



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。

院系	数据科学与计算机学院	班 级	电子政务	组长	刘硕
学号	16340148	16340171	16340154	15331183	
学生	刘虹奇	聂博业	刘硕	梁峻华	
实验分工					
刘虹奇	和组员完成实验操作，并书写实验报告。		聂博业	和组员完成实验操作，并书写实验报告。	
刘硕	和组员完成实验操作。		梁峻华	和组员完成实验操作。	

【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)

步骤 1：实验前基本设置。

- (1) 配置 3 台计算机的 IP 地址、子网掩码、网关。
- (2) 检查计算机与服务器的连通性。

```
C:\Users\Administrator>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=128

192.168.1.2 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 = 1ms, 最长 = 1ms, 平均 = 1ms

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。
请求超时。
请求超时。
请求超时。

10.1.1.200 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

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。
请求超时。
请求超时。
请求超时。

10.1.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Administrator>
```



```
C:\Users\Nby>ping 10.1.1.200

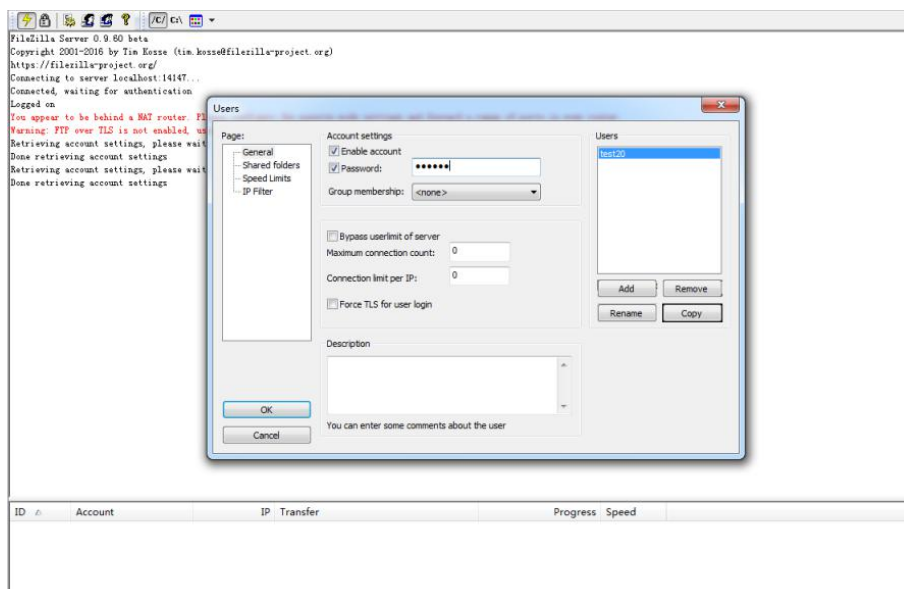
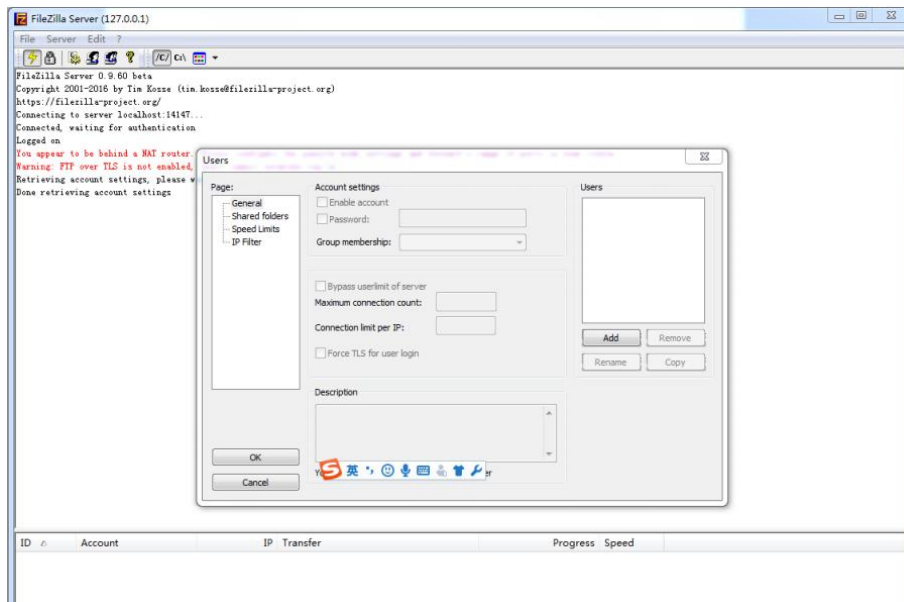
正在 Ping 10.1.1.200 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

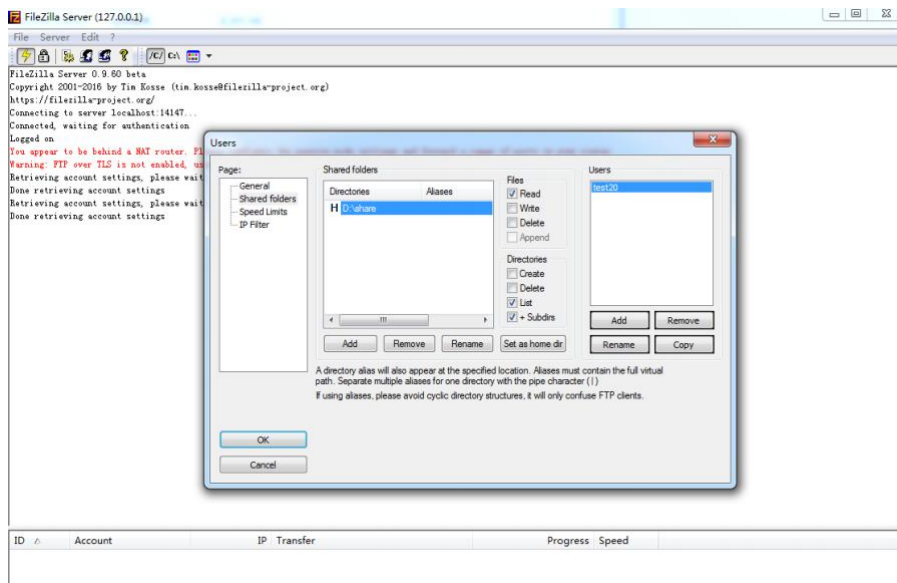
10.1.1.200 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Nby>ping 10.1.1.100

正在 Ping 10.1.1.100 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
```

