



## 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。

院系	计算机学院	班 级	软工1班	组长	崔子潇
学号	19308024	19335040	19335286		
学生	崔子潇	丁维力	郑有为		
实验分工					
崔子潇	操作 Manager，搭建路由环境，收集实验截图，分析实验现象		丁维力	操作 PC2，搭建 FTP 服务器，手机实验截图，分析实验现象	
郑有为	操作 PC1，搭建 WWW 服务器，收集结果，分析实验现象，写实验报告。				

【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】

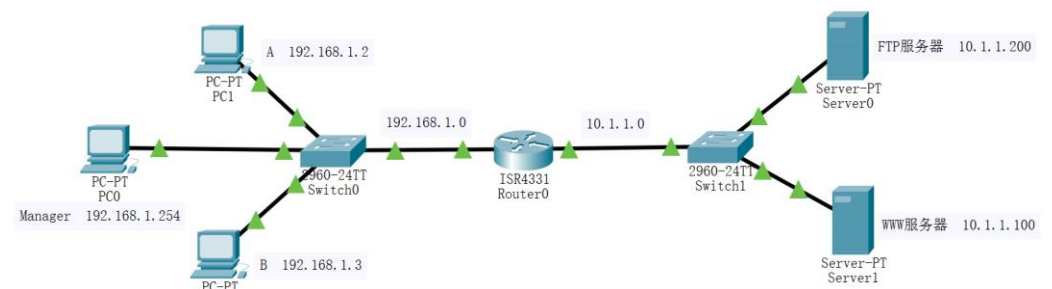
完成教材实例 8-4（P296），请写出步骤 1 安装与建立 FTP、WEB 的步骤，并完成 P297~P298 的测试要求。

### 【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)

## 实验拓扑结构和要求：



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。

- 客户机 A、B、C（Manager）连交换机 1 端口分别是 1、2、3
- 服务器 WWW 服务器（左） FTP 服务器（右） 连交换机 2 端口 2、1
- FTP：用户 hhh 密码 123456；用户 aaa 密码 123456



## 实验步骤:

### 分析:

本实验不同于以往的实验,不能直接通过 ping 验证访问控制列表的结果,因为我们使用的扩展访问列表可以限制数据包的类型,而 ping 为 ICMP 数据包,按照实验要求,我们需要在另两台 PC 上搭建 FTP 服务器和 WWW 服务器,二者可以分别通过软件 FileZilla 和 Apache 搭建。

实验要求的是基于时间的访问控制列表,对此,我们需要通过查看和修改路由器的时间来完成不同时间段的测试实验。

总言之,本实验的控制列表需要限制 IP、时间和服务类型(WWW 和 FTP)。

本实验的预期目标通题目要求所示,使得在这个网络下,Manager 可以在任意时间下访问两个服务器,而普通 PC 只能在上班时间访问 FTP,只能在下班时间访问 WWW。完成实验需要配置路由器的路由,并按题目需求配置 ACL,并在对应的端口上应用 ACL。

### 步骤 1:

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

如下表所示:

PC	PC1 (A)	PC2 (B)	PC Manager	WWW Server	FTP Server
IP 地址	192.168.1.2	192.168.1.3	192.168.1.254	10.1.1.100	10.1.1.200
子网掩码	255.255.255.0	255.255.255.0	255.255.255.0	255.0.0.0	255.0.0.0
网关	192.168.1.1	192.168.1.1	192.168.1.1	10.1.1.0	10.1.1.0

#### (2) 检查计算机与服务器的连通性。

根据网路拓扑结构,在未配置路由器时,路由器一端的无法 ping 通另一端的,但 PC1、PC2 和 Manager 通过交换机互通,两台服务器通过交换机互通,部分互 ping 截图如下:

```
C:\Users\Administrator>ping 192.168.1.254
正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=64

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.1.3
正在 Ping 192.168.1.3 具有 32 字节的数据:
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64

192.168.1.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 10.1.1.100
正在 Ping 10.1.1.100 具有 32 字节的数据:
请求超时。

10.1.1.100 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 0, 丢失 = 1 (100% 丢失),
    Control-C
^C

C:\Users\Administrator>ping 10.1.1.200
正在 Ping 10.1.1.200 具有 32 字节的数据:
请求超时。

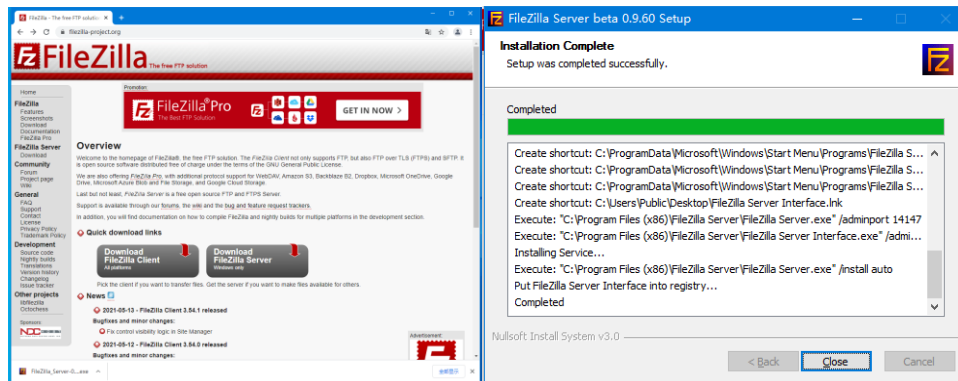
10.1.1.200 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 0, 丢失 = 1 (100% 丢失),
    Control-C
^C
```

(左图: PC1 ping PC2 和 Manager, ping 通, 右图: PC1 ping 两台服务器, 无法 ping 通)

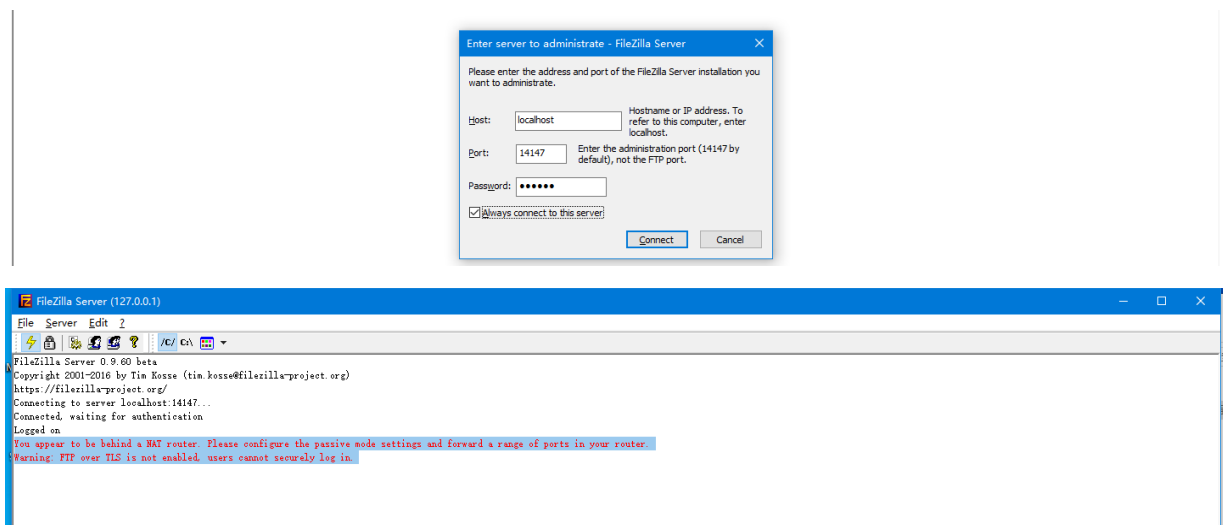
#### (3) 在服务器上安装 FTP 服务器和 WWW 服务器。FTP 服务器需至少创建一个用户名和口令。

##### ● FTP 服务器建立流程:

1. 下载 FileZilla: 网址 [filezilla-project.org](http://filezilla-project.org), 下载完成后安装。

