《计算机网络》实验报告

姓　　名：　涂奕钿　　**学号：　201541402313**
专业班级：　计算机科学与技术 3 班

时间：　**2017.09.28**　　**地点：7B409**

==========

1. 实验题目：分组嗅探器的使用和网络协议的层次观察

2. 实验目的：

1、 了解网络协议的层次结构
2、 初步掌握分组嗅探器 **Wireshark** 的使用方法

3. 实验环境
1．Wireshark 网络分析软件
2．实验文件“计算机网络－实验文件”

4. 实验内容及步骤

1、Wireshark 介绍

Wireshark 是一个优秀的网络数据包分析软件，可以捕获**(Capture)** 和浏览**(Display)** 网络侦测的内容，还可以定义 **Filters** 规则，监视所有在网络上被传送的封包，并分析其内容。**Wireshark** 通常用来检查网络运作的状况，或是用来发现网络程序的 **bugs**。它可以分析的协议有：**RTP**、**IP**、**ISAKMP**、**ICMP**、**SMB**、**SMB-PIPE**、**VTP**、**SNMPv3**、**Ethernet**、**GRE**、**EIGRP**、**DHCP**、**IPX**、**X.25**、**RSVP** 等。

2、Wireshark 的使用

启动 **Wireshark** 后，选择菜单 **Capature－>Options,** 定义获取数据包的方式。主要选项有，**Interface:** 指定在哪个接口（网卡）上抓包；**Limit each packet:** 限制每个包的大小以避免数据过大，缺省情况下可不限制；**Capture packets in promiscuous mode:** 是否打开混杂模式。如果打开，则抓取共享网络上可以探测的所有数据包。一般情况下只需要监听本机收到或者发出的包，可以关闭这个选项。**Filter**：设定过滤规则，只抓取满足过滤规则的包；**File**：如果需要将抓到的包写到文件中，在这里输入文件名称。其他的项选择缺省的就可以了。选择 **start** 开始抓包。选择 **stop**，则停止抓包。

3．实验文件“计算机网络－实验文件**.cap**”的获取

该实验文件的建立是在本人主机上完成的，运行以下命令，期间通过浏览器访问 **BAIDU**，同时使用 **Wireshark** 抓取期间网络数据包：

ipconfig /release　（释放当前 **IP** 配置）
arp –d　　（释放当前 **ARP** 缓存）
ipconfig /flushdns　（释放当前 **DNS** 缓存）
pause　　（准备开始抓取网络数据包）

ipconfig /renew （重新配置当前 IP 配置，本人主机需要执行 DHCP 协议）
ping -l 2000 -f 219.222.170.254 （不拆分 2000 字节数据包，发送至网关 ）
ping -l 2000 219.222.170.254 （发送 2000 字节数据包至网关，允许拆分）
tracert www.sina.com （跟踪当前主机到 www.sina.com 的路由）
pause

4．数据包的分析

打开文件“计算机网络－实验文件.cap”，这是一个包括 204 个分组的网络通信记录，当前主机 IP 地址是 219.222.170.14 、网关地址是 219.222.170.254、文件中出现的 119.75.217.56 是百度公司的 IP 地址、172.30.0.19 是东莞理工学院网络中心提供的 Windows Server Update Services (WSUS)。

文件详细记录了分组的序号、相对时间、源地址、目标地址、协议类型、内容，如图 1 是对第 52 个分组的详细信息。在协议框内，分别显示了该分组的各层协议：接口层以太网协议(eth)、网络层 IP 协议、传输层 UDP 协议、应用层 DNS 协议，对于这些协议可以进一步显示非常多的信息，（这些信息的含义以后会陆续介绍）；在最下面的 16 进制数字，则是传递的最原始数据（比特流）。

第 52 个分组的部分信息如下：

到达的标准时间是 2010 年 12 月 13 日 10：47：19.903808，相对时间 9.957484000 seconds；源物理地址 00:25:11:4e:02:34；目标物理地址 00:04:96:10:64:30；源 IP 地址 219.222.170.14； 目的 IP 地址 219.222.191.9； 协议类型分别是 Ethernet、IP(Internet Protocol)、UDP(TUser Datagram Protocol)、DNS。传递的信息内容是解析域名 www.baidu.com 的 IP 地址。

4．网络协议的层次结构

计算机网络的体系结构(architecture)是计算机网络的各层及其协议的集合。TCP/IP 是四层的体系结构：应用层、运输层、网际层和网络接口层。最下面的网络接口层并没有具体内容。（见图 2）

应用层：为了解决某一类应用问题（Http、SMTP、FTP、DNS……），规定应用进程在通信时所遵循的协议。

运输层:为应用进程之间提供端到端的逻辑通信（但网络层是为主机之间提供逻辑通信）,运输层还要对收到的报文进行差错检测;运输层需要有两种不同的运输协议，即面向连接的 TCP 和无连接的 UDP。

