



警示

1. 实验心得体会如有雷同，雷同各方当次实验心得体会成绩均以 0 分计。
2. 在规定时间内未上交实验报告的，不得以其他方式补交，当次心得体会成绩按 0 分计。
3. 报告文件以 PDF 文件格式提交。

本报告主要描述学生在实验中承担的工作、遇到的困难以及解决的方法、体会与总结等。

院系	计算机学院	班 级	计科一班
学号	22336057	实验名称:	ftp 协议分析实验
学生	丁晓琪		

一. 本人承担的工作

- 实现实验设备的物理拓扑连接
- 完成在浏览器和文件管理器上登录 FTP 和分析其报文
- 帮助组员完成 FTP 登录和 FTP 上下载文件的报文收集

二. 遇到的困难及解决方法

- 问题：交换机上插口众多，不知道如何连接也不知道如何判断是否连接正确

解决：查找交换机的使用手册，学习插口对应信息和提示灯信息

10/100/1000Base-T 以太网端口指示灯	1-48	指示灯灭	端口未 Link
		绿色常亮	端口 1000M Link Up
		绿色闪烁	端口 1000M 数据收发
		黄灯常亮	端口 100/10M Link Up
		黄灯闪烁	端口 100/10M 数据收发



- | | |
|------------------|---------------------|
| 1. 状态指示灯 | 7. 端口状态指示灯 |
| 2. 电源状态指示灯(PWR1) | 8. USB 接口 |
| 3. 电源状态指示灯(PWR2) | 9. MiniUSB 接口 |
| 4. MGMT 接口状态指示灯 | 10. 管理用以太网接口 (MGMT) |
| 5. Console 口 | 11. 万兆 SFP Plus 接口 |



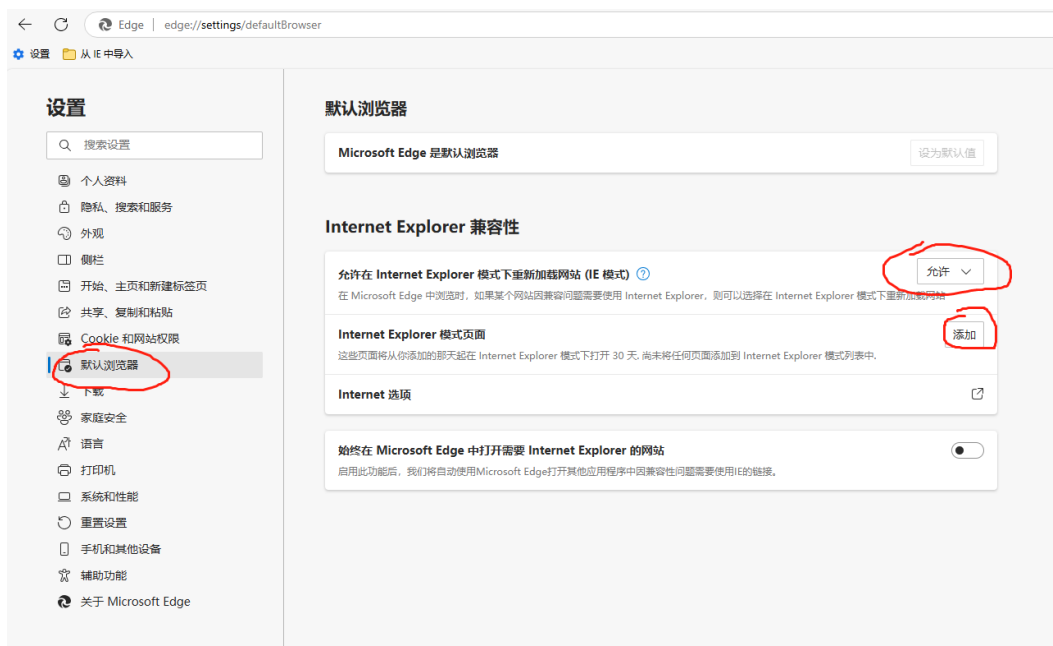
- 问题：不知道如何配置哪个网络连接：

解决：首先在网络资料上找到了电脑上设置两台机器的局域网的页面（并且还和组员尝试终端命令行设置）

然后又遇到了两台机器上空闲的网络连接名字不一致的问题，我们认为需要两个连接名字相同才能设置成功。经过向老师求问，我们了解到这个只是网络适配器的自定义名字，它们的性质是一样的和名字无关

