实验十一 FTP 协议分析

【实验目的】

1、理解 FTP 协议的工作原理；
2、了解 FTP 协议的常用命令；
3、了解应用层协议与传输层协议的关系。

【实验学时】

2 学时

【实验环境】

本实验中需要有一台开启 FTP 服务的主机，并提供一个公共帐号：welcome，密码：welcome。实验拓扑图如图 5- 11 所示：

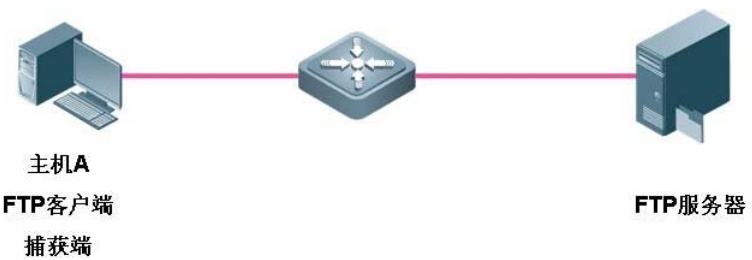

图 5- 11 实验拓扑图

【实验内容】

1、学习 FTP 协议的工作原理；
2、学习 FTP 的使用方法；
3、了解 FTP 的常用命令；
4、了解 FTP 的工作过程；
5、理解 FTP 的主动模式和被动模式。

【实验流程】

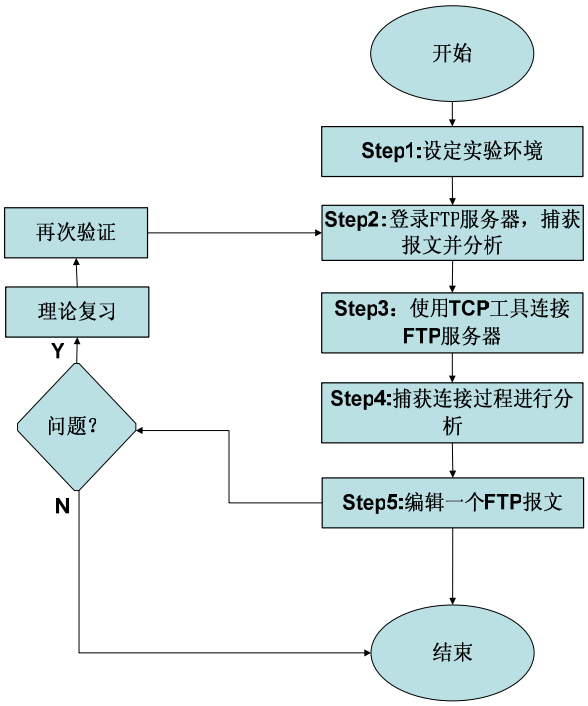

图 5- 12 实验流程图

【实验原理】

FTP（File Transfer Protocal），是文件传输协议的简称。

FTP 使得主机间可以共享文件，用于控制 Internet 上文件的双向传输。它是一个客户机/服务器系统。用户通过一个支持 FTP 协议的客户机程序，连接到在远程主机上的 FTP 服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户所发出的命令，并将执行的结果返回到客户机。

当 FTP 客户端与服务器建立 FTP 连接时，将与服务器上的两个端口建立联系：端口 20 和 21。FTP 使用不同的端口号传输不同的内容，会建立不同的 TCP 连接。首先，使用 TCP 生成一个虚拟连接用于控制信息，然后再生成一个单独的 TCP 连接用于数据传输。

FTP 的工作过程

FTP 使用 2 个 TCP 端口，一个数据端口和一个命令端口（也可叫做控制端口）。通常来说这两个端口是 21——命令端口和 20——数据端口，但根据 FTP 工作在主动模式还是被动模式，21 和 20 端口的使用方法略有不同。

主动模式的 FTP 是这样的：客户机从一个任意的非特权端口 N（N≥1024），连接到 FTP 服务器的命令端口，也就是 21 端口，建立一个控制连接。这个连接用于传递客户端的命令和服务器端对命令的响应，生存期是整个 FTP 会话时间。

如果期间需要传输文件和其它数据，例如：目录列表等，客户端就需要建立数据连接了。

这种连接在需要数据传输时建立，而一旦数据传输完毕就关闭，整个 FTP 期间可能会建立多次。在主动模式下，建立数据连接时，客户端会开始监听端口 N+1，并发送 FTP 命令“port N+1”到 FTP 服务器。接着服务器会从它自己的数据端口（20）连接到客户端指定的数据端口（N+1），开始进行数据传输。

