0
生存周期	40	每跳生存时间为 64 秒
协议	11	携带的数据来自 UDP 协议
头部校验和	b7bc	IP 头部校验和为 b7bc
源地址	a9feba79	源地址为 169.254.186.121
目的地址	a9feffff	目的地址 169.254.255.255

2）描述 IP 包头校验和的校验原理，并针对上述 IP 包头进行校验和的验证。

3）描述 IP 包分段原理，并通过所捕获到的 IP 包的相关字段进行验证。

9.3 ICMP 协议分析

1） 对照讲义，理解 ICMP 的功能，
2） 记录 ICMP 的包格式，自己查找资料总结各字段的功能。

9.4 DHCP 协议分析

1） 对照讲义和教材理解 DHCP 的功能，观察 DHCP ACK 消息的各字段，自己查找资料理解各字段的功能，总结采用 DHCP 协议可以提供哪些配置参数。
2） 根据捕获到消息，画出 DHCP 地址分配过程的消息序列图。注意 DHCP 是采用 client-server 模式工作的，你捕获到的消息中，DHCP server 是否由路由器充当？是否有 DHCP Relay?

9.5 ARP 协议分析

1） 根据捕获到的消息，对照讲义，理解 ARP 的功能和操作原理。
2） 记录 ARP 的包格式，自己查找资料总结各字段的功能。

9.6 TCP 协议分析

1） 对照讲义和教材理解 TCP 报文段的首部各字段的功能，以表格的方式总结每个字段的名字、长度和功能。
2） 针对连接建立消息和连接释放消息，分析相应标志位和序号的作用，参照讲义中的示例画出连接建立和连接释放过程的消息序列图，在图上标出对应的标志位和序号。
3） 针对 TCP 的数据传输过程中的数据报文段和应答报文段，分析发送序号、应答序号、应答标志位、窗口大小、数据长度、MSS 等字段的作用，参照讲义中的示例画出数据传输过程的消息序列图，其中应包括数据校验错和数据丢失导致的数据重传情形，在图上应标出对应的序号、标志位和窗口大小。

9.7 实验结论和实验心得

总结实验中遇到的问题和解决方案，总结实验心得。