FTP服务器的工作模式及流程

FTP协议
FTP(File transfer Protocol)是一种在互联网中进行文件传输的协议，基于客户端/服务器模式，默认使用20、21号端口，
其中端口20（数据端口）用于进行数据传输，端口21（命令端口）用于接受客户端发出的相关FTP命令与参数。
FTP服务器一般部署于内网中，具有容易搭建、方便管理的特点。而且有些FTP客户端工具还可以支持文件的多点下载以及断点续传技术，因此FTP服务得到了广大用户的青睐。

Ftp有两种工作模式：
主动模式(PORT)：服务器主动向客户端发起连接请求.
被动模式(PAVS)：FTP服务器等待客户端发起连接请求（FTP的默认工作模式）.

Ftp协议需要用到两个TCP连接：
命令连接：用来在FTP客户端与服务器之间传递命令。
数据连接：用来在服务器和客户端进行文件传输。

无论是主动模式还是被动模式，其要进行文件传输都必须依次建立两个连接，分别为命令连接与数据连接。而主动模式与被动模式的差异主要体现在数据连接通道上。

命令连接:

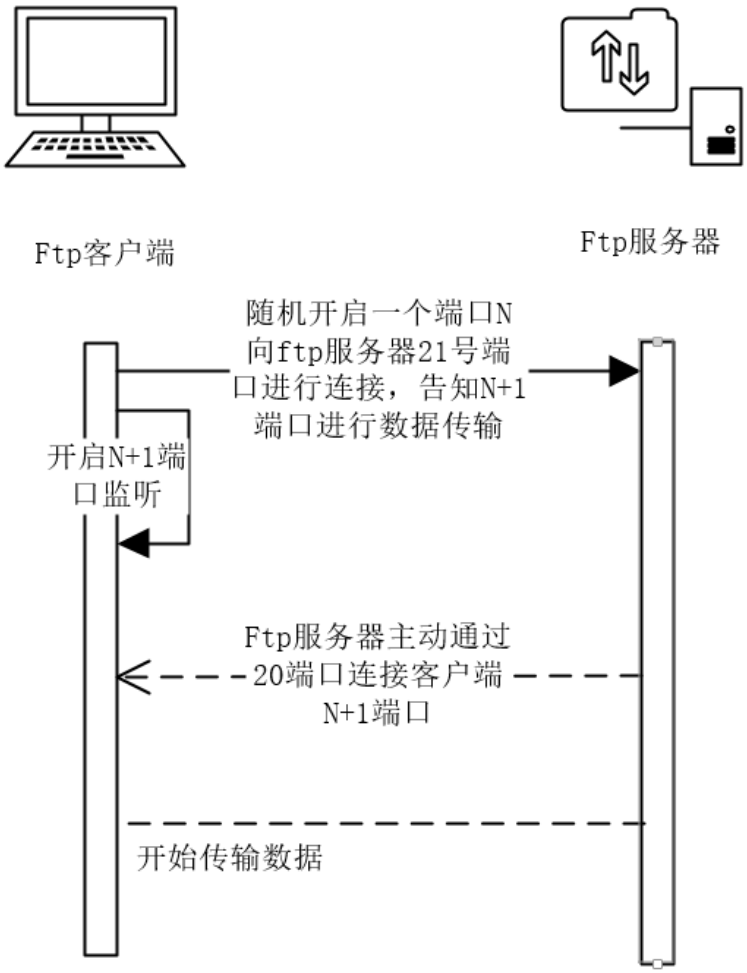
当FTP客户端需要登陆到FTP服务器上的时候，服务器与客户端需要进行一系列的身份验证过程，这个过程就叫做命令连接。
如在客户端向服务器发起连接请求的时候，客户端会随即的选择某个TCP端口来跟FTP服务器的21号端口进行连接，这主要是通过TCP三方握手来实现的。当三方握手完成之后，客户端与 服务器之间便建立了命令连接通道。不过这个通道的用途是非常有限的，其主要用来传输FTP的相关指令。如查看文件列表、删除文件等等，而不能够用来在客户 端与服务端进行文件传输

数据连接:

