计算机网络实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

专业	软件工程	班 级	19 级软件工程	组长	冼子婷
学号	18338072	18346019	18322043		
学生	冼子婷	胡文浩	廖雨轩		
实验分工					
冼子婷	进行实验，截图，编写和分析实验报告	廖雨轩	进行实验，截图，编写和分析实验报告		
胡文浩	进行实验，截图，编写和分析实验报告				

【实验题目】访问控制列表（ACL）实验。

【实验目的】

1. 掌握标准访问列表规则及配置。
2. 掌握扩展访问列表规则及配置。
3. 了解标准访问列表和扩展访问列表的区别。

【实验内容】

完成教材实例 8-4（P296），请写出步骤 1 安装与建立 FTP、WEB 的步骤，并完成 P297～P298 的测试要求。

【实验要求】

重要信息需给出截图， 注意实验步骤的前后对比。

【实验记录】(如有实验拓扑请自行画出)

【实验拓扑】

某公司的网络中使用 1 台路由器提供子网间的互连。子网 192.168.1.0/24 为公司员工主机所在的网段，其中公司经理的主机地址为 192.168.1.254/24；子网 10.1.1.0/24 为公司服务器网段，其中有 2 台服务器、1 台 WWW 服务器（10.1.1.100/24）和 1 台 FTP 服务器（10.1.1.200/24）。现在要实现基于时间段的访问控制，使公司员工只有在正常上班时间（周一至周五 9:00-18:00）可以访问 FTP 服务器，并且只有在下班时间才能访问 WWW 服务器，而经理的主机可以在任何时间访问这 2 台服务器。