图 5- 13 展示了一个 FTP 主动模式的例子，从中可以清楚的看到 FTP 主动模式下，控制连接和数据连接是如何建立的：

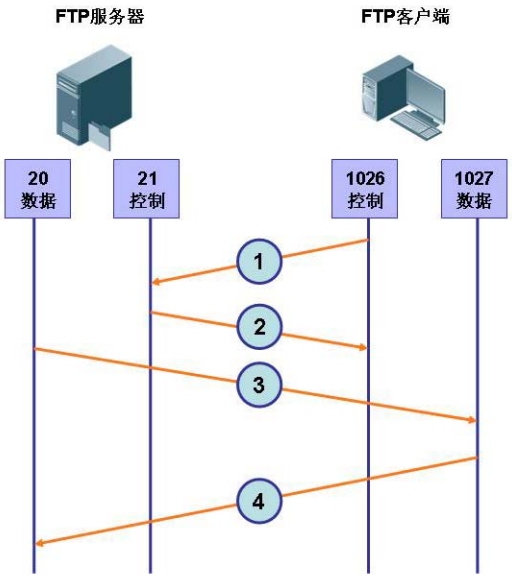

图 5- 13 FTP 的主动模式

但是，由于我们访问的 FTP 服务器大多在外网，和我们所在的内网之间通常会有防火墙进行保护，由外网的 FTP 服务器主动发起的连接，往往被防火墙所阻拦。为了解决这个问题，需要使用另外一种 FTP 模式，叫做被动模式（passive mod）。在这种模式下，数据连接是由客户程序发起的，和刚才讨论过的主动模式相反。

图 5- 14 展示了一个 FTP 被动模式的例子，从中可以清楚的看到 FTP 被动模式下，控制连接和数据连接是如何建立的：

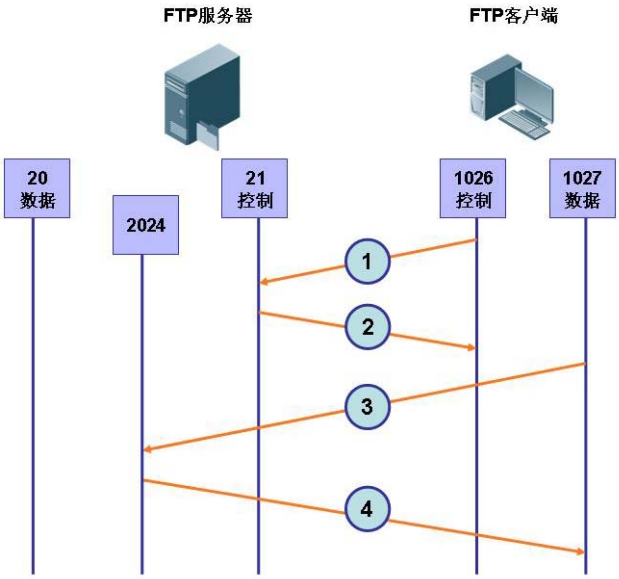

图 5- 14 FTP 的被动模式

被动模式下开启一个 FTP 连接时，客户端打开两个任意的非特权本地端口 N 和 N＋1（N ≥1024）。第一个端口连接服务器的 21 端口，但与主动方式的 FTP 不同，客户端不会提交 PORT 命令并允许服务器来回连它的数据端口，而是提交 PASV 命令。这样做的结果是服务器会开启一个任意的非特权端口（P ≥ 1024），并发送 PORT P 命令给客户端。然后客户端发起从本地端口 N+1 到服务器的端口 P 的连接用来传送数据。

FTP 的命令

FTP 的控制连接使用类似 TELNET 协议的方式在主机间交换命令和消息。FTP 控制帧包含 FTP 的命令和选项。大多数 FTP 控制帧是简单的 ASCII 文本，可以分为 FTP 命令或 FTP 消息。FTP 消息是对 FTP 命令的响应，它由带有解释文本的应答代码构成。

表 5-2 FTP 命令列表

命令	描述
ABOR	中断数据连接程序
ACCT <account>	系统特权帐号
ALLO <bytes>	为服务器上的文件存储器分配字节
APPE <filename>	添加文件到服务器同名文件
CDUP <dir path>	改变服务器上的父目录
CWD <dir path>	改变服务器上的工作目录
DELE <filename>	删除服务器上的指定文件
HELP <command>	返回指定命令信息
LIST <name>	如果是文件名列出文件信息，如果是目录则列出文件列表

