**北京科技大学实验报告**

学院：计算机与通信工程学院 专业：计算机科学与技术 班级：计1503

41524189 41503302

41503365 61562038

姓名： 学号： 实验日期：2017年 12 月 22 日

蒋晓桐 唐誉源

杨博铭 钠力

**实验名称：**

网络应用实验

**实验目的：**

1.了解 DNS、HTTP、FTP、SMTP、POP 协议的工作过程。

2.理解网络应用的组织方式。

3.理解应用层和传输层的关系。

**实验仪器：**

PC 机一台(能连接 Internet)

**实验原理：**

1. DNS是域名系统，因特网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。通过主机名，最终得到该主机名对应的IP地址的过程叫做域名解析。其运行在UDP协议之上的53号端口。如图1为DNS请求报文格式。
2. HTTP协议是一种超文本传输协议，HTTP请求报文格式如图2，HTTP应答报文格式如图3。
3. FTP协议是一种文件传输协议，它在主机之间建立两条连接，一条连接用于数据传送，另一条连接用于传送控制信息(命令和响应)。通常来说FTP的命令端口是21，数据端口是20。本实验中采用被动模式，工作过程是发送PASV，建立数据连接使用服务器返回的端口号。
4. SMTP是简单邮件传输协议，SMTP的通信过程为客户端与服务器端建立TCP连接，客户端向服务器端发送各种命令，请求服务，服务器解析用户命令，做出相应动作并返回给客户端一个响应。SMTP命令的一般格式是COMMAND [Parameter] <CRLF>，响应的一般形式是: XXX Readable Illustration，其中XXX以2开头的表示成功，4与5开头的表示失败，3开头的表示未完成。
5. POP协议是邮局协议，用于电子邮件的接收，在用户阅读邮件时，POP命令所有的邮件信息立即下载到用户的计算机上，不在服务器上保留。它与SMTP协议共同构成电子邮件系统。POP命令的一般格式是COMMAND [Parameter] <CRLF>。

|  |
| --- |
|  |
| 图1 DNS请求报文格式 |
|  |
| 图2 HTTP请求报文格式 |
|  |
| 图3 HTTP响应报文格式 |

**实验内容与步骤：**

1. DNS

使用命令行的 DNS 客户端 nslookup 命令发出 DNS 查询，得到资源记录(Resource Record)。

(1) 在 Windows 命令行下执行 nslookup，进入 nslookup 提示符“›”。

(2) 输入主机名，如“teach.ustb.edu.cn”，查看返回结果。

(3) 输入“set type=NS”。

(4) 输入域的名称，查询根域(.)、cn 域、edu.cn 域、ustb.edu.cn 域的权限名字服务器(authoritative name server)主机名。

(5) 输入“set type=A”。

(6) 输入(4)中查询得到的主机名， 查询其对应的 IP 地址。

(7) 捕获 DNS 查询和回答，分析 DNS 协议数据。

1. HTTP

(1) 命令行下执行 telnet www.baidu.com 80

(2) 输入HEAD / HTTP/1.1

Host: www.baidu.com

(3) 输入两个回车，查看输出结果。

(4) 捕获通信数据并分析。

1. FTP

(1) 打开第一个 cmd 窗口，输入“telnet ftp.ustb.edu.cn 21”和 ftp.ustb.edu.cn 上的服 务器程序建立一个连接。

(2) 输入“USER anonymous”进行匿名登录。

(3) 输入“PASS”

(4) 输入“PASV”进入被动模式。

(5) 查看返回信息“227 Entering Passive Mode (n1,n2,n3,n4,p1,p2)”，计算 p1×256+p2，得出服务器数据连接的端口号 port。

(6) 打开第二个 cmd 窗口，执行”telnet ftp.ustb.edu.cn port”，其中 port 为(5)中计算得出的端口号。

(7) 在第一个 cmd 窗口中输入“RETR README.txt”，获取服务器上的“README.txt”文件，同时观察第二个 cmd 窗口。

(8) 捕获通信数据并分析。

1. SMTP

用户 41503302@ustb.edu.cn 给用户 41524189@ustb.edu.cn 发邮件。

(1) 输入“telnet smtp.ustb.edu.cn 25”和邮件服务器建立连接。

(2) 输入“EHLO ustb.edu.cn”。

(3) 输入“AUTH LOGIN PLAIN”进行明文认证。

(4) 输入 base64 编码的发送方用户名。

(5) 输入 base64 编码的发送方密码。

(6) 输入“MAIL FROM: 41503302@ustb.edu.cn“

(7) 输入“RCPT TO 41524189@ustb.edu.cn”