本实验的拓扑结构如下图所示：

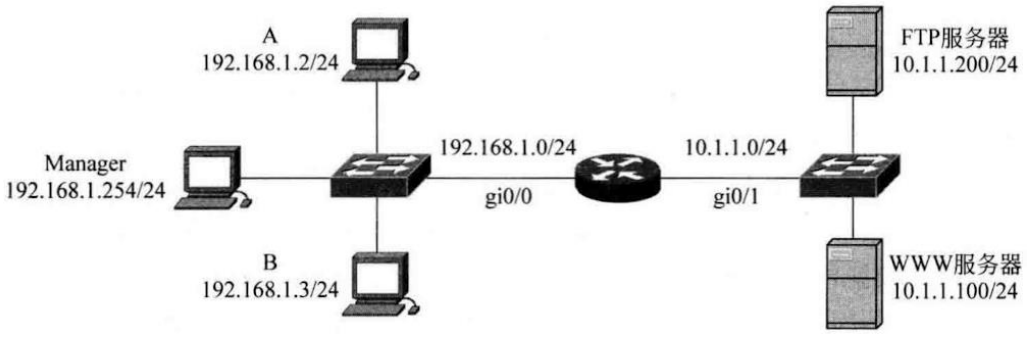


图 8-8 基于时间 ACL 的实验拓扑

【实验设备】

路由器 1 台，计算机 5 台（其中 2 台作为 WWW 服务器和 FTP 服务器）

步骤 1：

（1）配置 3 台计算机（A、B 和 Manager）的 IP 地址、子网掩码、网关。

按照拓扑图配置 A 的 IP 地址、子网掩码和网关如下：

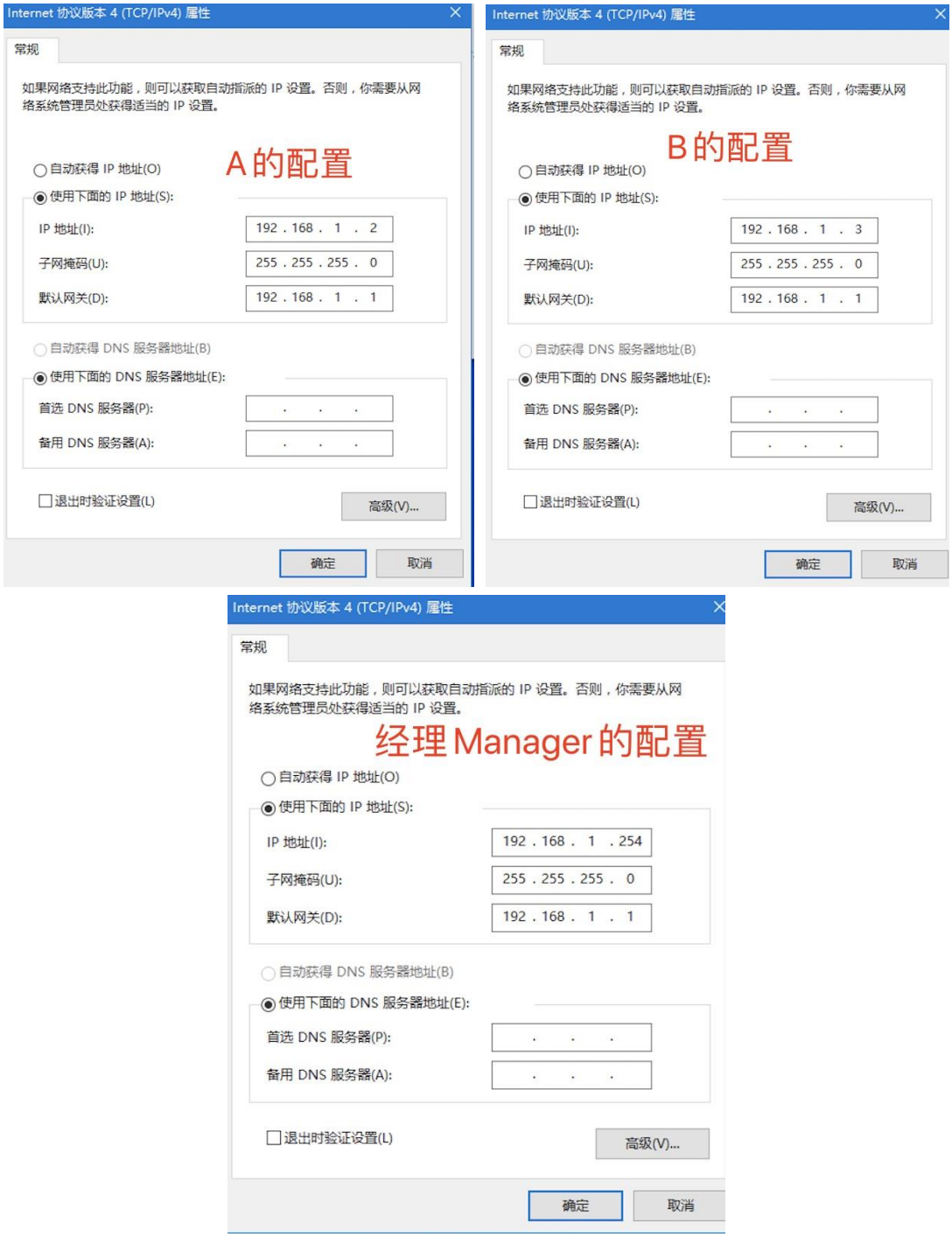


图 1：A、B 和 Manager 的 IP 地址、子网掩码、网关配置图

（2）检查计算机与服务器的连通性。

首先设置服务器的 IP 地址（注意：需要禁用校园网使用局域网）：

图 2：FTP 和 WWW 服务器的 IP 地址、子网掩码、网关配置图

此时，分别 ping WWW 服务器的 IP 地址以及 FTP 服务器的 IP 地址可知，与 WWW 服务器连通性差，与 FTP 服务器连通性好？？？

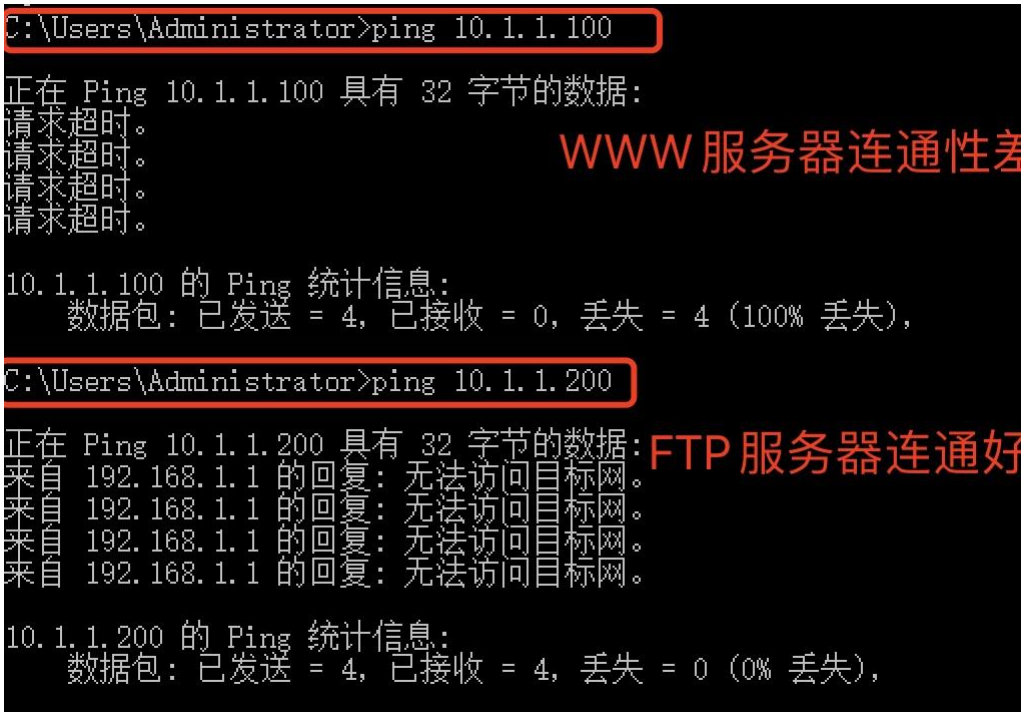


图 3：检查计算机与服务器的连通性

（3）在服务器上安装 FTP 服务器和 WWW 服务器。FTP 服务器至少创建一个用户名和口令。

FTP 服务器的安装与设置：

1）安装 FTP 服务器：

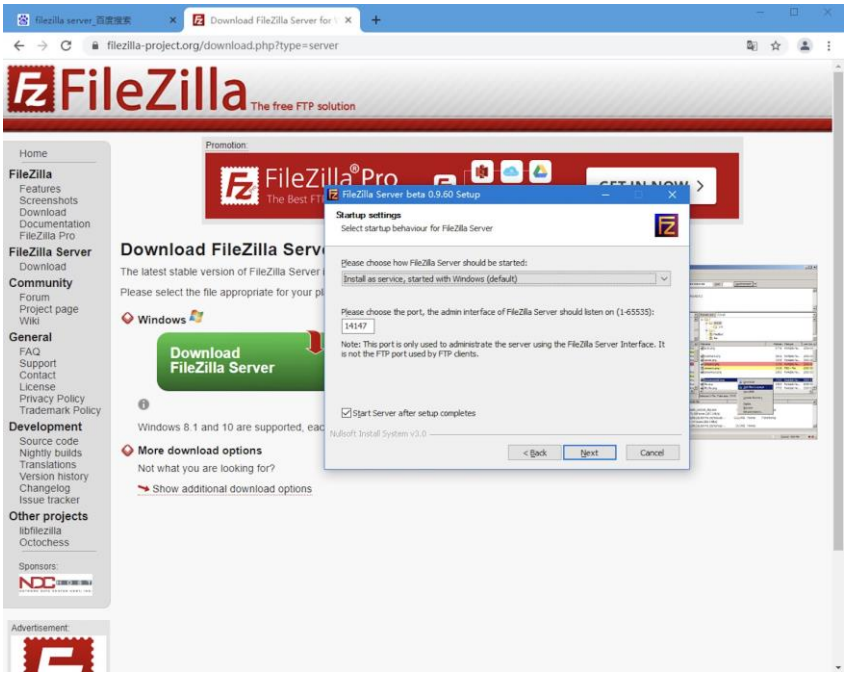


图 4：安装 FTP 服务器

2）打开 FTP 服务器

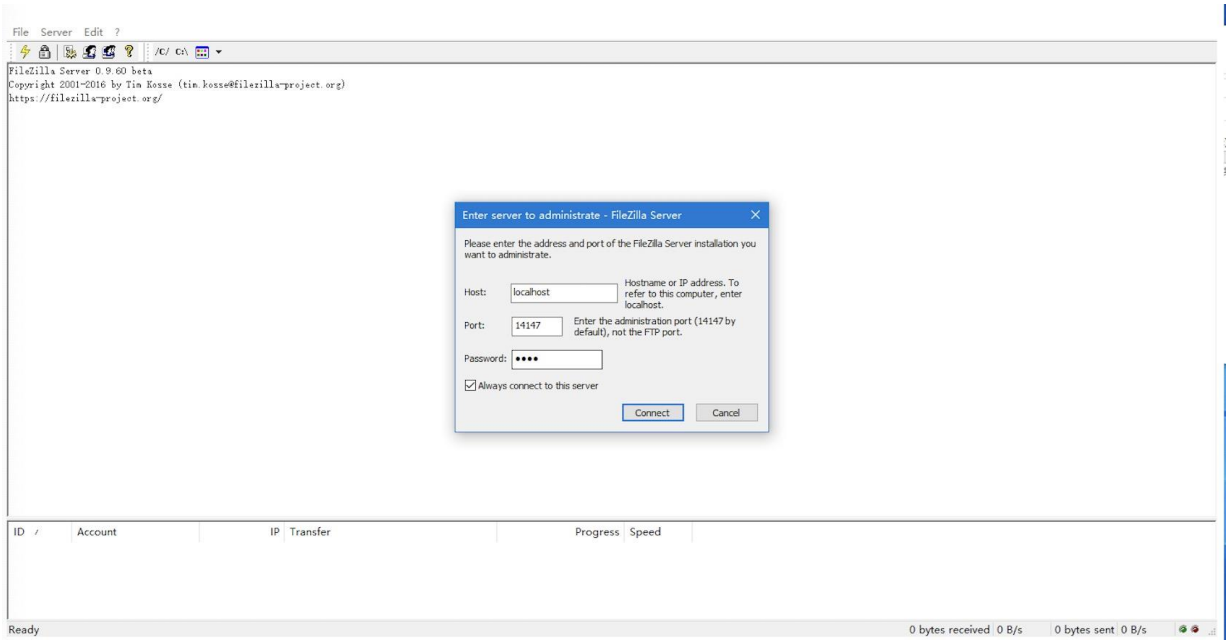
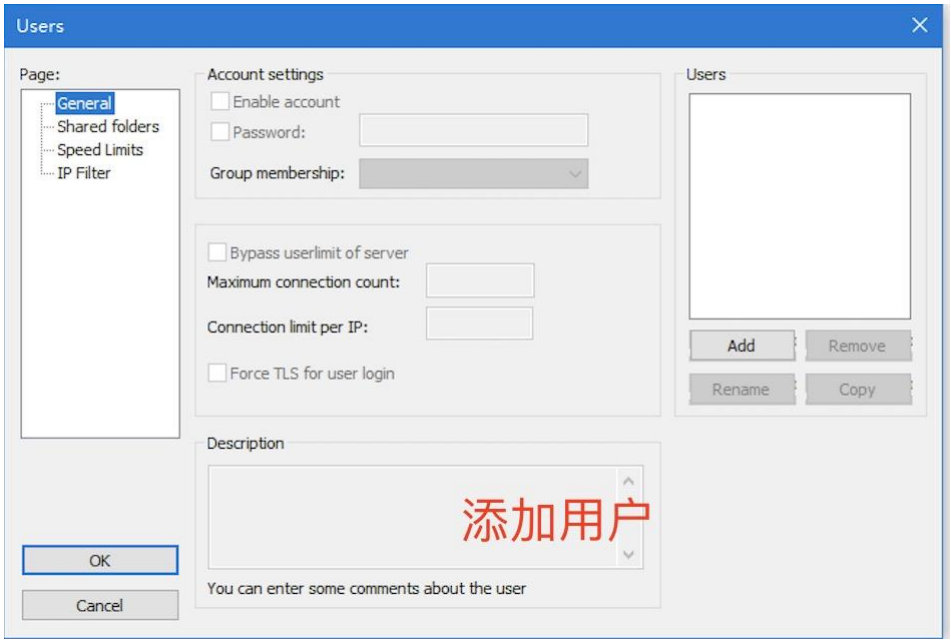
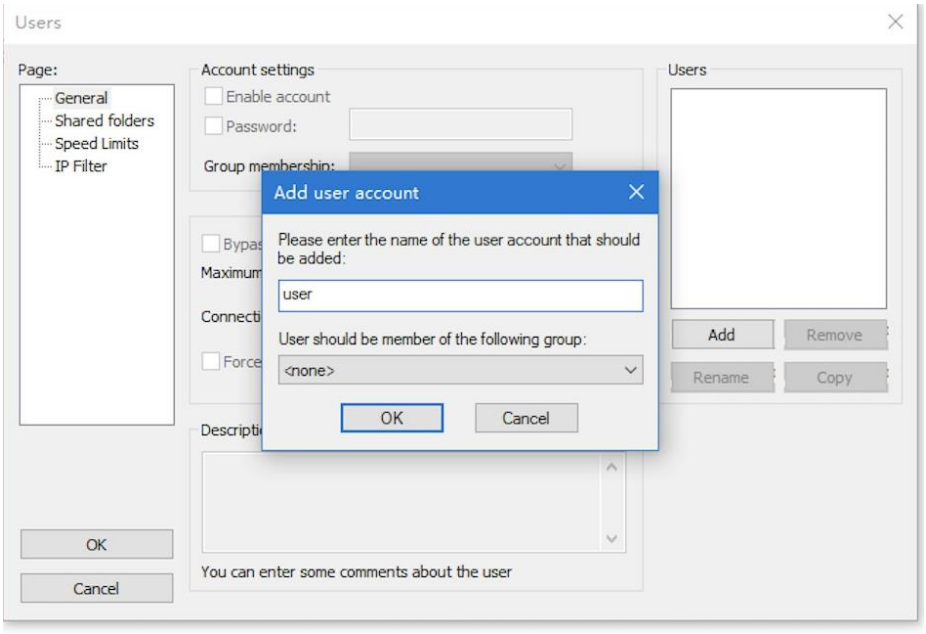


图 5：打开 FTP 服务器

3）创建一个用户，并设置用户名和口令


Users
Page:
General
Shared folders
Speed Limits
IP Filter
Account settings
Enable account
Password:
Group membership:
Bypass userlimit of server
Maximum connection count:
Connection limit per IP:
Force TLS for user login
Users
Add
Remove
Rename
Copy
Description
添加用户
You can enter some comments about the user
OK
Cancel


Users
Page:
General
Shared folders
Speed Limits
IP Filter
Account settings
Enable account
Password:
Group membership:
Add user account
Please enter the name of the user account that should be added:
user
User should be member of the following group:
<none>
OK
Cancel
Users
Add
Remove
Rename
Copy
You can enter some comments about the user
OK
Cancel

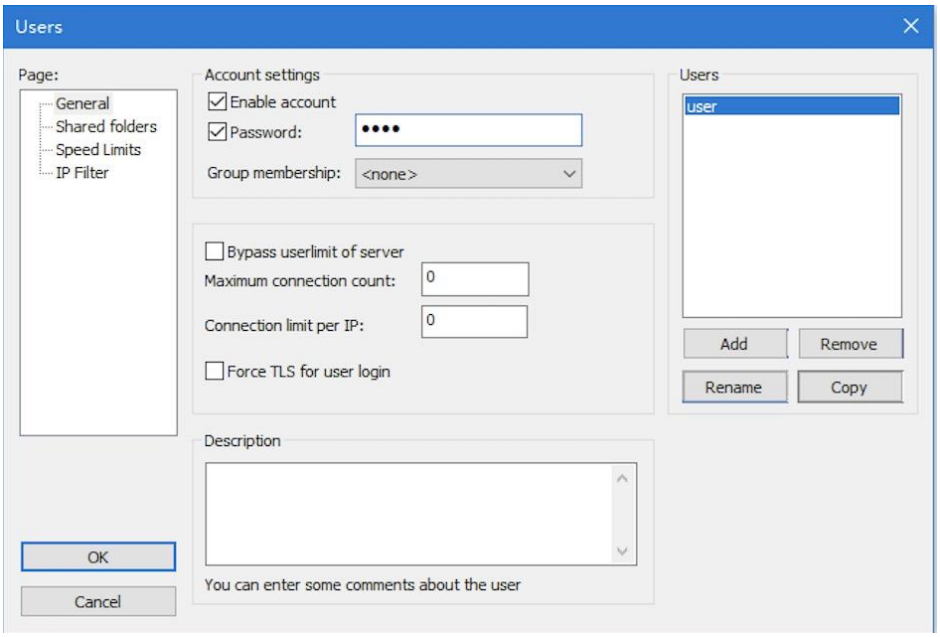
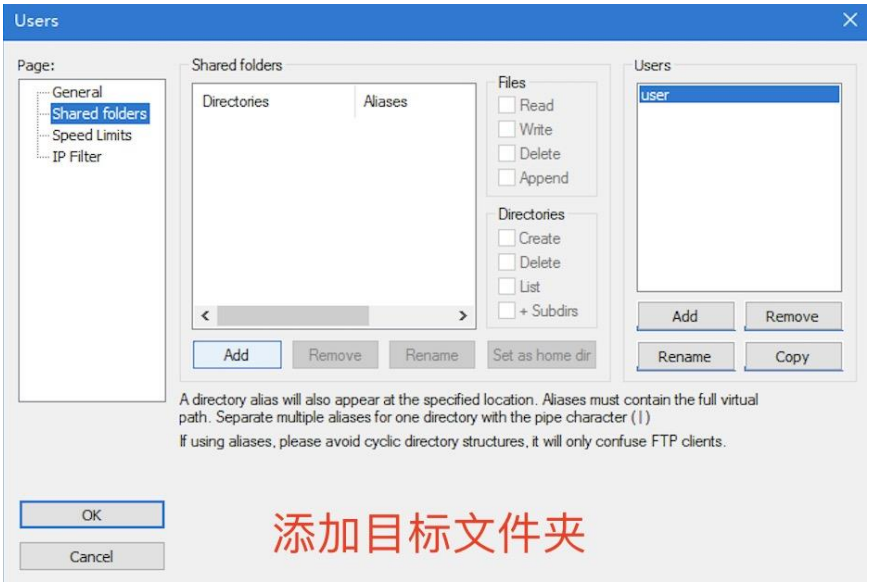