MODE <mode>	传输模式（S=流模式，B=块模式，C=压缩模式）
MKD <directory>	在服务器上建立指定目录
NLST <directory>	列出指定目录内容
NOOP	无动作，除了来自服务器上的承认
PASS <password>	系统登录密码
PASV	请求服务器等待数据连接
PORT <address>	IP 地址和两字节的端口 ID
PWD	显示当前工作目录
QUIT	从 FTP 服务器上退出登录
REIN	重新初始化登录状态连接
REST <offset>	由特定偏移量重启文件传递
RETR <filename>	从服务器上找回（复制）文件
RMD <directory>	在服务器上删除指定目录
RNFR <old path>	对旧路径重命名
RNTO <new path>	对新路径重命名
SITE <params>	由服务器提供的站点特殊参数
SMNT <pathname>	挂载指定文件结构
STAT <directory>	在当前程序或目录上返回信息
STOR <filename>	储存（复制）文件到服务器上
STOU <filename>	储存文件到服务器上
STRU <type>	数据结构（F=文件，R=记录，P=页面）
SYST	返回服务器使用的操作系统
TYPE <data type>	数据类型（A=ASCII，E=EBCDIC，I=binary）
USER <username>>	系统登录的用户名

标准 FTP 消息如下：

表 5-3 FTP 响应代码列表

响应代码	解释说明
110	新文件指示器上的重启标记
120	服务器准备就绪的时间（分钟数）
125	打开数据连接，开始传输
150	打开连接
200	成功
202	命令没有执行
211	系统状态回复

212	目录状态回复
213	文件状态回复
214	帮助信息回复
215	系统类型回复
220	服务就绪
221	退出网络
225	打开数据连接
226	结束数据连接
227	进入被动模式（IP 地址、ID 端口）
230	登录因特网
250	文件行为完成
257	路径名建立
331	要求密码
332	要求帐号
350	文件行为暂停
421	服务关闭
425	无法打开数据连接
426	结束连接
450	文件不可用
451	遇到本地错误
452	磁盘空间不足
500	无效命令
501	错误参数
502	命令没有执行
503	错误指令序列
504	无效命令参数
530	未登录网络
532	存储文件需要帐号
550	文件不可用
551	不知道的页类型
552	超过存储分配
553	文件名不允许

FTP 的使用方法

FTP 尽管可以直接被终端用户使用，但其应用主要还是通过程序实现。用户可以通过它把自己的 PC 机与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序

和信息。

在 Windows 系统中使用 FTP，可以在命令提示符下键入：
ftp 192.168.1.10（实验室 FTP 服务器的 IP 地址）；
用户被提示输入用户名和口令，确认口令输入正确后，用户将获得 FTP 提示符“ftp>”。

FTP 常用的命令：
Binary： 将文件传输模式设为二进制方式
Bye： 退出，结束远程连接
Case： 打开 case 功能
Close： 关闭远程连接
cd<directory>： 改变远程系统目录名
cd up： 进入父目录
debug<level>： 设置调试级别
dir： 显示路径名
delete<filename>： 在远程计算机中删除文件：
get<filename>： 将文件从远程系统下载到本地系统
glob： 在文件传输时使用通配符
hash： 每传输 1024 字节打印一个“#”
help： 打印帮助文件
lcd<directory>： 改变本地系统路径
ls： 打显示远程主机目录
lpwd： 打印本地主机工作路径
mget<filenames>： 将多个文件从远程系统下载到本地系统
mkdir<directory>： 在远程计算机上创建路径
input<filenames>： 将多个文件上载到远程计算机
prompt： 交互式提示
put<filename>： 将文件上载到远程计算机
pwd： 显示当前工作路径
user： 登录到远程计算机系统

【实验步骤】

步骤一：登录 FTP 服务器，捕获数据报文并进行分析

1、确认 FTP 服务器工作正常，记录 FTP 服务器的 IP 地址：192.168.1.10/24，用户名：welcome，密码：welcome。

2、在实验主机上启动网络协议分析仪，设置过滤条件并进行数据捕获。在工具栏点击“过滤器”按钮，会弹出“设置&过滤器”对话框，在“过滤器类型”中选择“类型过滤器”，类型值中选择“ftp 协议”，点击“设置参数”按钮后“确定”，然后启动协议分析仪进行捕获：