此时经理主机可以和员工主机相互 ping 通。但是二者均无法 ping 通服务器。
(3) 在服务器上安装 FTP 服务器和 WWW 服务器。
安装 FTP 服务器:





安装 WWW 服务器：

用老师提供的实验室电脑中 Apache2.2 的安装包安装 Apache Http Service。在浏览器上访问 127.0.0.1 (localhost)，若能弹出相应页面，则表示安装 Apache Http Service 成功。

步骤 2：路由器的基本配置。

```
21-RSR20-1(config)#interface gigabitEthernet 0/0
21-RSR20-1(config-if-GigabitEthernet 0/0)#2.168.1.1 255.255.255.0
21-RSR20-1(config-if-GigabitEthernet 0/0)#exit
21-RSR20-1(config)#interface giga
21-RSR20-1(config)#interface gigabitEthernet 0/1
21-RSR20-1(config-if-GigabitEthernet 0/1)#10.1.1.1 255.255.255.0
% Unknown command.

21-RSR20-1(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
21-RSR20-1(config-if-GigabitEthernet 0/1)#exit
21-RSR20-1(config-if-GigabitEthernet 0/1)#
```

步骤 3：验证当前配置。

(1) 验证主机与服务器的连通性。

```
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=127
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.100 的回复: 字节=32 时间=4ms TTL=127

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 = 4ms, 平均 = 1ms

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=2ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间=1ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间=4ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=127

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 = 4ms, 平均 = 1ms
```



```
C:\Users\Nby>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=127
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.100 的回复: 字节=32 时间<1ms TTL=127

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 = 1ms, 平均 = 0ms

C:\Users\Nby>ping 10.1.1.200

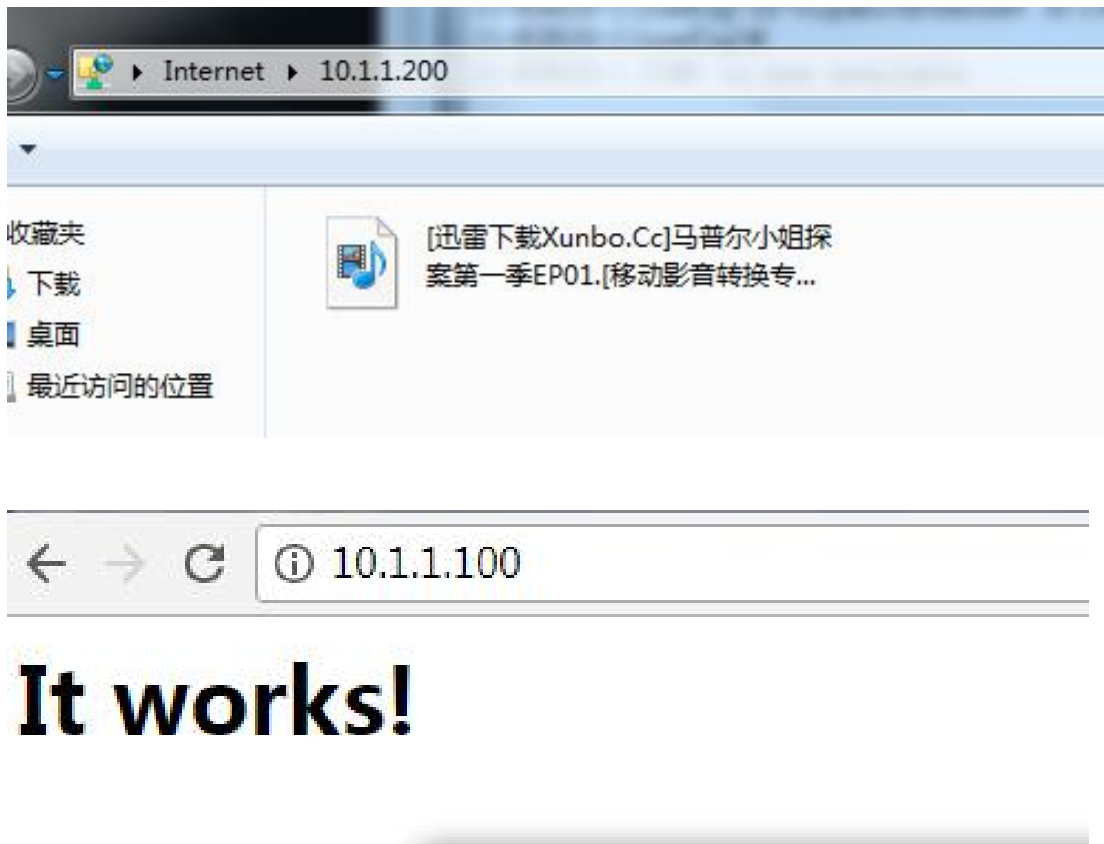
正在 Ping 10.1.1.200 具有 32 字节的数据:
来自 10.1.1.200 的回复: 字节=32 时间=1ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间=3ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.200 的回复: 字节=32 时间<1ms TTL=127

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 = 3ms, 平均 = 1ms
```

