

《计算机网络》实验报告



**实验： 网络协议分析工具Wireshark的使用**

**学 生： 周录松**

**学 号： 201605020427**

**学 院： 电子信息与人工智能学院**

**系 别： 计算机系**

**专 业： 计算机科学与技术**

## 实验三 网络协议分析工具Wireshark的使用（预习报告）

**一、实验目的**

1）学习安装、使用网络协议分析工具Wireshark的方法；

2）通过Wireshark对arp、icmp、ip、udp、tcp等协议进行分析。

**二、实验器材**

Pc机、双绞线

**三、实验内容**

**3.1 Wireshark的安装及使用**

1、下载wireshark

<https://www.wireshark.org/>

2、安装wireshark

3、Wireshark报文捕获常用过滤规则（http://www.tcpdump.org/tcpdump\_man.html）

4、wireshark显示常用过滤规则

5、Wireshark TCP流还原

**3.1 用Wireshark观察ARP协议以及ping命令的工作过程**

**3.1.1 arp表为空的情况，目的地址为本网段**

1、用“ipconfig”命令获得本机的MAC地址和缺省路由器的IP地址；

ipconfig/all 00-15-C5-7B-30-A6 192.168.1.1

1. 用“arp”命令清空本机的缓存；

arp -d

1. 运行Wireshark，开始捕获所有属于ARP协议或ICMP协议的，并且源或目的MAC地址是本机的包（提示：在设置过滤规则时需要使用（1）中获得的本机的MAC地址）;

过滤规则：ether host 00:15:C5:7B:30:A6 and (arp or icmp)

4、执行命令：“ping 本网段的IP地址” ；

ping 192.168.1.1

5、分析执行流程、以太网帧中的MAC地址；

**3.1.2 arp表不为空的情况，目的地址为本网段**

1、重复3.1.1的步骤，进行试验；

2、分析执行过程有何不同；

**3.1.2 arp表为空的情况，目的地址不为本网段**

1、重复3.1.1的步骤，进行试验；

2、分析arp解析与3.1.1有何不同；

3、分析以太网帧中的MAC地址；

**3.2用Wireshark观察tracert命令的工作过程：**

1、运行Wireshark, 开始捕获tracert命令中用到的消息；

2、执行“tracert -d [www.sust.edu.cn](http://www.sust.edu.cn)”

3、分析tracert的工作原理。

**3.3用Wireshark观察IP报文分片及以太网最小传输长度**

1、设置过滤规则，运行Wireshark捕获相应的IP报文；

2、执行ping –l 长度 目的IP；

3、分析参数长度大于多少时，产生IP报文分片；

4、分析参数长度小于多少时，数据链路层进行填充；

5、分析IP报文分片的过程（原始数据包被分成了多少片？这些分片中IP数据报头部哪些字段发生了变化？、IP报文如何分片的）。

**3.4用Wireshark观察TCP连接的建立过程和终止过程**

1. 启动Wireshark，配置过滤规则

2、浏览器访问：www.163.com

3、当网页内容全部显示完后，停止抓包；

4、利用TCP流还原功能，选择一个完整的TCP会话进行分析；

5、分析TCP三次握手过程及参数协商（如何建立连接、双方的初始序列号、初始窗口大小、协商了那些参数及参数功能）;

6、分析TCP连接关闭过程，并分析哪一方先关闭连接。（如何关闭连接、哪一方先发起的）

7、分析数据传输阶段，主机发送确认报文过程，选取一个确认报文，分析已正确接收的字节数？接收方缓冲区的情况？发送方是否还能发送的字节数？

8、分析整个过程中是否有重传？是否是快速重传；

**3.5用Wireshark观察使用DNS来进行域名解析的过程**

1、在Windows命令窗口中执行命令“nslookup↙(回车)”，进入该命令的交互模式；

2、启动Wireshark, 配置过滤规则为捕获所有源或目的是本机的DNS协议中的包（提示：DNS使用的传输层协议是UDP，它使用UDP端口号53）；

3、在提示符“>”下直接键入域名www.sust.edu.cn，解析它所对应的IP地址；

4、在提示符“>”下键入命令“set type=mx”，设置查询类型为MX记录;

