**广州大学学生实验报告**

开课学院及实验室：计算机科学与工程实验室电子楼518室 2018年11月 13 日

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 计算机科学与教育软件 | | 年级、专业、班 | 软件162 | 姓名 | 吴广城 | 学号 | 1606100138 |
| 实验课程名称 | | 计算机网络实验 | | | | | 成绩 |  |
| 实验项目名称 | | 使用网络协议分析器捕捉和分析协议数据包 | | | | | 指导老师 | 綦科 |

**（1）实验目的**

熟悉ethereal的使用；验证各种协议数据包格式；学会捕捉并分析各种数据包。

**（2）实验环境**

操作系统windows xp、以太网；

**（3）实验内容**

1. 安装ethereal软件
2. 捕捉数据包，验证数据帧、IP数据报、TCP数据段的报文格式。
3. 捕捉并分析ARP报文。
4. 捕捉ping过程中的ICMP报文， 分析结果各参数的意义。
5. 捕捉tracert过程中的ICMP报文，分析跟踪的路由器IP是哪个接口的。
6. 捕捉并分析TCP三次握手建立连接的过程。

（7） 捕捉整个FTP工作工程的协议包

对协议包进行分析说明，依据不同阶段的协议分析，画出FTP工作过程的示意图

a.. 地址解析ARP协议执行过程

b. FTP控制连接建立过程

c . FTP 用户登录身份验证过程

d. FTP 数据连接建立过程

e. FTP数据传输过程

f. FTP连接释放过程（包括数据连接和控制连接）

1. 捕捉及研究WWW应用的协议报文，回答以下问题：

a. .当访问某个主页时，从应用层到网络层，用到了哪些协议？

b. 对于用户请求的百度主页（[www.baidu.com](http://www.baidu.com)），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？

c. 两个存放在同一个服务器中的截然不同的Web页（例如， http://www.gzhu.edu.cn/index.jsp，和http://www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？

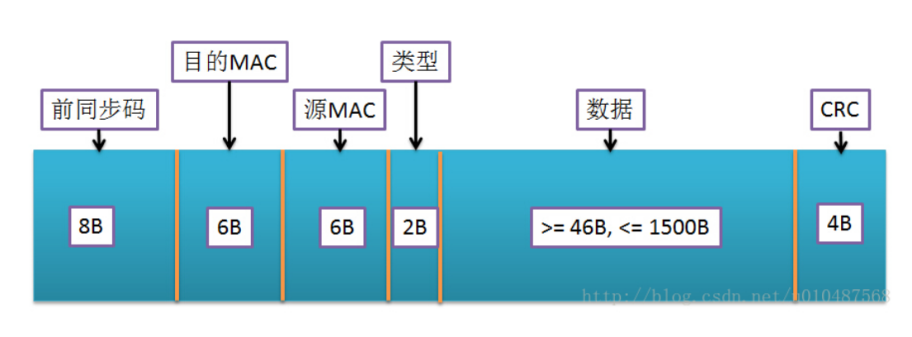
d. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？

e. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像，那么需要建立几次TCP连接和有几个UDP过程？

**（4）实验步骤、记录和结果**

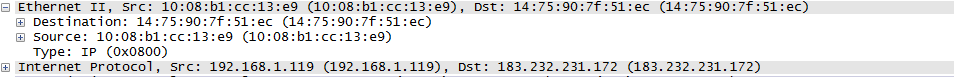
（2）捕捉数据包，验证数据帧、IP数据报、TCP数据段的报文格式。

验证数据帧：

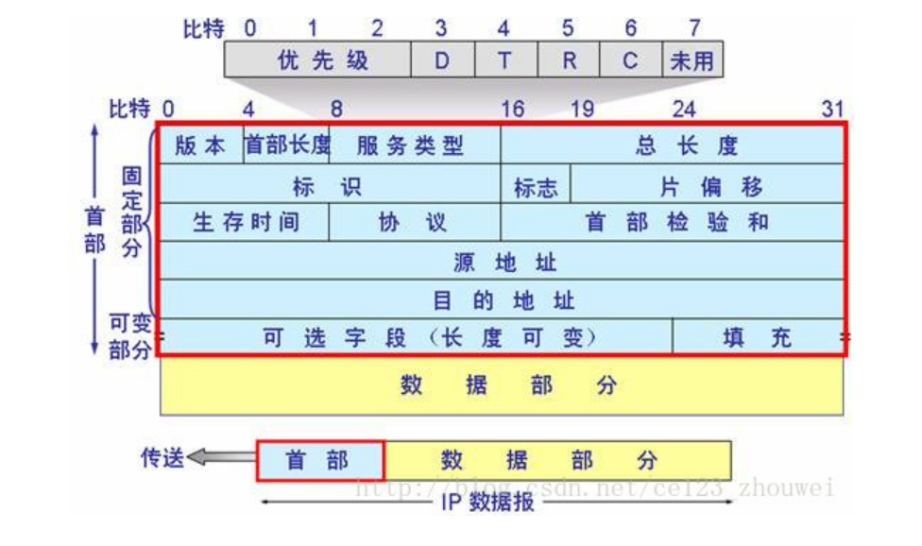


源自百度图片：数据帧格式

实验截图记录：

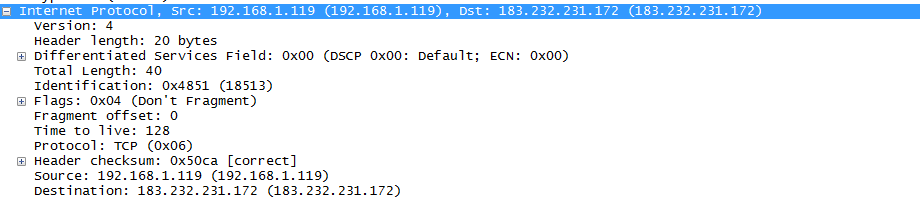


IP数据报：



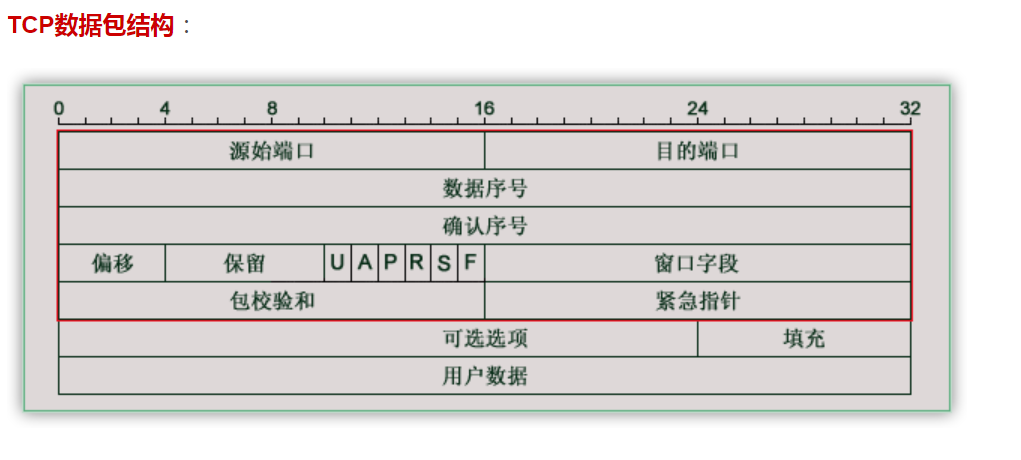
源自百度图片：ip数据报

实验截图记录：

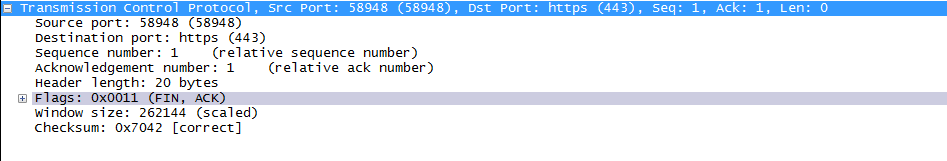


从截图可以得到该ip是ipv4，首部字节长20，以及其他信息。

TCP数据段：



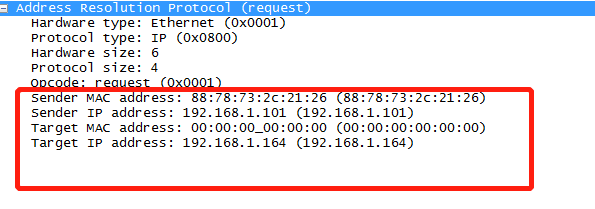
实验截图记录：



1. 捕捉并分析ARP报文。



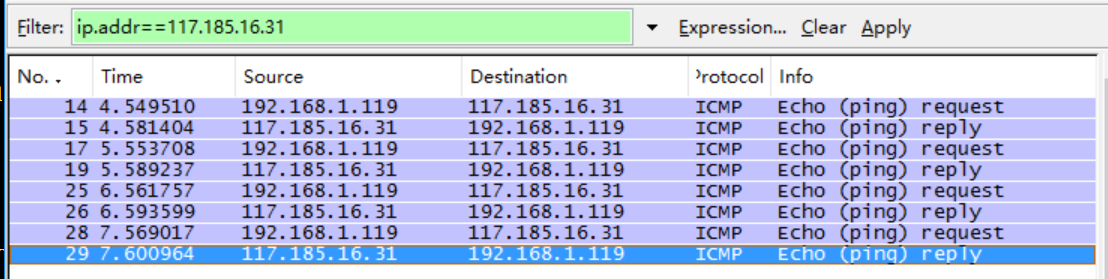
Arp报文：