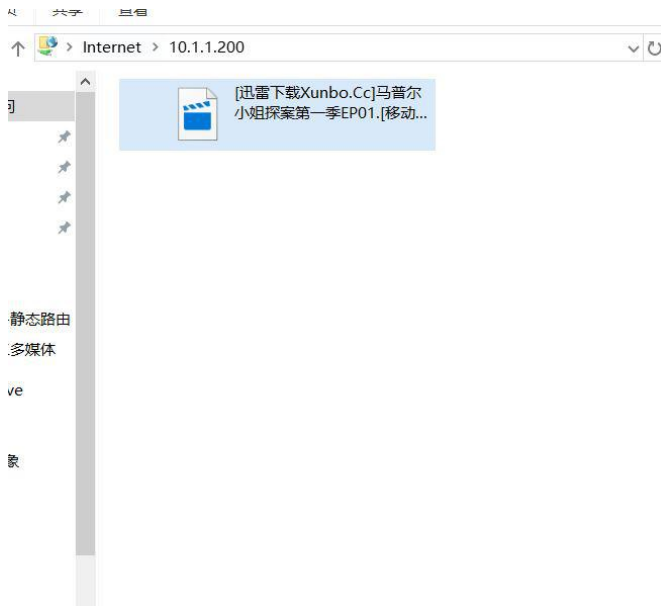
此时，经理主机和员工主机均可以与服务器 ping 通。

(2) 验证经理机、员工机能否登陆 FTP 服务器，通过 <http://10.1.1.100> 能否访问 WWW 服务器。分析原因。

经理主机：



员工主机：



It works!

经理主机和员工主机均可以与 FTP 服务 WWW 服务器相连接。

步骤 4：配置时间段。

定义正常上班的时间段。

```
Enter configuration commands, one per line. End with CNTL/Z.
21-RSR20-1(config)#time-rang work-time
21-RSR20-1(config-time-range)#periodic weekdays 09:00 to 18:00
21-RSR20-1(config-time-range)#exit
21-RSR20-1(config)#■
```

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。

```
1-RSR20-1(config)#time-rang work-time
1-RSR20-1(config-time-range)#periodic weekdays 09:00 to 18:00
1-RSR20-1(config-time-range)#exit
1-RSR20-1(config)#ip access-list extended accessctrl
1-RSR20-1(config-ext-nacl)#permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
1-RSR20-1(config-ext-nacl)#$host 10.1.1.200 eq ftp time-range work-time
1-RSR20-1(config-ext-nacl)#$8.1.0 0.0.0.255 host 10.1.1.200 eq ftp-data time-$
1-RSR20-1(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 eq $
1-RSR20-1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.100 e$
1-RSR20-1(config-ext-nacl)#exit
1-RSR20-1(config)#■
```




步骤 6：应用 ACL。

将 ACL 应用到端口 0/0 的输出方向。

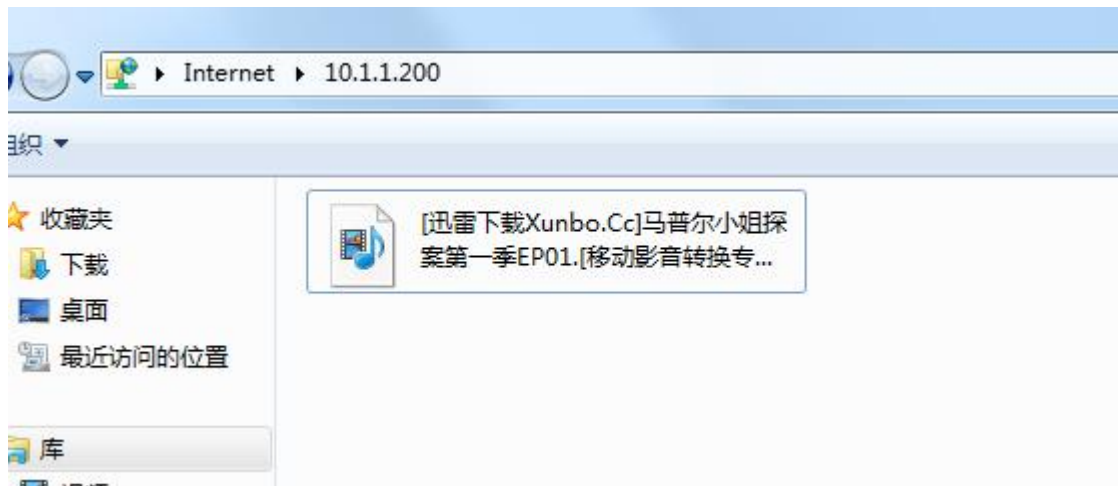
```
21-RSR20-1(config)#interface gigabitEthernet 0/0
21-RSR20-1(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
21-RSR20-1(config-if-GigabitEthernet 0/0)#end
21-RSR20-1#*Dec 11 01:19:30: %SYS-5-CONFIG_I: Configured from console by console
```

