# 暨南大学本科实验报告专用纸

课程名称 《计算机网络实验》 成绩评定

实验项目名称 FTP协议分析实验 指导教师 雷小林 、魏林锋

实验项目编号 实验项目类型 综合 实验地点 N117

学生姓名 陈宇 学号 2020101642

学院 信息科学技术学院 系 计算机系 专业 软件工程

实验时间 2022 年 11 月 22 日 下 午～ 11 月 22 日 下 午

# 1. FTP 协议简介协议简介

FTP 是文件传输协议（File Transfer Protocol）的简称。是一种 C/S 架构的应用层协议，用于客户端从远程的服务器下载、上传文件。FTP 协议与操作系统无关。

FTP 基于 TCP 协议，它通过两个 TCP 连接来传输一个文件，一个是控制连接，另一个是数据连接。相应的，在进行文件传输时，FTP 需要两个端口，分别用于控制连接端口（用于给服务器发送指令以及等待服务器响应）和数据传输端口（在客户机和服务器之间发送一 个文件或目录列表）

两种连接的建立都要经过一个“三次握手”的过程，同样，连接释放也要采用 “四次握手”方法。控制连接在整个回话期间一直保持打开状态。数据连接是临时建立的，在文件 传送结束后被关闭。

FTP 的连接模式有两种，PORT 和 PASV。PORT 模式是一个主动模式，PASV 是被动模式，这里都是相对于服务器而言的。

当 FTP 客户以 PORT 模式连接服务器时，它首先动态地选择一个端口号连接服务器的 21 端口，注意这个端口号一定是 1024 以上的，因为 1024 以前的端口都已经预先被定义好，被一些典型的服务使用或保留给以后会用到这些端口的资源服务。经过 TCP 的三次握手后，控制连接被建立。这时客户就可以利用这个连接向服务器发送指令和等待服务器响应了。当需要从（或向）服务器传送数据时，客户会发出 PORT 指令告诉服务器用自己的那个端口来建立一条数据连接（这个命令由控制连接发送给服务器），当服务器接到这一指令时，会使用20 端口连接客户指定的端口号，用以数据传送。

当 FTP 客户以 PASV 模式连接服务器时，控制连接的建立过程与 PORT 模式相同，不同的是，在数据传送时，客户不向服务器发送 PORT 指令而是发送 PASV 指令，服务器则将自己空闲可用的端口通过命令发送给客户端并监听该端口。客户端向服务器该端口发送同步请 求，经过 TCP 的三次握手后，数据连接被建立。这也就是 PASV 模式下数据连接建立的协商过程。

需要强调的是微软自带的 FTP 客户端命令，不支持 PASV 模式。

# 2.FTP 工作流程

FTP工作流程如下图所示，在该图中的客户端是希望从服务器端下载或上传文件的计算机。

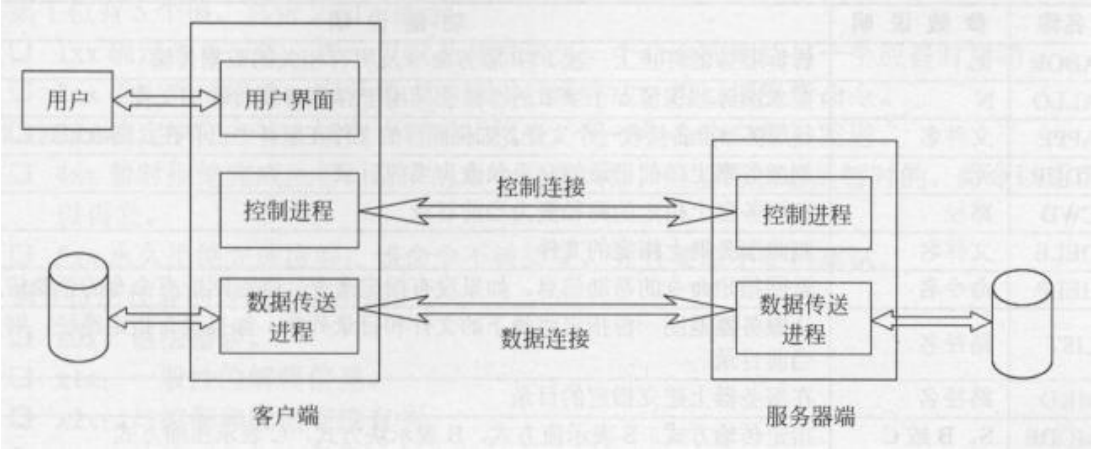
服务器端是提供 FTP 服务的计算机，它监听某一端口的 TCP 连接请求。控制连接和数据连接均是 TCP 连接，控制连接用于传送用户名、密码及设置传输方式等控制信息，数据连接用于传送文件数据。客户端和服务器端分别运行着控制进程和数据传送进程。