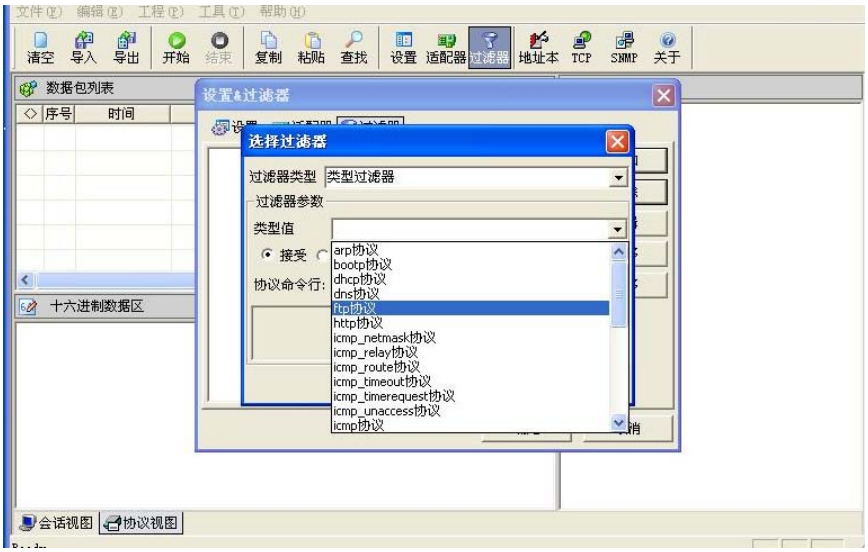

图 5- 15 设置 FTP 协议过滤器

3、登录 FTP 服务器，在命令行提示符下运行：ftp 192.168.1.10 ，即可建立与 FTP 服务器的连接，按照提示输入账号（welcome），密码（welcome），便进入了 FTP 的命令行界面，此时运行 FTP 的命令 dir、get、quit 等，从中可以看到 FTP 的反馈信息，以及 FTP 服务器的文件内容：

图 5- 16 登录 FTP 服务器

4、暂停协议分析器的捕获，可以通过捕获的数据报文看到刚才的交互过程中，FTP 客户端和服务器端的工作详细情况， FTP 报文的格式和命令的使用，以及服务器端的响应代码。

如图 5- 17 中就可以看到 FTP 的 USER 命令，及其参数 welcome，也就是用户名；而图 5- 18 中则是 PASS 命令和密码 welcome：