(8) 输入“DATA“

(9) 输入邮件内容，包括

“From: 41503302@ustb.edu.cn”

“ To: 41524189@ustb.edu.cn”

“Subject:hello”

“邮件内容”

(10) 输入回车，输入”.”，输入回车。

(11) 输入”QUIT”退出。

(12) 查看邮箱 41524189@ustb.edu.cn 收件箱。

(14) 捕获通信数据并分析。

1. POP

(1) 输入“telnet pop.ustb.edu.cn 110”和邮件服务器建立连接。

(2) 输入“user 用户名”。

(3) 输入“pass 密码”。

(4) 输入“list”显示邮件列表。

(5) 输入“retr 邮件号码”显示邮件内容。

(6) 输入“quit”退出。

(7) 捕获通信数据并分析。

**实验数据：**

1. 实验中关键步骤及使用WireSharks抓到的包
   1. DNS

|  |
| --- |
| 网络实验4/dns-1.PNG |
| 图1.a.1 输入主机名返回结果 |
| 网络实验4/dns-2.PNG |
| 图1.a.2 查询根域的权限域名服务器的主机名 |
| 网络实验4/dns-3.PNG |
| 图1.a.3 查询cn域的权限域名服务器的主机名 |
| 网络实验4/dns-4.PNG |
| 图1.a.3 查询edu.cn域的权限域名服务器的主机名 |
| 网络实验4/dns-5.PNG |
| 图1.a.4 查询ustb.edu.cn域的权限域名服务器的主机名 |
| 网络实验4/dns-6.PNG |
| 网络实验4/dns-7.PNG |
| 图1.a.5 查询对应IP |
|  |
| 图1.a.6 捕获到的全部数据包 |

* 1. HTTP

|  |
| --- |
|  |
| 图1.b.1 HEAD操作步骤 |
|  |
| 图1.b.2 GET操作步骤 |
|  |
| 图1.b.3 HEAD请求过程 |
|  |
| 图1.b.4 响应过程 |
| 图1.b.5 GET请求过程    图1.b.5 响应过程 |

* 1. FTP

|  |
| --- |
| 网络实验4/ftp-1.PNG |
| 图1.c.1 操作步骤 |
| 网络实验4/ftp-2.PNG |
| 图1.c.2 README.txt内容 |
|  |
|  |
| 图1.c.3 FTP协议的全部帧 |

* 1. SMTP

|  |  |  |
| --- | --- | --- |
|  | | |
| 图1.d.1 STMP关键步骤 | | |
|  | | |
| 图1.d.2 STMP协议的全部帧 | | |
|  | | |
|  |
| 图1.d.3 接收邮件结果 |

* 1. POP

|  |
| --- |
|  |
|  |
|  |
|  |
| 图1.e.1 POP协议全部帧 |

1. 异常现象分析
   1. 异常现象：验证FTP协议时，输入计算得出的端口号无法登入

原因：超时后，分配的端口会失效

* 1. 异常现象：验证SMTP协议时，用户名输入出错

原因：编码base64时，空格符也会被编码，因此需要特别注意首尾的空格符是否删除

* 1. 异常现象：验证POP协议时，登陆邮箱失败

原因：

1. 使用学生邮箱进行实验时，POP服务器地址应为pop.xs.ustb.edu.cn，而不是pop.ustb.edu.cn，由于未连接正确的服务器，因此登录失败。
2. 使用163邮箱进行实验时，由于163邮箱设置了登陆POP服务时需要使用授权码，因此此时登陆密码应为授权码，旧密码不正确。
3. 输入密码时，删除键也会作为一个参数传给服务器，导致错误，如图2.e.1所示，\b被作为密码传入，导致-ERR错误