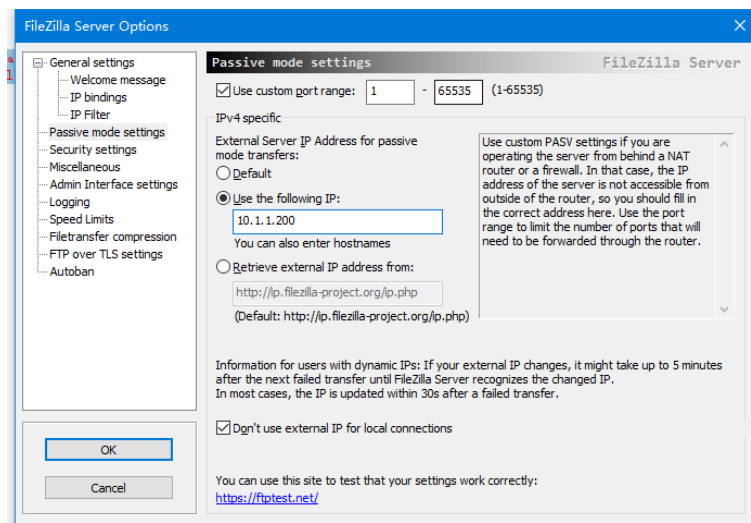


## 2. 配置服务器的管理密码和端口号

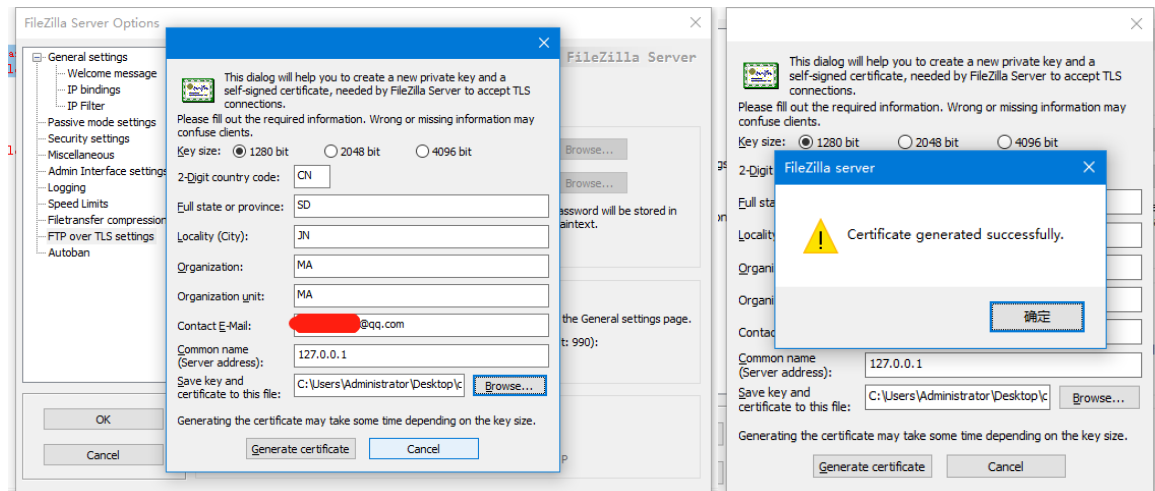


(返回配置成功)

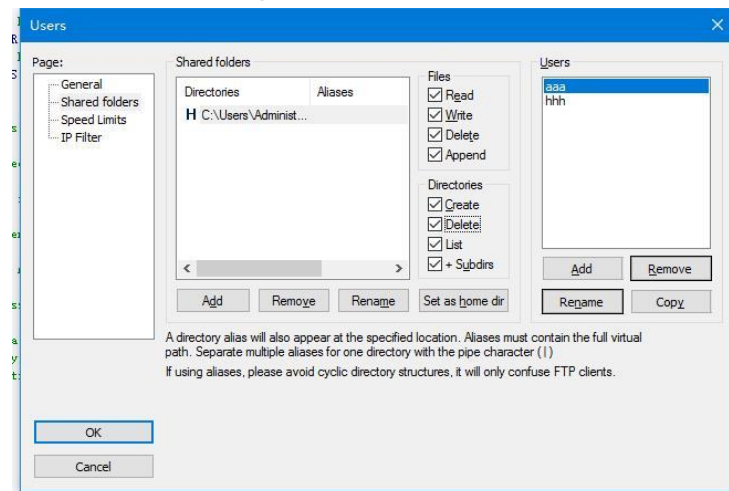
## 3. 直接点击设置-“Passive mode settings”选项卡，勾选“Use the following IP:”，填写服务器的 IP 地址，点击“OK”保存；



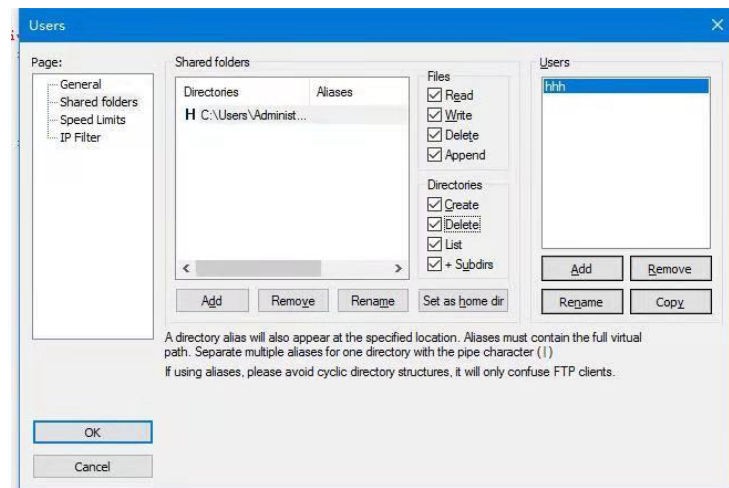
## 4. 生成一个新证书，服务器地址用机器的 ip；点击生成证书，然后提示成功；



5. 添加用户和密码；在实验中我们设置了用户 hhh 和用户 aaa，他们的密码都是 123456。hhh 给员工 PC（PC1 PC2）使用，aaa 由 Manager 使用。



6. 选择一个文件夹作为 FTP 的共享文件夹，将该目录设置为主目录。最后点击确定，完成配置



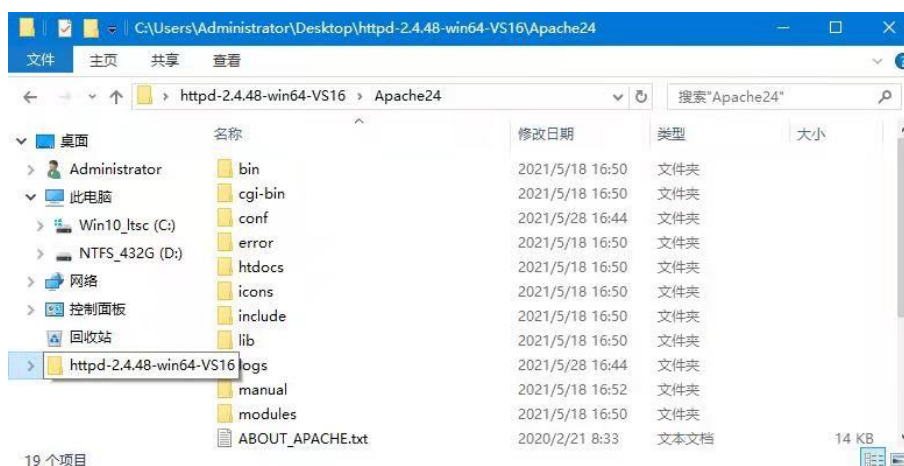
## ● WWW 服务器建立流程：

1. 网站 <https://www.apachelounge.com/download/> 下载 Apache，下载压缩文件，下载完成后使用 CMD 进行配置。



```
C:\Users\Administrator\Desktop>cd httpd-2.4.48-win64-VS16
C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16>cd Apache24
C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16\Apache24>cd bin
C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16\Apache24\bin>httpd -k install
Installing the 'Apache2.4' service
The 'Apache2.4' service is successfully installed.
Testing httpd.conf...
Errors reported here must be corrected before the service can be started.
httpd: Syntax error on line 39 of C:/Users/Administrator/Desktop/httpd-2.4.48-win64-VS16/Apache24/conf/httpd.conf: Se
rverRoot must be a valid directory
```

2. 进入 Apache 的 bin 文件夹执行命令 `httpd -k install`, 出现错误: Syntax error on line 39 of C:/Users/Administrator/Desktop/httpd-2.4.48-win64-VS16/Apache24/conf/httpd.conf: ServerRoot must be a valid directory。



3. 进入 `conf` 文件夹配置 `httpd.conf` 文件, 首先是修改路径:

```
27 #
28 # ServerRoot: The top of the directory tree under which the server's
29 # configuration, error, and log files are kept.
30 #
31 # Do not add a slash at the end of the directory path. If you point
32 # ServerRoot at a non-local disk, be sure to specify a local disk on the
33 # Mutex directive, if file-based mutexes are used. If you wish to share the
34 # same ServerRoot for multiple httpd daemons, you will need to change at
35 # least PidFile.
36 #
37 Define SRVROOT "C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16\Apache24"
38
39 ServerRoot "${SRVROOT}"
40
```