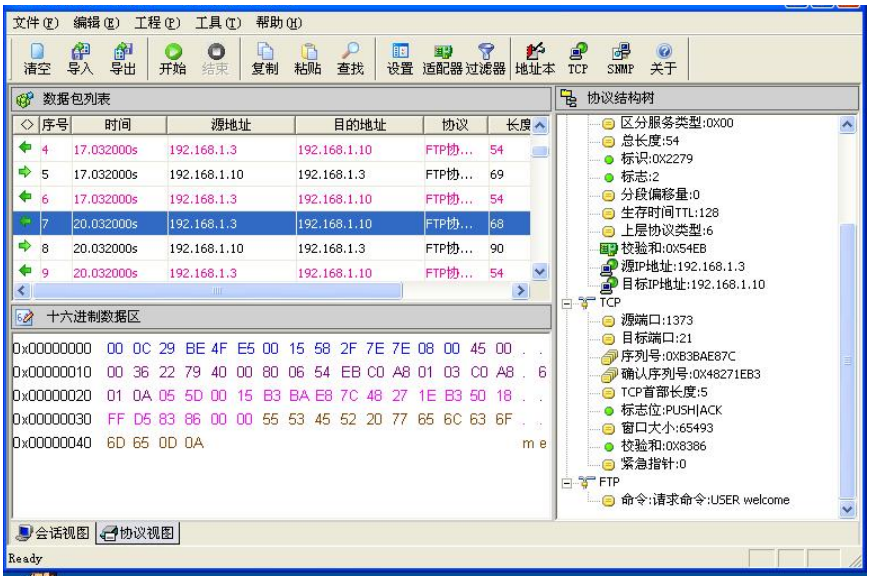

图 5- 17 FTP 报文中的 USER 命令

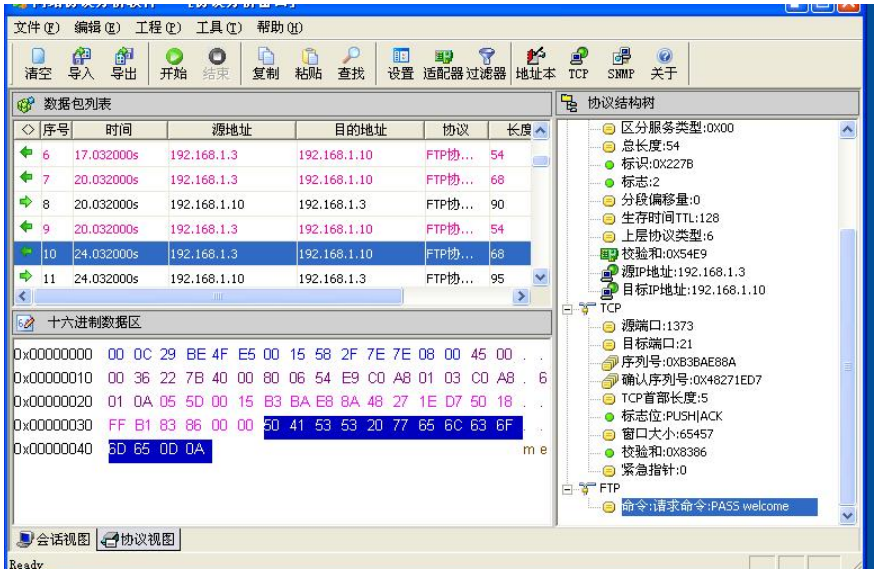

图 5- 18 FTP 报文中的 PASS 命令

5、记录这个过程中客户端和服务器端的 TCP 报头和数据信息，填写下表：

表 5-4 TCP 报头和数据信息列表

客户端	TCP 连接建立阶段（控制连接）	FTP 服务器
Port (　)	SYN=( ),ACK=( ),PSH=(),FIN=( )	Port (　)
	SYN= ( ),ACK=( ),PSH=( ),FIN=( )	
	SYN=( ),ACK=( ),PSH=( ),FIN=( )	

客户端	TCP 连接建立阶段（数据连接）	FTP 服务器
Port (　)	SYN=( ),ACK=( ),PSH=(),FIN=( )	Port (　)
	SYN= ( ),ACK=( ),PSH=( ),FIN=( )	
	SYN=( ),ACK=( ),PSH=( ),FIN=( )	

6、根据标志字段分析 FTP 的两个端口的连接建立、会话和断开连接的全部过程，分析该过程中的源、目的端口号。

7、这个 FTP 服务器工作在主动模式还是被动模式下？

8、是否可以捕获到用户名和密码？以此说明 FTP 连接的安全性。

步骤二：使用 TCP 连接工具连接 FTP 服务器

1、打开协议分析仪，准备好进行数据包的捕获，然后打开协议分析仪，点击工具栏中的“TCP”按钮，在弹出的“TCP 连接工具”中填写 FTP 服务器的 IP 地址（192.168.1.10）及 FTP 协议控制连接的端口号（21），点击“启动”，从而建立本机与 FTP 服务器 21 端口的 TCP 连接，如图 5- 19 所示：