在命令连接通道建立以后，如果想要在ftp服务器和客户端之间传输文件，则需要建立数据连接通道。

根据建立数据连接是由谁发起的可以分为主动模式（PORT）和被动模式（PAVS）

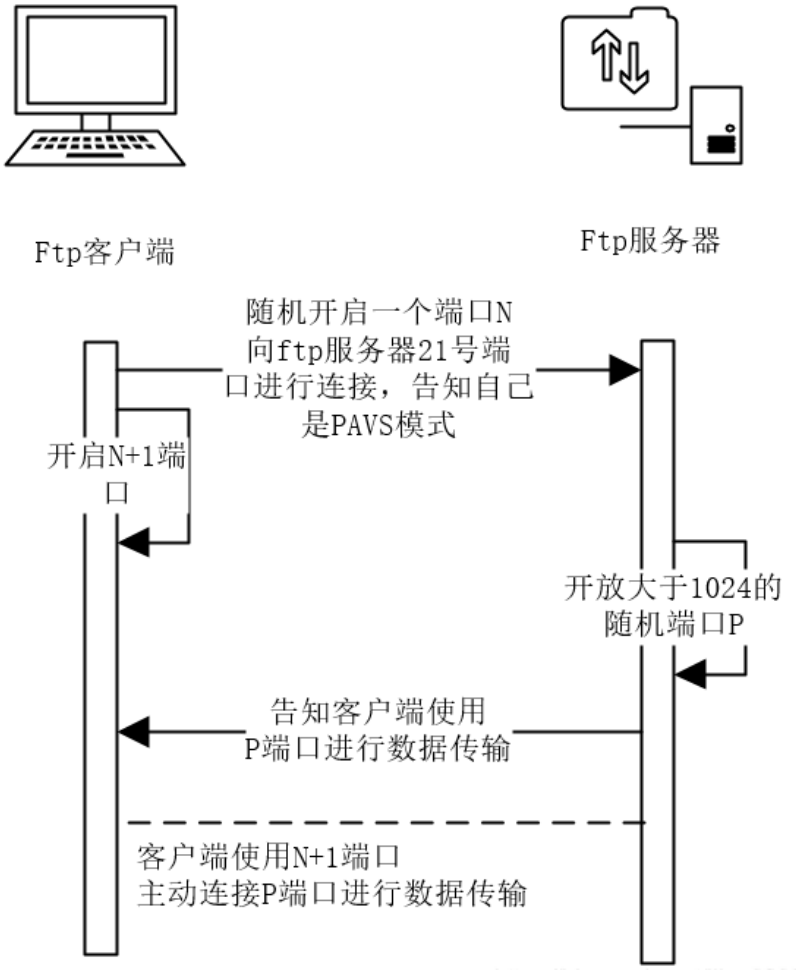
主动模式:



主动模式优点：

服务端配置简单，利于服务器安全管理，服务器只需要开放21端口
缺点：
如果客户端开启了防火墙，或客户端处于内网（NAT网关之后），那么服务器对客户端端口发起的连接可能会失败

被动模式：



被动模式通常用在处于防火墙之后的FTP客户访问外界FTp服务器的情况，因为在这种情况下，防火墙通常配置为不允许外界访问防火墙之后主机，而只允许由防火墙之后的Ftp客户端发起的连接请求通过。因此，在这种情况下不能使用主动模式的FTP传输，而被动模式的FTP可以良好的工作。
优点：
对客户端网络环境没有要求
缺点：
服务器配置管理稍显复杂，不利于安全，服务器需要开放随机高位端口以便客户端可以连接，因此大多数FTP服务软件都可以手动配置被动端口的范围

简单地说，支持FTP协议的服务器就是FTP服务器。

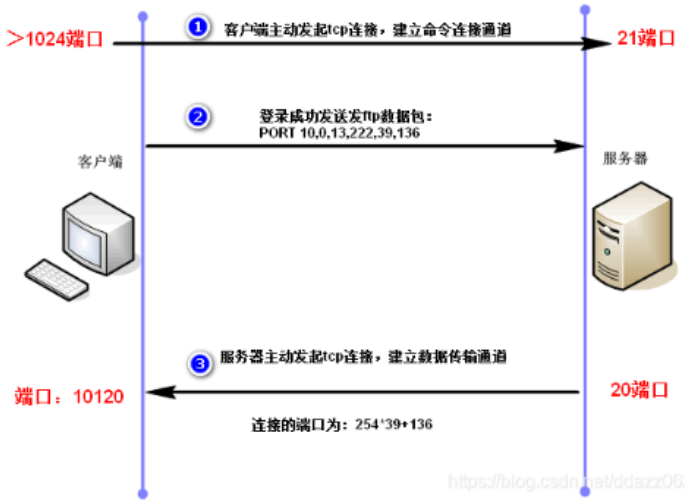
与大多数Internet服务一样，FTP也是一个C/S模式系统。用户通过一个支持FTP协议的客户机程序，连接到在远程主机上的FTP服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户所发出的命令，并将执行的结果返回到客户机。比如说，用户发出一条命令，要求服务器向用户传送某一个文件的一份拷贝，服务器会响应这条命令，将指定文件送至用户的机器上。客户机程序代表用户接收到这个文件，将其存放在用户目录中。