5、在提示符“>”下键入域名“sust.edu.cn”,解析它所对应的MX记录；

6、在提示符“>”下键入命令“set type=a”，恢复查询类型为A记录;

7、在提示符“>”下键入MX记录的查询结果，从而查出“tom.com”邮件服务器的IP地址；

8、在提示符“>”下键入“exit”，退出nslookup的交互模式。

9、了解DNS协议工作基本流程；

10、分析sust.edu.cn有几个邮件服务器。

**3.5用Wireshark观察使用DNS的迭代解析和递归解析过程**

1、运行nslookup；

2、输入set norecurse（使用迭代解析）

3、配置过滤规则，启动wireshark

4、输入解析域名（不是常用域名，防止dns服务器中有缓存）

5、输入set recurse（使用递归解析）

6、输入原来解析域名

7、输入set norecurse（使用迭代解析）

8、输入原来解析域名

10、迭代解析与递归解析dns报文有何不同。

11、分析整个过程，返回的结果及原因。

## 实验三 网络协议分析工具Wireshark的使用

**一、实验目的**

1）学习安装、使用网络协议分析工具Wireshark的方法；

2）通过Wireshark对arp、icmp、ip、udp、tcp等协议进行分析。

**二、实验器材**

Pc机、双绞线

**三、实验内容**

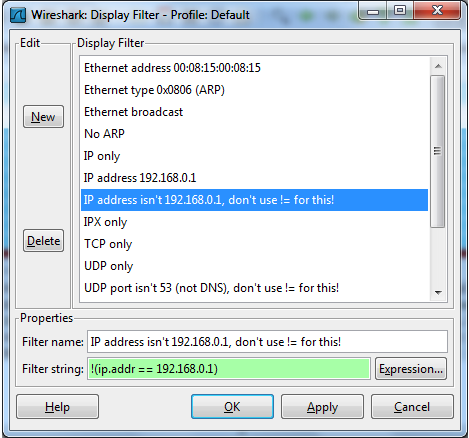
**3.1 Wireshark的安装及使用**

1、下载wireshark

<https://www.wireshark.org/>

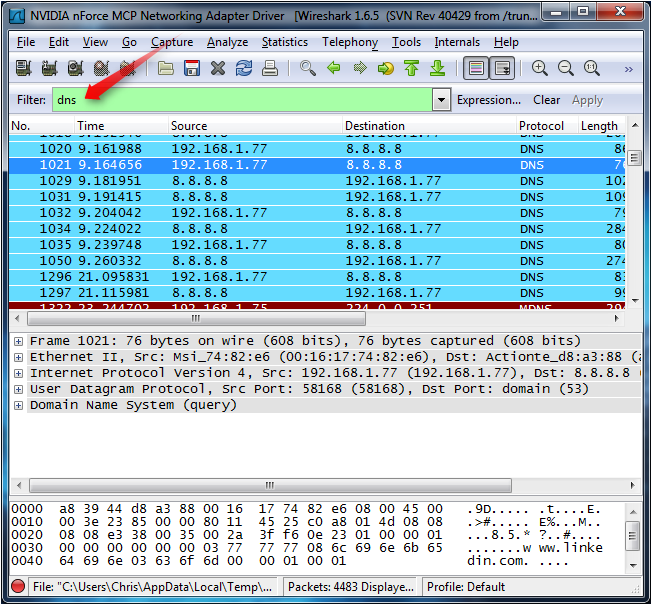
2、安装wireshark

3、Wireshark报文捕获常用过滤规则（http://www.tcpdump.org/tcpdump\_man.html）