图 6：创建一个用户并设置口令

4）添加目标文件夹并设置用户权限



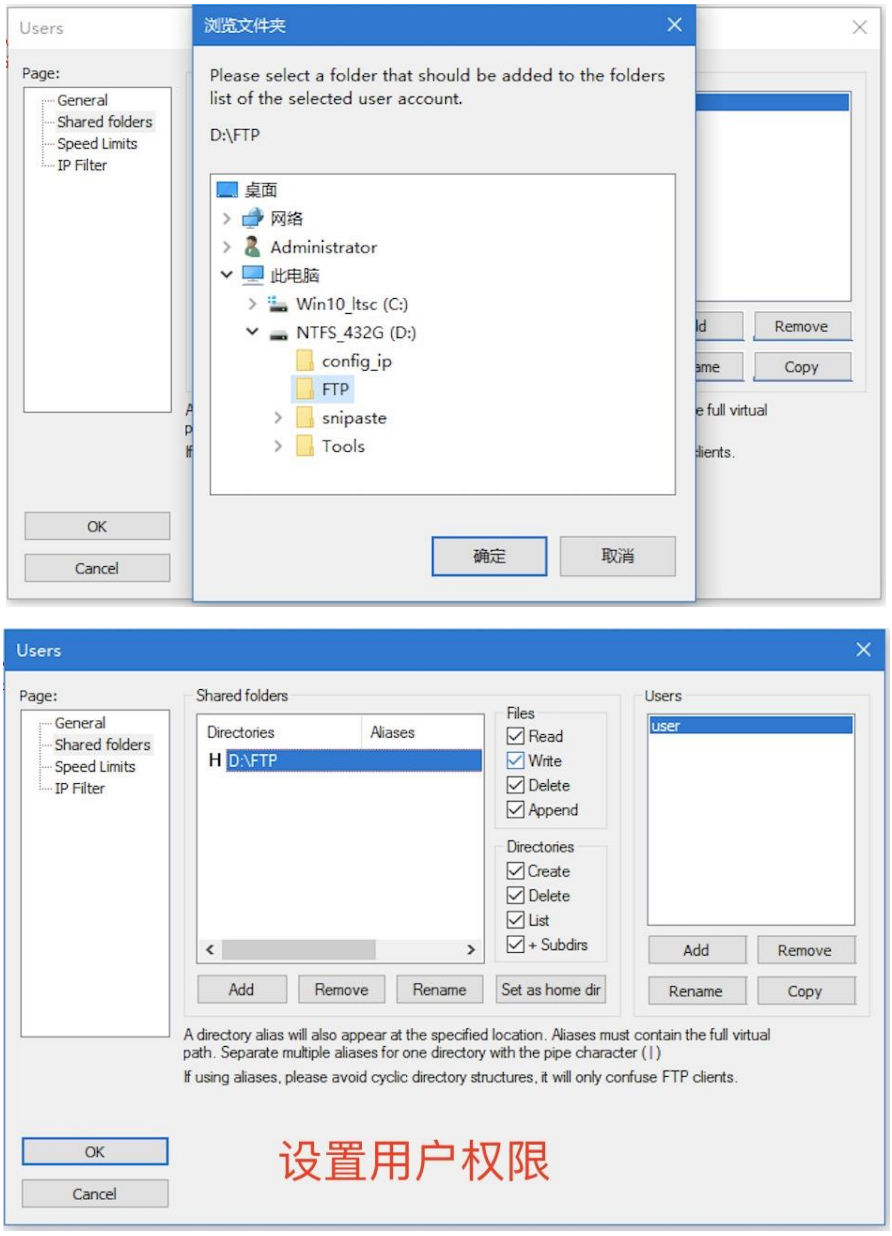


图 7：添加目标文件夹并设置用户权限

WWW 服务器的安装：

1）使用指令 httpd.exe -k install -n “Apache”安装 Apache 服务器

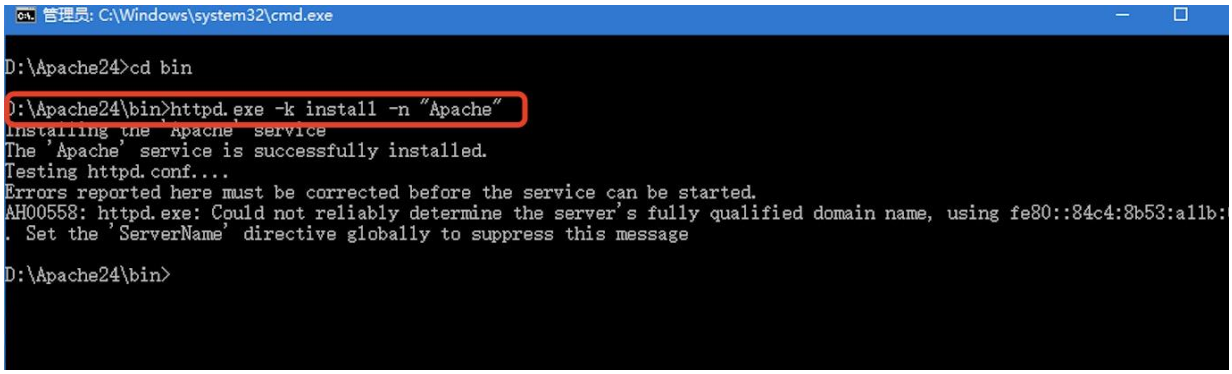


图 8：安装 Apache 服务器

2）更改 Apache 服务器的路径

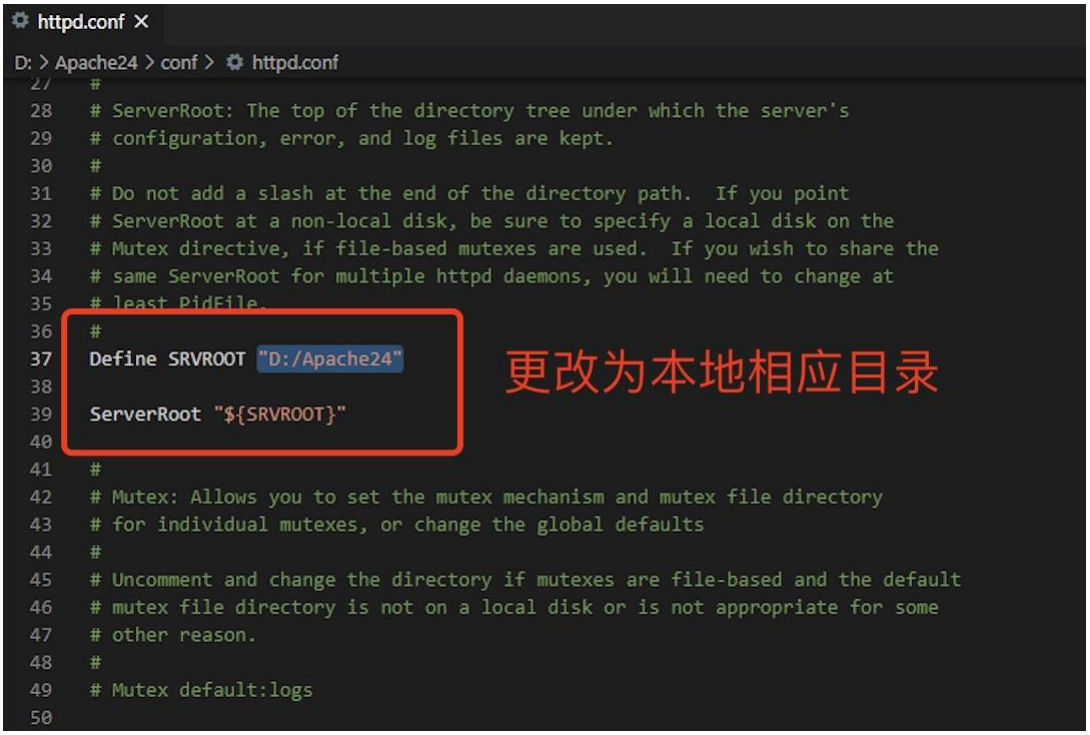


图 9：更改 Apache 运行路径

3）本地运行并访问服务器

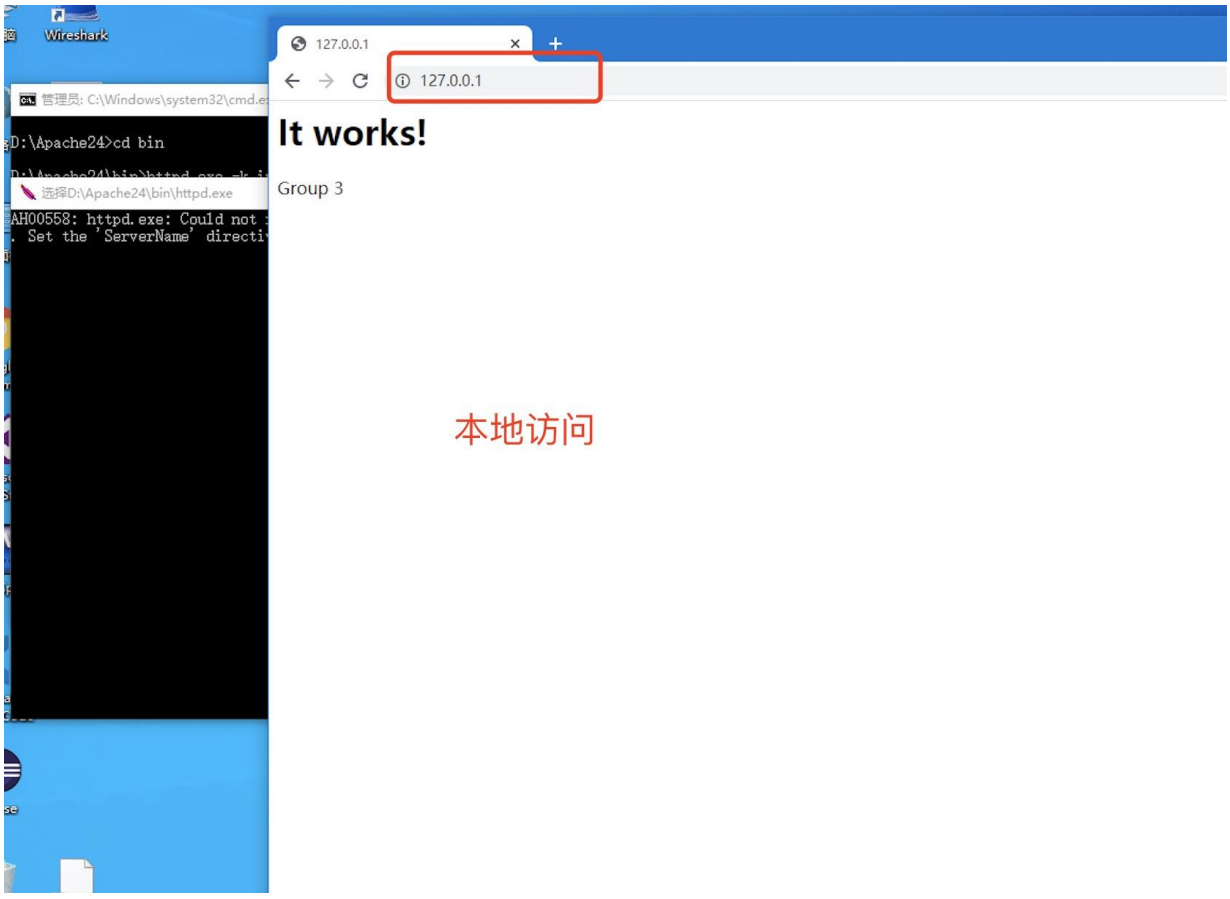


图 10：本地运行并访问服务器

步骤 2：路由器的基本配置。

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
Router(config-if-GigabitEthernet 0/0)#no shutdown
Router(config-if-GigabitEthernet 0/0)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
Router(config-if-GigabitEthernet 0/1)#no shutdown
Router(config-if-GigabitEthernet 0/1)#exit
```

图 11：配置路由器

步骤 3：验证当前配置。

（1）验证主机与服务器的连通性

完成步骤 2 路由器的基本配置后，使用分别 ping 服务器，可知：

图 12：验证主机与服务器连通性

（缺验证主机与服务器连通性图）

（2）经理机和员工机能否登陆 FTP 服务器？通过 htp://10.1.1.100 能否访问 WWW 服务器？判断目前结果是否达到预期目标，并说明原因。

经理机登陆 FTP 服务器：

图 13：经理机登陆 FTP 服务器

（缺经理机登陆 FTP 服务器图）

员工机 A、B 登陆 FTP 服务器：

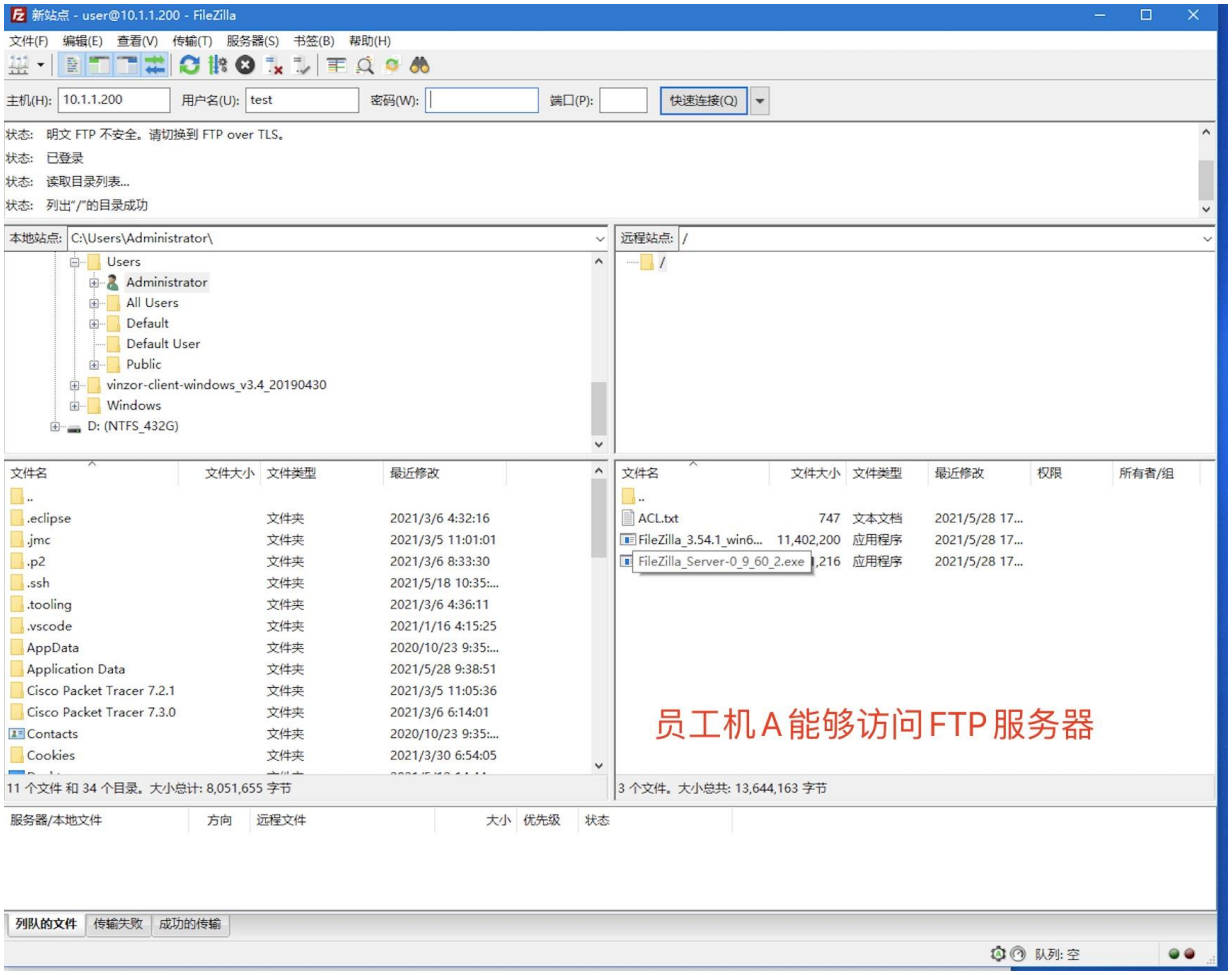


图 14：员工机 A 登陆 FTP 服务器

图 15：员工机 B 登陆 FTP 服务器

（缺员工机 B 登陆 FTP 服务器图）

经理机通过 http://10.1.1.100 能否访问 WWW 服务器：

图 16：经理机访问 WWW 服务器

（缺经理机访问 WWW 服务器图）

员工机 A、B 通过 http://10.1.1.100 能否访问 WWW 服务器：

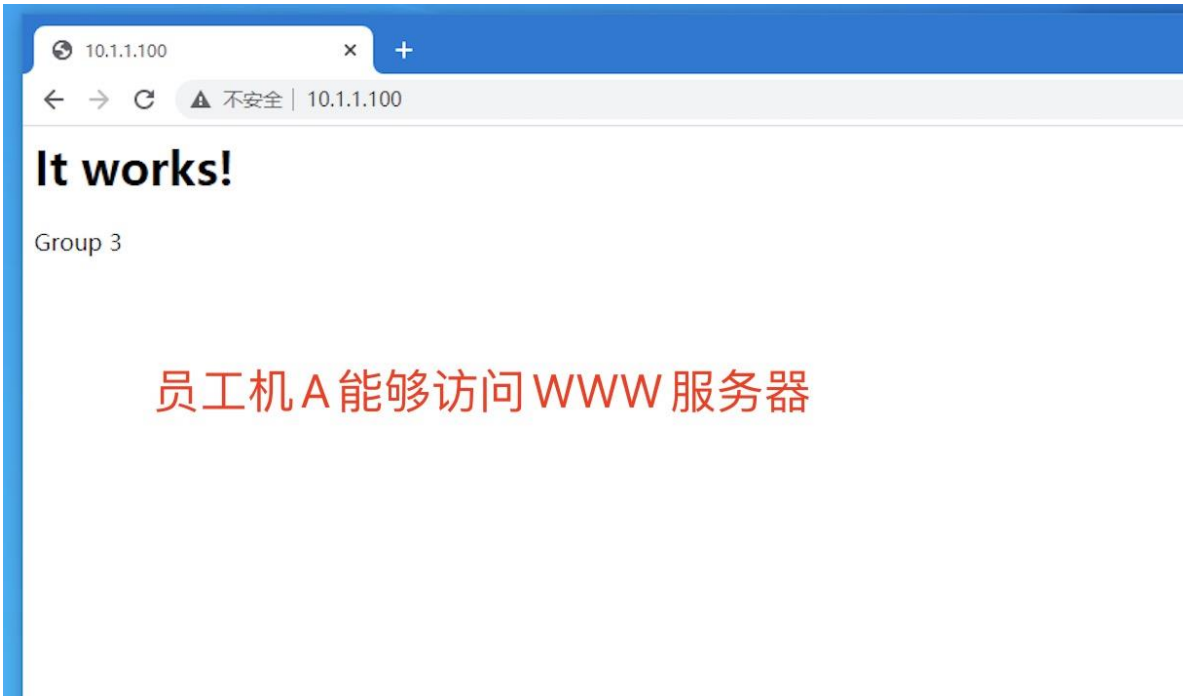


图 17：员工机 A、B 访问 WWW 服务器

（缺员工机 B 访问 WWW 服务器图）

由上可知，经理机和员工机 AB 都能登陆 FTP 服务器。

步骤 4：配置时间段。

定义正常上班的时间段。

```
Router(config)#time-range work-time
Router(config-time-range)#periodic weekdays 09:00 to 18:00
Router(config-time-range)#exit
```
配置时间段

图 18：配置时间段

步骤 5：配置 ACL。

配置 ACL 并应用时间段，以实现需求中基于时间段的访问控制。

```
Router(config)#time-range work-time
Router(config-time-range)#periodic weekdays 09:00 to 18:00
Router(config-time-range)#exit
