



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	计算机科学与技术	班 级	超级计算方向	组长	林天皓
学号	18324034				
学生					
实验分工					
林天皓	预习并完成实验		朱德鹏	预习并完成实验	
张钺奇	预习并完成实验				

【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。

【实验原理】

ACL 为访问控制列表策略，可以根据网络数据包中的 mac 地址，源端口，源地址，目的端口，上层协议等，根据网络管理员定义的规则决定哪些数据包可以被接收，从而达到访问控制的目的，本次实验中使用了基于时间的扩展 ACL 访问控制，根据上班时间和下班时间决定是否访问 FTP 服务器和 HTTP 服务器。

标准访问控制列表和扩展访问控制列表的区别在于标准访问控制列表只能基于源进行过滤 而扩展访问控制列表可以使用网络数据包的多种方法包括 基于源和目的地址、传输层协议和应用端口号进行过滤

【实验过程和结果】

本次实验中使用的网络拓扑与实验指导书中相同，如下

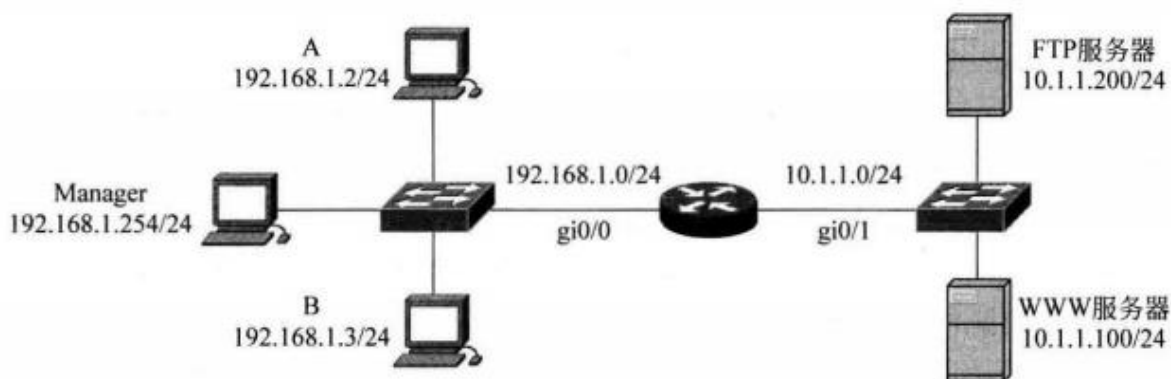


图 8-8 基于时间 ACL 的实验拓扑

图 1-实验网络拓扑

步骤 1: (1) 配置 3 台计算机的 IP 地址，子网掩码，网关。

1.配置 A 计算机 ip 地址 192.168.1.2，子网掩码 255.255.255.0，访问服务器的网关通过后续手动加入。

```
以太网适配器 以太网 4:
    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::11a:72c0:a995:1bae%6
    IPv4 地址 . . . . . : 192.168.1.2
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . :
```

图 2-配置员工 A 机 IP

2.配置 B 计算机 ip 地址 192.168.1.2，子网掩码 255.255.255.0，访问服务器的网关通过后续手动加入。

```
以太网适配器 以太网 4:
    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::11a:72c0:a995:1bae%6
    IPv4 地址 . . . . . : 192.168.1.3
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . :
```

图 3-配置员工 B 机 IP

3.配置 manager 计算机 ip 地址 192.168.1.254，子网掩码 255.255.255.0，访问服务器的网关通过后续手动加入。



```
以太网适配器 以太网 4:
```

```
连接特定的 DNS 后缀 . . . . . :  
本地链接 IPv6 地址. . . . . : fe80::11a:72c0:a995:1bae%6  
IPv4 地址 . . . . . : 192.168.1.254  
子网掩码 . . . . . : 255.255.255.0  
默认网关. . . . . :
```

图 4-配置 Manager 机 IP

4.配置 FTP 服务器 ip 地址 10.1.1.200，子网掩码 255.255.255.0。

```
以太网适配器 以太网 4:
```

```
连接特定的 DNS 后缀 . . . . . :  
本地链接 IPv6 地址. . . . . : fe80::e5bc:2a2b:7a9a:934%6  
IPv4 地址 . . . . . : 10.1.1.200  
子网掩码 . . . . . : 255.255.255.0  
默认网关. . . . . : 10.1.1.1
```