然后, 然后增加一行服务器网址 IP 配置:

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
ServerName localhost:80
#
```

否则会出现如下错误:

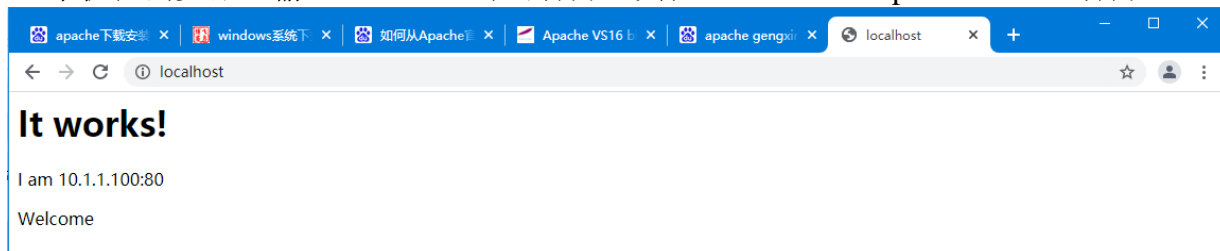




```
C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16\Apache24\bin>httpd.exe -w -n "Apache2.4" -k start
AH00558: httpd.exe: Could not reliably determine the server's fully qualified domain name, using fe80::143:124b:e64b:
c721. Set the 'ServerName' directive globally to suppress this message
(OS 10048)通常每个套接字地址(协议/网络地址/端口)只允许使用一次。 : AH00072: make_sock: could not bind to address [::
]:80
(OS 10048)通常每个套接字地址(协议/网络地址/端口)只允许使用一次。 : AH00072: make_sock: could not bind to address 0.0
.0.0:80
AH00451: no listening sockets available, shutting down
AH00015: Unable to open logs
Note the errors or messages above, and press the <ESC> key to exit. 19...
```

4. 最后保存配置文件，重新执行 `httpd -k install`，WWW 服务器建立成功，还可以修改 `index.html` 文件更新网页内容，如下图，会输出“I am 10.1.1.100:80 Welcome”的信息。

5. 本机在浏览器上输入 `localhost` 即可打开，其他 PC 上通过 `http://10.1.1.100` 打开。



## 步骤 2：路由器的基本配置

配置路由器，完成后检查路由表，如下图：

```
Router(config)#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.1.1.1/32 is local host.
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
Router(config)#
```

(配置路由器后的静态路由表)

## 步骤 3：验证当前配置

### (1) 验证主机与服务器的连通性

如下图，PC A 可以 ping 通 ftp 服务器和 www 服务机 ip，路由设置完毕。

```
C:\Users\Administrator>ping 10.1.1.100
正在 Ping 10.1.1.100 具有 32 字节的数据:
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=63

10.1.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 10.1.1.200
正在 Ping 10.1.1.200 具有 32 字节的数据:
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=63
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=63

10.1.1.200 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

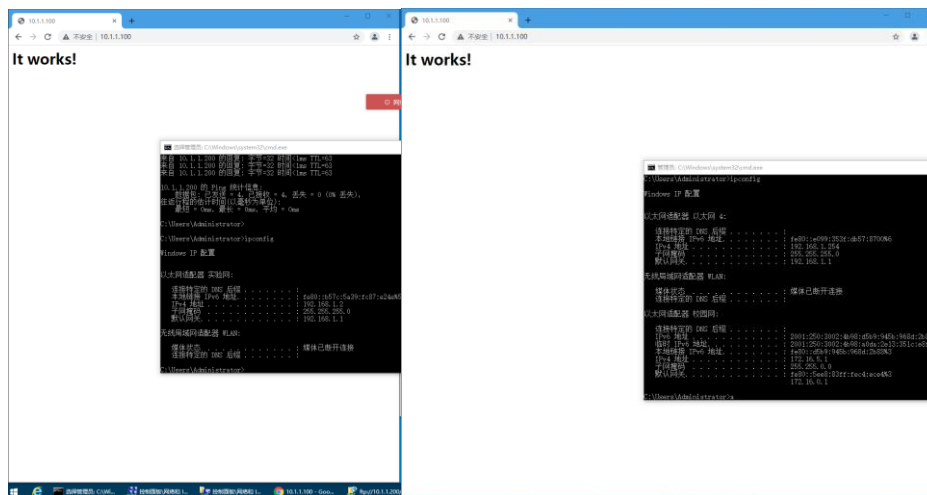
(2) 检查 Manager 和其他 PC 能否能登录 FTP 服务器，并通过 `http://10.1.1.100` 能否访问 WWW 服务器，判断目前效果是否达到预期，说明原因。

下图分别是员工机 PC1 和 Manager 经理机分别通过浏览器调用 WWW 服务器网址的



情景，都能访问，FTP 同理。但还不能达到不同 PC 规定时间和类型的访问控制预期。这部分截图较少，后续的实验步骤也可以说明 FTP 服务器和 WW 服务器在子网的成功搭建。

原因：在禁用校园网的情况下，通过路由器和交换机及其配置，整个拓扑结构是互通的，两台服务器也位于整个静态结构中，并且此时未设置任何访问控制，它们提供的服务，子网的其他客户机显然能获得。



(访问 WWW 服务器：左 PC1 右 PC Manager)

## 步骤 4：配置时间段

```
Router#con
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#time-range worktime
Router(config-time-range)#periodic weekdays 09:00 to 18:00
Router(config-time-range)#exit
```

## 步骤 5：配置 ACL

```
5-RSR20-2>en 14
Password:
5-RSR20-2#hostname Router
% Unknown command.

5-RSR20-2#config
Enter configuration commands, one per line. End with CNTL/Z.
5-RSR20-2(config)#hostname Router
Router(config)#in gi 0/0
Router(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
Router(config-if-GigabitEthernet 0/0)#exit
Router(config)#in gi 0/1
Router(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
Router(config-if-GigabitEthernet 0/1)#exit
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)#$ 10.1.1.100 eq www time-range work-time
Router(config-ext-nacl)#$ 10.1.1.100 eq www time-range work-time
Router(config-ext-nacl)#exit
Router(config)#in gi 0/0
Router(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
Router(config-if-GigabitEthernet 0/0)#*Mar 29 21:13:14: %ACL-6-NO_ACL_NAME: ACL accessctrl is not existed.
ip access-group accessctrl in
Router(config-if-GigabitEthernet 0/0)#end
Router#*Mar 29 21:13:31: %SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
ip access-list extended accessctrl
10 permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
20 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp time-range work-time (inactive)
30 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp-data time-range work-time (inactive)
40 deny tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www time-range work-time (inactive)
50 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www
Router#show clock
21:13:56 UTC Sun, Mar 29, 1970
Router#
```

(图为访问控制配置全程，红框部分为步骤 5 - ACL 配置)

## 步骤 6：应用 ACL

```
Router(config)#in gi 0/0
Router(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
Router(config-if-GigabitEthernet 0/0)#end
Router#*May 27 23:16:44: %SYS-5-CONFIG_I: Configured from console by console
```



```
Router#show access-list
```

```
ip access-list extended accessctrl
10 permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
20 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp time-range work-time (active)
30 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp-data time-range work-time (active)
40 deny tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www time-range work-time (active)
50 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq www
Router#
```

(查看 ACL)

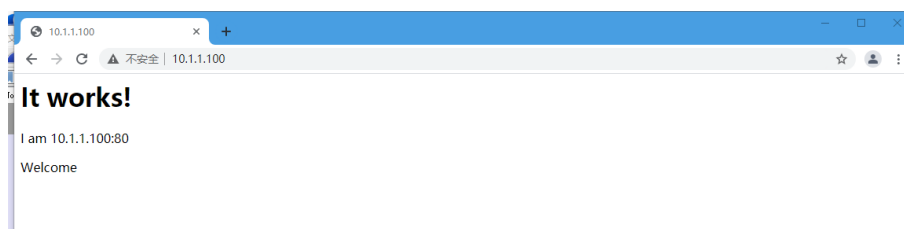
## 步骤 7: 验证测试

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

```
Router#show clock
23:19:50 UTC Thu, May 27, 2021
```

(如图显示为周四 23:19:50, 下班时间)

(2) 主机 Manager 使用步骤 1 建立的用户名登陆 FTP 服务器, 并通过 <https://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。



(Manager 访问 WWW 服务器, 可以访问)

