**北京邮电大学软件学院**

**\_\_2019-2020\_\_学年第\_1\_学期实验报告**

**课程名称： 通讯协议软件设计**

**实验名称： 实验一：数据链路层实验**

**实验完成人：**

**姓名：** 平雅霓 **学号：**\_2017211949\_**成绩：**\_\_\_\_\_\_\_\_

**指导教师：** 王文东 雷友珣

**日 期： 2019 年 10 月 28 日**

1. **实验目的**

通过本实验使学生理解协议数据单元（PDU）概念、掌握以太网帧结构字段定义和功能。

1. **实验任务**

搭建实验环境，使用网络抓包软件（如Wireshark软件等）抓取访问互联网所产生的数据包，分析其中的以太网帧结构字段组成，掌握以太网帧结构字段的功能。

1. **实验内容**
2. 在可以访问互联网的主机上下载并安装网络抓包软件Wireshark。
3. 运行Wireshark软件，启动Wireshark软件的抓包功能抓取本主机访问互联网中某网站过程中发送和接收的数据包。
4. 对所抓取的数据包进行分析，分析所发送和接收的数据包的以太网帧结构中的源MAC地址、目的MAC地址和类型（type）字段的使用方法；理解各字段的含义和功能。
5. 选做部分：分析所抓取的数据包中的DNS（Domain Name System）消息、TCP报文、IP分组、HTTP协议消息的字段组成及作用。
6. **实验环境**
7. Windows系统主机或Linux系统主机；
8. Wireshark软件，软件下载网址：<https://www.wireshark.org/>
9. **实验过程与结果**
10. **DNS域名解析过程**

**DNS解析过程：**

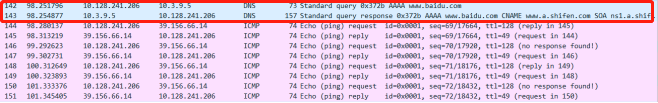
用户的PC机或者手机客户端运行着DNS客户端，浏览器将接收到的url中抽取出域名字段，即访问的主机名，比如http://www.baidu.com/, 并将这个主机名传送给DNS应用的客户端，之后DNS客户机端向DNS服务器端发送一份查询报文，报文中包含着要访问的主机名字段，该DNS客户机最终会收到一份回答报文，其中包含有该主机名对应的IP地址，一旦该浏览器收到来自DNS的IP地址，就可以向该IP地址定位的HTTP服务器发起TCP连接。

**实验结果：**

本次实验中，在抓取DNS包的时候，先进行了Ping操作，ping的是baidu.com，抓取到的包为2个DNS包和8个ICMP包（四次ping），在传回来的DNS包中返回了域名的解析。

Ping操作和wireshark抓到的包如下图所示：





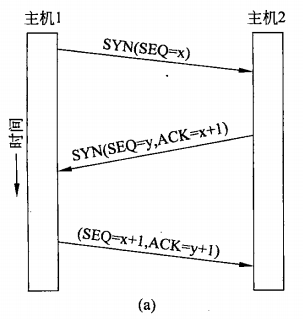
从图中cmd命令行的ping操作可以看出，在ping操作时，第一行显示了返回的解析出的域名（数据长度为32字节），下面四行显示了四次ping操作接收到的数据包，数据长度也为32字节，没有丢失数据包。

从图中Wireshark的抓包结果来看，由本机向地址10.3.9.5发送了一个DNS（query）包，然后返送回来一个DNS(response)包（第142，143行），下方是4次ping操作的请求和响应（第144-151行）。这就是DNS整个解析的过程。

1. **TCP连接建立过程**

**TCP协议过程：**

TCP建立连接经历了3次握手，理论图如下图所示



第一次握手：客户端发送syn包(seq=x)到服务器，并进入SYN\_SEND状态，等待服务器确认。

第二次握手：服务器收到syn包，必须确认客户的SYN(ack=x+1)，同时自己也发送一个SYN包(seq=y)，即SYN+ACK包，此时服务器进入SYN\_RECV状态。

第三次握手：客户端收到服务器的SYN+ACK包，向服务器发送确认包ACK(ack=y+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

握手过程中传送的包里不包含数据，三次握手完毕后，客户端与服务器才正式开始传送数据。理想状态下，TCP连接一旦建立，在通信双方中的任何一方主动关闭连接之前，TCP 连接都将被一直保持下去。

**实验结果：**

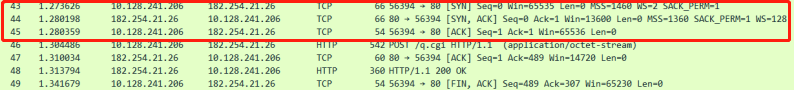
本次实验中，我访问了https://www.bupt.edu.cn/网站，三次握手中抓到的包为下图中前三行:

第一次握手是客户向服务器发送同步请求(第45行)，Seq=0;

第二次握手是服务器向客户回复一个ACK包（第46行），S其中Seq=0，ACK=1，Seq=0;