图 5-配置 FTP 服务器 IP

4.配置 WWW 服务器 ip 地址 10.1.1.100，子网掩码 255.255.255.0。

```
C:\Users\Administrator>ipconfig
```

```
Windows IP 配置
```

```
以太网适配器 实验网:
```

```
连接特定的 DNS 后缀 . . . . . :  
本地链接 IPv6 地址. . . . . : fe80::c871:4035:c61:445e%5  
IPv4 地址 . . . . . : 10.1.1.100  
子网掩码 . . . . . : 255.255.255.0  
默认网关. . . . . : 10.1.1.1
```

图 6-配置 WWW 服务器 IP

下面配置路由器接口 IP 地址，并查看路由表



```
09/06/2021 08:48.39 /home/mobaxterm telnet 172.16.14.5 2003
Trying 172.16.14.5...
Connected to 172.16.14.5.
Escape character is '^]'.

14-RSR20-1>enable 14

Password:
14-RSR20-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
14-RSR20-1(config)#interfa
14-RSR20-1(config)#interface gig
14-RSR20-1(config)#interface gigabitEthernet 0/1
14-RSR20-1(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
14-RSR20-1(config-if-GigabitEthernet 0/1)#exit
14-RSR20-1(config)#interface gig
14-RSR20-1(config)#interface gigabitEthernet 0/0
14-RSR20-1(config-if-GigabitEthernet 0/0)#2.168.1.1 255.255.255.0
14-RSR20-1(config-if-GigabitEthernet 0/0)#exit
14-RSR20-1(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.
14-RSR20-1(config)#
```

图 7-配置路由器，查看路由表

分析：设置端口 0 IP 地址为 192.168.1.1 配置端口 1 IP 地址为 10.1.1.1，可见 10.1.1.1 与 192.168.1.1 均联通在该路由器上。

(2) 检查网络的连通性

```
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=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 = 1ms, 平均 = 0ms
```

图 8-使用 A 计算机 ping WWW 服务器

分析：A 计算机可以联通 WWW 服务器



```
C:\Users\Administrator>route add 10.1.1.200 mask 255.255.255.255 192.168.1.1
操作完成!

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

C:\Users\Administrator>
```