- 问题：在浏览器上登录 ftp 服务器时，发现无法登录

解决：只有 edge 浏览器支持 ftp，而且需要更改配置



服务器端也要做出相应的更改设置：



Settings for server 127.0.0.1:14148

Select a page:	Server listeners			
Server listeners	Address	Port	Protocol	Add
Protocols settings	0.0.0.0	21	Explicit FTP over TLS and insecure plain FTP	Remove
FTP and FTP over TLS (FTPS)	::	21	Explicit FTP over TLS and insecure plain FTP	
Rights management				
Groups				
Users				
Administration				
Logging				
Let's Encrypt®				
PKCS#11				
Updates				

- 问题：在分析浏览器报文时发现数据控制连接端口不是 20:

解决：经过查询资料发现 FTP 只有主动连接时，数据控制连接端口才默认为 20。

FTP 还有被动模式，客户端向服务器请求开启被动模式，服务器返回数据连接指定端口。且数据控制连接是随开随关。已经在浏览器登录 FTP 报文中捕捉到了数据控制连接的打开，传输和断开

- 在观察 filezilla 中 FTP 登录报文中发现没有捕捉到账号密码的明文

解决：在和组员的讨论和查询资料中发现 filezilla 是用 TLS 加密传输，使用了安全认证，无法抓到明文

三. 体会与总结

体会：从一开始对物理连接到一头雾水到分析报文时的状况百出，在这个过程中我逐渐熟悉了 TCP 连接的三次握手和断开的四次挥手，也对 FTP 的控制连接和数据连接有了更深的了解，掌握了 FTP 报文的格式，同时对通过交换机在两台设备中建立局域网有了新的认识。

总结：



FTP主要功能:	<ul style="list-style-type: none">减少或消除在不同操作系统下处理文件的不兼容性文件的下载, 文件的上传 (HTTP仅支持文件的下载)
工作模式	<p>客户/服务器工作模式</p>  <pre>sequenceDiagram participant Client as FTP 客户机 participant Server as FTP 服务器 Note over Client, Server: ①FTP 连接请求 Client->>Server: ①FTP 连接请求 Note over Client, Server: ②FTP 连接回应 Server-->>Client: ②FTP 连接回应 Note over Client, Server: ③文件请求 Client->>Server: ③文件请求 Note over Client, Server: ④文件上传或下载 Client->>Server: ④文件上传或下载 Note over Client, Server: ⑤关闭连接 Client->>Server: ⑤关闭连接</pre>
FTP访问方式	<ul style="list-style-type: none">普通FTP: 登陆时提供正确的用户名匿名FTP: 直接访问 (安全起见, 只能下载, 不能上传)
双重连接	<ul style="list-style-type: none">控制连接, 传输FTP命令数据连接, 传输FTP数据(主动模式端口为20, 被动模式端口由服务器指定)请求格式: 命令+参数响应格式: 状态码+参数  <pre>graph LR subgraph Client [客户端] UI[用户界面] CP1[控制进程] DP1[数据传送进程] end subgraph Server [服务器端] CP2[控制进程] DP2[数据传送进程] end Internet((Internet)) CP1 -- "控制连接21" --> CP2 CP1 -- "数据连接20" --> DP2 DP1 <--> DP2</pre>