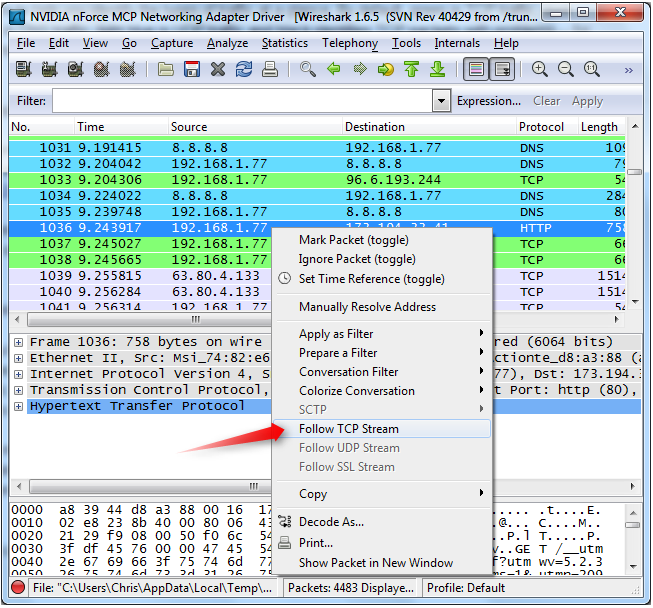


|  |  |
| --- | --- |
| 规则 | 描述 |
| [src|dst] host <host> | Src host 192.168.1.1 |
| ether [src|dst] host <ehost> | Ether src 00:23:cd:80:8c:80 |
| [src|dst] net <net> [{mask <mask>}|{len <len>}] | net 192.168.1.0/24  net 192.168.1.0 mask 255.255.255.0 |
| [tcp|udp] [src|dst] port <port> | tcp dst port 80 |
| less|greater <length> |  |
| ip|ether proto <protocol> | udp or arp or icmp or icmp |
| ether|ip broadcast|multicast | ether multicast  ip broadcast |

4、wireshark显示常用过滤规则



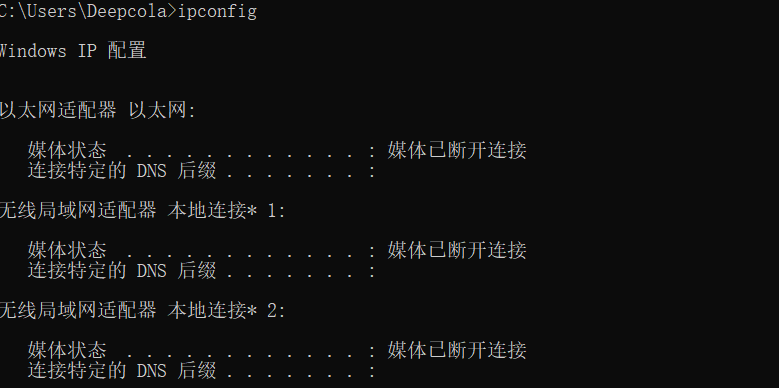
5、Wireshark TCP流还原



**3.1 用Wireshark观察ARP协议以及ping命令的工作过程**

**3.1.1 arp表为空的情况，目的地址为本网段**

1. 用“ipconfig”命令获得本机的MAC地址和缺省路由器的IP地址；



1. 用“arp”命令清空本机的缓存；

arp -d

1. 运行Wireshark，开始捕获所有属于ARP协议或ICMP协议的，并且源或目的MAC地址是本机的包（提示：在设置过滤规则时需要使用（1）中获得的本机的MAC地址）;

过滤规则：ether host D0:57:7B:33:A8:24 and (arp or icmp)

