实验三：网络协议分析

一、实验目的：

1．掌握抓包软件 Wireshark 的使用。

2、了解并掌握因特网中 MAC 帧、IP 数据报、TCP/UDP 段的字段及其含义。

3、了解并掌握三次握手、HTTP 协议的内容和功能。

二、以太网数据链路层协议分析实验

1、在 windows 中安装 Wireshark 软件。

2、配置包捕获模式为混杂模式，捕获网络中所有机器的数据包，当捕获到一定数量的数据报后，停止捕获，观察捕获到的数据包，并对照解析结果和原始数据包的具体字段，了解 MAC 地址字段、协议类型、数据来源等。

3、配置包**捕获**过滤器，只捕获特定 IP 地址、特定端口或特定类型的包，然后重新开始捕获包并分析。

4．以太网帧分析

（a）捕捉任何主机发出的 Ethernet 802.3 格式的帧（帧的长度字段<=1500），Wireshark 的 capture filter 的 filter string 设置为：ether[12:2] <= 1500。观察并分析帧结构，802.3 格式的帧的上一层主要是哪些 PDU？是 IP、LLC 还是其它哪种？为什么？

(b) 捕捉任何主机发出的 DIX Ethernet V2 (即 Ethernet II) 格式的帧 (帧的长度字段>1500, 帧的长度字段实际上是类型字段)，Wireshark 的 capture filter 的 filter string 设置为：ether[12:2] > 1500。观察并分析帧结构，Ethernet II 的帧的上一层主要是哪些 PDU？是 IP、LLC 还是其它哪种？为什么？

5. 捕捉并分析局域网上的所有 ethernet broadcast 广播帧，Wireshark 的 capture filter 的 filter string 设置为：ether broadcast

(1). 观察并分析哪些主机在发广播帧，这些帧的高层协议是什么？

(2). 1 分钟内有几个广播帧？有否发生广播风暴？

6.思考问题：

（1） 本地数据存放的字节顺序和网络包中的字节顺序是否相同？

（2） 怎样知道哪些数据包是 MAC 广播包或 IP 子网广播包？

（3） 通过包捕获软件能否捕获到通过交换机连接的计算机发出的包？能够捕捉到其他计算机发出的哪些包？

三、网络层、传输层协议分析实验

1. 捕捉局域网上本机（假设为主机 10.14.26.53）发出或接受的所有 ARP 包，Wireshark 的 capture filter 的 filter string 设置为：arp host 10.14.26.53.

(1).主机 10.14.26.53 上执行 ” arp -d * ” 清除 arp 缓存.

(2).观察并分析主机 10.14.26.53 发出或接受的所有 ARP 包，及 arp 包结构。

2. 捕捉局域网上的所有 IP 广播包，Wireshark 的 capture filter 的 filter string 设置为：ip broadcast。观察并分析哪些节点在发广播包，这些包的高层协议是什么?

3. 捕捉局域网上的所有 IP 组播包，Wireshark 的 capture filter 的 filter string 设置为： ip multicast。 观察并分析哪些节点在发组播包，这些包的高层协议是什么?

4. 捕捉局域网上的所有 icmp 包，Wireshark 的 capture filter 的 filter string 设置为：icmp

(1). 在主机 10.14.26.53 上 ping 局域网上的另一主机（例如 10.14.26.54）。

(2). 观察并分析主机 10.14.26.53 发出或接受的所有 icmp 包，及 icmp 包的类型和结构。

5、捕捉任意一个 IP 包，分析该包中的：IP 头中各个字段作用及其数值，解释其含义。

6、捕捉任意一个 TCP 包，分析该包中的：TCP 头中各个字段作用及其数值，解释其含义。

7、捕捉任意一个 UDP 包，分析该包中的：UDP 头中各个字段作用及其数值，解释其含义。

四、应用层协议分析实验

捕捉本机和某 www 服务器（如 www.hust.edu.cn）之间的通信，Wireshark 的 capture filter 的 filter string 设置为：host 本机 ip 地址 and www.hust.edu.cn。(本机 ip 地址需要替换为本机真正的 ip 地址，如 219.219.54.111，以下同)

（1）本机用 IE 访问 www 服务器 www.hust.edu.cn。

（2）观察并分析本机和 www 服务器之间传输的 IP 数据报结构，TCP segment 结构，HTTP 报文的结构。

（3）观察并分析本机和 www 服务器之间建立 TCP 连接时的三次握手过程。

五 实验要求：

（1） 按照实验内容要求，完成各项实验及分析。

（2） 在实验报告（有模板）中回答思考题。

（3） 实验结果截图并分析，在实验报告（有模板）中完成实验报告撰写。

六 实验时间： 2 机时