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。

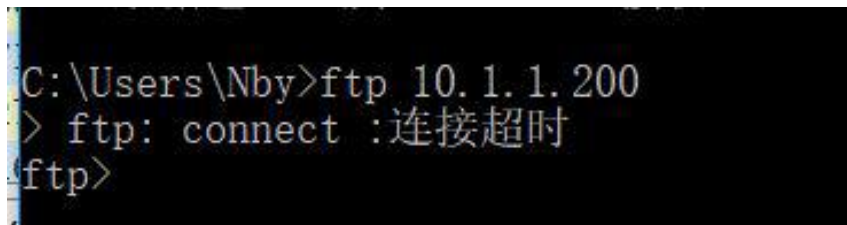
```
21-RSR20-1(config)#show clock
01:20:24 UTC Mon, Dec 11, 2017
```

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



It works!

(3) 普通员工主机 A、B 分别使用步骤 1 建立的用户名登陆 FTP 服务器，并通过 <http://10.1.1.100> 访问 WWW 服务器，验证在设定时间段内是否能登陆和访问？



It works!

(4) 改变路由器系统时间段，在其他时间段执行 (2) - (3) 的测试。

我们将时间设为上班时间。

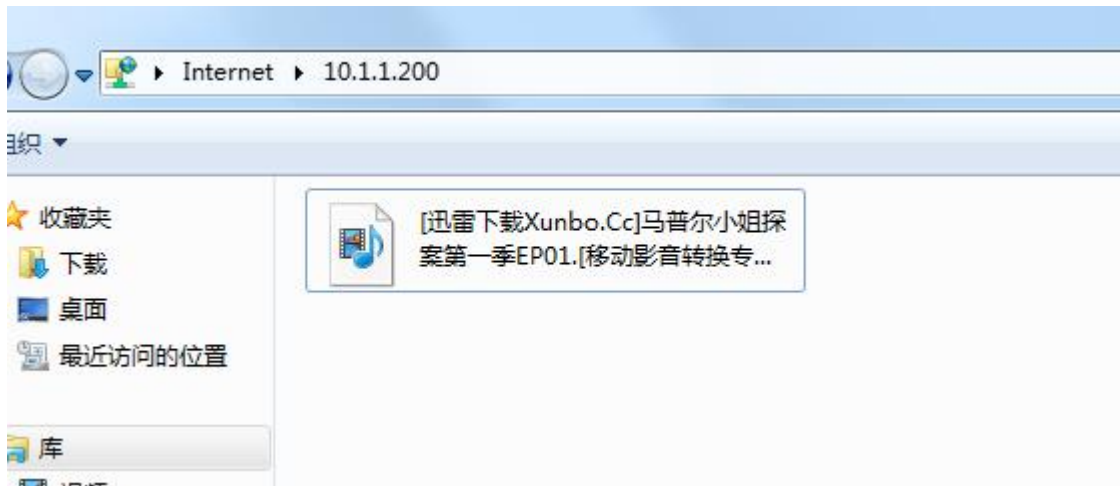
```
21-RSR20-1#clock set 12:00:11 12 12 2018
```

```
21-RSR20-1#*Dec 12 12:00:11: %SYS-6-CLOCKUPDATE: System clock has been updated to 12:00:11 UTC Wed Dec 12 2018.
```

```
21-RSR20-1#show clock
```

```
12:00:23 UTC Wed, Dec 12, 2018
```

经理的主机 Manager 使用步骤 1 建立的用户名登陆 FTP 服务器，并通过 <http://10.1.1.100> 访问 WWW 服务器，验证在设定时间段内是否能登陆和访问。



It works!