4、执行命令：“ping 本网段的IP地址” ；

ping 192.168.10.12

**3.1.2 arp表不为空的情况，目的地址为本网段**

1、重复3.1.1的步骤，进行试验；

2、分析执行过程有何不同；

arp通过进行查表操作，之间进行单播，而不进行广播。

**3.1.3 arp表为空的情况，目的地址不为本网段**

1、重复3.1.1的步骤，进行试验；

2、分析arp解析与3.1.1有何不同；

3、分析以太网帧中的MAC地址；

**3.2用Wireshark观察tracert命令的工作过程：**

1、运行Wireshark, 开始捕获tracert命令中用到的消息；

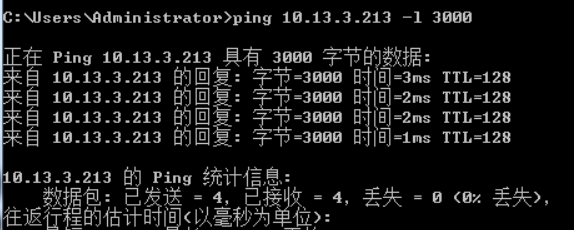
2、执行“tracert -d [www.sust.edu.cn](http://www.sust.edu.cn)”

3、分析tracert的工作原理。

**3.3用Wireshark观察IP报文分片及以太网最小传输长度**

1、设置过滤规则，运行Wireshark捕获相应的IP报文；

2、执行ping –l 长度 目的IP；

****

3、分析参数长度大于多少时，产生IP报文分片；

4、分析参数长度小于多少时，数据链路层进行填充；

5、分析IP报文分片的过程（原始数据包被分成了多少片？这些分片中IP数据报头部哪些字段发生了变化？、IP报文如何分片的）。

**3.4用Wireshark观察TCP连接的建立过程和终止过程**

1. 启动Wireshark，配置过滤规则

2、浏览器访问：www.163.com

3、当网页内容全部显示完后，停止抓包；

4、利用TCP流还原功能，选择一个完整的TCP会话进行分析；

5、分析TCP三次握手过程及参数协商（如何建立连接、双方的初始序列号、初始窗口大小、协商了那些参数及参数功能）;

6、分析TCP连接关闭过程，并分析哪一方先关闭连接。（如何关闭连接、哪一方先发起的）

7、分析数据传输阶段，主机发送确认报文过程，选取一个确认报文，分析已正确接收的字节数？接收方缓冲区的情况？发送方是否还能发送的字节数？

8、分析整个过程中是否有重传？是否是快速重传；

**3.5用Wireshark观察使用DNS来进行域名解析的过程**

1. 在Windows命令窗口中执行命令“nslookup↙(回车)”，进入该命令的交互模式；



2、启动Wireshark, 配置过滤规则为捕获所有源或目的是本机的DNS协议中的包（提示：DNS使用的传输层协议是UDP，它使用UDP端口号53）；

3、在提示符“>”下直接键入域名www.sust.edu.cn，解析它所对应的IP地址；

4、在提示符“>”下键入命令“set type=mx”，设置查询类型为MX记录;

5、在提示符“>”下键入域名“sust.edu.cn”,解析它所对应的MX记录；

6、在提示符“>”下键入命令“set type=a”，恢复查询类型为A记录;