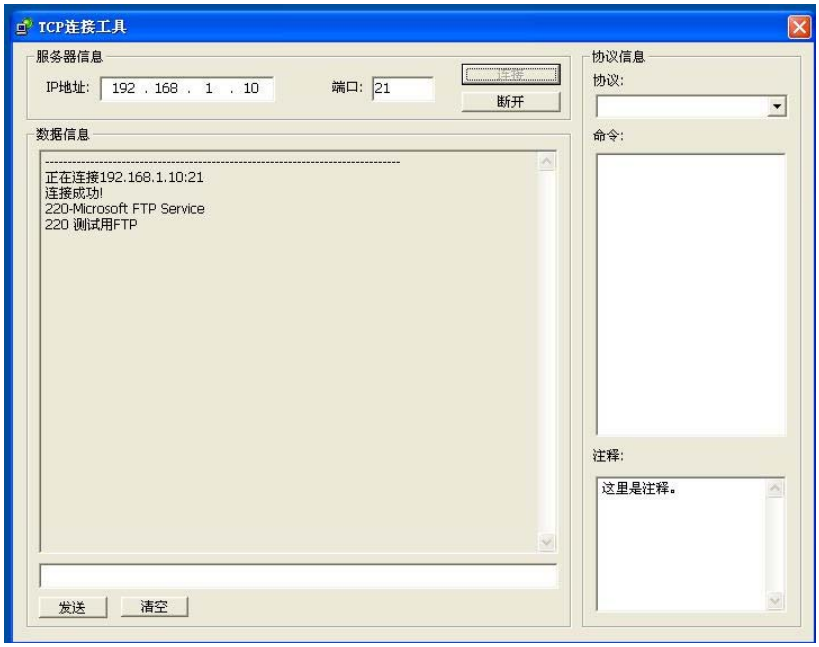

图 5- 19 使用 TCP 连接工具连接 FTP 服务器

在“数据信息”区域显示成功连接的信息：“220-Microsoft FTP Service”，并返回了 FTP 服务器的名称“测试用 FTP”。若不成功，再次尝试进行连接，直到成功。此时，在协议分析仪端，可以看到与 FTP 服务器建立控制连接的 TCP 三次握手过程：

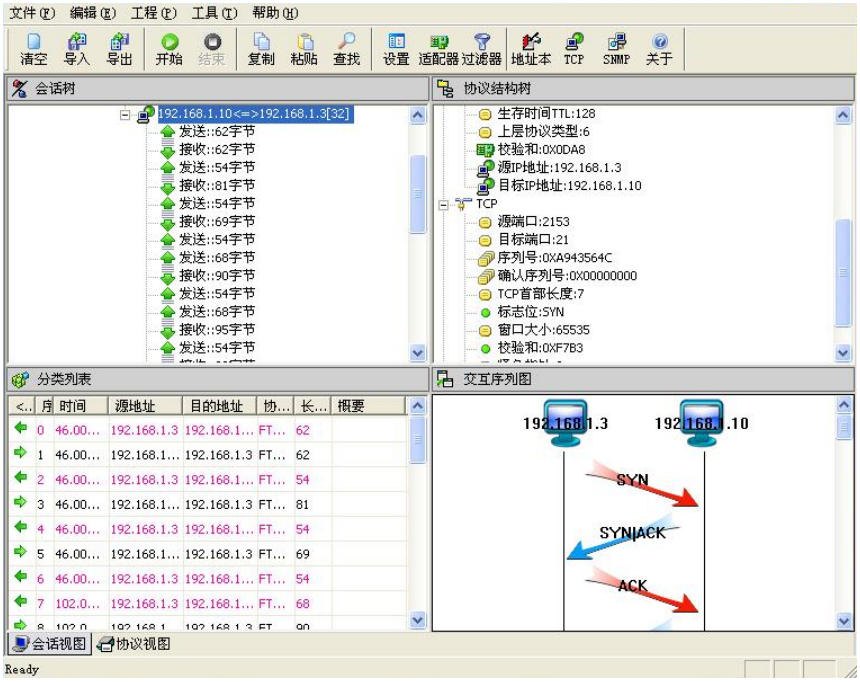

图 5- 20 是用 TCP 连接工具建立 FTP 控制连接

2、在发送区输入 FTP 命令，与 FTP 服务器进行交互：

（1）、在发送的编辑栏里面编辑发送 FTP 命令 USER，参数为 FTP 帐号：USER welcome，这时服务器返回响应“331 Password required for welcome”，提示输入密码；

（2）、发送命令 PASS welcome，输入 FTP 的账号密码，服务器返回“230 User welcome logged in.”，说明验证通过，已经进入 FTP 服务器，并回送了 FTP 服务器设置的欢迎词“欢迎使用，这是一个测试用的 FTP 服务器”；

（3）、发送命令“NOOP”，这是一个空操作，服务器返回“200 NOOP command successful”说明登录用户已经得到服务器的承认；

（4）、发送命令“HELP”，服务器返回相应的帮助信息，即所有命令的列表；

（5）、发送命令“STAT”，服务器返回信息为当前的 FTP 服务状态：

211-Microsoft FTP Service status:
Connected to vserver
Logged in as welcome
TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: STREAM
No data connection
211 End of status.

（6）、使用命令“QUIT”退出 FTP 服务。

下面是在协议分析仪的 TCP 工具“数据信息”区域显示的全部交互过程：

正在连接 192.168.1.10:21

```
连接成功!
220-Microsoft FTP Service
220  测试用 FTP
--------------------------------------------------------------------------------
发送 USER welcome
发送成功!
331 Password required for welcome.
--------------------------------------------------------------------------------
发送 PASS welcome
发送成功!
230-欢迎使用，这是一个测试用的 FTP 服务器
230 User welcome logged in.
--------------------------------------------------------------------------------
发送 NOOP
发送成功!
200 NOOP command successful.
--------------------------------------------------------------------------------
发送 HELP
发送成功!
214-The following   commands are recognized(* ==>'s unimplemented).
   ABOR
   ACCT
   ALLO
   APPE
   CDUP
   CWD
   DELE
   FEAT
   HELP
   LIST
   MDTM
   MKD
   MODE
   NLST
   NOOP
   OPTS
   PASS
   PASV
   PORT
   PWD
   QUIT
   REIN
   REST
   RETR
   RMD
```

RNFR
RNTO
SITE
SIZE
SMNT
STAT
STOR
STOU
STRU
SYST
TYPE
USER
XCUP
XCWD
XMKD
XPWD
XRMD
214 HELP command successful.