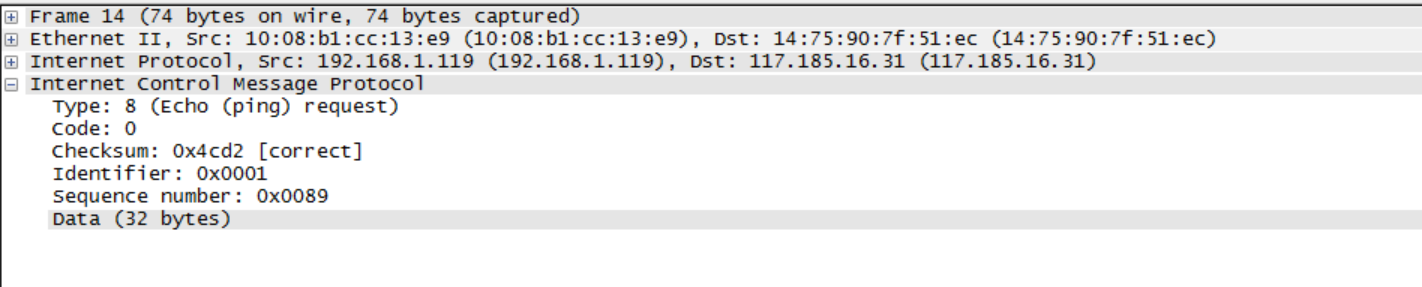
1. 捕捉ping过程中的ICMP报文， 分析结果各参数的意义。



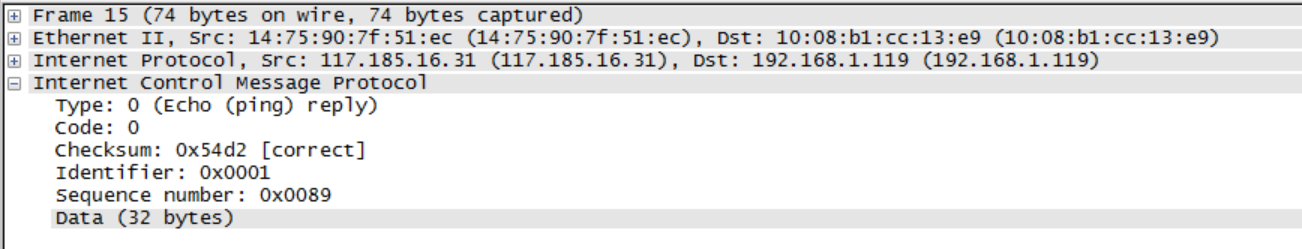
通过显示过滤器查找对baidu的请求和响应：



Request报文：

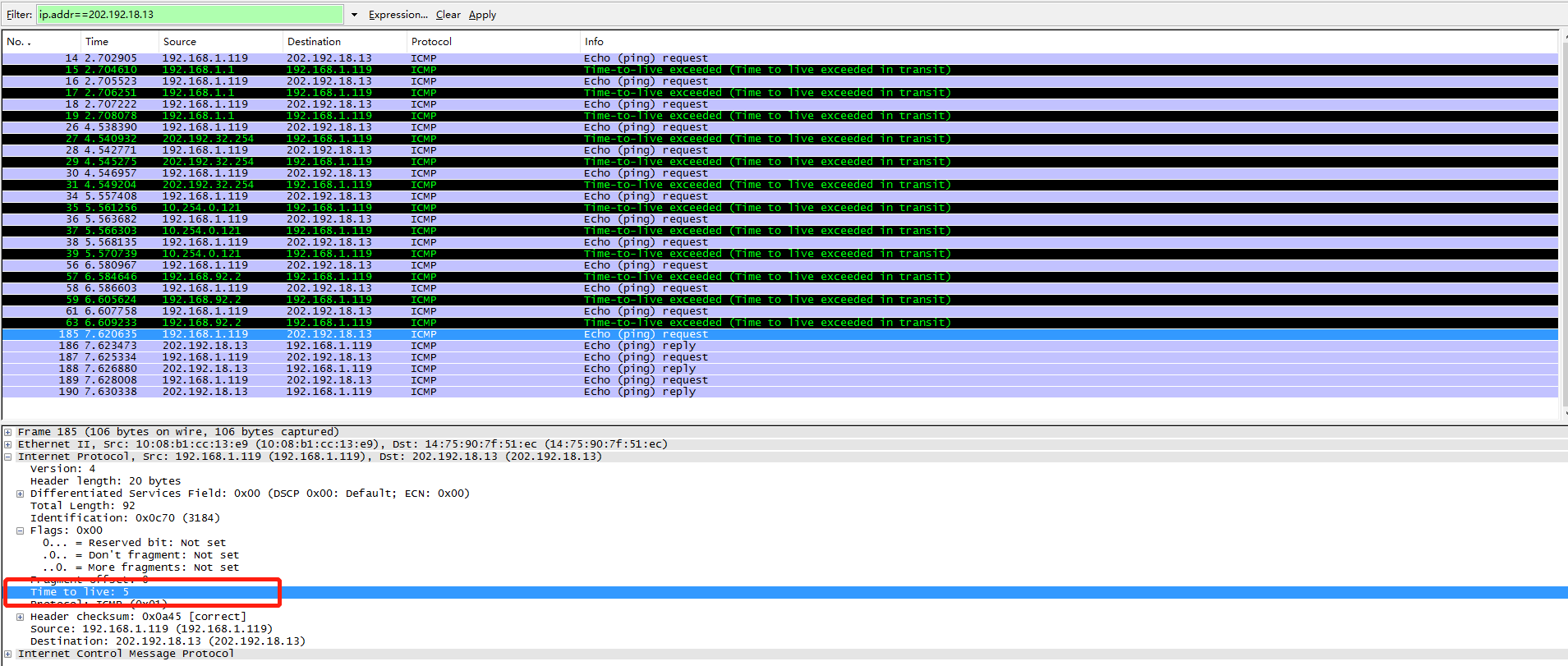


Reply报文：



1. 捕捉tracert过程中的ICMP报文，分析跟踪的路由器IP是哪个接口的。



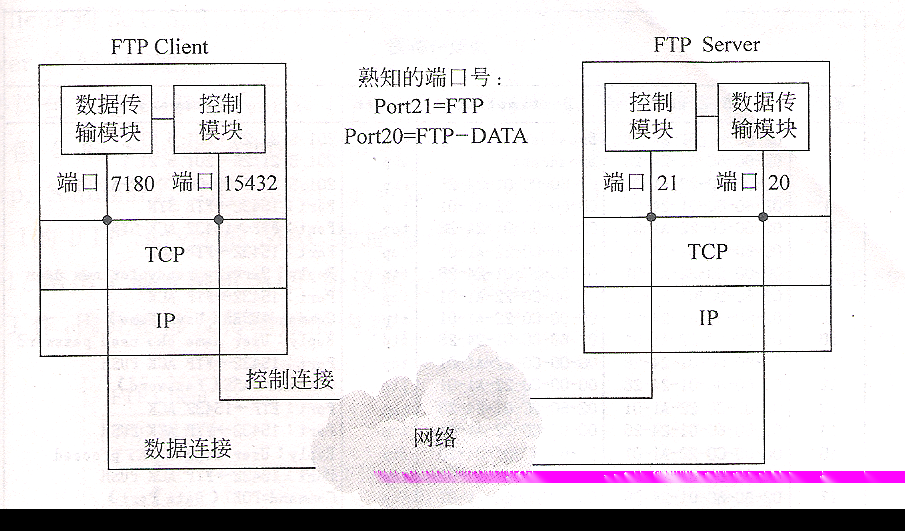


1. 捕捉并分析TCP三次握手建立连接的过程。



（7） 捕捉整个FTP工作工程的协议包

对协议包进行分析说明，依据不同阶段的协议分析，画出FTP工作过程的示意图

****

先建立控制连接，其次建立数据连接。

1. . 地址解析ARP协议执行过程

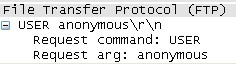
VG6RCU@JUFY60{{9F99U2IB

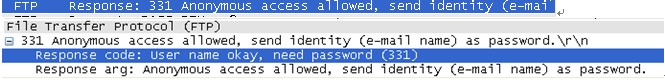
1. FTP控制连接建立过程

}DBA_MHMHDVE((8WY9U1([S

