

Ftp 协议分析实验 实验体会

21307289 刘森元

本次试验我完成的是第一部分，实验中涉及到了FTP客户端的数据传输过程和TCP连接的建立与关闭过程。以下是我的实验心得：

1. 在FTP客户端的mac地址问题中，通过查看Wireshark抓包数据中的源地址，可以获取到FTP客户端的mac地址。
2. 通过分析第1、2、3号报文，可以了解到TCP连接的三次握手过程，其中客户端发送SYN报文请求连接，服务器回复SYN-ACK报文确认连接，最后客户端发送ACK报文确认连接建立。
3. 通过过滤器规则和追踪流功能，我们可以分析出FTP的命令连接和数据连接。命令连接是持续连接，用于传输FTP的命令和控制信息；而数据连接是非持续连接，仅在需要传输文件等数据时才建立。
4. FTP的连接模式是主动模式，客户端向服务器发送IP地址和端口号，服务器主动连接客户端进行数据传输。
5. 最后四个报文是TCP连接的四次挥手过程，用于关闭连接。主动关闭方发送FIN报文表示请求关闭连接，被动关闭方发送ACK报文进行确认，然后被动关闭方也发送FIN报文请求关闭，最后主动关闭方发送ACK报文进行确认。
6. 实验中还涉及到FTP的命令和应答，通过分析FTP报文中的命令和响应类型，可以了解到不同的FTP操作，例如登录、上传、下载、重命名等。

通过这次实验，我对FTP的工作原理和TCP连接的建立与关闭过程有了更深入的了解。我也学会了使用Wireshark等抓包工具来分析网络数据流，并从中获取有用的信息。这对于网络故障排查和网络性能优化都是非常有帮助的。