|  |
| --- |
|  |
| 图2.e.1 |

**实验数据处理：**

**一、主机名与地址**

根名字服务器:a.root-server.net 198.41.0.4

cn 域名字服务器:a.dns.cn 203.119.25.1

edu.cn 域名字服务器:dns.edu.cn 202.112.0.35

ustb.edu.cn 域名字服务器:dns.ustb.edu.cn 202.204.48.6

**二、基于 一个TCP 的应用分析通信过程中 TCP某些字段的变化**

* **三次握手建立连接过程：**

|  |
| --- |
|  |
| **第一次握手（SYN=1）：**    源端口：f8 e7 为63719号  目的端口：00 50 为80号  序号：41 ba 77 b5  确认号：00 00 00 00  首部长度：b0为44字节  标志位：02(0000 0010)表明SYN为1，这是一个连接请求  窗口值：ff ff 为65545  校验和：1d bf  紧急指针：00 00  接下来是可选项，包括MSS等信息 |
| **第二次握手（SYN，ACK=1）**    源端口：00 50 为80号  目的端口：f8 e7 为63719号  序号：9b 70 d6 dd  确认号：41 ba 77 b6为1  首部长度：b0为44字节  标志位：12(0001 0010)表明SYN为1，ACK为1，表示同意连接  窗口值：20 00 为8129  校验和：c5 f0  紧急指针：00 00  接下来是可选项，包括MSS等信息 |
| **第三次握手（ACK=1）**    源端口：f8 e7 为63719号  目的端口：00 50 为80号  序号：41 ba 77 b6  确认号：9b 70 d6 de  首部长度：50为20字节  标志位：10(0001 0000)表明ACK为1，客户机收到同意的报文给出的回复  窗口值：20 00为8129  校验和：3b ca  紧急指针：00 00  接下来是可选项，包括MSS等信息 |

* **HTTP传输数据过程**

|  |
| --- |
|  |
| **第一次（ACK=1）**    源端口：00 50 为80号  目的端口：f8 e7 为63719号  标志位：10（00010000）表明ACK为1，确认收到了上一帧 |
| **第二次（ACK=1）**    源端口：f8 e7 为63719号  目的端口：00 50 为80号  标志位：10（00010000）表明ACK为1，确认收到了上一帧 |

* **四次挥手断开连接**

|  |
| --- |
| **第一次挥手（ACK，FIN=1）**    源端口：00 50 为80号  目的端口：f8 e7 为63719号  序号 9b 70 d8 2a  标志位：11（00010001）表明FIN和ACK为1，63719号发出关闭信息，关闭客户端到服务器端的数据传送 |
| **第二次挥手（ACK=1）**    源端口：f8 e7 为63719号  目的端口：00 50 为80号  确认号 ：9b 70 d8 2b为收到的序号加一  标志位：10（00010000）表明ACK为1，确认收到了上一帧 |
| **第三次挥手（FIN，ACK=1）**    源端口：f8 e7 为63719号  目的端口：00 50 为80号  序号：41 ba 77 dd  标志位：11（00010001）表明FIN和ACK为1，80号发出关闭信息，关闭服务器端到客户端的数据传送 |
| **第四次挥手（ACK=1）**    源端口：00 50 为80号  目的端口：f8 e7 为63719号  确认号：41 ba 77 de为收到的序号加一  标志位：10（00010000）表明ACK为1，确认收到了上一帧 |

**具体流程如下：**

　　1. 主机发起一个TCP连接请求（TCP）

　　2. 服务器响应连接请求（TCP）

　　3. 主机返回ACK完成3次握手成功建立连接（TCP）

　　4. 主机发送一个HTTP请求（HTTP）

　　5. 服务器收到请求返回一个ACK帧（TCP）

　　6. 服务器根据请求发送数据到主机（HTTP）

7. 主机收到服务器数据返回一个ACK帧（TCP）

8. TCP客户端发送一个FIN，关闭客户端到服务器端的数据传送。（客户端不再发送报文给服务器端，但可接受服务器端报文）

9. 服务器收到这个FIN，它发回一个ACK，确认序号为收到的序号加1。   
　　10.服务器关闭客户端的连接，发送一个FIN给客户端。（服务器端关闭到客户端的数据传送）