No.	Time	Source	Destination	Protocol	Length	Info
45	3.866581	192.168.1.254	10.1.1.100	TCP	66	1418 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
46	3.866644	192.168.1.254	10.1.1.100	TCP	66	1419 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
47	3.866936	10.1.1.100	192.168.1.254	TCP	70	80 → 1418 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
48	3.866976	192.168.1.254	10.1.1.100	TCP	54	1418 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
49	3.866994	10.1.1.100	192.168.1.254	TCP	70	80 → 1419 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
50	3.867012	192.168.1.254	10.1.1.100	TCP	54	1419 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
52	3.898003	192.168.1.254	10.1.1.100	HTTP	423	GET /favicon.ico HTTP/1.1
53	3.891972	10.1.1.100	192.168.1.254	HTTP	470	HTTP/1.1 404 Not Found (text/html)
56	3.141984	192.168.1.254	10.1.1.100	TCP	54	1418 → 80 [ACK] Seq=368 Ack=413 Win=525056 Len=0
135	8.892540	10.1.1.100	192.168.1.254	TCP	64	80 → 1418 [FIN, ACK] Seq=413 Ack=368 Win=525568 Len=0
136	8.892589	192.168.1.254	10.1.1.100	TCP	54	1418 → 80 [ACK] Seq=368 Ack=414 Win=525056 Len=0
231	20.847863	192.168.1.254	10.1.1.100	TCP	54	1418 → 80 [FIN, ACK] Seq=368 Ack=414 Win=525056 Len=0
232	20.848091	10.1.1.100	192.168.1.254	TCP	64	80 → 1418 [ACK] Seq=414 Ack=369 Win=525568 Len=0
316	48.066812	192.168.1.254	10.1.1.100	TCP	55	[TCP Keep-Alive] 1419 → 80 [ACK] Seq=0 Ack=1 Win=525568 Len=1
317	48.067267	10.1.1.100	192.168.1.254	TCP	70	[TCP Window Update] 80 → 1419 [ACK] Seq=1 Ack=1 Win=525568 Len=0 SLE=0 SRE=1
368	63.067471	10.1.1.100	192.168.1.254	TCP	64	80 → 1419 [FIN, ACK] Seq=1 Ack=1 Win=525568 Len=0
369	63.067532	192.168.1.254	10.1.1.100	TCP	54	1419 → 80 [ACK] Seq=1 Ack=2 Win=525568 Len=0

(对访问 WWW 服务器过程抓包, 可以捕获到 HTTP 报文, 看到 GET 命令)

```
C:\Users\Administrator>ftp
ftp> open 10.1.1.200
连接到 10.1.1.200。
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
用户(10.1.1.200:(none)): aaa
331 Password required for aaa
密码:
230 Logged on
```

(DOS 访问 FTP 服务器, 可以访问)

No.	Time	Source	Destination	Protocol	Length	Info
710	132.114399	192.168.1.254	10.1.1.200	TCP	66	1586 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
711	132.114829	10.1.1.200	192.168.1.254	TCP	70	21 → 1586 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
712	132.114864	192.168.1.254	10.1.1.200	TCP	54	1586 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
713	132.115979	10.1.1.200	192.168.1.254	FTP	201	Response: 220-FileZilla Server 0.9.60 beta
714	132.125108	192.168.1.254	10.1.1.200	FTP	68	Request: OPTS UTF8 ON
715	132.125493	10.1.1.200	192.168.1.254	FTP	122	Response: 202 UTF8 mode is always enabled. No need to send this command.
716	132.176756	192.168.1.254	10.1.1.200	TCP	54	1586 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
729	135.194204	192.168.1.254	10.1.1.200	FTP	64	Request: USER aaa
730	135.194701	10.1.1.200	192.168.1.254	FTP	89	Response: 331 Password required for aaa
731	135.244689	192.168.1.254	10.1.1.200	TCP	54	1586 → 21 [ACK] Seq=25 Ack=239 Win=7954 Len=0
761	139.283159	192.168.1.254	10.1.1.200	FTP	67	Request: PASS 123456
762	139.284081	10.1.1.200	192.168.1.254	FTP	73	Response: 230 Logged on
763	139.334237	192.168.1.254	10.1.1.200	TCP	54	1586 → 21 [ACK] Seq=38 Ack=254 Win=7939 Len=0

(访问 FTP 捕获数据包, 可以看到 USER PASS 的登录过程报文)

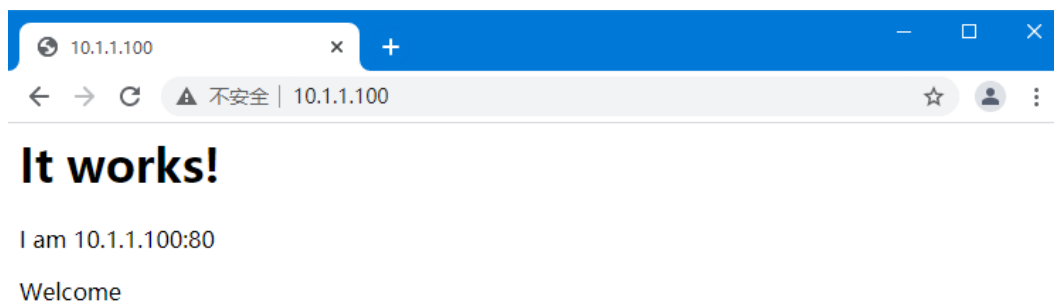




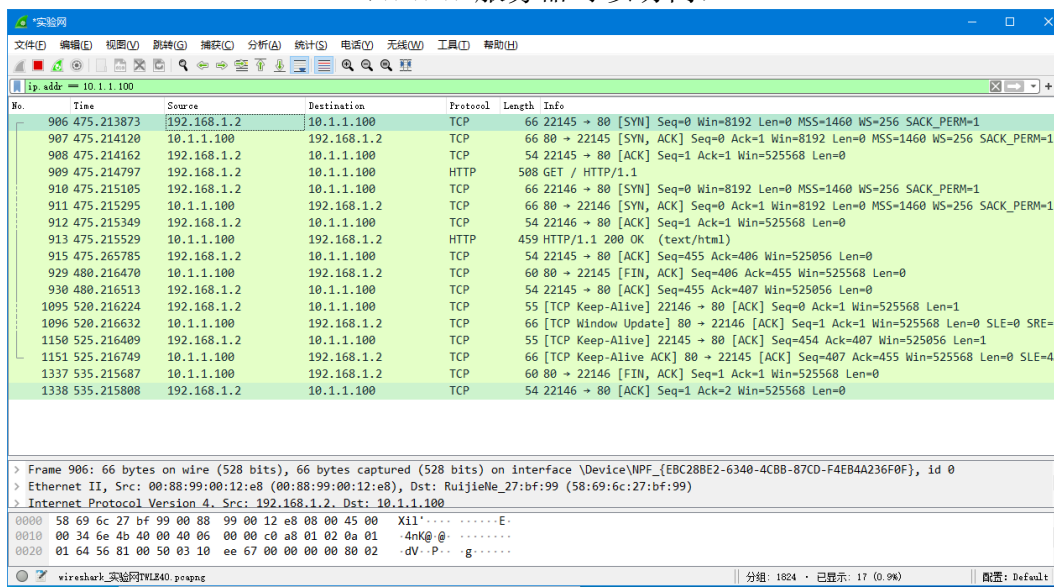
(IE 浏览器访问 FTP 服务器，可以访问)

(3) 用户机 A、B 分别使用步骤 1 建立的用户名登陆 FTP 服务器，并通过 <https://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（登录 FTP 时分别通过 DOS 和浏览器方式，结合捕获报文分析）。

● 用户机 A (PC1) 下班时间访问服务器情况：



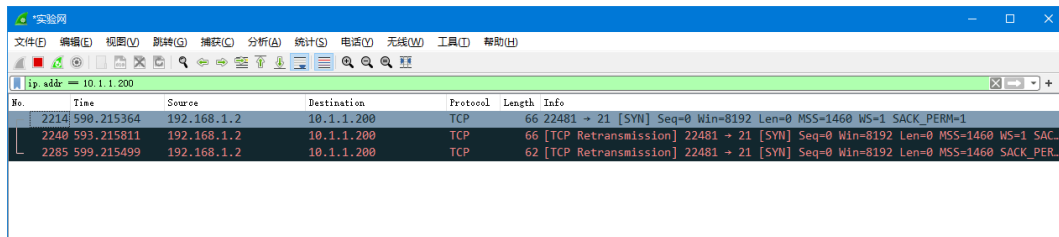
(WWW 服务器可以访问)



(PC1 访问 WWW 服务器过程抓包)