Router(config)#ip access-list extended accessctrl
Router(config-ext-nacl)#permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
Router(config-ext-nacl)#$ 10.1.1.200 eq ftp time-range work-time
Router(config-ext-nacl)#$ 10.1.1.200 eq ftp-data time-range work-time
Router(config-ext-nacl)#$0.1.1.100 eq www time-range work-time
Router(config-ext-nacl)#$1.0 0.0.0.255 host 10.1.1.100 eq www
Router(config-ext-nacl)#exit
```

图 19：配置 ACL 并应用时间段

其中：

1）允许经理的主机在任何时间访问两台服务器：permit ip host 192.168.1.254 10.1.1.0 0.0.0.255

2）只允许员工主机在上班时间访问 FTP 服务器：

permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp time-range work-time

permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp-data time-range work-time

3）不允许员工主机在上班时间访问 WWW 服务器：

deny tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www time-range work-time

4）允许员工访问 WWW 服务器，但是仅当系统时间不在定义的时间段范围内，才会执行此规则。

permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www

步骤 6：应用 ACL。

将 ACL 应用到端口 0/0 的输入方向。

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
Router(config-if-GigabitEthernet 0/0)#end
```

应用ACL

图 20：应用 ACL

步骤 7：验证测试。

在使用基于时间的 ACL 时，要保证设备（路由器或交换机）的系统时间的准确性，因为设备是根据自己的系统时间（而不是主机时间）判断当前时间是否在时间段范围内。可以在特权模式下使用 show clock 命令查看当前系统时间，并使用 clock set 命令调整系统时间。通过调整设备的系统时间是现在不同时间段测试 ACL 是否生效。

本实验分别做下列测试：

（1）查看路由器的系统时间：使用 show clock 命令判断当前时间段。

查看路由时间可知，**此时，路由器的系统时间为 19:58:36 UTC Fri，May 28，2021，也即是工作日的下班时间（不属于 weekdays 且不在 9:00 - 18:00）。**

```
Router#show clock
19:58:36 UTC Fri, May 28, 2021
Router#show clock
19:58:41 UTC Fri, May 28, 2021
```

查看路由时间

图 21：查看路由器的系统时间

（2）经理的主机 Manager 使用步骤 1 建立的用户名登录 FTP 服务器，并通过 http://10.1.1.100 访问 WWW 服务器，在设定时间段内是否能登录和访问？