发送 STAT
发送成功!
211-Microsoft FTP Service status:
Connected to vserver
Logged in as welcome
TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: STREAM
No data connection
211 End of status.

发送 QUIT
发送成功!
221
连接结束

步骤三：编辑一个 FTP 报文

1、在主机上打开协议数据发生器，在工具栏上选择“添加”，会弹出“网络包模版”对话框，选择“FTP 协议模版”，建立一个 FTP 数据报文：

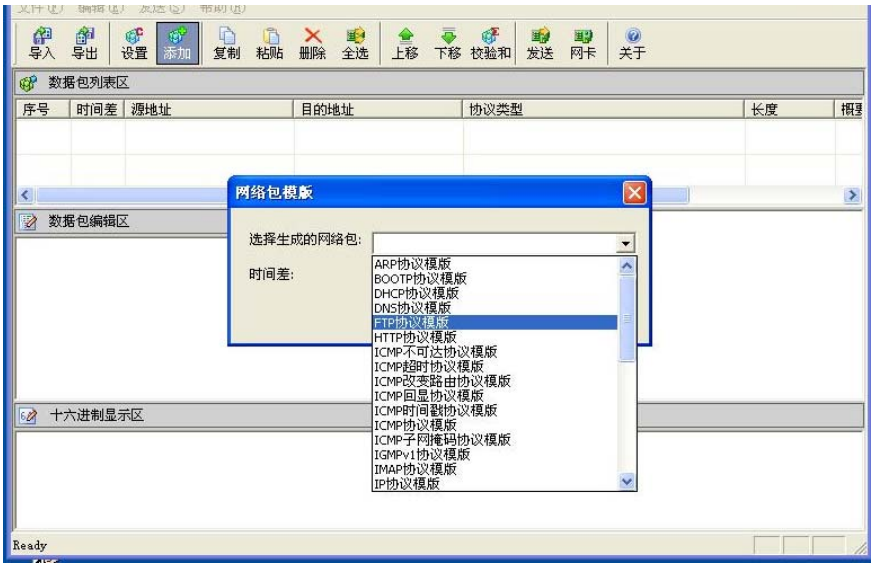

图 5- 21 建立 FTP 协议报文

2、填写其中以太网帧头、IP 首部、TCP 首部和 FTP 报文的内容：

- 填写以太网协议首部信息：
  - 目的物理地址：在地址本中选择 FTP 服务器的 IP 地址（192.168.1.10），确认后自动填入交换机的 MAC 地址：00-0C-29-BE-4F-E5；
  - 源物理地址：在地址本中选择实验主机（192.168.1.3），确认后自动填入主机 A 的 MAC 地址：00-15-58-2F-7E-7E；
  - 类型或长度：该字段应为 0800（即 IP 协议的类型值）。
- 填写 IP 协议头信息：
  - 总长度字段：包括 TCP 段内容的总长度，20 IP+20 TCP+12 FTP = 52；
  - 高层协议字段：即上层协议类型为 6（TCP 协议的类型为 6）；
  - 发送 IP 地址：在地址本中选择实验主机的 IP 地址，确认后自动填入主机的 IP 地址 192.168.1.3；
  - 目标 IP 地址：在地址本中选择 FTP 服务器的 IP 地址，确认后自动填入 FTP 服务器的 IP 地址 192.168.1.10；
  - 点击工具栏中的“校验和”按钮计算 IP 头校验和。
- 填写 TCP 协议的各个字段信息：
  - 16 位源端口号：任意大于 1024 的数；
  - 16 位目的端口号：21；
  - 32 位序号：选择一个序号（例如：19425898）；
  - 32 位确认序号：设置为 0；
  - 首部长度：首部长度设为 5，即长度为 20 字节；
  - 标志位：标志位设为 2，即标志位 SYN=1；
  - 窗口大小：任意，例如填入 32768；
  - 紧急指针：0；
  - 校验和：点击工具栏中的“校验和”按钮计算 TCP 校验和（覆盖 TCP 首部（包