普通员工主机 A、B 分别使用步骤 1 建立的用户名登陆 FTP 服务器，并通过 <http://10.1.1.100> 访问 WWW 服务器，验证在设定时间段内是否能登陆和访问。



```
C:\Users\Nby>ftp 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)): test2333
331 Password required for test2333
密码:
230 Logged on
ftp>
```




(5) 捕获主机访问服务器的数据包, 并进行分析。

经理主机抓包:

14	24.675838	192.168.1.254	10.1.1.200	TCP	66	1459 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	24.676515	10.1.1.200	192.168.1.254	TCP	66	21 → 1459 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	24.676552	192.168.1.254	10.1.1.200	TCP	54	1459 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
17	24.677532	10.1.1.200	192.168.1.254	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
18	24.677563	192.168.1.254	10.1.1.200	TCP	54	1459 → 21 [ACK] Seq=1 Ack=144 Win=65536 Len=0
19	24.678029	192.168.1.254	10.1.1.200	FTP	70	Request: USER anonymous
20	24.678444	10.1.1.200	192.168.1.254	FTP	91	Response: 331 Password required for anonymous
21	24.678469	192.168.1.254	10.1.1.200	TCP	54	1459 → 21 [ACK] Seq=17 Ack=181 Win=65280 Len=0
22	24.678845	192.168.1.254	10.1.1.200	FTP	66	Request: PASS User@
23	24.681404	10.1.1.200	192.168.1.254	FTP	88	Response: 530 Login or password incorrect!
24	24.681429	192.168.1.254	10.1.1.200	TCP	54	1459 → 21 [ACK] Seq=29 Ack=215 Win=65280 Len=0
25	24.681793	192.168.1.254	10.1.1.200	TCP	54	1459 → 21 [FIN, ACK] Seq=29 Ack=215 Win=65280 Len=0
26	24.682127	10.1.1.200	192.168.1.254	TCP	60	21 → 1459 [ACK] Seq=215 Ack=30 Win=65536 Len=0
27	24.682315	10.1.1.200	192.168.1.254	TCP	60	21 → 1459 [RST, ACK] Seq=215 Ack=30 Win=0 Len=0
28	25.422966	192.168.1.254	192.168.1.255	NBNS	92	Name query NB STU61<1c>
29	25.554028	192.168.1.254	192.168.1.255	UDP	1482	55494 → 1689 Len=1440
30	26.172996	192.168.1.254	192.168.1.255	NBNS	92	Name query NB STU61<1c>
31	26.436106	192.168.1.2	192.168.1.255	NBNS	92	Name query NB LAPTOP-I1H5PA5F<1c>
32	27.187705	192.168.1.2	192.168.1.255	NBNS	92	Name query NB LAPTOP-I1H5PA5F<1c>
33	27.936670	192.168.1.2	192.168.1.255	NBNS	92	Name query NB LAPTOP-I1H5PA5F<1c>
34	34.083023	192.168.1.254	192.168.1.255	UDP	1482	55494 → 1689 Len=1440
35	35.171619	192.168.1.254	10.1.1.200	TCP	66	1460 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
36	35.171926	10.1.1.200	192.168.1.254	TCP	66	21 → 1460 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
37	35.171981	192.168.1.254	10.1.1.200	TCP	54	1460 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
38	35.172835	10.1.1.200	192.168.1.254	FTP	197	Response: 220-FileZilla Server 0.9.60 beta