11.客户段发回ACK报文确认，并将确认序号设置为收到序号加1。

**三、几种应用层协议的报文结构**

1. DNS

|  |
| --- |
|  |
| **DNS请求报文：**  标识ID：00 0c  标志字段:01 00（首位为0表示DNS请求，第八位为0表示客户端希望递归查询）  问题数:00 01  资源记录数:00 00  授权资源记录数:00 00  额外资源记录数:00 00  查询的域名:05 74 65 61 63 68 04 75 73 74 62 03 65 64 75 02 63 6e 00（teach.ustb.edu.cn）  类型:00 01类型为A表示请求将域名转换为IP  类:00 01表示class IN表示因特网 |

|  |
| --- |
|  |
| **DNS回应报文：**  标识ID：00 0c与请求报文一致  标志字段：85 80（首位为1表示DNS回应，第6-9表示授权的回答不可截断的，授权可用的）  问题数：00 01  资源记录数：00 01  授权资源记录数：00 03  额外资源记录数：00 03  查询的域名：05 74 65 61 63 68 04 75 73 74 62 03 65 64 75 02 63 6e 00（teach.ustb.edu.cn）  查询类型00 01类型A表示请求将域名转化为IP  查询类：00 01因特网  指针c0 0c指向DNS头部偏移12字节，即查询名开始位置  第一个资源记录的响应类型：00 01类型A  第一个资源记录的响应类：00 01因特网  第一个资源记录的生存时间：00 00 1c 20生存时间7200s  第一个资源记录的数据长度：00 04  表示地址：ca cc 34 75 （202.204.52.117）  指针：C0 12指向DNS头部偏移18字节，即第一个资源记录中的数据  第二个资源记录的响应类型：00 02(NS)  第二个资源记录的响应类：00 01代表因特网  第二个资源记录的生存时间：00 00 1c 20  第二个资源记录的数据长度：00 07  表示地址：04 64 6e 73 32 c0 12（dns2.ustb.edu.cn）  指针:C0 52:，指向DNS头部偏移第二个资源记录中的数据  第三个资源记录的响应类型:00 02(NS)  第三个资源记录的响应类:00 01  第三个资源记录的生存空间:00 00 1c 20:  第三个资源记录的数据长度:00 06  表示地址:03 64 6e 73 c0 12 (dns.ustb.edu.cn)  指针C0 12指向DNS头部偏移第三个资源记录中的数据  第四个资源记录的响应类型:00 02(NS)  第四个资源记录的响应类:00 01  第四个资源记录的生存空间:00 00 1c 20  第四个资源记录的数据长度:00 07  表示地址 :04 64 6e 73 34 c0 12(dns4.ustb.edu.cn) |
| 问答区域  头部区域 | |
| 图1.1 DNS 请求报文 | |
| 附加区域  权威区域  回答区域  问题区域  头部区域 | |
| 图1.2 响应报文 | |

1. HTTP协议

|  |
| --- |
|  |
| **HTTP请求报文：**  *请求行:*  请求方式：48 45 41 44 采用HAED方式（服务端接受到HEAD请求后只返回响应头，而不会发送响应内容。）  空格：20  URI：2f  HTTP版本：48 54 54 50 2f 31 2e 31（表明是1.1版本）  *请求头部：*  关键字/值 ：48 6f 73 74 3a 77 77 77 2e 62 61 69 64 75 2e 63 6f 6d 0d 0a  说明请求的主机名为[www.baidu.com](http://www.baidu.com)  *空行：*0d 0a |
|  |
| **HTTP响应报文**  *状态行：*  HTTP版本：48 54 54 50 2f 31 2e 31版本为1.1  状态码：32 30 30状态码200表示客户端请求成功  状态代码的文本描述：4f 4bOK 表示客户端请求成功  由于使用HEAD请求，其余部分全部为消息报头 |
|  |
| **HTTP请求报文：**  *请求行:*  请求方式：47 45 54采用GET方式  空格：20  URI：2f  HTTP版本：48 54 54 50 2f 31 2e 31（表明是1.1版本）  *请求头部：*  关键字/值 ：48 6f 73 74 3a 77 77 77 2e 62 61 69 64 75 2e 63 6f 6d 0d 0a  说明请求的主机名为[www.baidu.com](http://www.baidu.com)  *空行：*0d 0a |
|  |
| **HTTP响应报文**  可以看出：H  TTP版本版本为1.1  状态码200表示客户端请求成功  状态代码的文本描述OK 表示客户端请求成功  传回文件长度为14613字节，格式为text/html：HTML格式  及文件的具体内容 |