含伪首部)和 TCP 数据两部分，计算方法同 UDP 协议一样）。

- 5、填写 FTP 协议报文的内容：
  可填入 FTP 的常用命令及参数，例如 USER welcome。

最终的编辑结果如图 5- 22 所示：

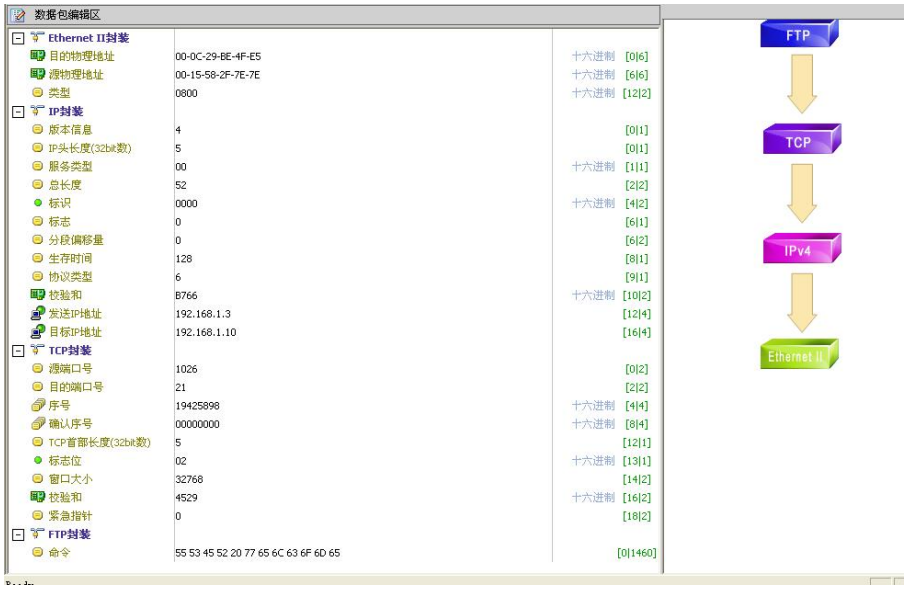

图 5- 22 编辑 FTP 报文的内容

3、点击工具栏上的“发送”按钮，将编辑好的 FTP 数据报文发送，可设置循环发送。

4、在实验主机上运行网络协议分析仪，捕获数据，捕获结果如所示，从中可以看到这是一个 FTP 报文，携带的命令是 USER welcome：

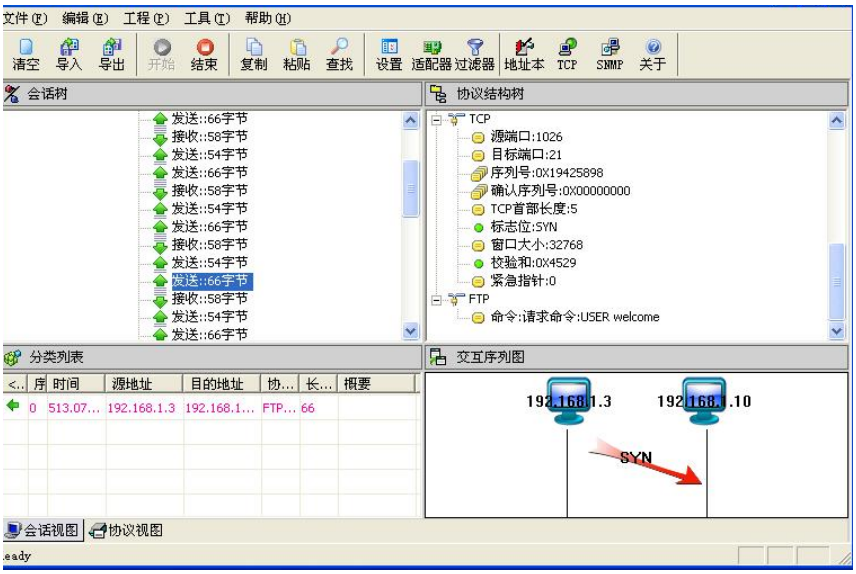

图 5- 23 捕获编辑的 FTP 报文

【思考问题】

1、在 ACTIVE 模式的 FTP 中，服务器端为何使用 20 和 21 两个端口，其作用分别是什么？客户端与这两个端口建立起的连接分别是谁（客户端还是服务器端）主动发起的？