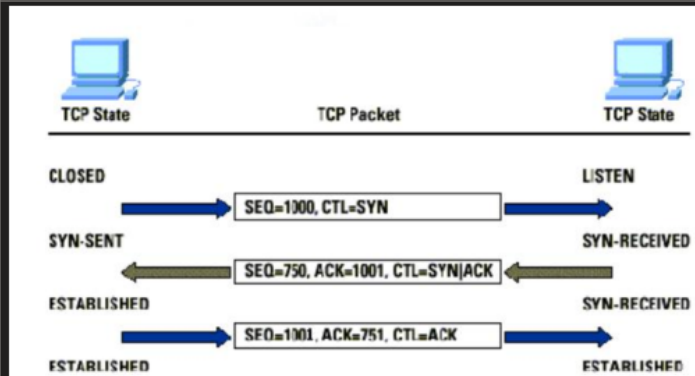


TCP数据报格式

源端口（16 位）								目的端口（16 位）							
顺序号（32 位）															
确认号（32 位）															
TCP 头长 （4 位）		保留位 （6 位）	U R G	A C K	P S H	R S T	S Y N	F I N	窗口大小（16 位）						
校验和（16 位）								紧急指针（16 位）							
可选项（0 或更多的 32 位字）															
数据（可选项）															

ACK确认标志, RST复位标志, URG紧急标志, SYN建立连接标志, PSH推标志, FIN结束标志

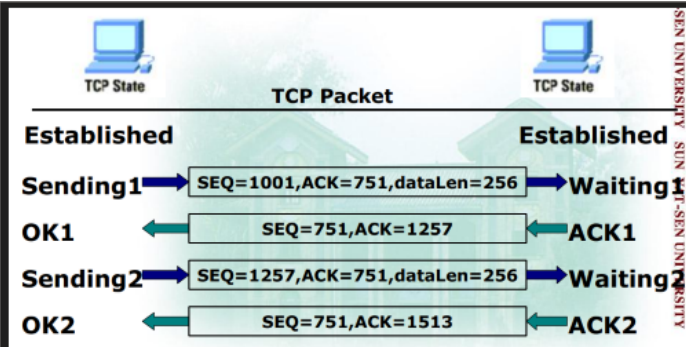
TCP连接建立过程



1. 客户端发送 $SEQ=1000$ (也就是该报文在客户端服务器的序号), $CTL=SYN$ (控制标志为建立连接同步序列号)
2. 服务器收到SYN报文, 回应确认报文ACK, ACK确认好为客户端STN报文的序列号加1 (1001), 同时包含自己的叙事序列号 (750), 控制型号CTL为确认ACK和连接请求SYN
3. 客户端收到SYN报文, 发送ACK报文 (ACK为对方序列号+1, 751), CTL为确认ACK

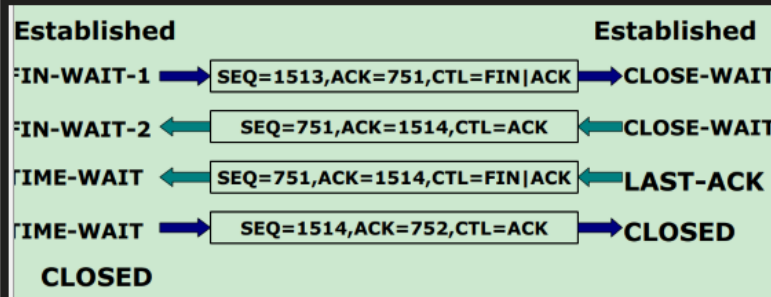


TCP数据传输过程



1. 发送方发送第一个TCP数据包, SEQ=1001 (序列号为1001), ACK=751 (希望对方收到后返回的数据包的序列号为751 (表示它已经接到序列号750以及以前的数据包)), datalen=256数据包数据量为256
2. OK1: 接收方收到了数据包, 发送确认报文SEQ=751, ACK=1257 (确认发送方接收到了确认报文)
3. 下面两个过程一样

TCP连接断开过程



1. 发送方关闭连接: SEQ=1513当前序列号为1513, ACK=751发送方期望从接收方接收到的下一个数据包序列号751, 控制位为想要关闭连接FIN, 和确认收到的数据包 (上面数据传输过程)
2. 接收方回复确认报文, 接收方还能发数据给发送方, 但是发送方不会再发送数据了, 确认号为包1的SEQ+1
3. TIME-WAIT维持一段时间, 确保发送的报文被接受
4. 接收方关闭连接, 和1一样
5. 发送方恢复接收报文

【交报告】

上传报告: 助教

说明: 上传文件名: 小组号_学号_姓名_XX 实验.pdf