由于以下协议发送时均为一个字一个字发送（见实验数据），篇幅较长，分析不便，因此，我们将其摘录为文本格式，假定其按照整条指令发送，进行分析，此处仅改变了格式，内容均未改变，因此某些输入指令修改时由于输入删减符”/b”而出现错误（当按照整条指令发送时不会出现这样的错误）的情况也予以保留。

1. FTP协议

将包中主要信息摘录为文本如下

1. Response: 220 USTB FTP server (IPv6 mode) ready. All transfers are logged. /\*返回220，确认连接成功\*/
2. Request:USER anonymous /\*匿名登录\*/
3. Response: 331 Please specify the password. /\*返回331，服务器要求密码\*/
4. Request:PASS /\*密码为空\*/
5. Response: 230 Login successful. /\*返回230登录成功\*/
6. Request:PASV /\*请求被动模式\*/
7. Response: 227 Entering Passive Mode (0,0,0,0,103,203). /\*计算可得服务器传输的端口为26571，如图3.1\*/
8. Request:RETR REM\bADME.txt /\*客户端发送给服务器的RETR命令报文，用户要求检索文件的名字为REM\bADME.txt\*/
9. Response: 550 Failed to open file. /\*打开失败，如图3.2\*/
10. Request:RETR README.txt /\*客户端发送给服务器的RETR命令报文，用户要求检索文件的名字为README.txt\*/
11. Response: 150 Opening BINARY mode data connection **for** README.txt (686 bytes). /\*服务器向客户端发回检索文件的状态信息如图3.3\*/
12. Response: 226 Transfer complete. /\*服务器通知客户端传输结束\*/

|  |
| --- |
|  |
| 图3.1 服务器分配的端口 |
|  |
| 图3.2 失败信息 |
|  |
| 图3.3 返回文件状态信息 |

如图1.1，服务器分配的被动端口是26571，我们可以通过103\*256+203计算得出使用。

如图1.2，当文件名作为参数输入错误时，返回的代号是550，其意义为：File unavailable，也即该文件名的文件不可用。

如图1.3，文件README.TXT大小为686字节

1. SMTP协议

将包中的主要信息摘要为文本如下：

1. S: 220 smtp-2.qy.internal ESMTP ready/\*服务器发送220状态码确认连接已经建立\*/
2. C: ehlo xs.ustb.edu.cn /\*客户端收到应答后发送EHLO，启动客户端和服务器的SMTP会话\*/
3. S: 250 smtp-2.qy.internal | 250 PIPELINING | 250 8BITMIME | 250 AUTH=LOGIN PLAIN | 250 AUTH PLAIN LOGIN | 250 STARTTLS
4. C: auth login /\*明文认证\*/
5. S: 334 VXNlcm5hbWU6 /\*服务器要求用户输入用户名\*/
6. C: User: NDE1MDMzMDJAeHMudXN0Yi5lZHUuY24= /\*客户端输入用户名使用的base6编码\*/
7. S: 334 UGFzc3dvcmQ6 /\*服务器要求用户输入密码\*/
8. C: Pass: /\*客户端输入密码使用的base64编码\*/
9. S: 235 2.0.0 OK /\*认证成功/
10. C: mail from:41503302@xs.ustb.edu.cn /\*输入发信人邮箱\*/
11. S: 250 2.1.0 Ok /\*服务器返回状态码250 OK\*/
12. C: rcpt to:41524189@xs.ustb.edu.cn /\*客户端输入收件人邮箱\*/
13. S: 250 2.1.5 Ok /\*服务器返回状态码250 OK\*/
14. C: data /\*客户端发出data命令\*/
15. S: 354 End data with <CR><LF>.<CR><LF>
16. C: DATA fragment, 30 bytes/\*然后输入数据传输到服务器\*/
17. C: DATA fragment, 28 bytes
18. from: 41503302@xs.ustb.edu.cn, subject: hello, , from:41503302@xs.ustb.edu.cn  , to:41524189@xs.ustb.edu.cn  , subject:hello  , Hello it's me  , I was wondering if after all these years you'd like to meet ……
19. [TCP ACKed unseen segment] S: 250 2.0.0 Ok: queued as 7EFB442B38
20. ......
21. C:quit /\*客户端发出quit命令\*/
22. POP协议