网络层：负责网络不同主机间通信，IP 是 TCP/IP 体系中两个最主要的协议之一，配套使用的还有 ARP（地址解析协议）、ICMP（因特网控制报文协议）。

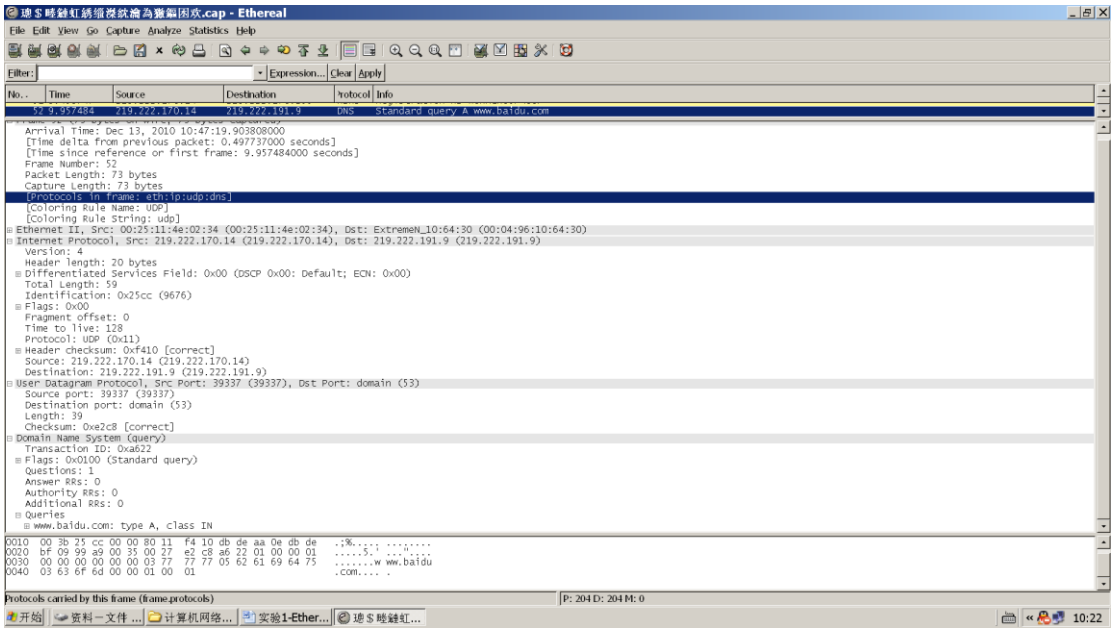

图 1 分组 52 的网络通信记录

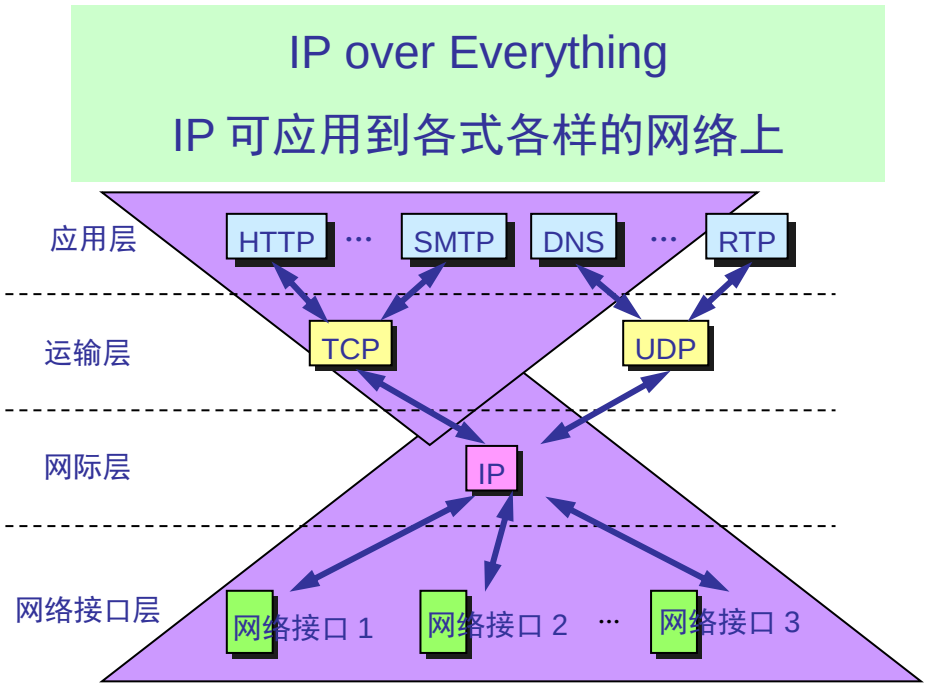

图 2 TCP/IP 的四层体系结构

5．数据包的自行抓取和分析

参照以上内容，抓取本机网络的 100 个数据包，期间包括输入命令“ping www.163.com”.

5． 实验总结及问题回答

（1） 第 1 个分组到达的相对时间、源物理地址、目标物理地址、源 IP 地址、目的 IP 地址、每层的网络协议类型、传递的信息内容是怎样的？

相对时间:0.000000　　源物理地址:ff:ff:ff:ff:ff:ff　　目标物理地址:00:25:11:4e:02:34　　源 IP 地址：0.0.0.0　　目的 IP 地址:255.255.255.255　每层的网络协议类型:IP　传递的信息内容

（2） 第 8 个分组到达的相对时间、源物理地址、目标物理地址、源 IP 地址、目的 IP 地址、每层的网络协议类型、传递的信息内容是怎样的？

（3） 第 32 个分组到达的相对时间、源物理地址、目标物理地址、源 IP 地址、目的 IP 地址、每层的网络协议类型、传递的信息内容是怎样的？

（4） 观察这个记录，以分组 184、73 为例，参考图 2 举例说明 DNS、HTTP 的下层支撑协议。（重点说明 DNS、HTTP 分别使用那种传输层协议）