time	source	destination	protocol	length	info
1 0.000000	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2 0.000045	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
3 0.004214	Shenzhen_0e:be:62	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.254
4 0.004381	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
5 0.004427	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
6 0.004524	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
7 0.004545	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
8 0.007473	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
9 0.007525	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
10 0.010669	RuijieNe_27:bf:4d	Shenzhen_0e:be:62	ARP	60	192.168.1.1 is at 58:69:6c:27:bf:4d
11 0.108387	fe80::34fe:95c2:2ba...	ff02::1:3	LLMNR	85	Standard query 0x7dbb ANY STU61
12 0.108446	192.168.1.254	224.0.0.252	LLMNR	65	Standard query 0x7dbb ANY STU61
13 0.220229	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
14 0.220321	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
15 0.224901	192.168.1.254	192.168.1.255	UDP	1482	55494 → 1689 Len=1440
16 0.265914	192.168.1.254	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
17 3.019164	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
18 3.019182	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
19 3.023728	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
20 3.023769	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
21 3.023786	Shenzhen_0e:be:62	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.254
22 3.023892	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
23 3.023898	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
24 3.027844	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
25 3.027940	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
26 3.031482	RuijieNe_27:bf:4d	Shenzhen_0e:be:62	ARP	60	192.168.1.1 is at 58:69:6c:27:bf:4d
27 3.128030	fe80::34fe:95c2:2ba...	ff02::1:3	LLMNR	85	Standard query 0xc88a ANY STU61
28 3.128069	192.168.1.254	224.0.0.252	LLMNR	65	Standard query 0xc88a ANY STU61
29 3.224965	192.168.1.254	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
30 3.225029	fe80::34fe:95c2:2ba...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
31 3.271078	192.168.1.254	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
32 3.461003	fe80::34fe:95c2:2ba...	ff02::1:3	LLMNR	84	Standard query 0xad16 A wpad

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0



计算机网络实验报告

上图可以看出经理主机可以在任何时间段访问到两个服务器。

上班时间员工主机抓包：

27	5.608810	192.168.1.2	183.3.224.141	TCP	66 3583 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
28	5.672455	192.168.1.2	10.1.1.200	TCP	66 3584 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
29	5.675315	10.1.1.200	192.168.1.2	TCP	66 21 → 3584 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	5.675444	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
31	5.679222	10.1.1.200	192.168.1.2	FTP	197 Response: 220-FileZilla Server 0.9.60 beta
32	5.679284	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=1 Ack=144 Win=261888 Len=0
33	5.679352	192.168.1.2	10.1.1.200	FTP	69 Request: USER test2333
34	5.682869	10.1.1.200	192.168.1.2	FTP	90 Response: 331 Password required for test2333
35	5.682971	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=16 Ack=180 Win=261888 Len=0
36	5.683537	192.168.1.2	10.1.1.200	FTP	67 Request: PASS 123456
37	5.685131	10.1.1.200	192.168.1.2	FTP	69 Response: 230 Logged on
38	5.685177	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=29 Ack=195 Win=261888 Len=0
39	5.685288	192.168.1.2	10.1.1.200	FTP	68 Request: opts utf8 on
40	5.688297	10.1.1.200	192.168.1.2	FTP	118 Response: 202 UTF8 mode is always enabled. No need to send this command.
41	5.688342	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=43 Ack=259 Win=261632 Len=0
42	5.688505	192.168.1.2	10.1.1.200	FTP	59 Request: PWD
43	5.690706	10.1.1.200	192.168.1.2	FTP	85 Response: 257 "/" is current directory.
44	5.690781	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [ACK] Seq=48 Ack=290 Win=261632 Len=0
45	6.130530	192.168.1.2	10.1.1.200	TCP	54 3584 → 21 [FIN, ACK] Seq=48 Ack=290 Win=261632 Len=0
46	6.131713	10.1.1.200	192.168.1.2	TCP	60 21 → 3584 [ACK] Seq=290 Ack=49 Win=66048 Len=0
47	6.131714	10.1.1.200	192.168.1.2	TCP	60 21 → 3584 [RST, ACK] Seq=290 Ack=49 Win=0 Len=0