报文分析：分析 HTTP 数据报，GET（第四行）和 HTTP/1.1 200 OK（第八行）还可以捕获 TCP Keep Alive（保持连接）和 Window Update（刷新网页）的数据包。

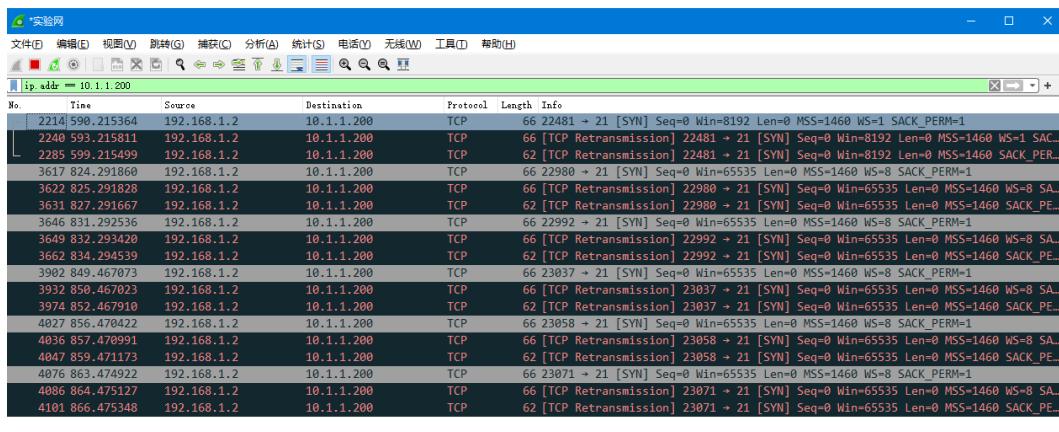




No.	Time	Source	Destination	Protocol	Length	Info
2214	590.215364	192.168.1.2	10.1.1.200	TCP	66	22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
2240	593.215811	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
2285	599.215499	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

(DOS 访问 FTP 服务器和抓包)

报文分析: DOS 访问 FTP 服务器, 无法访问, 可以捕获到 PC1 发向 FTP 服务器的包, 但服务器没有回应。

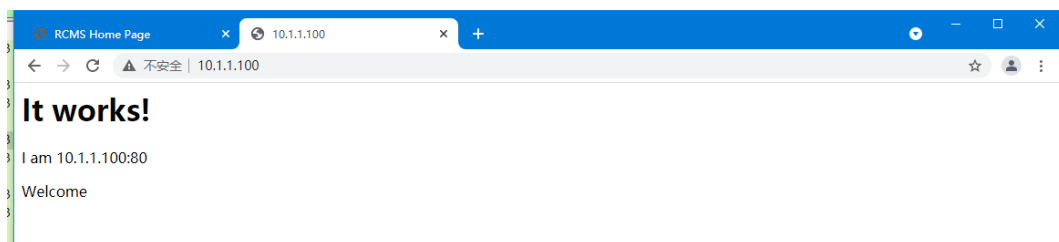


No.	Time	Source	Destination	Protocol	Length	Info
2214	590.215364	192.168.1.2	10.1.1.200	TCP	66	22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
2240	593.215811	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
2285	599.215499	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 22481 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
3617	824.291060	192.168.1.2	10.1.1.200	TCP	66	22980 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3622	825.291828	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 22980 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3631	827.291667	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 22980 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
3646	831.292536	192.168.1.2	10.1.1.200	TCP	66	22992 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3649	832.293420	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 22992 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3662	834.294539	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 22992 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
3902	849.467073	192.168.1.2	10.1.1.200	TCP	66	23037 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3932	850.467023	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 23037 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
3974	852.467910	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 23037 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
4027	856.470422	192.168.1.2	10.1.1.200	TCP	66	23058 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
4036	857.470991	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 23058 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
4047	859.471173	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 23058 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
4076	863.474922	192.168.1.2	10.1.1.200	TCP	66	23071 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
4086	864.475127	192.168.1.2	10.1.1.200	TCP	66	[TCP Retransmission] 23071 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
4101	866.475348	192.168.1.2	10.1.1.200	TCP	62	[TCP Retransmission] 23071 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

(IE 浏览器访问 FTP 服务器和抓包)

报文分析: FTP 服务器无法访问, 可以捕获到 PC1 发往服务器的 Retransmission 报文, 而 FTP 服务器没有回应。多次刷新, 可以看到每次发送一个 TCP SYN 包和两个 Retransmission 重发包。

## ● 用户机 B (PC2) 下班时间访问服务器情况:



(WWW 服务器可以访问)



No.	Time	Source	Destination	Protocol	Length	Info
121	16.778994	192.168.1.3	10.1.1.100	TCP	66	2383 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
122	16.779475	10.1.1.100	192.168.1.3	TCP	70	80 → 2383 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
123	16.779509	192.168.1.3	10.1.1.100	TCP	54	2383 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
124	16.779673	192.168.1.3	10.1.1.100	HTTP	501	GET / HTTP/1.1
125	16.780650	10.1.1.100	192.168.1.3	HTTP	463	HTTP/1.1 200 OK (text/html)
127	16.831374	192.168.1.3	10.1.1.100	TCP	54	2383 → 80 [ACK] Seq=448 Ack=406 Win=525056 Len=0
131	17.279023	192.168.1.3	10.1.1.100	TCP	66	2386 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
132	17.279424	10.1.1.100	192.168.1.3	TCP	70	80 → 2386 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
133	17.279483	192.168.1.3	10.1.1.100	TCP	54	2386 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
147	18.859302	192.168.1.3	10.1.1.100	HTTP	421	GET /favicon.ico HTTP/1.1
148	18.860461	10.1.1.100	192.168.1.3	HTTP	469	HTTP/1.1 404 Not Found (text/html)
149	18.910709	192.168.1.3	10.1.1.100	TCP	54	2383 → 80 [ACK] Seq=815 Ack=817 Win=524544 Len=0
174	23.860498	10.1.1.100	192.168.1.3	TCP	64	80 → 2383 [FIN, ACK] Seq=817 Ack=815 Win=525056 Len=0
175	23.860576	192.168.1.3	10.1.1.100	TCP	54	2383 → 80 [ACK] Seq=815 Ack=818 Win=524544 Len=0
495	62.280521	192.168.1.3	10.1.1.100	TCP	55	[TCP Keep-Alive] 2386 → 80 [ACK] Seq=0 Ack=1 Win=525568 Len=1
496	62.280972	10.1.1.100	192.168.1.3	TCP	70	[TCP Window Update] 80 → 2386 [ACK] Seq=1 Ack=1 Win=525568 Len=0 SLE=0 SRE=1
511	68.861074	192.168.1.3	10.1.1.100	TCP	55	[TCP Keep-Alive] 2383 → 80 [ACK] Seq=814 Ack=818 Win=524544 Len=1
512	68.861402	10.1.1.100	192.168.1.3	TCP	70	[TCP Keep-Alive ACK] 80 → 2383 [ACK] Seq=818 Ack=815 Win=525056 Len=0 SLE=814 SRE=815
553	77.279812	10.1.1.100	192.168.1.3	TCP	55	[TCP Keep-Alive] 2386 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
554	77.279876	192.168.1.3	10.1.1.100	TCP	54	2386 → 80 [ACK] Seq=1 Ack=2 Win=525568 Len=0
675	113.862193	192.168.1.3	10.1.1.100	TCP	55	[TCP Keep-Alive] 2383 → 80 [ACK] Seq=814 Ack=818 Win=524544 Len=1
676	113.862635	10.1.1.100	192.168.1.3	TCP	70	[TCP Keep-Alive ACK] 80 → 2383 [ACK] Seq=818 Ack=815 Win=525056 Len=0 SLE=814 SRE=815
693	122.279478	192.168.1.3	10.1.1.100	TCP	55	[TCP Keep-Alive] 2386 → 80 [ACK] Seq=0 Ack=2 Win=525568 Len=1
694	122.280006	10.1.1.100	192.168.1.3	TCP	70	[TCP Keep-Alive ACK] 80 → 2386 [ACK] Seq=2 Ack=1 Win=525568 Len=0 SLE=0 SRE=1

(PC2 访问 WWW 服务器过程抓包)