第三次握手是客户向服务器发送ACK（第47行），其中Seq=1,ACK=1。

从图中可以看出，在三次握手的过程中，传送的数据长度len=0，即不包含数据。



1. **HTTP协议过程**

**实验结果：**

HTTP协议首先要TCP经过三次握手来建立连接

第一次握手：客户向服务器发送同步请求(第43行)，Seq=0;

第二次握手：服务器向客户回复一个ACK包，S其中Seq=0(第44行)，ACK=1，Seq=0;

第三次握手：是客户向服务器发送ACK，其中Seq=1,ACK=1(第45行):

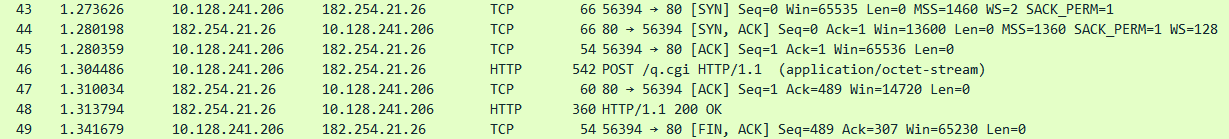
TCP三次握手结束之后就是HTTP请求(第46行)；

客户发出HTTP请求之后，服务器收到请求发送ACK(第47行)；

服务器发送报文(第48行)；

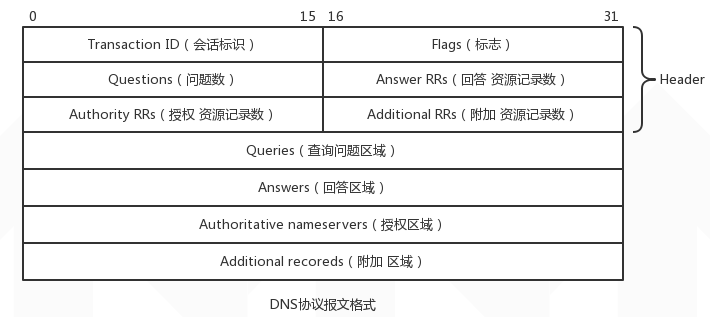
客户收到保文后发送应答报文(第49行)。

从图中可以看出，HTTP首先发出了一个POST请求，这个请求意在Request-URI所标识的资源后附加新的数据，在第49行连接结束后即可进行数据传输。



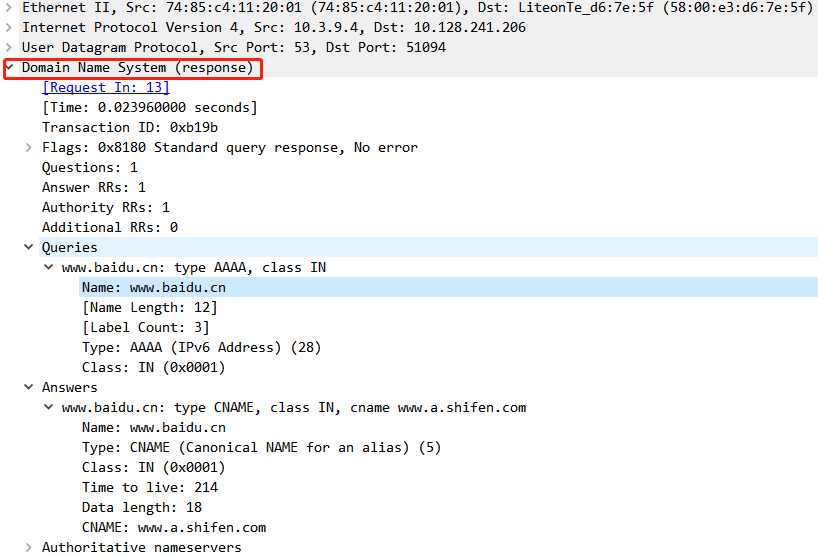
1. **分析DNS协议消息**

DNS协议消息的报文格式如下图所示：



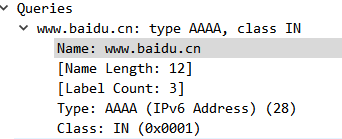
下面我们将接收到的DNS报文与之对应

这次ping的依旧是www.baidu.cn的网址，其中返送回来的DNS包如下图所示：



从图可以看到以下信息：

1. **Transaction ID**(会话标识)：0x372b。长度为2字节。
2. **Flags**（标志）：0x8180。这是一个标准查询。
3. **Questions**(问题数)：1。即只有一个问题，对应的请求帧中的问题。
4. **Answeer RRs**（回答 资源记录数）:1。
5. **Authority RRs**（授权 资源记录数）:1。
6. **Addutional RRs**（附加 资源记录数）:0。
7. **Queries**（查询问题区域）：