由于此时处于下班时间，经理主机 Manager 在下班时间登陆 FTP 服务器，经理机能够成功登陆 FTP 服务器，并且访问 WWW 服务器。

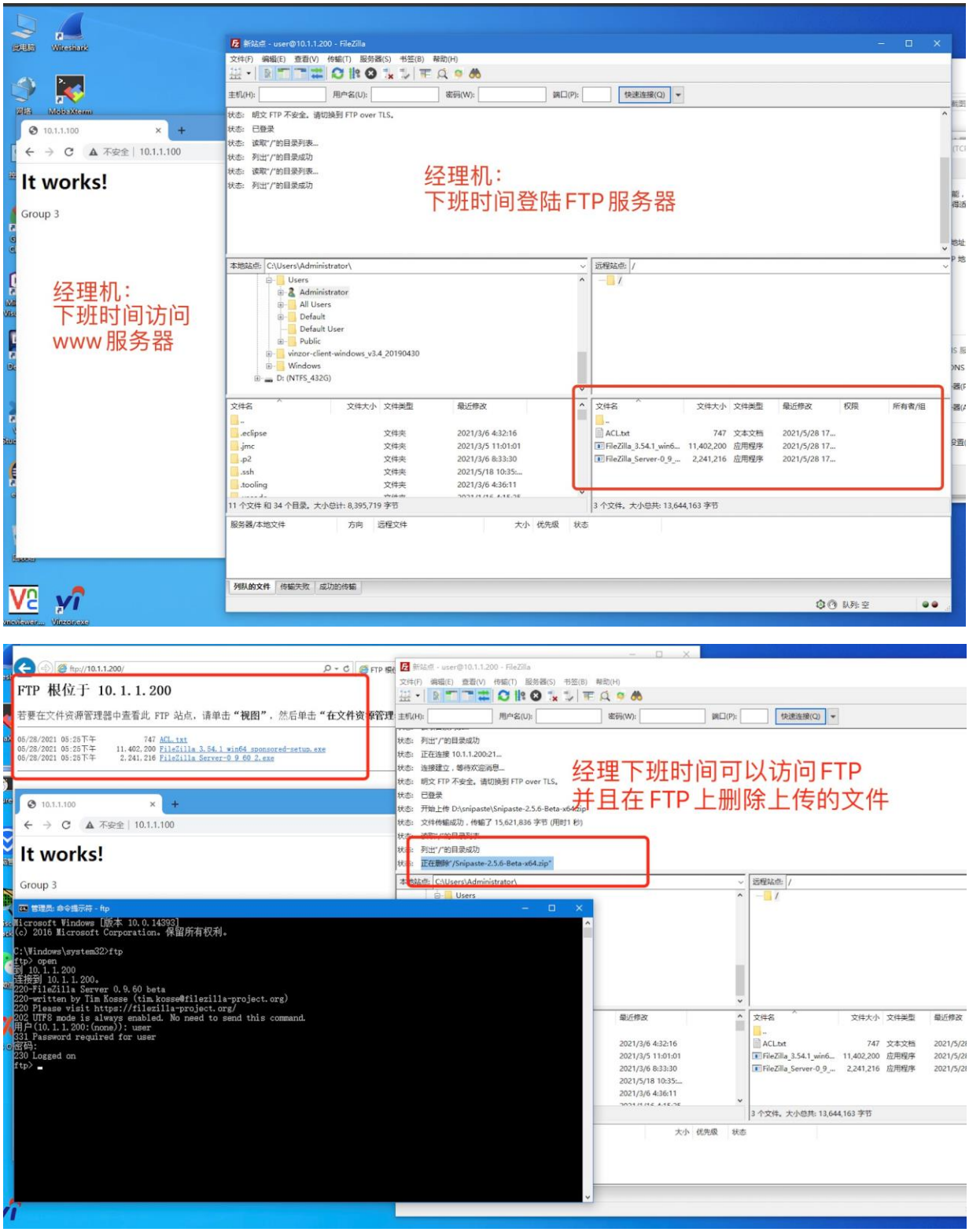


图 23：经理机下班时间登陆 FTP 服务器，访问 WWW 服务器

（3）普通员工主机 A、B 分别使用步骤 1 建立的用户名登录 FTP 服务器，并通过 http://10.1.100 访问 WWW 服务器，在设定时间段内是否能登录和访问？（登录 FTP 时分别通过 DOS 命令与浏览器方式，结合捕获报文分析）？

员工主机 A：

- 在**下班时间**登陆 FTP 服务器和访问 WWW 服务器，此时，员工主机 A 可以访问 WWW 服务器，但是不能登陆 FTP 服务器，显示连接超时。

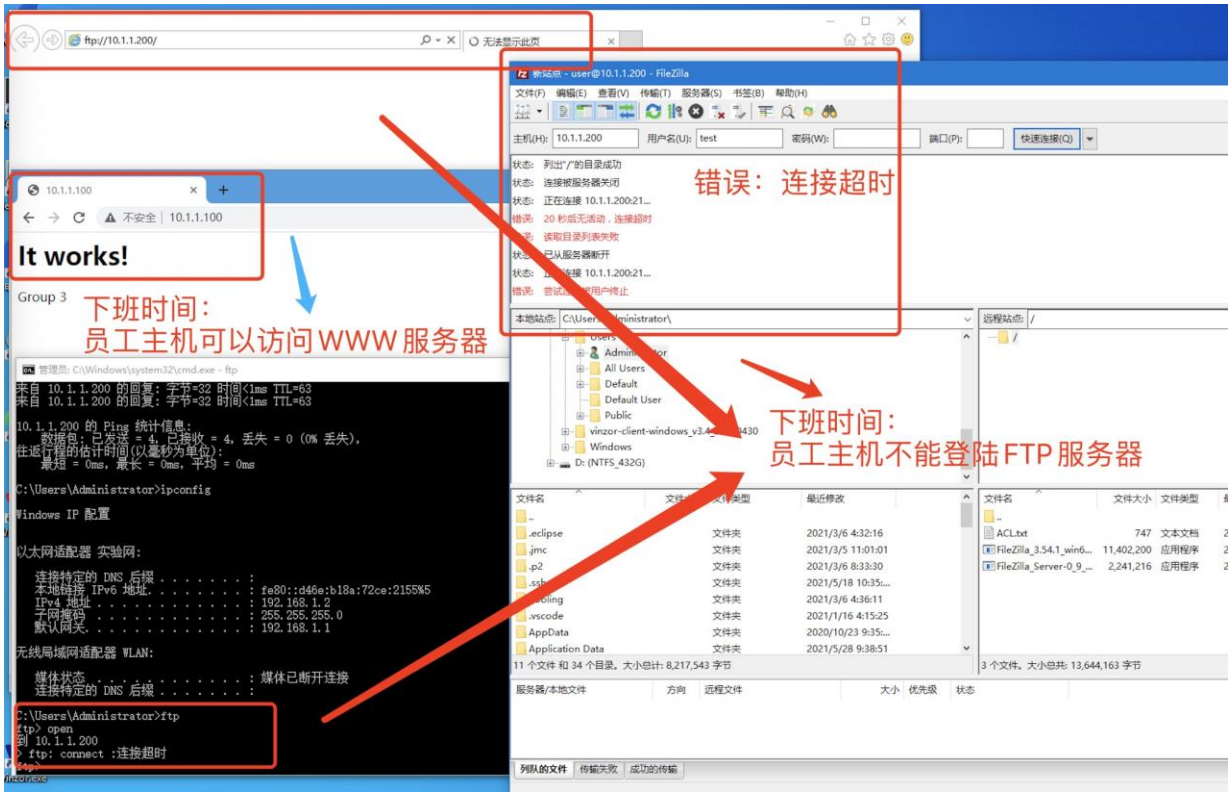


图 23：员工机 A 下班时间登陆 FTP 服务器，访问 WWW 服务器

- 登录 FTP 时通过浏览器方式，并捕获报文：Wireshark 捕获到 [TCP Retransmission]，即超时重发的报文，并且发生了两次连接请求和四次重传。其中 SACK_PERM 字段表示两台主机间可以进行选择重传。

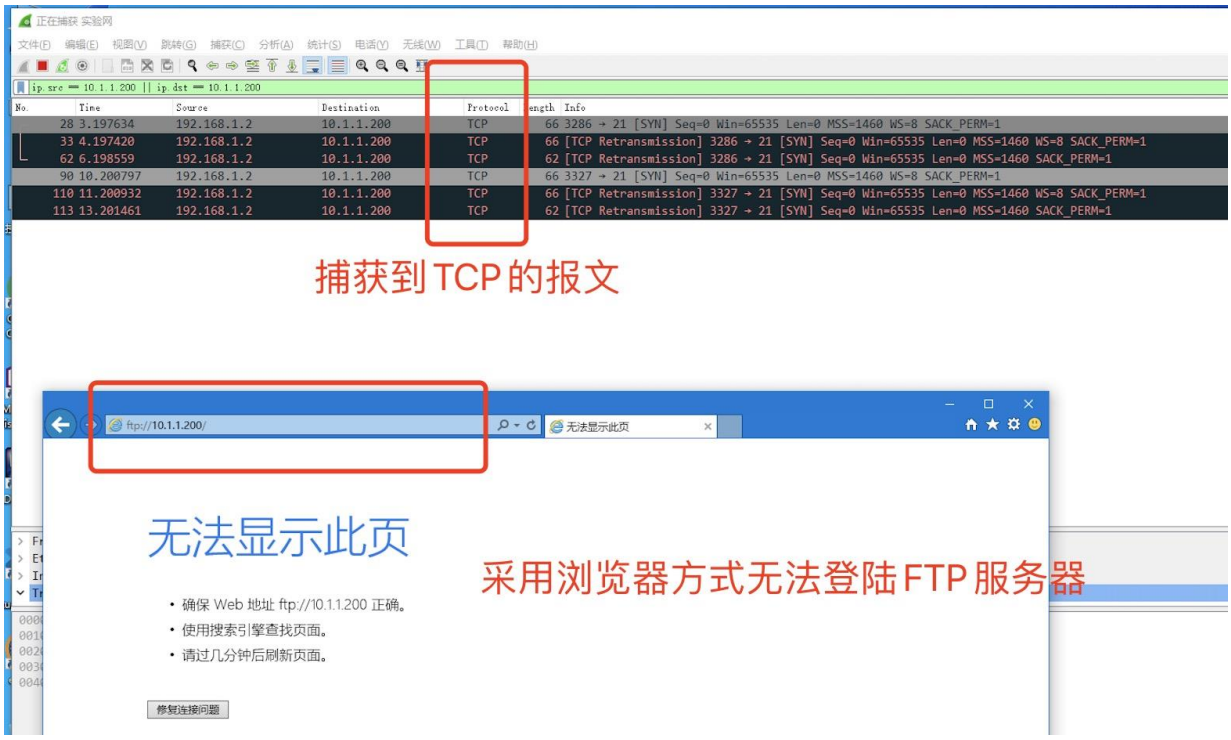


图 24：员工机 A 下班时间使用浏览器方式登陆 FTP 服务器

- 登录 FTP 时通过 DOS 命令方式，并捕获报文：Wireshark 捕获到 [TCP Retransmission]，即超时重发的报文，并且发生了一次连接请求和两次重传。其中 SACK_PERM 字段表示两台主机间可以进行选择重传。