No.	Time	Source	Destination	Protocol	Length	Info
4	7.478634	192.168.1.3	10.1.1.200	TCP	54	2114 → 21 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
C:\Windows\system32\cmd.exe - ftp
> ftp: connect :软件造成连接中止
ftp> quit
C:\Users\Administrator>ftp
ftp> open 10.1.1.200
连接到 10.1.1.200.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
用户(10.1.1.200:(none)): aaa
331 Password required for aaa
密码:
230 Logged on
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
test.txt
226 Successfully transferred "/"
ftp: 收到 13 字节, 用时 0.00秒 6.50千字节/秒。
ftp> quit
421 Connection timed out.
C:\Users\Administrator>ftp
ftp> quit
C:\Users\Administrator>ftp
ftp> open 10.1.1.200
> ftp: connect :连接超时
ftp>
```

(DOS 访问 FTP 服务器)

报文分析: DOS 访问 FTP 服务器, 无法访问, 可以捕获到 PC2 发向 FTP 服务器的包, 但服务器没有回应。

No.	Time	Source	Destination	Protocol	Length	Info
139	88.578058	192.168.1.3	10.1.1.200	TCP	66	2608 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 SACK_PERM=1
172	89.578736	192.168.1.3	10.1.1.200	TCP	66	[TCP Retransmission] 2608 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 SACK_PERM=1
205	91.579534	192.168.1.3	10.1.1.200	TCP	62	[TCP Retransmission] 2608 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
236	95.582241	192.168.1.3	10.1.1.200	TCP	66	2614 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 SACK_PERM=1
239	96.582935	192.168.1.3	10.1.1.200	TCP	66	[TCP Retransmission] 2614 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 SACK_PERM=1
260	98.583664	192.168.1.3	10.1.1.200	TCP	62	[TCP Retransmission] 2614 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

(IE 浏览器访问 FTP 服务器和抓包)

报文分析: FTP 服务器无法访问, 可以捕获到 PC2 发往服务器的 Retransmission 报文, 而 FTP 服务器没有回应。

小结: PC1 的访问权限与 PC2 一致, 可以看到在下班时间, 都不能访问 FTP 服务器, 而可以访问 WWW 服务器, 而对于 Manager, 他在下班时间既可以访问 FTP 服务器, 又可以访问 WWW 服务器。



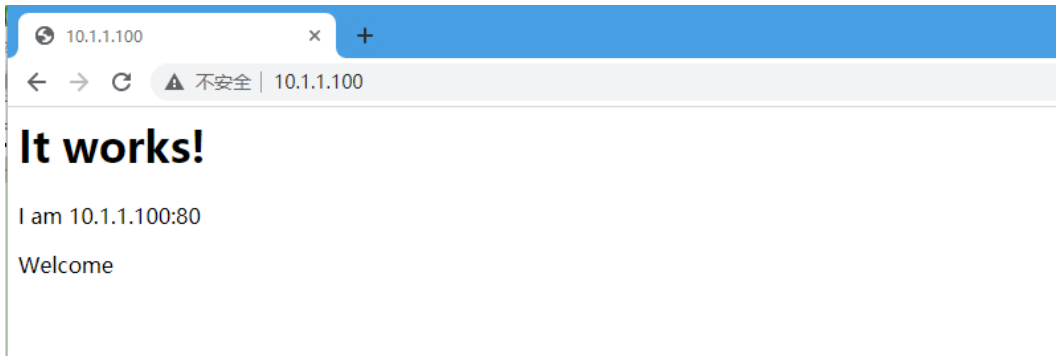
(4) 改变路由器系统的时间段，执行(2)~(3)都测试。

- 修改路由器时间：修改为上午 10 点，即上班时间。

```
Router#clock set 10:00:00 5 27 2021
Router#May 27 10:00:00: %SYS-6-CLOCKUPDATE: System clock has been updated to 10:00:00 UTC Thu May 27 2021.