当用户需要从服务器下载文件时，可以通过用户界面让客户端的控制进程发起一个 TCP 连接请求。服务器端的控制进程接受了该请求后，建立了控制连接。于是，双方就可以相互传递控制信息了，但此时双方还不能传输文件数据。为传输数据，双方的数据传送进程还需要再建立一个数据连接。

当客户端向服务器端发出建立 TCP 控制连接请求时，使用的服务器端的端口号是 21（默认），同时要告诉服务器端一个空闲的端口号，用于以后建立数据传送连接。然后，服务器端用端口号 20（默认）与客户端所提供的端口建立数据传送连接，然后开始数据传送。

一般情况下，控制连接是一直存在的，但数据连接在一个文件传输完成后要断开。如果还需要传输另一个文件，要重新建立数据连接。这个特性使得 FTP 在传输大量的小文件时效率比较低，因为每一个文件传输时都需要建立和关闭 TCP 连接。这样会消耗一定的时间，不像有些协议（如Samba）可以在一个连接内把所有的文件一次性传输完毕。

FTP 的工作模式和其他网络通信协议有很大的区别。通常在采用 HTTP 等协议进行通信时，通信双方只用一个通信端口进行通信，即只有一个连接。而 FTP 使用两个独立的连接，其主要优点是使网络数据传输分工更加明确，同时在文件传输时还可以利用控制连接传送控制信息。




图． FTP 的工作流程

# 3．实验工具软件简介

（FTP 服务器端软件及搭建过程不在本实验范围内，可根据服务器操作系统类型选择合适的 FTP 服务器端软件）

（1） Serv-U 软件

Serv-U 是一种被广泛运用的 FTP 服务器端软件，支持 9x/ME/NT/2K 等全 Windows 系列。FTP 服务器用户通过它用 FTP 协议能在 internet 上共享文件。它设置简单，功能强大，性能稳定。此外，Serv-U 并不是简单地提供文件的下载，还为用户的系统安全提供了相当全面的保护。

本次实验中，我们使用 Serv-U FTP Server 6.2.0.1 汉化版软件作为 FTP 服务器。有关Serv-U 的系统配置请阅读软件的帮助文档。

（2） 微软 FTP 客户端命令

实验中，我们使用 Windows 自带的 FTP 命令和 IE 浏览器来作为 FTP 的客户端。下面简
单的介绍一下常用 FTP 客户端命令。

FTP 的命令格式：ftp [-v] [-d] [-i] [-n] [-g ] [-w:windowsize] [主机名/IP 地址]

其中：

-v 不显示远程服务器的所有响应信息；

-n 限制 ftp 的自动登录；

-i 在多个文件传输期间关闭交互提示

-d 允许调试、显示客户机和服务器之间传递的全部 ftp 命令；

-g 不允许使用文件名通配符；

-w：windowsize 忽略默认的 4096 传输缓冲区。

使用 FTP 命令登录成功远程 FTP 服务器后进入 FTP 子环境，在这个子环境下，用户可
以使用 FTP 的内部命令完成相应的文件传输操作。

FTP 常用内部命令如下：

* open host[port]：建立指定 ftp 服务器连接，可指定连接端口

*user user-name[password][account]：向远程主机表明身份，需要口令时必须输入。

*append local-file [remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。

* cd remote-dir：进入远程主机目录。

* cdup：进入远程主机目录的父目录。

* cd [dir]：将本地工作目录切换至 dir。

* dir [remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件。

* get remote-file[local-file]：将远程主机的文件 remote-file 传至本地硬盘的 local-file。

* ls [remote-dir][local-file] ： 显示远程目录 remote-dir， 并存入本地文件 local-file。

* put local-file [remote-file]：将本地文件 local-file 传送至远程主机。

* mput local-file：将多个文件传输至远程主机。

*nlist [remote-dir][local-file] ：显示远程主机目录的文件清单，存入本地硬盘 local-file。

* bye 或 quit：退出 ftp 会话过程。

3. 实验环境与说明

（1）实验目的

学习 Serv-U FTP Server 服务软件的基本配置和 FTP 客户端命令的使用，分析 FTP 报文格式和 FTP 协议的工作过程。

（2）实验设备和连接

实验设备和连接图如图 40 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为主机 A、主机 B，交换机命名为 Switch。