图 9 - 使用 A 计算机 ping FTP 服务器

分析：A 计算机可以联通 FTP 服务器

综上，经过 ping 测试，计算机均能访问 FTP 服务器和 WWW 服务器

(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。

在服务器上使用 filezilla server 软件建立 FTP 服务器，使用 manager 计算机访问

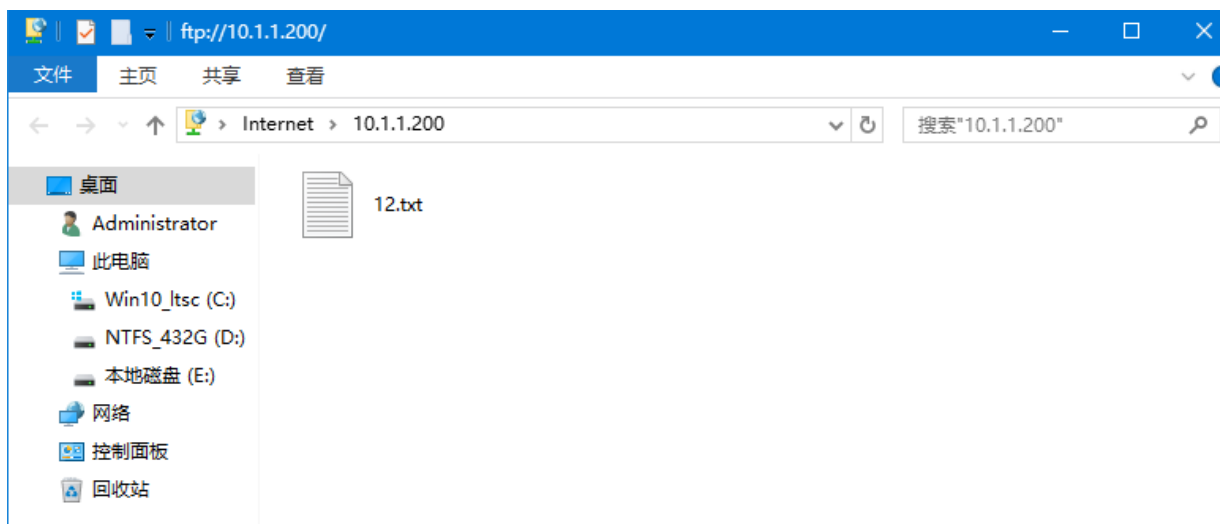


图 10-manager 使用 FTP 服务

分析：可以查看远程服务器中的文件，代表 FTP 服务正常。

下面，使用 wireshark 抓包，进一步查看 FTP 的连接过程



文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)						
Etlp						
No.	Time	Source	Destination	Protocol	Length	Info
15	15.299858	192.168.1.254	10.1.1.200	FTP	60	Request: noop
16	15.299538	10.1.1.200	192.168.1.254	FTP	66	Response: 200 OK
18	15.299590	192.168.1.254	10.1.1.200	FTP	61	Request: CWD /
19	15.300149	10.1.1.200	192.168.1.254	FTP	105	Response: 250 CWD successful. "/" is current directory.
21	15.300192	192.168.1.254	10.1.1.200	FTP	62	Request: TYPE A
22	15.300586	10.1.1.200	192.168.1.254	FTP	77	Response: 200 Type set to A
24	15.300656	192.168.1.254	10.1.1.200	FTP	60	Request: PASV
25	15.301388	10.1.1.200	192.168.1.254	FTP	106	Response: 227 Entering Passive Mode (10,1,1,200,249,160)
30	15.301738	192.168.1.254	10.1.1.200	FTP	60	Request: LIST
31	15.302703	10.1.1.200	192.168.1.254	FTP	113	Response: 150 Opening data channel for directory listing of "/"
38	15.302953	10.1.1.200	192.168.1.254	FTP	92	Response: 226 Successfully transferred "/"

> Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F79B1DFF-B47D-45C5-8AFD-605A02562A6C}, id 0

> Ethernet II, Src: Shenzhen_0e:ab:7d (44:33:4c:0e:ab:7d), Dst: RuijieNe_27:b8:1d (58:69:6c:27:b8:1d)

> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 10.1.1.200

> Transmission Control Protocol, Src Port: 3916, Dst Port: 21, Seq: 1, Ack: 1, Len: 6

> File Transfer Protocol (FTP)

[Current working directory:]

0000 58 69 6c 27 b8 1d 44 33 4c 0e ab 7d 08 00 45 00 Xl1'...D3 L..}-E-
0010 00 2e 3b 89 40 00 40 06 30 d2 c0 a8 01 fe 0a 01 .,; @ @ 0-----
0020 01 c8 0f 4c 00 15 b9 7a 25 7f b0 9e c1 68 50 18 ---L---z %----hP-
0030 80 00 16 0b 00 00 6e 6f 6f 70 0d 0a -----no op--

图 11-捕获 FTP 数据包

分析：由抓包展示，FTP 传输的命令正常。

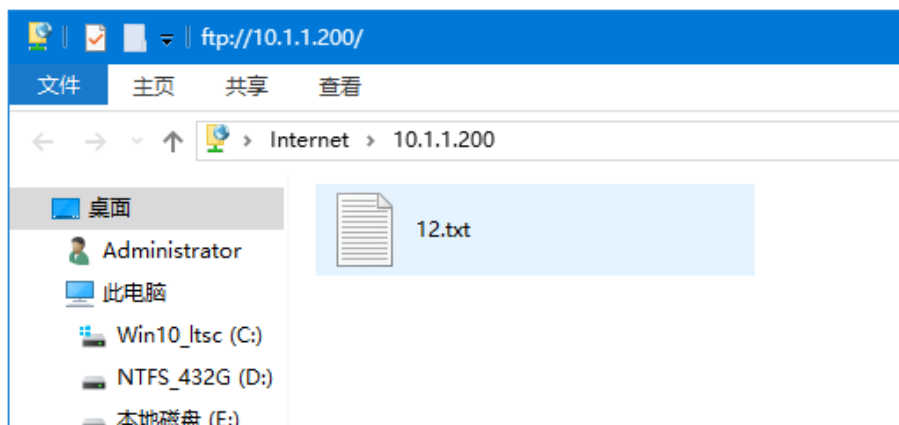


图 12-manager 计算机访问 ftp 服务器。

分析：manager 计算机访问 ftp 服务器正常。

下面使用 nginx 软件在 WWW 服务器上开启 HTTP 服务

使用员工机和经理机访问可以查看网页。



10.1.1.100

Welcome Computer Network LAB

山中计算大学招生中

Now You can try to use ACL block the website.