c . FTP 用户登录身份验证过程

V8_1W08IF{WFR}4I2U[AAIN



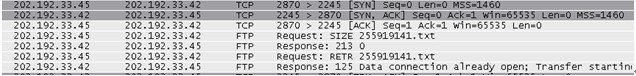


d. FTP 数据连接建立过程

FTP数据连接建立分为：连接建立准备、连接建立阶段。

e. FTP数据传输过程

传输的为文本文件：



f. FTP连接释放过程（包括数据连接和控制连接）

PN97}I%`)FJ_TK]2X%C$V]U

**（5）实验分析**

(2)捕捉数据包，验证数据帧、IP数据报、TCP数据段的报文格式。

分析：

分析：由图可知，捕捉到的数据帧格式与上述格式基本一致，数据帧由目的MAC地址，源MAC地址，数据包类型，数据组成。IP数据报，TCP数据报同是。

1. 捕捉并分析ARP报文。

分析：

图一：Destination:broadcast 说明是以广播的形式传送数据报

Source则是本机的mac地址。

图二：截图中Sender表示本机，而target则是目标，从图中可以看出源地址和目的地址各自的mac 地址和ip地址。

1. 捕捉ping过程中的ICMP报文， 分析结果各参数的意义。

分析：

图一：ping [www.baidu.com](http://www.baidu.com)

其余截图显示了reply报文与request报文的结构，

由图可知，版本号为ipv4，目的ip地址为117.185.16.31，源ip地址为192.168.1.119

1. 捕捉tracert过程中的ICMP报文，分析跟踪的路由器IP是哪个接口的。

分析：

图一：跟踪到达www.gzhu.edu.cn所经过的路由器

图二：由显示过滤器筛选后可以看到前半部分的请求都是超时的，但是后半部分到达目的ip后就可以得到reply了。

由红色框可知要经过5个路由器才可到达目的ip地址。

1. 捕捉并分析TCP三次握手建立连接的过程。

分析：

第一次握手：建立连接时，客户端192.168.1.119发送syn包(syn=j)到服务器，并进入SYN\_SEND 状态，等待服务器183.232.231.173确认；   
第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN 包 （syn=k），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=k+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。 完成三次握手，客户端与服务器 开始传送数据.