Router#show clock
10:00:06 UTC Thu, May 27, 2021
Router#
```

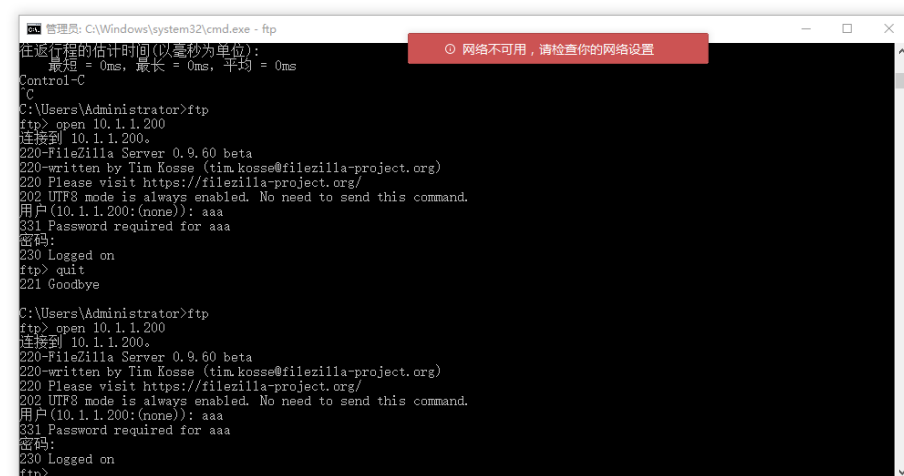
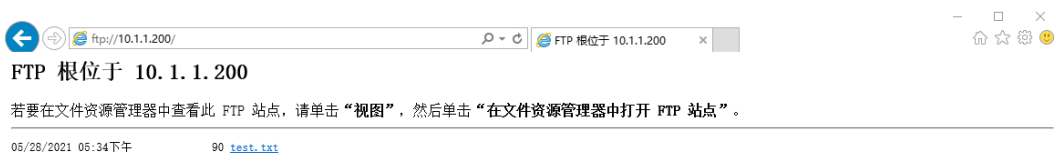
- Manager 上班时间访问服务器情况：



(WWW 服务器可以访问)

No.	Time	Source	Destination	Protocol	Length	Info
103	10.003519	192.168.1.254	10.1.1.100	TCP	66	3179 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
104	10.003601	192.168.1.254	10.1.1.100	TCP	66	3180 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
105	10.003871	10.1.1.100	192.168.1.254	TCP	70	80 → 3179 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
106	10.003914	192.168.1.254	10.1.1.100	TCP	54	3179 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
107	10.003933	10.1.1.100	192.168.1.254	TCP	70	80 → 3180 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
108	10.003951	192.168.1.254	10.1.1.100	TCP	54	3180 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
110	10.029642	192.168.1.254	10.1.1.100	HTTP	421	GET /favicon.ico HTTP/1.1
111	10.030751	10.1.1.100	192.168.1.254	HTTP	470	HTTP/1.1 404 Not Found (text/html)
113	10.080916	192.168.1.254	10.1.1.100	TCP	54	3179 → 80 [ACK] Seq=368 Ack=413 Win=525056 Len=0
203	15.031048	10.1.1.100	192.168.1.254	TCP	64	80 → 3179 [FIN, ACK] Seq=413 Ack=368 Win=525568 Len=0
204	15.031129	192.168.1.254	10.1.1.100	TCP	54	3179 → 80 [ACK] Seq=368 Ack=414 Win=525056 Len=0
230	16.626851	192.168.1.254	10.1.1.100	TCP	54	3179 → 80 [FIN, ACK] Seq=368 Ack=414 Win=525056 Len=0
231	16.627279	10.1.1.100	192.168.1.254	TCP	64	80 → 3179 [ACK] Seq=414 Ack=369 Win=525568 Len=0

(Manager 访问 WWW 服务器过程抓包)



(DOS 访问 FTP 服务器，IE 浏览器访问 FTP 服务器)

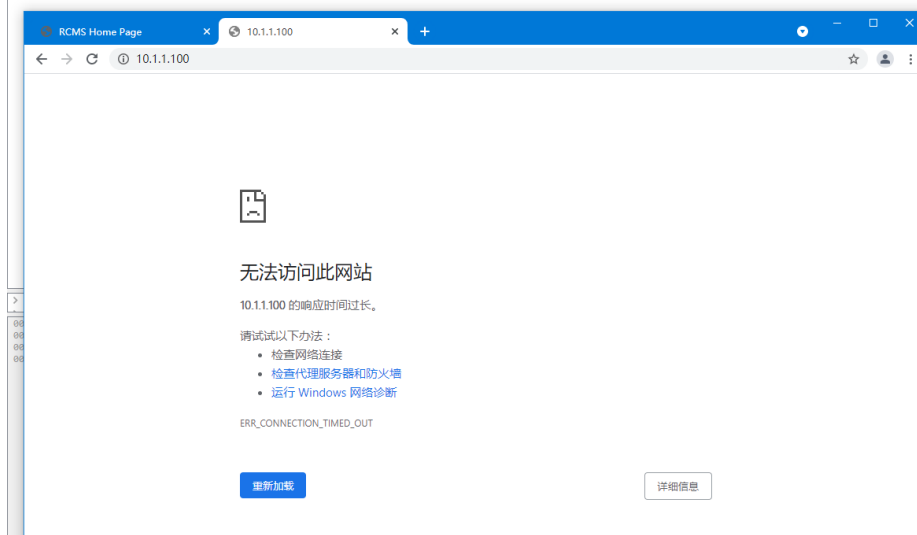


No.	Time	Source	Destination	Protocol	Length	Info
625	84.594539	192.168.1.254	10.1.1.200	TCP	66	3248 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
626	84.594957	10.1.1.200	192.168.1.254	TCP	70	21 → 3248 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
627	84.594997	192.168.1.254	10.1.1.200	TCP	54	3248 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
628	84.596132	10.1.1.200	192.168.1.254	FTP	201	Response: 220-FileZilla Server 0.9.60 beta
629	84.603467	192.168.1.254	10.1.1.200	FTP	68	Request: OPTS UTF8 ON
630	84.603866	10.1.1.200	192.168.1.254	FTP	122	Response: 202 UTF8 mode is always enabled. No need to send this command.
652	84.654427	192.168.1.254	10.1.1.200	TCP	54	3248 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
713	86.066490	192.168.1.254	10.1.1.200	FTP	64	Request: USER aaa
714	86.067099	10.1.1.200	192.168.1.254	FTP	89	Response: 331 Password required for aaa
715	86.117827	192.168.1.254	10.1.1.200	TCP	54	3248 → 21 [ACK] Seq=25 Ack=239 Win=7954 Len=0
808	89.883383	192.168.1.254	10.1.1.200	FTP	67	Request: PASS 123456
809	89.884370	10.1.1.200	192.168.1.254	FTP	73	Response: 230 Logged on
810	89.934586	192.168.1.254	10.1.1.200	TCP	54	3248 → 21 [ACK] Seq=38 Ack=254 Win=7939 Len=0

(访问 FTP 抓包，有 USER、PASS 还有 230 Logged On 的成功登录返回)

## ● 用户机 A (PC1) 上班时间访问服务器情况:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	10.1.1.100	TCP	62	3229 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
18	3.429236	192.168.1.3	10.1.1.100	TCP	66	3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	6.429846	192.168.1.3	10.1.1.100	TCP	66	[TCP Retransmission] 3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	12.430665	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
58	12.776866	192.168.1.3	10.1.1.100	TCP	66	3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
70	15.777203	192.168.1.3	10.1.1.100	TCP	66	[TCP Retransmission] 3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92	21.777691	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3240 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
123	29.441390	192.168.1.3	10.1.1.100	TCP	66	3262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
140	32.442463	192.168.1.3	10.1.1.100	TCP	66	[TCP Retransmission] 3262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
160	38.443022	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1



(WWW 服务器不可以访问与抓包)

No.	Time	Source	Destination	Protocol	Length	Info
47	5.381393	192.168.1.3	10.1.1.200	TCP	66	2891 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
48	5.381692	10.1.1.200	192.168.1.3	TCP	70	21 → 2891 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
49	5.381734	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
50	5.382345	10.1.1.200	192.168.1.3	FTP	201	Response: 220-FileZilla Server 0.9.60 beta
51	5.391857	192.168.1.3	10.1.1.200	FTP	68	Request: OPTS UTF8 ON
54	5.392280	10.1.1.200	192.168.1.3	FTP	122	Response: 202 UTF8 mode is always enabled. No need to send this command.
55	5.442377	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
83	11.157087	192.168.1.3	10.1.1.200	FTP	64	Request: USER aaa
84	11.157718	10.1.1.200	192.168.1.3	FTP	89	Response: 331 Password required for aaa
85	11.207743	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=25 Ack=239 Win=7954 Len=0
99	13.286109	192.168.1.3	10.1.1.200	FTP	67	Request: PASS 123456
100	13.287026	10.1.1.200	192.168.1.3	FTP	73	Response: 230 Logged on
101	13.326917	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=38 Ack=254 Win=7939 Len=0
115	15.365406	192.168.1.3	10.1.1.200	FTP	78	Request: PORT 192,168,1,3,11,93
116	15.366152	10.1.1.200	192.168.1.3	FTP	87	Response: 200 Port command successful
117	15.369304	192.168.1.3	10.1.1.200	FTP	60	Request: NLST
118	15.370469	10.1.1.200	192.168.1.3	TCP	70	20 → 2909 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
119	15.370549	192.168.1.3	10.1.1.200	TCP	66	2909 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
120	15.370564	10.1.1.200	192.168.1.3	FTP	113	Response: 150 Opening data channel for directory listing of "/"
121	15.370746	10.1.1.200	192.168.1.3	TCP	64	20 → 2909 [ACK] Seq=1 Ack=1 Win=525568 Len=0
122	15.371013	10.1.1.200	192.168.1.3	FTP-DATA	68	FTP Data: 10 bytes (PORT) (NLST)
123	15.371038	10.1.1.200	192.168.1.3	TCP	64	20 → 2909 [FIN, ACK] Seq=11 Ack=1 Win=525568 Len=0
124	15.371050	192.168.1.3	10.1.1.200	TCP	54	2909 → 20 [ACK] Seq=1 Ack=12 Win=525568 Len=0
125	15.371166	10.1.1.200	192.168.1.3	FTP	92	Response: 226 Successfully transferred "/"
126	15.371176	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=68 Ack=372 Win=7821 Len=0
127	15.373554	192.168.1.3	10.1.1.200	TCP	54	2909 → 20 [FIN, ACK] Seq=1 Ack=12 Win=525568 Len=0
128	15.373837	10.1.1.200	192.168.1.3	TCP	64	20 → 2909 [ACK] Seq=12 Ack=2 Win=525568 Len=0
354	55.901128	192.168.1.3	10.1.1.200	FTP	60	Request: QUIT
355	55.901857	10.1.1.200	192.168.1.3	FTP	71	Response: 221 Goodbye
356	55.901857	10.1.1.200	192.168.1.3	TCP	64	21 → 2891 [FIN, ACK] Seq=385 Ack=74 Win=525312 Len=0
357	55.901902	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [ACK] Seq=74 Ack=386 Win=7808 Len=0
358	55.903329	192.168.1.3	10.1.1.200	TCP	54	2891 → 21 [FIN, ACK] Seq=74 Ack=386 Win=7808 Len=0
359	55.903461	10.1.1.200	192.168.1.3	TCP	64	21 → 2891 [ACK] Seq=386 Ack=75 Win=525312 Len=0

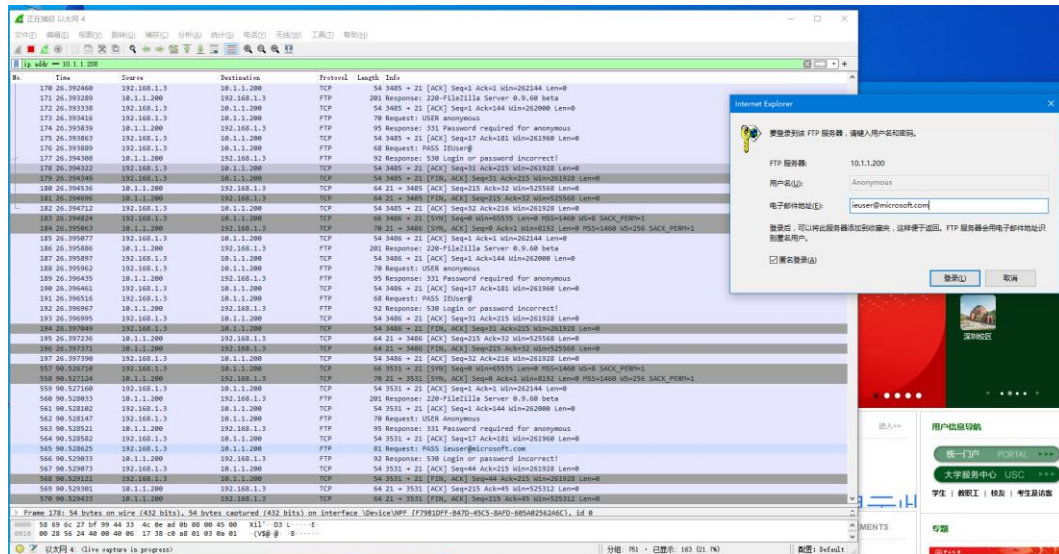
```
C:\Windows\system32\cmd.exe
> Frame 124
C:\Users\Administrator>ftp
ftp> open 10.1.1.200
0000 58 69 连接到 10.1.1.200。
0010 00 28 220-FileZilla Server 0.9.60 beta
0020 01 c8 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
0030 08 05 220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
用户(10.1.1.200:(none)): aaa
331 Password required for aaa
密码:
230 Logged on
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
test.txt
226 Successfully transferred "/"
ftp> 收到 13 字节, 用时 0.00秒 13.00千字节/秒。
ftp> quit
221 Goodbye
```





# 计算机网络实验报告

(DOS 访问 FTP 服务器和抓包)



(IE 浏览器访问 FTP 服务器和抓包)

报文分析：如图，IE 浏览器也可以通过用户名登录 FTP 服务器，浏览器会弹出窗口填写账户和密码，我们尝试错误的账号密码，FTP 服务器返回错误信息：“530 Login or password incorrect”。

## ● 用户机 B (PC2) 下班时间访问服务器情况：



(WWW 服务器不可以访问)



No.	Time	Source	Destination	Protocol	Length	Info
67	8.775748	192.168.1.2	10.1.1.100	TCP	66	24420 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	8.776096	192.168.1.2	10.1.1.100	TCP	66	24421 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	9.026339	192.168.1.2	10.1.1.100	TCP	66	24423 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
161	11.776308	192.168.1.2	10.1.1.100	TCP	66	[TCP Retransmission] 24421 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
162	11.776315	192.168.1.2	10.1.1.100	TCP	66	[TCP Retransmission] 24420 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
165	12.026055	192.168.1.2	10.1.1.100	TCP	66	[TCP Retransmission] 24423 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
241	17.777079	192.168.1.2	10.1.1.100	TCP	62	[TCP Retransmission] 24420 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
242	17.777080	192.168.1.2	10.1.1.100	TCP	62	[TCP Retransmission] 24421 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
246	18.026097	192.168.1.2	10.1.1.100	TCP	62	[TCP Retransmission] 24423 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

(PC2 访问 WWW 服务器过程抓包)

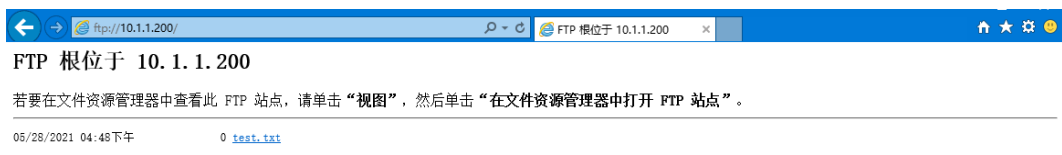
报文分析：出现若干 Retransmission 重发包，从 PC2 发往 FTP 服务器，服务器没有回应。