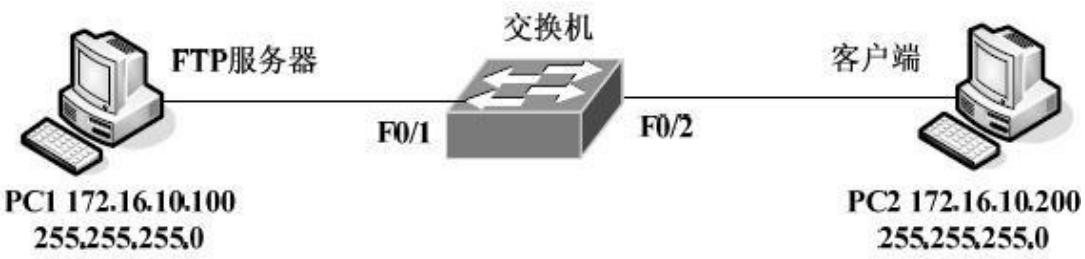



图 40 FTP 协议分析实验连接图

（3） 实验分组

本实验每台主机独立完成实验，现仅以主机 A 为例，其它主机的操作参考主机 A。

# 4.实验步骤

步骤 1：在主机 A 和主机 B 上运行 Wireshark，开始截获报文。

步骤 2：在主机 B 命令行窗口中登录 FTP 服务器，根据步骤 2 中的配置信息输入用户名和口令，参考命令如下：

```
C:\ >ftp
ftp> open
To 114.132.91.174                          //登录 ftp 服务器
Connected to 114.132.91.174.
220 （vsFTPd 3.0.3）
User(none):student                         //输入用户名
331 Please specify the password.
Password:student                           //输入用户密码
230 Login successful.                      //通过认证，登录成功
ftp> quit                                  //退出FTP
221 Goodbye.
```

步骤 3：停止截获报文，将截获的报文保存为 FTP-1-学号。

步骤 4：在主机 A 和主机 B 上再次运行 Wireshark，开始截获报文。

步骤 5：在主机 B 上打开浏览器窗口，地址栏输入 ftp:// 114.132.91.174；登陆对话框中输入用户名和密码，登陆 FTP 服务器；


图46 FTP 登陆对话框

步骤 6：在浏览器显示的用户目录下创建一个名为 ftp-学号的文件夹，并将本地的一个文本文件 f1.txt 粘贴到新建文件夹下，停止截获报文，将截获的报文保存为 FTP-2-学号。分析两次截获的报文，回答如下问题。

1）对 FTP-1-学号进行分析，找到 TCP 三次握手后第一个 FTP 报文，分析并填写表 1。

表1 FTP 报文格式分析

| | | | |
|---|---|---|---|
| 源IP 地址 | 175.178.242.159 | 源端口 | 21 |
| 目标 IP 地址 | 10.45.241.125 | 目标端口 | 9677 |
| FTP 字段 | 字段值 | 字段所表达的信息 | |
| Response Code | 220 | 服务器准备好接收一个新用户登陆 | |
| Response Arg | Welcome to Pure-FTPd [privsep] [TLS]<br>---------- | 返回信息，表示已经准备好 | |

2）在 FTP-1-学号中找出 FTP 指令传送和响应的报文，填写表 2；

表2 FTP 指令和响应过程分析

| 过程 | 指令/响应 | 报文号 | 报文信息 |
|---|---|---|---|
| | Request | 5 | User NaCl |

| | | | |
|---|---|---|---|
| User | Response | 6 | 331 User NaCl OK. Password required |
| Password | Request | 7 | PASS 123456 |
| | Response | 8 | 230 OK. Current directory is / |
| Quit | Request | 9 | QUIT |
| | Response | 10 | 221 GoodBye |

3）对第二次截获的报文进行综合分析，观察 FTP 协议的工作过程。特别观察两种连接
的建立过程和释放过程，以及这两种连接建立和释放的先后顺序，将结果填入表
3。

表 3 FTP 传送过程中的报文

| 文类型 | 所包括的报文序号 | 客户端口号 | 服务器端口 |
|---|---|---|---|
| 控制连接的建立 | 40，41，43 | 9531 | 21 |
| 数据连接的建立 | 44，46，47 | 9534 | 21 |
| FTP 数据传送 | 49 | 9534 | 21 |
| FTP 指令传送和响应 | 51，52 | 9534 | 21 |
| 数据连接的释放 | 109，113，116，119 | 9534 | 21 |
| 控制连接的释放 | 120，121，122，123 | 9531 | 21 |

4）第二次截获的报文中，FTP 客户是以 PORT 模式还是 PASV 模式连接服务器？你是如何判断的？

**答：以PASV模式连接服务器。服务端口为21。**

5）FTP 中的匿名帐户是 anonymous

PASV 模式双方协商数据连接端口时发送的命令是 PASV ？

文件下载用到的命令是 CWD ftp-2020101320 ？

6）FTP 数据连接服务器的端口一定是 20 吗？如果不一定，原因是什么？

**答：数据端口不一定是20，这和FTP的应用模式有关，如果是主动模式，应该为20，如果为被动模式，由服务器端和客户端协商而定**

7）简述 PORT 和 PASV 两种模式的优缺点

**答：主动FTP对FTP服务器的管理有利，但对客户端的管理不利。因为FTP服务器企图与客户端的高位随机端口建立连接，而这个端口很有可能被客户端的防火墙阻塞掉。**

**被动FTP对FTP客户端的管理有利，但对服务器端的管理不利。因为客户端要与服务器端建立两个连接，其中一个连到一个高位随机端口，而这个端口很有可能被服务器端的防火墙阻塞掉。**