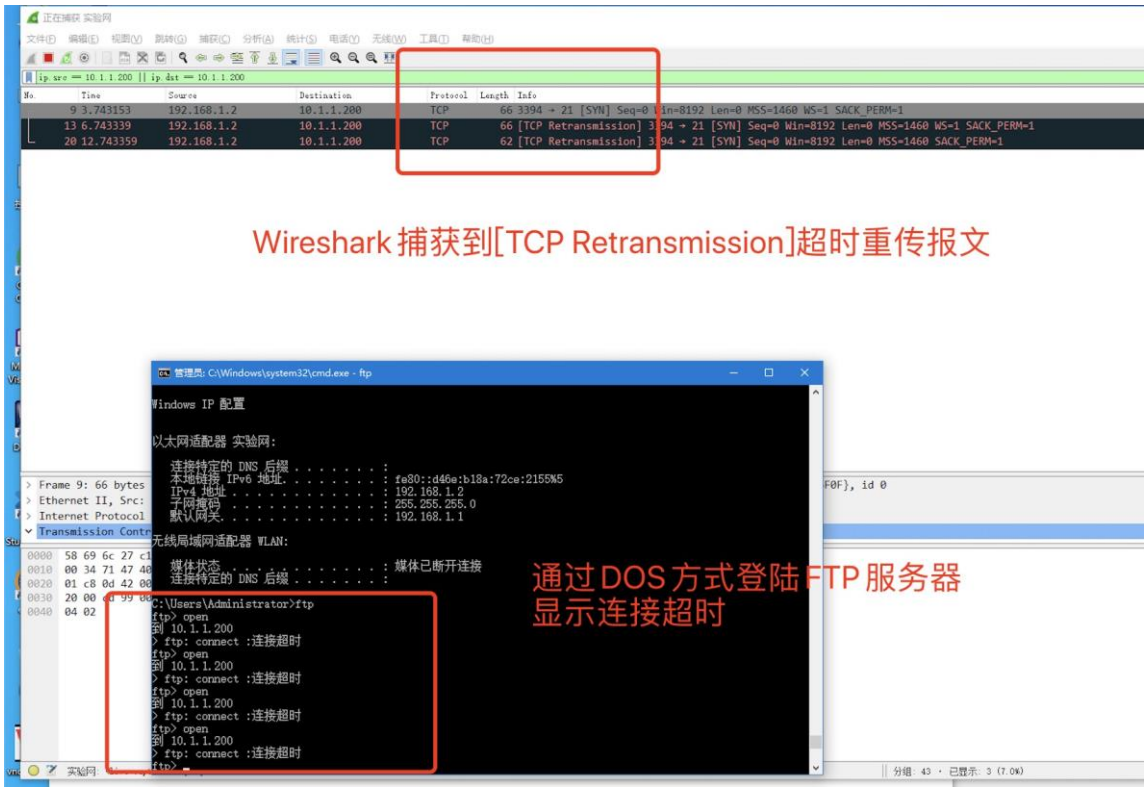


图 25：员工机 A 下班时间使用 DOS 方式登陆 FTP 服务器

员工主机 B：

- 在**下班时间**登陆 FTP 服务器和访问 WWW 服务器，此时，员工主机 B 可以访问 WWW 服务器，但是不能登陆 FTP 服务器，显示连接超时。

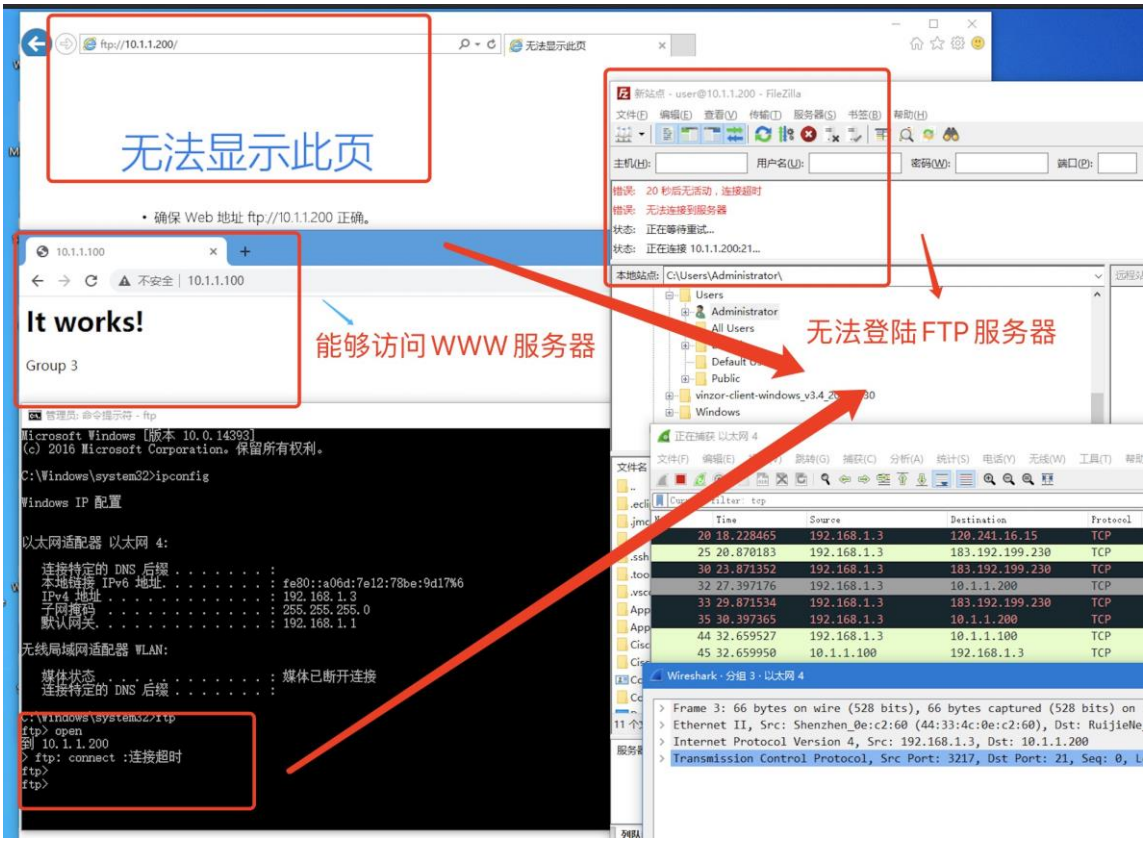


图 26：员工机 B 下班时间登陆 FTP 服务器，访问 WWW 服务器

- 登录 FTP 时通过浏览器方式，并捕获报文：Wireshark 捕获到 [TCP Retransmission]，即超时重发的报文，并且发生了两次连接请求和四次重传。其中 SACK_PERM 字段表示两台主机间可以进行选择重传。

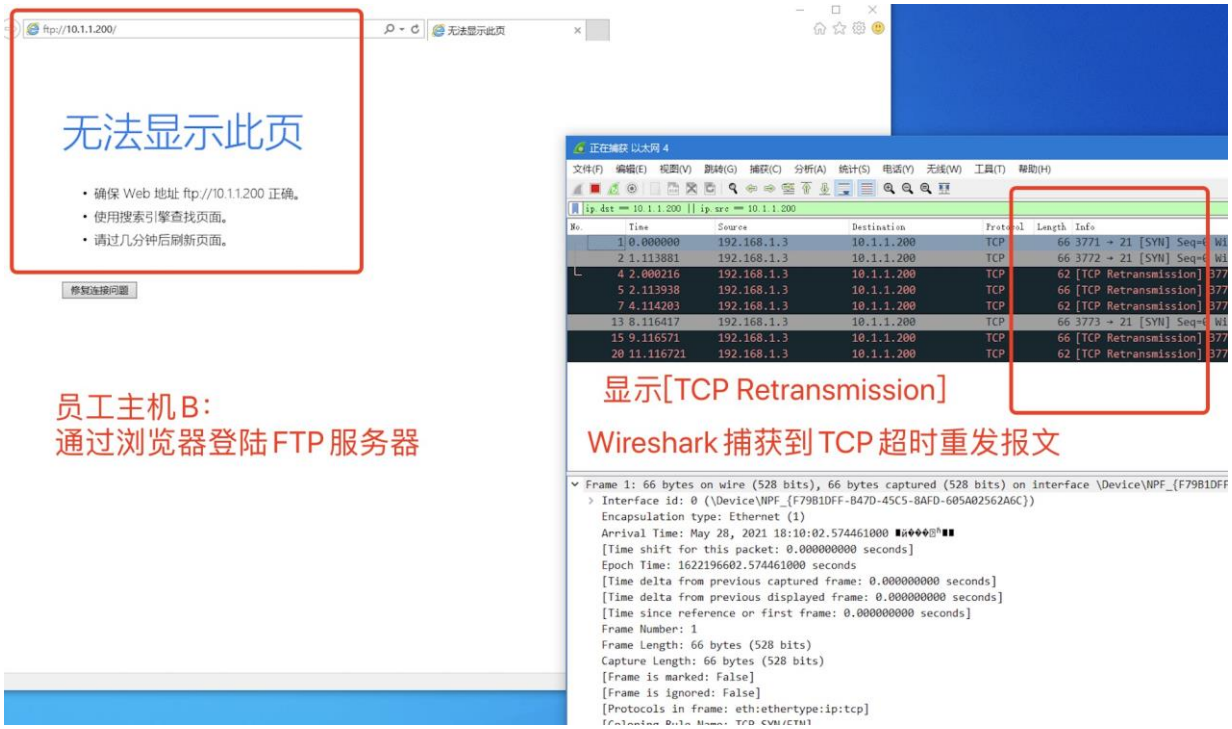


图 27：员工机 B 使用浏览器方式登陆 FTP 服务器

- 登录 FTP 时通过 DOS 命令方式，并捕获报文：Wireshark 捕获到 [TCP Retransmission]，即超时重发的报文，并且发生了一次连接请求和两次重传。其中 SACK_PERM 字段表示两台主机间可以进行选择重传。

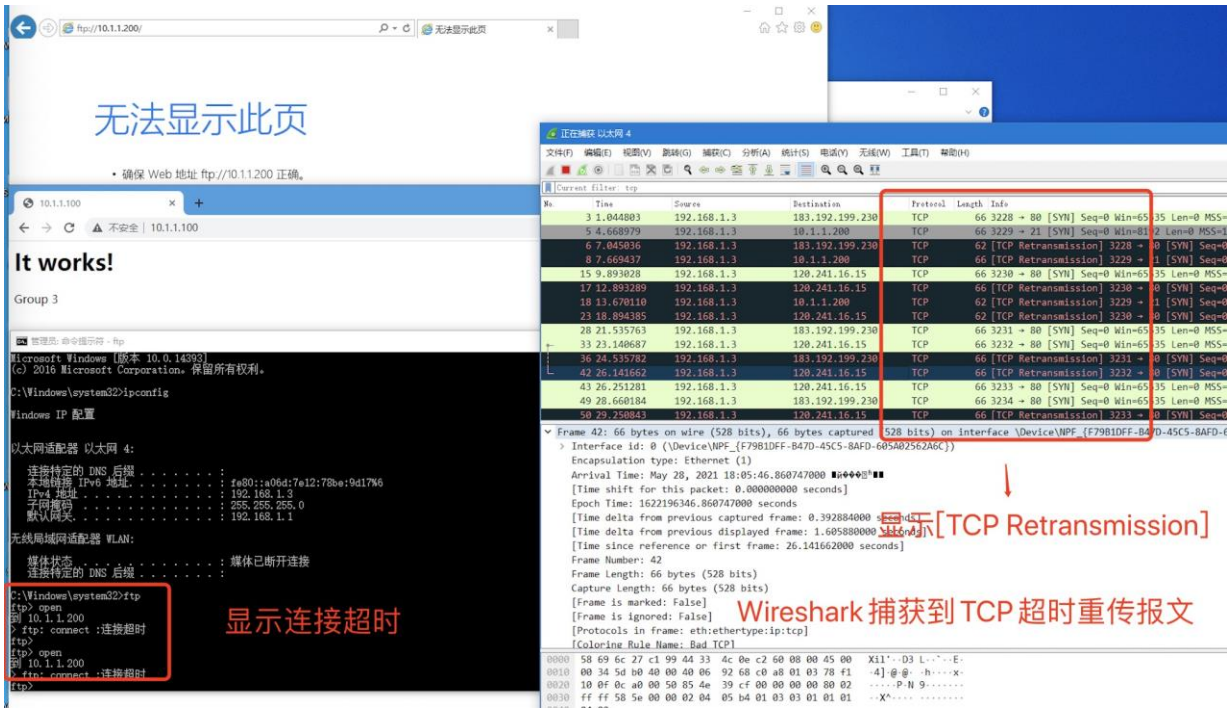


图 28：员工机 B 使用 DOS 方式登陆 FTP 服务器

（4）改变路由器系统时间段，在其他时间段执行（2）～（3）的测试。
使用 clock set 重新设置路由器系统时间段。
把系统时间段设为**上班时间**：09:18:54 UTC Fri May 28 2021。

```
Router#
Router#clock set 09:18:54 5 28 2021
Router#*May 28 09:18:54: %SYS-6-CLOCKUPDATE: System clock has been updated to 09:18:54 UTC Fri May 28 2021.

Router#
```