展开其内容包括三个部分：Name、Type、Class

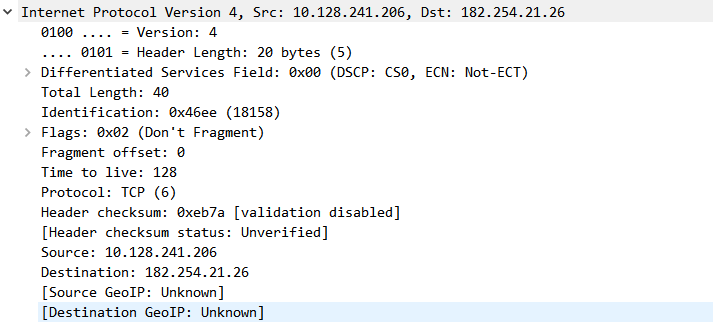
Name：一般该字段表示的就是需要查询的域名。

Type：AAAA为由域名获得IPv6地址。

Class：通常为IN，值为1，表明是Internet数据。

1. **Answers**(回答区域)**:**可以看出，这里只有一个回答，类型为CNAME，代表别名，别名为www.a.shifen.com。
2. **Authoritative nameservers**（授权区域**）:**a.shifen.com:type SOA.class IN.mname ns1.a.shifen.com
3. **IP协议消息**

下图为抓取的一个包中的IPV4协议



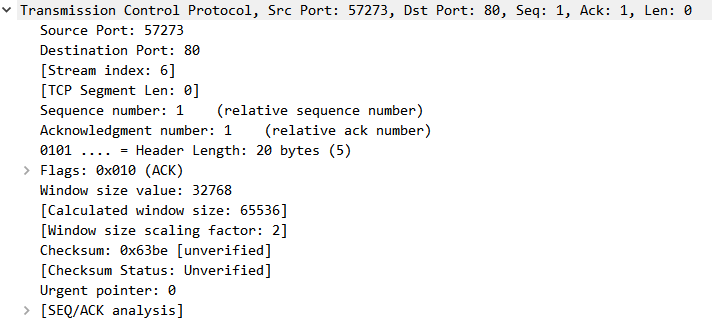
Ip协议的报文由以下几个部分组成：

1. **版本号**：IP协议的版本。对于IPv4来说值是4
2. **头部长度**（Header Length）：20字节
3. **服务类型**(Type Of Service，TOS)：此报文中为0x00 。
4. **总长度**（Total Length）: 此报文长度为40字节。总长度为整个IP数据报的长度，单位为字节。
5. **标识**(ID)：0x46ee。它唯一地标识主机发送的每一个数据报，其初始值是随机的，每发送一个数据报其值就加1。
6. **标志**(Flags)：0x02。
7. **位偏移**(fagment offset)：0.
8. **生存时间**（TTL）:128。这是数据报到达目的地之前允许经过的路由器跳数。
9. **协议**（protocol）:TCP。这是区分IP协议上的上层协议。
10. **首部校验和**（Header Checksum）：0xeb7a。 这是由发送端填充接收端对其使用CRC算法校验，检查IP数据报头部在传输过程中是否损坏。
11. **源IP地址**（Source）:数据报的发送端。

**目的IP地址**（Destination）: 数据报的接收端。

1. **TCP协议消息**

下图是抓取到的一个TCP报文



1. **源端口**(Source Port）:57273。
2. **目的端口**(Destination Port)：80.
3. **序列号**(Sequence number )：1。每一个“TCP报文段中的第一个字节”都会被赋予一个序列号。
4. **确认号**(Acknowledgement number)：1。也称ACK号或ACK字段。
5. **头部长度**(Header Length):20字节。该字段表示TCP头部的长度，以32位字为单位。
6. **状态标识**(Flags)：0x010(ACK)。ACK：确认（确认号字段有效，连接建立后一般都是启用状态）
7. **窗口大小**(Window size scaling factor)：2。窗口中的分组数量称之为：“窗口大小”。
8. **TCP检验和**(Checksum)：0x63be。该校验算法与IP、ICMP、UDP校验算法一致，其覆盖了TCP头部和数据中的一些字段。
9. **紧急指针**(Urgent pointer)：0。只有在有URG字段时才有效。该指针是一个加到“序列号字段”上的正偏移，以产生“紧急数据”的最后一个字节的序列号。
10. **HTTP协议消息格式**

这是由wireshark抓取到的一个HTTP协议报文，这是一个请求报文。



**前三行为请求行，其余部分称为请求首部。**

**请求行中**：method表示这次请求使用的是get方法，表示的请求页面信息，返回页面实体；方法之后是URI，表示请求的页面地址，图中的“/”表示服务器的根目录，之后是表示http的版本。

**请求首部**：

**Accept**：请求的对象类型。这里请求的是一个html类型的对象。

**Accept-Language**：使用的语言种类。这里表示中文。

**User-Agent**：提供了客户端浏览器的类型和版本。

**Host**：连接的目标主机。

**Connection**：对于HTTP连接的处理，keep-alive表示保持连接，如果是在响应报文中发送页面完毕就会关闭连接，状态变为close。这里表示保持连接。

**Accept-Encording**：页面编码种类。