FTP协议是基于TCP协议之上的应用层协议，支持两种模式：Standard (PORT方式，主动方式)，Passive (PASV，被动方式)。

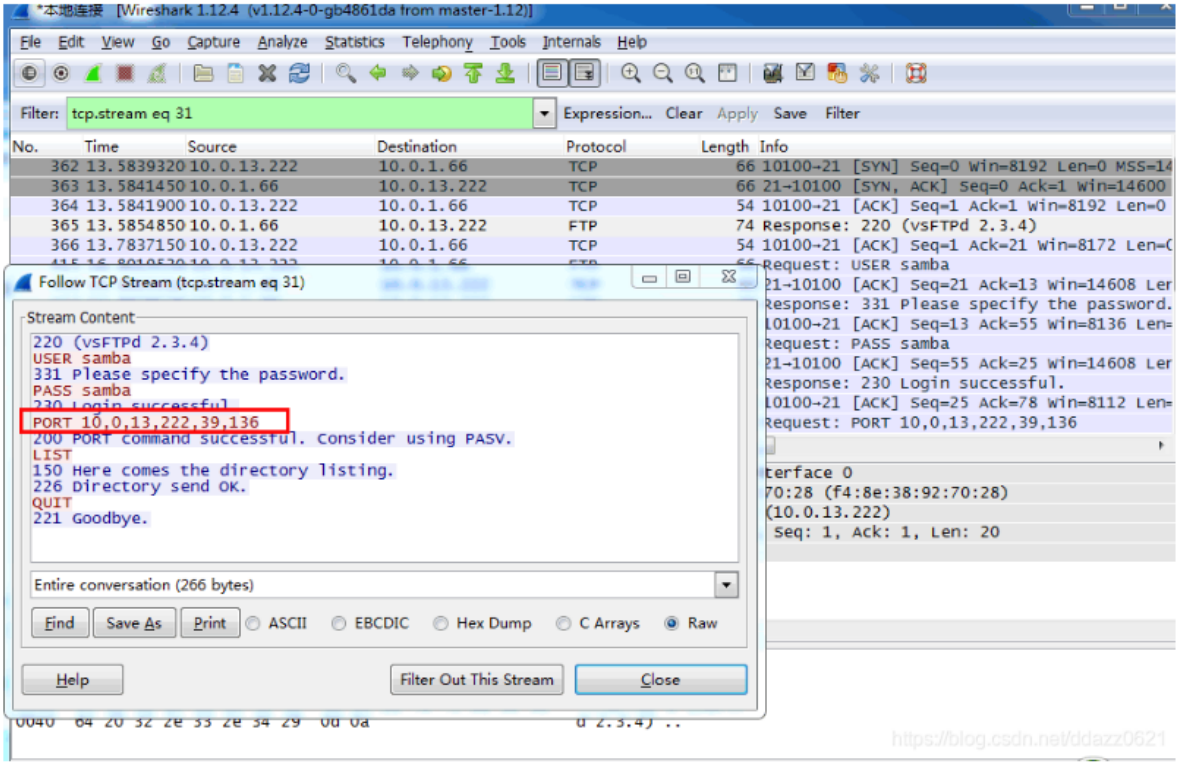
Port模式

FTP 客户端首先和服务器的TCP 21端口建立连接，用来发送命令，客户端需要接收数据的时候在这个通道上发送PORT命令。PORT命令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的TCP 20端口连接至客户端的指定端口发送数据。FTP server必须和客户端建立一个新的连接用来传送数据。