图 29：重新设置路由器系统时间为上班时间。

此时处于上班时间，经理主机 Manager 在上班时间登陆 FTP 服务器，经理机能够成功登陆 FTP 服务器，并且访问 WWW 服务器。

图 30：经理机上班时间登陆 FTP 服务器，访问 WWW 服务器

（缺图 30——经理机上班时间登陆服务器图）

员工主机 A：

- 在**上班时间**登陆 FTP 服务器和访问 WWW 服务器，此时，员工主机 A 可以不能 WWW 服务器，显示连接超时，但是可以登陆 FTP 服务器。

图 31：员工机 A 上班时间登陆 FTP 服务器，访问 WWW 服务器

- 登录 FTP 时通过浏览器方式，并捕获报文：

图 32：员工机 A 使用浏览器方式登陆 FTP 服务器

- 登录 FTP 时通过 DOS 命令方式，并捕获报文：

图 33：员工机 A 使用 DOS 方式登陆 FTP 服务器

（缺图 31，32，33——员工 A 上班时间登陆服务器图）

员工主机 B：

- 在**上班时间**登陆 FTP 服务器和访问 WWW 服务器，此时，员工主机 B 不能访问 WWW 服务器，显示连接超时，但是可以登陆 FTP 服务器。

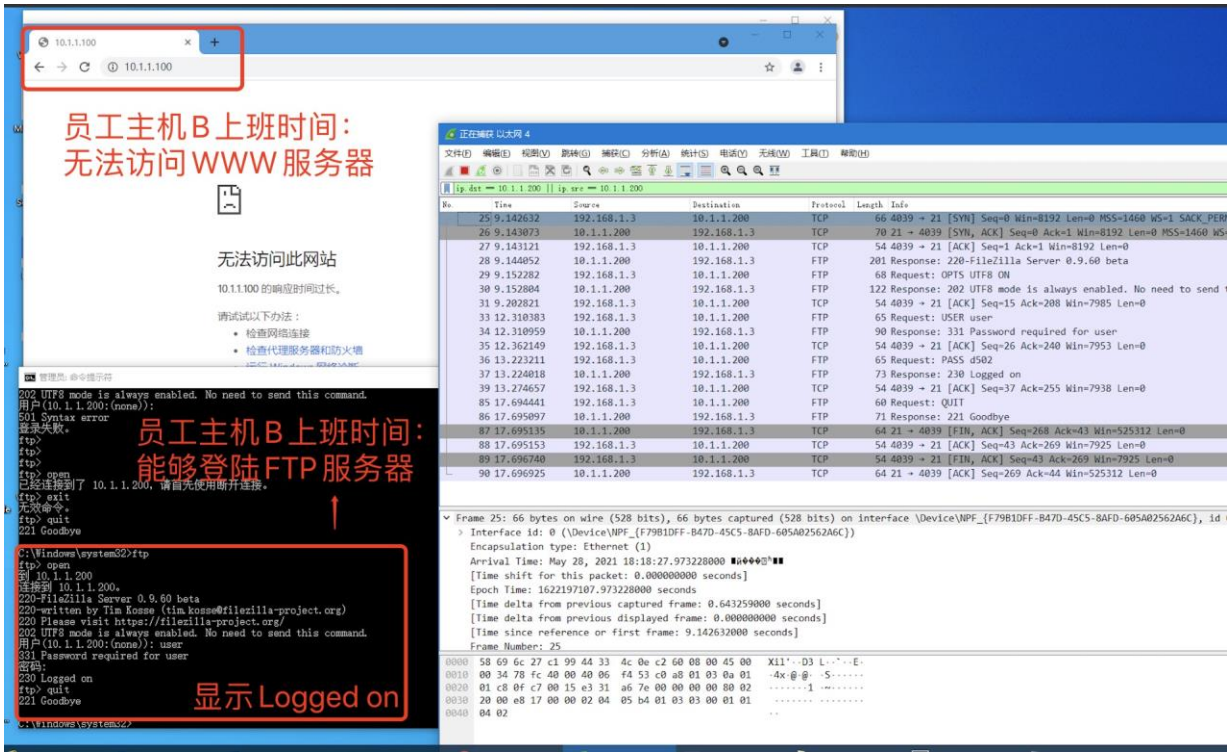


图 34：员工机 B 上班时间登陆 FTP 服务器，访问 WWW 服务器

- 登录 FTP 时通过浏览器方式，并捕获报文：

图 35：员工机 B 使用浏览器方式登陆 FTP 服务器

（缺图 35——员工 B 上班时间浏览器登陆 FTP 图）

- 登录 FTP 时通过 DOS 命令方式，并捕获报文：捕获到了 TCP、FTP 的协议报文，其中 FTP 的协议报文，用于 FTP 服务器的连接与响应。详情如下：

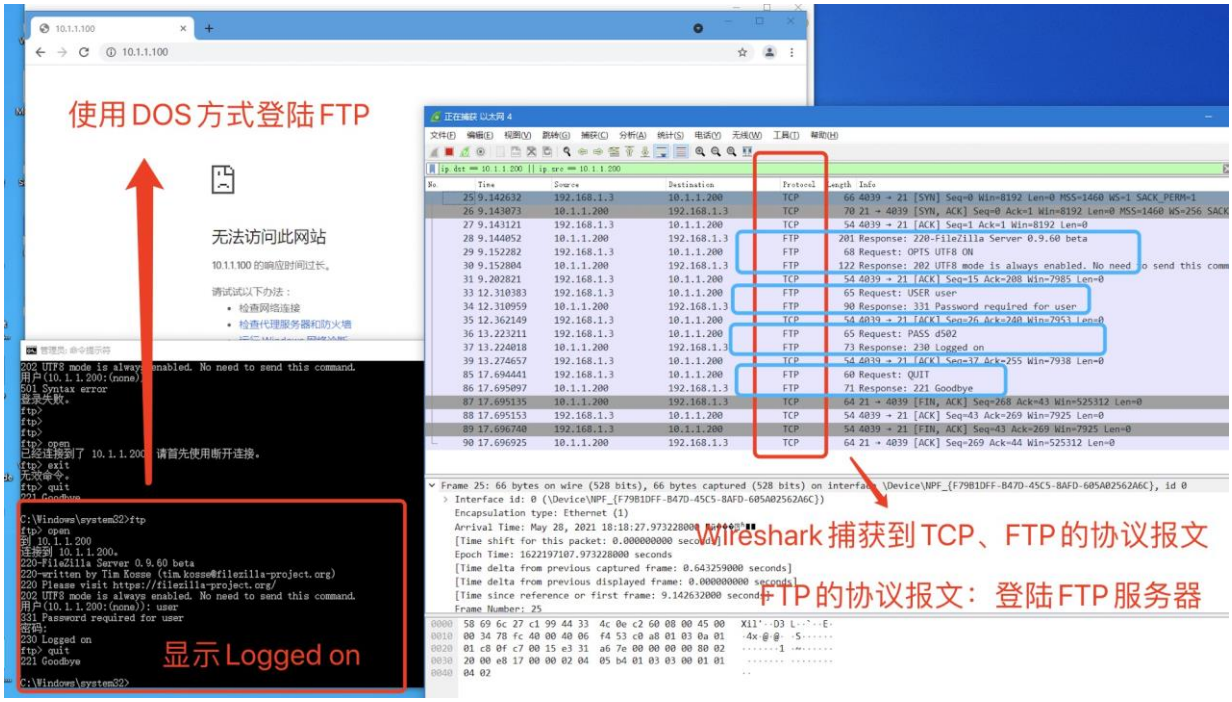
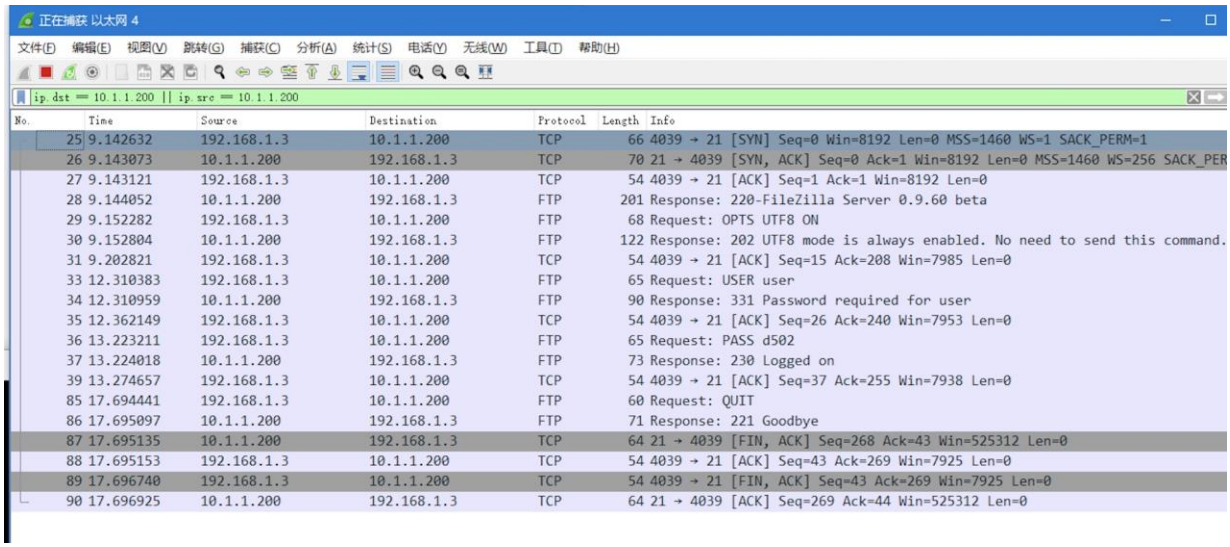