```
C:\Users\Administrator>ftp
ftp> open 10.1.1.200
连接到 10.1.1.200。
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
用户(10.1.1.200:(none)): hhh
331 Password required for hhh
密码:
230 Logged on
ftp> quit
221 Goodbye
```

No.	Time	Source	Destination	Protocol	Length	Info
3415	375.900893	192.168.1.2	10.1.1.200	TCP	66	24328 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
3416	375.901435	10.1.1.200	192.168.1.2	TCP	66	21 → 24328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3417	375.901484	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
3418	375.902434	10.1.1.200	192.168.1.2	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
3419	375.912299	192.168.1.2	10.1.1.200	FTP	68	Request: OPTS UTF8 ON
3420	375.912503	192.168.1.2	10.1.1.200	FTP	118	Response: 202 UTF8 mode is always enabled. No need to send this command.
3423	375.962861	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [ACK] Seq=15 Ack=208 Win=7985 Len=0
3432	378.796245	192.168.1.2	10.1.1.200	FTP	64	Request: USER hhh
3433	378.796847	10.1.1.200	192.168.1.2	FTP	85	Response: 331 Password required for hhh
3434	378.846770	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [ACK] Seq=25 Ack=239 Win=7954 Len=0
3437	380.380529	192.168.1.2	10.1.1.200	FTP	67	Request: PASS 123456
3438	380.381391	10.1.1.200	192.168.1.2	FTP	69	Response: 230 Logged on
3439	380.431657	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [ACK] Seq=38 Ack=254 Win=7939 Len=0
3446	383.396316	192.168.1.2	10.1.1.200	FTP	60	Request: QUIT
3447	383.396895	10.1.1.200	192.168.1.2	FTP	67	Response: 221 Goodbye
3448	383.397137	10.1.1.200	192.168.1.2	TCP	60	21 → 24328 [FIN, ACK] Seq=267 Ack=44 Win=525312 Len=0
3449	383.397162	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [ACK] Seq=44 Ack=268 Win=7926 Len=0
3450	383.399547	192.168.1.2	10.1.1.200	TCP	54	24328 → 21 [FIN, ACK] Seq=44 Ack=268 Win=7926 Len=0
3451	383.399733	10.1.1.200	192.168.1.2	TCP	60	21 → 24328 [ACK] Seq=268 Ack=45 Win=525312 Len=0

(DOS 访问 FTP 服务器和抓包)

报文分析：使用用户名 hhh 进行登录，登陆成功（返回包：“230 Logged on”），最后 DOS 下输入 quit，发出 QUIT 包，随后服务器返回“221 Goodbye”。





No.	Time	Source	Destination	Protocol	Length	Info
1279	101.987855	10.1.1.200	192.168.1.2	TCP	60	21 → 24657 [ACK] Seq=215 Ack=32 Win=525568 Len=0
1280	101.987884	192.168.1.2	10.1.1.200	TCP	54	24657 → 21 [RST, ACK] Seq=32 Ack=215 Win=0 Len=0
1281	101.987905	192.168.1.2	10.1.1.200	TCP	66	24658 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
1282	101.988038	10.1.1.200	192.168.1.2	TCP	60	21 → 24657 [FIN, ACK] Seq=215 Ack=32 Win=525568 Len=0
1283	101.988048	192.168.1.2	10.1.1.200	TCP	54	24657 → 21 [RST] Seq=32 Win=0 Len=0
1284	101.988224	10.1.1.200	192.168.1.2	TCP	66	21 → 24658 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1285	101.988247	192.168.1.2	10.1.1.200	TCP	54	24658 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1286	101.988946	10.1.1.200	192.168.1.2	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
1287	101.989036	192.168.1.2	10.1.1.200	TCP	54	24658 → 21 [ACK] Seq=1 Ack=144 Win=262000 Len=0
1288	101.989059	192.168.1.2	10.1.1.200	FTP	70	Request: USER anonymous
1289	101.989509	10.1.1.200	192.168.1.2	FTP	91	Response: 331 Password required for anonymous
1290	101.989529	192.168.1.2	10.1.1.200	TCP	54	24658 → 21 [ACK] Seq=17 Ack=181 Win=261960 Len=0
1291	101.989547	192.168.1.2	10.1.1.200	FTP	68	Request: PASS IEUser@
1292	101.990104	10.1.1.200	192.168.1.2	FTP	88	Response: 530 Login or password incorrect!
1293	101.990122	192.168.1.2	10.1.1.200	TCP	54	24658 → 21 [ACK] Seq=31 Ack=215 Win=261928 Len=0
1294	101.990136	192.168.1.2	10.1.1.200	TCP	54	24658 → 21 [FIN, ACK] Seq=31 Ack=215 Win=261928 Len=0
1295	101.990468	10.1.1.200	192.168.1.2	TCP	60	21 → 24658 [ACK] Seq=215 Ack=32 Win=525568 Len=0

(IE 浏览器访问 FTP 服务器和抓包)

报文分析：红色的 TCP 包为刷新 ftp 网页导致，用与重新与 ftp 服务器建立连接，在网页登录 FTP 的过程中，我们没有输入用户名和密码，让它使用匿名登录，可以看到返回包中的信息 “Login or password incorrect”，拒绝访问。

小结：在上班时，PC1 的访问权限与 PC2 一致，都能访问 FTP 服务器，而不可以访问 WWW 服务器，而对于 Manager，他在上班时既可以访问 FTP 服务器，又可以访问 WWW 服务器。

## (5) 捕获主机访问服务器时的数据包，并进行分析。

- 报告上一问已给出并已分析。

- 实验结果汇总：

时间	所属区间	用户 A 192.168.1.2	用户 B 192.168.1.3	Manager 192.168.1.254
周四早 10 点	上班	FTP (✓) WWW (×)	FTP (✓) WWW (×)	FTP (✓) WWW (✓)
周四晚 23 点	下班	FTP (×) WWW (✓)	FTP (×) WWW (✓)	FTP (✓) WWW (✓)

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）

学号	学生	自评分
19308024	崔子潇	100
19335040	丁维力	100
19335286	郑有为	100