（7） 捕捉整个FTP工作工程的协议包

分析：对协议包进行分析说明，依据不同阶段的协议分析，画出FTP工作过程的示意图

1. 地址解析ARP协议执行过程

要访问ip192.168.1.147 ,但是本地主机的arp缓存表没有ip的映射，就通过广播的方式，询问哪个主机的ip是192.168.1.147，在得到响应后，就把该ip和mac的映射存入arp缓存表。

1. FTP控制连接建立过程

分析：通过TCP三次握手可知如何实现FTP的控制连接。

c . FTP 用户登录身份验证过程

*分析：*输入anonymous匿名登陆后，服务器会提示使用者输入电子邮件 (E-MAIL) 账号作为密码，由于匿名登录，所以即使不输入密码也可以登陆，因此可以直接按回车就可以完成登录。

d. FTP 数据连接建立过程

*分析：*首先，FTP客户给FTP服务器发送Port命令请求包，接着FTP服务器给FTP客户发送 Port命令答应包，然后就完成FTP数据连接的建立。

e. FTP数据传输过程

*分析：*FTP的客户发出传输请求后，FTP的服务器就向FTP客户发回文件的状态信息，如果文 件可以发送，就开始进行数据发送。

f. FTP连接释放过程（包括数据连接和控制连接）

*分析：*FTP的连接释放要通过TCP进行四次挥手释放，包括释放控制连接与释放数据连接两个 阶段，首先释放数据连接，然后再释放控制连接。

(8)捕捉及研究WWW应用的协议报文，回答以下问题：

a. .当访问某个主页时，从应用层到网络层，用到了哪些协议？

答：HTTP协议、DNS服务协议、地址解析协议ARP、Internet组织管理协议IGMP、传输控制协议TCP、用户数据报协议UDP， IP协议。

b.对于用户请求的百度主页（[www.baidu.com](http://www.baidu.com)），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？

答：会接受到两个报文。第一个是第二次握手的应答报文SYN/ACK，第二个是HTTP应答报文。时间为：2\*RTT+文档传输时间。

1. 两个存放在同一个服务器中的截然不同的Web页（例如， [http://www.gzhu.edu.cn/index.jsp，和http://www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？](http://www.gzhu.edu.cn/index.jsp，和http:/www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？)

答：如果是HTTP/1.0的协议，则不可以，因为每次传输完毕数据之后，都会释放TCP连接，如果是HTTP/1.1的协议就可以，因为它使用了持续连接。使用了同一浏览器，和该服务器可以继续在这条连接上传送的后续的HTTP请求报文和响应报文，这些文件都是在同一服务器上面的。

1. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？

答：404 Not Found。

1. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像，那么需要建立几次TCP连接和有几个UDP过程？

答：若使接；

若使用HTTP/1.1，则需要用HTTP/1.0，则需要0次UDP连接，4次TCP连0次UDP连接，1次TCP连接。

**（6）实验建议**

通过此次实验，我对五层协议的体系结构有了更加深入的认识（物理层，数据链路层，网络层，运输层，应用层），毕竟实践才是真正能促进认识的，还有在相应的协议的使用及用法，例如数据帧，IP数据报，tcp数据包，https协议，DNS服务器，arp协议等。印象深刻是tcp的三次握手，即（第一次，发送请求）客户端到服务器端，（第二次确认信号）服务器端到客户端，（第三次确认包）客服端到服务端。对于这次实验还是得先熟悉相关知识，再加上实验实践才能更大的进步。