图 36：员工机 B 使用 DOS 方式登陆 FTP 服务器

（5）捕获主机访问服务器时的数据包，并进行分析。

主机在上班时间访问服务器时，捕获到了 TCP 与 FTP 数据包。

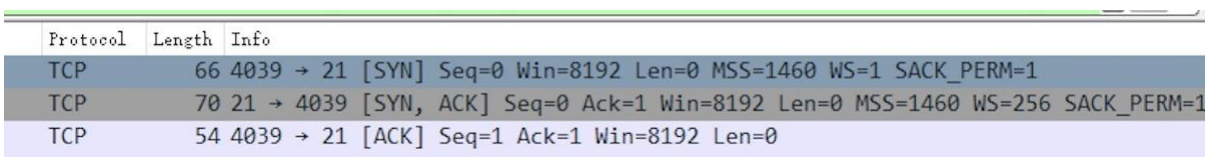


No.	Time	Source	Destination	Protocol	Length	Info
25	9.142632	192.168.1.3	10.1.1.200	TCP	66	4039 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
26	9.143073	10.1.1.200	192.168.1.3	TCP	70	21 → 4039 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PER
27	9.143121	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
28	9.144052	10.1.1.200	192.168.1.3	FTP	201	Response: 220-FileZilla Server 0.9.60 beta
29	9.152282	192.168.1.3	10.1.1.200	FTP	68	Request: OPTS UTF8 ON
30	9.152804	10.1.1.200	192.168.1.3	FTP	122	Response: 202 UTF8 mode is always enabled. No need to send this command.
31	9.202821	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
33	12.310383	192.168.1.3	10.1.1.200	FTP	65	Request: USER user
34	12.310959	10.1.1.200	192.168.1.3	FTP	90	Response: 331 Password required for user
35	12.362149	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [ACK] Seq=26 Ack=240 Win=7953 Len=0
36	13.223211	192.168.1.3	10.1.1.200	FTP	65	Request: PASS d502
37	13.224018	10.1.1.200	192.168.1.3	FTP	73	Response: 230 Logged on
39	13.274657	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [ACK] Seq=37 Ack=255 Win=7938 Len=0
85	17.694441	192.168.1.3	10.1.1.200	FTP	60	Request: QUIT
86	17.695097	10.1.1.200	192.168.1.3	FTP	71	Response: 221 Goodbye
87	17.695135	10.1.1.200	192.168.1.3	TCP	64	21 → 4039 [FIN, ACK] Seq=268 Ack=43 Win=525312 Len=0
88	17.695153	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [ACK] Seq=43 Ack=269 Win=7925 Len=0
89	17.696740	192.168.1.3	10.1.1.200	TCP	54	4039 → 21 [FIN, ACK] Seq=43 Ack=269 Win=7925 Len=0
90	17.696925	10.1.1.200	192.168.1.3	TCP	64	21 → 4039 [ACK] Seq=269 Ack=44 Win=525312 Len=0

图 37：上班时间捕获的数据包

其中，TCP 数据包分析如下：

- TCP 三次握手建立连接请求：第一次用户端发送初始序号 Seq=0 和 syn=1 请求标志；第二次服务器发送请求标志 syn，发送确认标志 ACK，发送自己的序号 seq=0，发送客户端的确认序号 ACK=1；第三次客户端发送 ACK 确认号，发送自己的序号 Seq=1，发送对方的确认号 ACK=1



Protocol	Length	Info
TCP	66	4039 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
TCP	70	21 → 4039 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP	54	4039 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0

图 38：TCP 三次握手过程

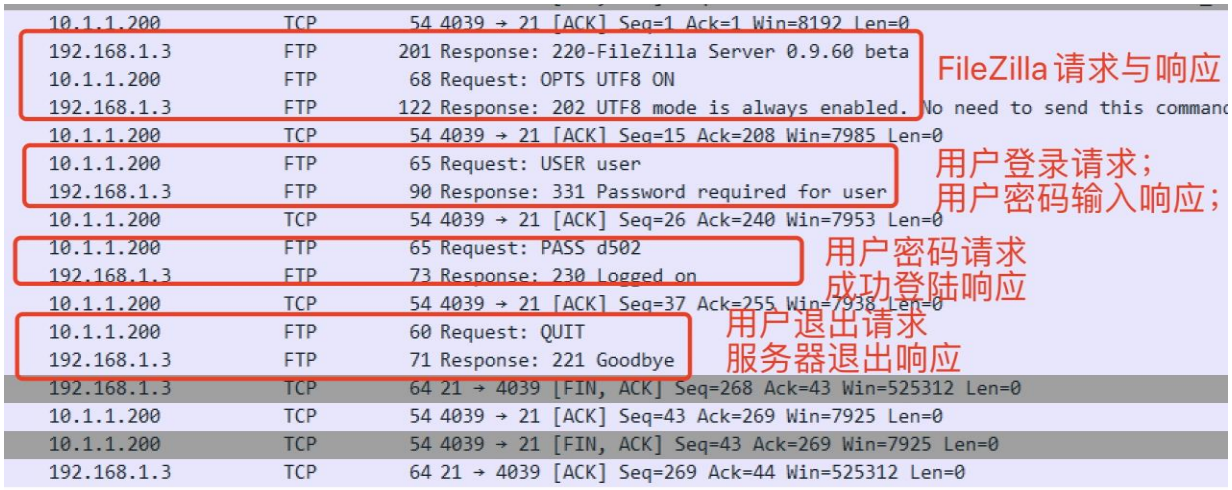
- TCP 四次挥手关闭连接：第一次挥手客户端发出释放 FIN=1，自己序列号 Seq=268，进入 FIN-WAIT-1 状态；第二次挥手服务器收到客户端确认结果后，发出 ACK=1 确认标志和客户端的确认号 ACK=269，自己的序列号 Seq=43，进入 CLOSE-WAIT 状态；第三次挥手客户端收到服务器确认结果后，进入 FIN-WAIT-2 状态。此时服务器发送释放 FIN=1 信号，确认标志 ACK=1，确认序号 ACK=269，自己序号 Seq=43，服务器进入 LAST-ACK（最后确认态）；第四次挥手：客户端收到回复后，发送确认 ACK=1，ack=w+1，自己的 Seq=269，客户端进入 TIME-WAIT（时间等待）。客户端经过 2 个最长报文段寿命后，客户端 CLOSE；服务器收到确认后，立刻进入 CLOSE 状态。

TCP	64 21 → 4039 [FIN, ACK] Seq=268 Ack=43 Win=525312 Len=0
TCP	54 4039 → 21 [ACK] Seq=43 Ack=269 Win=7925 Len=0
TCP	54 4039 → 21 [FIN, ACK] Seq=43 Ack=269 Win=7925 Len=0
TCP	64 21 → 4039 [ACK] Seq=269 Ack=44 Win=525312 Len=0

图 39：TCP 四次挥手过程

其中，FTP 数据包分析如下：

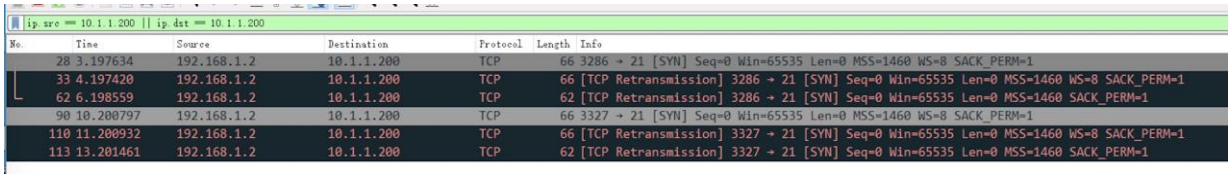
- FileZilla 请求与响应
- 用户登陆请求 [Request: USER user]
- 用户密码输入响应 [Response: 331 Password required for user]
- 用户密码请求 [Request: PASS d502]
- 成功登陆响应 [Response: 230 Logged on]
- 用户退出请求 [Request: QUIT]
- 服务器退出响应 [Response: 221 Goodbye]



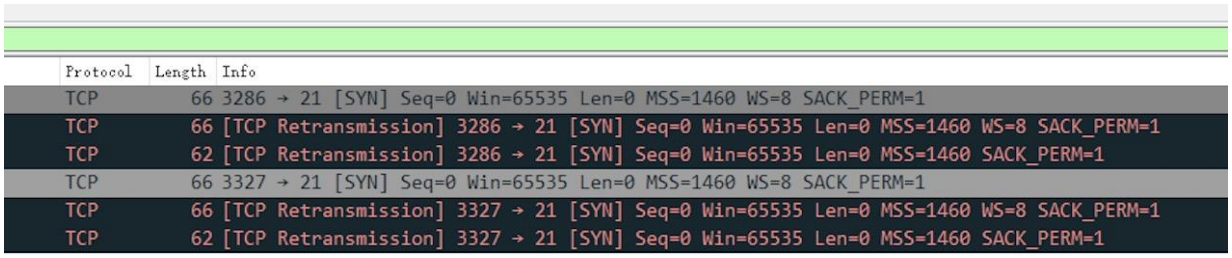
10.1.1.200	TCP	54 4039 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
192.168.1.3	FTP	201 Response: 220-FileZilla Server 0.9.60 beta
10.1.1.200	FTP	68 Request: OPTS UTF8 ON
192.168.1.3	FTP	122 Response: 202 UTF8 mode is always enabled. No need to send this comman
10.1.1.200	TCP	54 4039 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
10.1.1.200	FTP	65 Request: USER user
192.168.1.3	FTP	90 Response: 331 Password required for user
10.1.1.200	TCP	54 4039 → 21 [ACK] Seq=26 Ack=240 Win=7953 Len=0
10.1.1.200	FTP	65 Request: PASS d502
192.168.1.3	FTP	73 Response: 230 Logged on
10.1.1.200	TCP	54 4039 → 21 [ACK] Seq=37 Ack=255 Win=7938 Len=0
10.1.1.200	FTP	60 Request: QUIT
192.168.1.3	FTP	71 Response: 221 Goodbye
192.168.1.3	TCP	64 21 → 4039 [FIN, ACK] Seq=268 Ack=43 Win=525312 Len=0
10.1.1.200	TCP	54 4039 → 21 [ACK] Seq=43 Ack=269 Win=7925 Len=0
10.1.1.200	TCP	54 4039 → 21 [FIN, ACK] Seq=43 Ack=269 Win=7925 Len=0
192.168.1.3	TCP	64 21 → 4039 [ACK] Seq=269 Ack=44 Win=525312 Len=0

图 40：FTP 请求响应报文

下班时间连接 FTP 服务器捕获的数据包，均为 TCP 超时重发数据包 [TCP Retransmission]。



No.	Time	Source	Destination	Protocol	Length	Info
28	3.197634	192.168.1.2	10.1.1.200	TCP	66	3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
33	4.197420	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
62	6.198559	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
90	10.200797	192.168.1.2	10.1.1.200	TCP	66	3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
110	11.200932	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
113	13.201461	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1



Protocol	Length	Info
TCP	66	3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
TCP	66	[TCP Retransmission] 3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
TCP	62	[TCP Retransmission] 3286 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
TCP	66	3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
TCP	66	[TCP Retransmission] 3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
TCP	62	[TCP Retransmission] 3327 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

图 41：TCP 超时重发报文

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

计算机网络实验报告

【交实验报告】

上传实验报告：　　截止日期（不迟于）：1 周之内

上传包括两个文件：

（1）小组实验报告。上传文件名格式：小组号_ Ftp 协议分析实验.pdf （由组长负责上传）

例如: 文件名“10_ Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告

（2）小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号_学号_姓名_ Ftp 协议分析实验.pdf （由组员自行上传）

例如: 文件名“10_05373092_张三_ Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告。

注意：不要打包上传！

学号	学生	自评分
18338072	冼子婷	98
18322043	廖雨轩	98
18346019	胡文浩	98