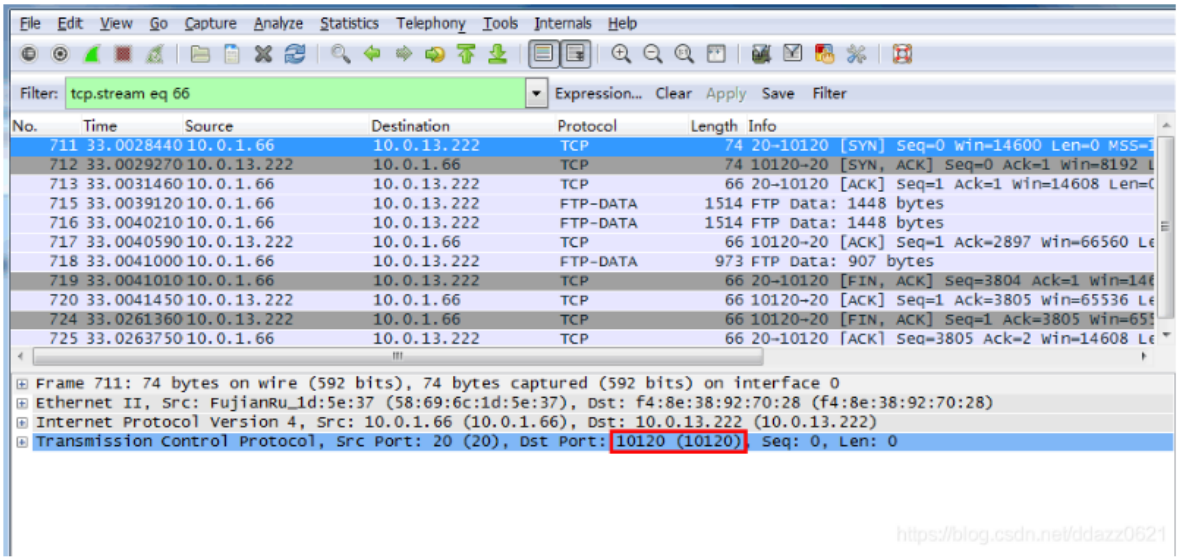
具体步骤详情如下（笔者所用FTP服务器地址：10.0.1.66，客户端地址：10.0.13.222）：



客户端主动发起TCP连接，连接服务器的21端口，建立用于传输命令的通道。
客户端通过第一步建立的命令传输通道发送FTP数据包（含PORT信息）。
服务器通过解析客户端发来的数据包计算所要连接客户端端口，用本地的20端口主动去与计算出的端口建立数据通道的TCP连接。
实验截图如下：



抓包可以看到，FTP客户端（IP：10.0.13.222，端口：10100）与FTP服务器（IP：10.0.1.66，端口：21）建立三次连接。然后登陆成功（230 login successful）后FTP客户端发送 "PORT 10,0,13,222,39,136"。

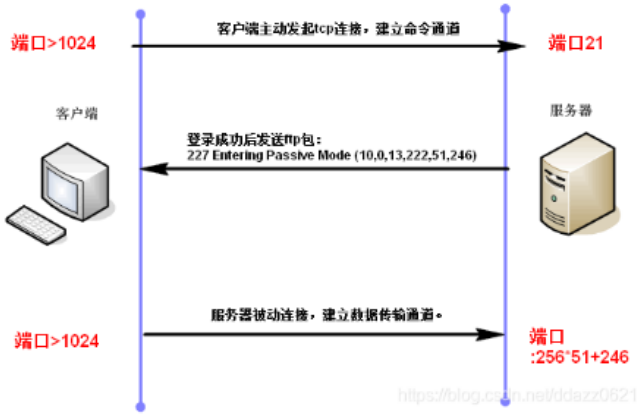


接着可以看到服务器主动去发起TCP连接，该连接用于FTP数据传输的通道，协议包名为FTP-DATA。可以发现服务器用20端口去连接客户端的10120端口，10120其实就是客户端发送的"PORT 10,0,13,222,39,136"中根据后俩个数值得到的：*连接端口（10120）= 256 * 倒数第二位（39）+ 倒数第一位（136）*