POP服务器响应第一行以”+OK”或”-ERR”开头，分别表示相应的操作是成功还是失败。

POP命令一般形式为COMMAND [Parameter] <CRLF>

将包中的主要信息摘要为文本如下：

1. C：telnet pop.xs.ustb.edu.cn 110   /\*　以telnet方式连接邮件服务器　\*/
2. S：+OK POP3 ready /\* +OK,代表命令成功\*/
3. C：USER 41524189@xs.ustb.edu.cn /\* 采用明文认证 \*/
4. S：+OK send PASS
5. C：PASS \*\*\*\*\*\*\*\* /\* 发送邮箱密码 \*/
6. S：+OK 17 message(s) [140882981 byte(s)]/\* 认证成功，转入处理状态 \*/
7. C：LIST /\* 显示邮箱列表 \*/
8. S：+OK 17 messages /\* 成功 \*/
9. 1 136246  , 2 4593  , 3 336394  , 4 1162414  , 5 245818  , 6 464274  , 7 3361418  , 8 4078974  , 9 4665  , 10 3352  , 11 6926  , 12 9816  , 13 10804  , 14 4491  , 15 15173  , 16 3008  , 17 131034615  , .
10. /\*表明第一封邮件为136246字节...\*/
11. C：RETR 1 /\* 下载第一封邮件 \*/
12. S：+OK message follows
13. /\* 第一封邮件的具体内容 \*/
14. C: QUIT /\* 退出连接 \*/
15. S：+OK GoodBye/\* 成功地退出了连接 \*/

注：RETR下载下来的邮件难以看懂，这是因为其可能使用了quoted-printable编码或base64编码

**实验结果与分析：**

**DNS：**实验中通过DNS协议学习了域名和IP的转换，使得课堂中所学的理论知识得到了实践。同时我们在实践中还了解如何判断DNS是否解析故障，主要是借助系统自带的NSLOOKUP，如果解析想要访问的域名却收到DNS request timed out，timeout was 2 seconds的提示信息。这说明本地计算机确实出现了DNS解析故障。

**HTTP：**

实验中通过分析HTTP协议的报文，了解了HTTP与服务器交互的不同方法，实验中实践了GET与HEAD，GET的本质就是发送一个请求来取得服务器上的某一资源。资源通过一组HTTP头和呈现据（如HTML文本，或者图片或者视频等）返回给客户端。而HEAD和GET本质是一样的，区别在于HEAD不含有呈现数据，而仅仅是HTTP头信息。

**FTP：**

通过对FTP协议的验证，了解了文件传输协议的在被动模式下的工作流程，服务器将给主机返回一条包含了数据端口的信息，客户端通过计算可以得出端口号，从而实现文件的传输。在被动方式FTP中，命令连接和数据连接都由客户端发起，这样就可以解决从服务器到客户端的数据端口的入方向连接被防火墙过滤掉的问题。

**SMTP和POP：**

通过对SMTP协议的验证，我们更好的了解了邮件系统的工作方式，SMTP是一个简单的邮件传输协议，而POP是一个用于接收的邮局协议。实际上还有另一种用于接收邮件的协议IMAP（交互式邮件存取协议）。他们之间的主要区别在于：POP3协议允许电子邮件客户端下载服务器上的邮件，但是在客户端的操作（如移动邮件、标记已读等），不会反馈到服务器上，比如通过客户端收取了邮箱中的3封邮件并移动到其他文件夹，邮箱服务器上的这些邮件是没有同时被移动的 。而IMAP提供webmail 与电子邮件客户端之间的双向通信，客户端的操作都会反馈到服务器上，对邮件进行的操作，服务器上的邮件也会做相应的动作。同时，IMAP像POP3那样提供了方便的邮件下载服务，让用户能进行离线阅读。IMAP提供的摘要浏览功能可以让你在阅读完所有的邮件到达时间、主题、发件人、大小等信息后才作出是否下载的决定。此外，IMAP 更好地支持了从多个不同设备中随时访问新邮件。

总之，通过本次的实验，我们更好的理解了应用层上的各常用协议的工作流程。由于应用层上的各个实验都与日常我们对于互联网的使用息息相关，因此本次实验实际上是比较有趣的，同时也帮助我们理解了日常生活中我们的各种操作背后的工作流程。同时通过分析各个协议的报文，我们可以找出各个协议的框架，是对我们理论知识的又一次巩固。