7、在提示符“>”下键入MX记录的查询结果，从而查出“tom.com”邮件服务器的IP地址；

8、在提示符“>”下键入“exit”，退出nslookup的交互模式。

9、了解DNS协议工作基本流程；

10、分析sust.edu.cn有几个邮件服务器。

**3.6用Wireshark观察使用DNS的迭代解析和递归解析过程**

1、运行nslookup；

2、输入set norecurse（使用迭代解析）

3、配置过滤规则，启动wireshark

4、输入解析域名（不是常用域名，防止dns服务器中有缓存）

5、输入set recurse（使用递归解析）

6、输入原来解析域名

7、输入set norecurse（使用迭代解析）

8、输入原来解析域名

10、迭代解析与递归解析dns报文有何不同。

11、分析整个过程，返回的结果及原因。

**四、实验总结**

1、分析以太网报文格式

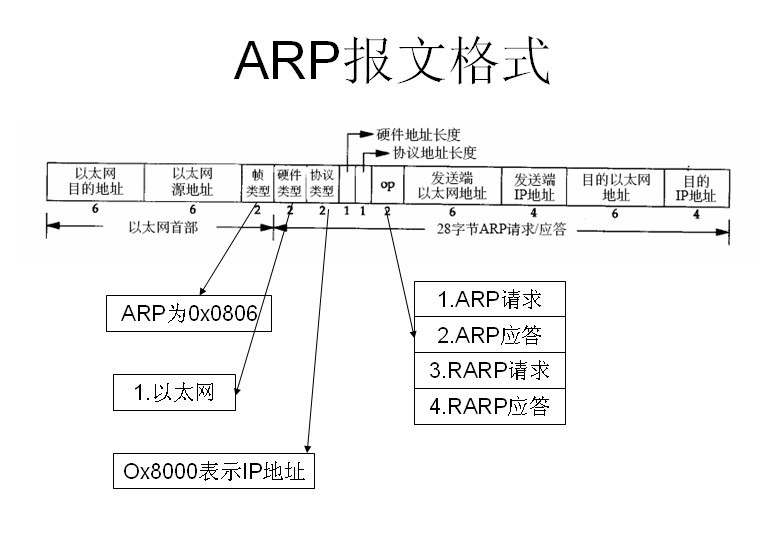
其中的源地址和目的地址是指网卡的硬件地址（也叫MAC 地址），长度是48 位，是在网卡出厂时固化的。

注意网卡芯片收到的数据就是如上所示的一长串数据；其中包括以太网帧头、IP报报头、传输层协议段头、应用层所需数据。

以太网帧中的数据长度规定最小46 字节，最大1500 字节，ARP 和RARP 数据包的长度不够46 字节，要在后面补填充位。最大值1500 称为以太网的最大传输单元（MTU），不同的网络类型有不同的MTU，如果一个数据包从以太网路由到拨号链路上，数据包度大于拨号链路的MTU了，则需要对数据包进行分片。ifconfig命令的输出中也有“MTU:1500”。

2、分析arp协议

地址解析协议，即ARP，是根据[IP地址](https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80" \t "/Users/ck\x/_blank)获取[物理地址](https://baike.baidu.com/item/%E7%89%A9%E7%90%86%E5%9C%B0%E5%9D%80/2129" \t "/Users/ck\x/_blank)的一个[TCP/IP协议](https://baike.baidu.com/item/TCP/IP%E5%8D%8F%E8%AE%AE" \t "/Users/ck\x/_blank)。[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "/Users/ck\x/_blank)发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的，网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存；由此攻击者就可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个[ARP欺骗](https://baike.baidu.com/item/ARP%E6%AC%BA%E9%AA%97" \t "/Users/ck\x/_blank)。[ARP命令](https://baike.baidu.com/item/ARP%E5%91%BD%E4%BB%A4" \t "/Users/ck\x/_blank)可用于查询本机ARP缓存中IP地址和[MAC地址](https://baike.baidu.com/item/MAC%E5%9C%B0%E5%9D%80" \t "/Users/ck\x/_blank)的对应关系、添加或删除静态对应关系等。相关协议有[RARP](https://baike.baidu.com/item/RARP" \t "/Users/ck\x/_blank)、[代理ARP](https://baike.baidu.com/item/%E4%BB%A3%E7%90%86ARP" \t "/Users/ck\x/_blank)。[NDP](https://baike.baidu.com/item/NDP" \t "/Users/ck\x/_blank)用于在[IPv6](https://baike.baidu.com/item/IPv6" \t "/Users/ck\x/_blank)中代替地址解析协议。



3、总结实验结果：

通过本次实验，能够加深学生对于网络协议辨识能力和分析能力，并掌握报文分析工具的使用。在实验中成功使用Wireshark对ARP,IP,TCP,DNS,HTTP等协议进行了细致的观察。并更加深入的了解了各个协议的工作流程。

通过本次试验，使我对ARP、ICMP协议和以太网报文格式有了更加深入的理解。