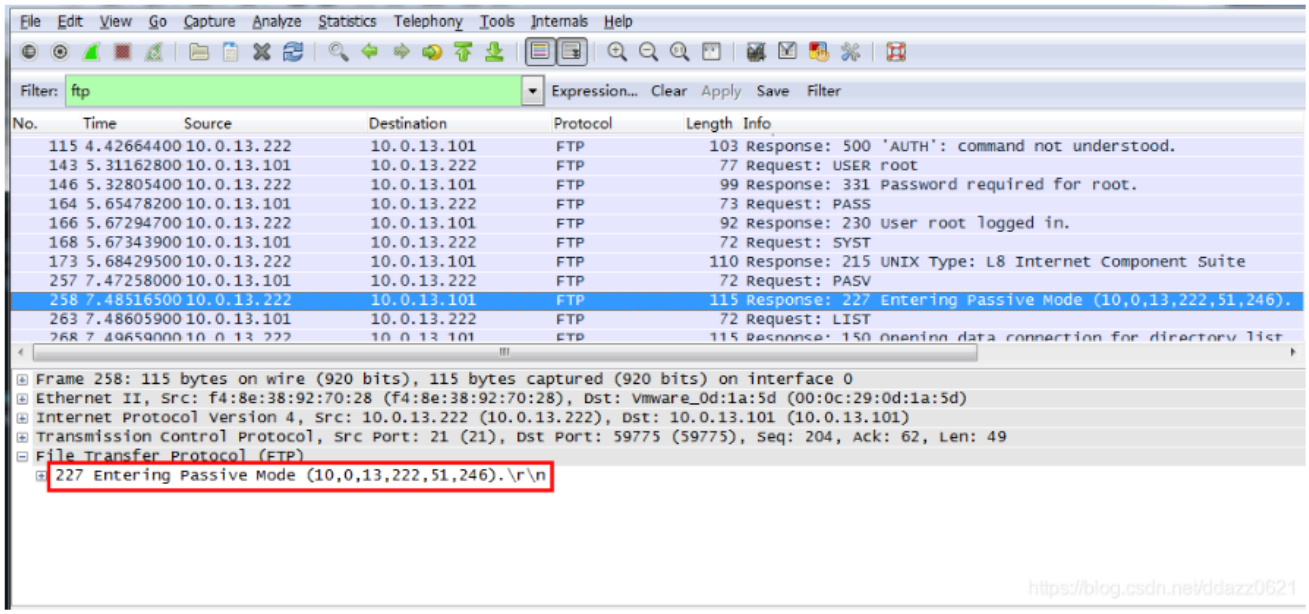
Passive模式

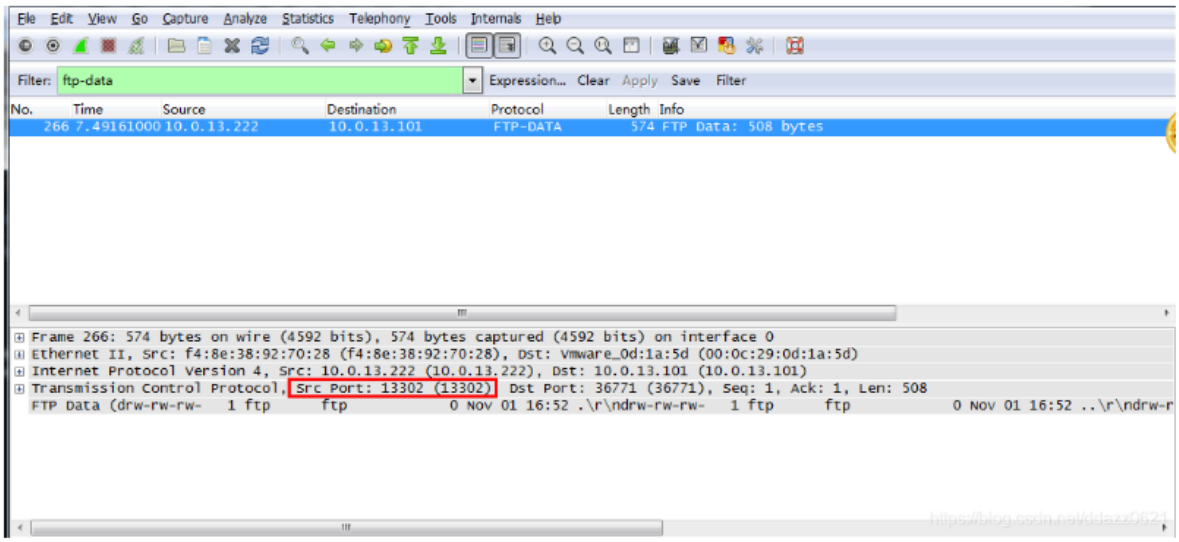
建立控制通道和Standard模式类似，但建立连接后发送Pasv命令。服务器收到Pasv命令后，打开一个临时端口（端口号大于1023小于65535）并且通知客户端在这个端口上传送数据的请求，客户端连接FTP服务器此端口，然后FTP服务器将通过这个端口传送数据。

具体步骤详情如下（笔者所用FTP服务器地址：10.0.13.222，客户端地址：10.0.13.111）：



客户端主动发起TCP连接，连接服务器的21端口，建立用于传输命令的通道。
服务器通过第一步建立的命令传输通道发送FTP数据包（含PASS信息）。
客户端通过解析服务器发来的数据包计算所要连接服务器端口，主动去与计算出的端口建立数据通道的TCP连接，对于服务器来说此次连接是被连接。
实验截图如下：





主动和被动模式计算端口的方法都是相同的。