9	4.767886	192.168.1.2	60.238.110.104	UDP	289 35112 → 7004 Len=247
10	5.564068	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4202 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
11	5.564982	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4203 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
12	5.788507	192.168.1.2	60.238.110.104	UDP	246 1195 → 7004 Len=284
13	6.648390	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4204 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
14	8.069519	192.168.1.254	192.168.1.255	NBNS	92 Name query NB WWW.BAIDU.COM<00>
15	8.819077	192.168.1.254	192.168.1.255	NBNS	92 Name query NB WWW.BAIDU.COM<00>
16	9.124240	192.168.1.2	189.163.17.5	TCP	66 4205 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
17	9.569082	192.168.1.254	192.168.1.255	NBNS	92 Name query NB WWW.BAIDU.COM<00>
18	10.165656	HewlettP_40:ab:14	RuijieNe_27:bf:4d	ARP	42 Who has 192.168.1.1? Tell 192.168.1.2
19	10.169169	RuijieNe_27:bf:4d	HewlettP_40:ab:14	ARP	60 192.168.1.1 is at 58:69:6c:27:bf:4d
20	10.782982	192.168.1.254	192.168.1.255	UDP	1482 55494 → 1689 Len=1440
21	11.565301	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4202 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
22	11.565301	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4203 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
23	12.124761	192.168.1.2	189.163.17.5	TCP	66 [TCP Retransmission] 4205 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
24	12.648543	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 4204 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1

上图可以看出员工主机可以在上班时间段访问到 FTP 服务器，但无法访问 HTTP 服务器。

下班时间员工主机抓包：

56	18.085641	192.168.1.254	192.168.1.255	UDP	1482 55494 → 1689 Len=1440
57	18.857165	192.168.1.2	10.1.1.200	TCP	66 [TCP Retransmission] 5578 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
58	19.686584	192.168.1.254	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
59	20.479556	192.168.1.254	224.0.0.252	LLMNR	64 Standard query 0x8ac7 A wpad
60	20.479587	fe80::34fe:95c2:2ba...ff02::1:3	ff02::1:3	LLMNR	84 Standard query 0x8ac7 A wpad
61	20.679690	192.168.1.254	192.168.1.255	NBNS	92 Name query NB WPAD<00>
62	20.858173	192.168.1.2	10.1.1.200	TCP	66 [TCP Retransmission] 5578 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
63	21.036913	192.168.1.2	60.238.110.104	UDP	194 1310 → 7004 Len=152

17	4.187521	10.1.1.100	192.168.1.2	TCP	66 80 → 5883 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	4.187595	192.168.1.2	10.1.1.100	TCP	54 5883 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
19	4.556429	192.168.1.2	101.226.4.6	TCP	66 5575 → 53 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
20	4.621517	192.168.1.2	10.1.1.100	TCP	66 5576 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
21	4.626698	10.1.1.100	192.168.1.2	TCP	66 80 → 5576 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	4.626823	192.168.1.2	10.1.1.100	TCP	54 5576 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
23	4.634798	192.168.1.2	10.1.1.100	HTTP	351 GET / HTTP/1.1
24	4.638659	10.1.1.100	192.168.1.2	HTTP	394 HTTP/1.1 200 OK (text/html)
25	4.638752	192.168.1.2	10.1.1.100	TCP	54 5576 → 80 [ACK] Seq=298 Ack=341 Win=261632 Len=0
26	4.939364	192.168.1.2	10.1.1.100	HTTP	253 GET /favicon.ico HTTP/1.1
27	4.942847	10.1.1.100	192.168.1.2	HTTP	478 HTTP/1.1 404 Not Found (text/html)
28	4.942985	192.168.1.2	10.1.1.100	TCP	54 5576 → 80 [ACK] Seq=497 Ack=765 Win=261376 Len=0
29	4.986899	192.168.1.2	60.238.110.104	UDP	272 1195 → 7004 Len=230

上图可以看出员工主机可以在下班时间段访问到 HTTP 服务器，但无法访问 FTP 服务器。



计算机网络实验报告

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
16340148	刘虹奇	98
16340171	聂博业	98
16340154	刘硕	96
15331183	梁峻华	96

【交实验报告】

上传实验报告：<ftp://222.200.180.109/>

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！