图 13-访问 WWW 服务器的 HTTP 页面

分析：目前没有配置 ACL 策略，员工机和经理机都可以访问 FTP 和 WWW 服务器

步骤 4：配置时间段

定义正常上班时间段

```
14-RSR20-1(config)#time-range work-time
14-RSR20-1(config-time-range)#periodic weekdays 09:00 to 18:00
14-RSR20-1(config-time-range)#exit
14-RSR20-1(config)#show time
14-RSR20-1(config)#show time-range
time-range entry: work-time (active)
periodic Weekdays 9:00 to 18:00
```

图 14-配置路由器上班时间段

步骤 5：配置 ACL

配置 ACL 并且应用时间段，实现基于时间段访问控制

```
14-RSR20-1(config)#ip access-list extended accessctrl
14-RSR20-1(config-ext-nacl)#permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
14-RSR20-1(config-ext-nacl)#host 10.1.1.200 eq ftp time-range work-time
14-RSR20-1(config-ext-nacl)#1.200 eq ftp-data time-range work-time
14-RSR20-1(config-ext-nacl)#st 10.1.1.100 eq www time-range work-time
14-RSR20-1(config-ext-nacl)#8.1.0 0.0.0.255 host 10.1.1.100 eq www
14-RSR20-1(config-ext-nacl)#exit
14-RSR20-1(config)#show acc
14-RSR20-1(config)#show access-l
14-RSR20-1(config)#show access-lists

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
14-RSR20-1(config)#
```

图 15-配置路由器上班时间段的访问控制

应用完毕后，展示目前已经使用该 ACL 控制策略的端口



```
14-RSR20-1#show access-group
ip access-group accessctrl in
Applied On interface GigabitEthernet 0/0.
```

图 16-查看应用的 ACL 控制策略

分析：目前 ACL 控制策略已经被应用在路由器 1 端口 0 上

步骤 7：验证测试

```
Applied On interface GigabitEtherne
14-RSR20-1#show clock
16:11:29 UTC Fri, Jun 4, 2021
14-RSR20-1#
```

图 17-查看路由器当前时间

通过 show clock 查看当前时间，可见当前时间为上班时间。

使用经理的主机访问 FTP 服务器，并访问 WWW 服务器，在设定的时间段内是否能登录和访问？



图 18-manager 访问 WWW 服务器的 HTTP 页面

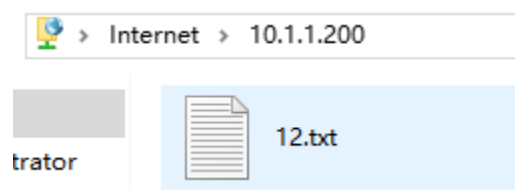


图 19-manager 访问 FTP 服务器



正在捕获 以太网 4						
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)						
应用显示过滤器 ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::11a:72c0:a995...	ff02::1:2	DHCPv6	157	Solicit XID: 0x815b27 CID: 00010001
2	2.240210	192.168.1.3	10.1.1.200	TCP	66	1592 → 21 [SYN] Seq=0 Win=65535 Len=
3	2.240457	10.1.1.200	192.168.1.3	TCP	70	21 → 1592 [SYN, ACK] Seq=0 Ack=1 Wi
4	2.240485	192.168.1.3	10.1.1.200	TCP	54	1592 → 21 [ACK] Seq=1 Ack=1 Win=262
5	2.241229	10.1.1.200	192.168.1.3	FTP	201	Response: 220-FileZilla Server 0.9.
6	2.241242	192.168.1.3	10.1.1.200	TCP	54	1592 → 21 [ACK] Seq=1 Ack=144 Win=2
7	2.241267	192.168.1.3	10.1.1.200	FTP	70	Request: USER anonymous
8	2.241662	10.1.1.200	192.168.1.3	FTP	95	Response: 331 Password required for
9	2.241676	192.168.1.3	10.1.1.200	TCP	54	1592 → 21 [ACK] Seq=17 Ack=181 Win=
10	2.241699	192.168.1.3	10.1.1.200	FTP	68	Request: PASS IEUser@
11	2.242053	10.1.1.200	192.168.1.3	FTP	92	Response: 530 Login or password inc
12	2.242063	192.168.1.3	10.1.1.200	TCP	54	1592 → 21 [ACK] Seq=31 Ack=215 Win=
13	2.242084	192.168.1.3	10.1.1.200	TCP	54	1592 → 21 [FIN, ACK] Seq=31 Ack=215
14	2.242225	10.1.1.200	192.168.1.3	TCP	64	21 → 1592 [ACK] Seq=215 Ack=32 Win=

> Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{F79B1DFF-B47D-4}

> Ethernet II, Src: Shenzhen_0e:ab:7d (44:33:4c:0e:ab:7d), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)

> Internet Protocol Version 6, Src: fe80::11a:72c0:a995:1bae, Dst: ff02::1:2

> User Datagram Protocol, Src Port: 546, Dst Port: 547

> DHCPv6

图 20-manager 访问 FTP 数据包捕获

分析：该上班时间段内经理可以访问 WWW 服务器和 FTP 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，并访问 WWW 服务器，在设定的时间段内能否登录和访问。



无法访问此网站

10.1.1.100 的响应时间过长。

请试试以下办法：

- 检查网络连接
- 检查代理服务器和防火墙
- 运行 Windows 网络诊断

ERR_CONNECTION_TIMED_OUT

重新加载

图 21-员工上班时间段不能访问 WWW 服务器



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	10.1.1.100	TCP	66	3474 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000000	192.168.1.3	10.1.1.100	TCP	66	3473 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.250808	192.168.1.3	10.1.1.100	TCP	66	3477 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	2.794162	192.168.1.3	192.168.1.255	UDP	1482	58410 → 1689 Len=1440
5	5.053961	Shenzhen_0e:ab:7d	RuijieNe_27:b8:1d	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
6	5.059870	RuijieNe_27:b8:1d	Shenzhen_0e:ab:7d	ARP	64	192.168.1.1 is at 58:69:6c:27:b8:1d
7	5.999766	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3473 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8	5.999773	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3474 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
9	6.250997	192.168.1.3	10.1.1.100	TCP	62	[TCP Retransmission] 3477 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
10	9.285674	RuijieNe_15:57:56	LLDP_Multicast	LLDP	394	MA/58:69:6c:15:57:56 MA/58:69:6c:15:57:56 I21 SysID=14-55750-2 SysOr=Ruijie Lay
11	11.326241	192.168.1.3	192.168.1.255	UDP	1482	58410 → 1689 Len=1440

图 21-员工上班时间段尝试访问 WWW 服务器数据包

分析：此时员工不能访问 WWW 服务器，不能接受到来自 WWW 服务器的数据包

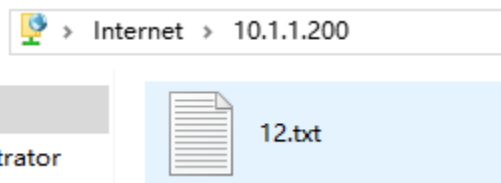


图 21-员工上班时间段访问 FTP 服务器

分析：此时员工允许访问 FTP 服务器。

改变路由器系统时间测试，更改时间为下班时间

更改时间后使用 Show clock 显示当前时间

```
14-RSR20-1#show clock
22:00:11 UTC Wed, Jun 9, 2021
14-RSR20-1#show time cl
```

图 22-当前为下班时间

目前时间为 22:00，不属于 worktime

再次测试，员工机已经不能访问 FTP 服务器

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	10.1.1.200	TCP	66	1289 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
2	0.689044	Shenzhen_0e:ab:7d	RuijieNe_27:b8:1d	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
3	0.694511	RuijieNe_27:b8:1d	Shenzhen_0e:ab:7d	ARP	64	192.168.1.1 is at 58:69:6c:27:b8:1d
4	1.001507	192.168.1.3	10.1.1.200	TCP	66	[TCP Retransmission] 1289 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
5	1.971387	192.168.1.3	192.168.1.255	UDP	1482	55236 → 1689 Len=1440
6	3.002341	192.168.1.3	10.1.1.200	TCP	62	[TCP Retransmission] 1289 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
7	7.110315	192.168.1.3	10.1.1.200	TCP	66	1290 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
8	7.688330	Shenzhen_0e:ab:7d	RuijieNe_27:b8:1d	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
9	7.694567	RuijieNe_27:b8:1d	Shenzhen_0e:ab:7d	ARP	64	192.168.1.1 is at 58:69:6c:27:b8:1d
10	8.110522	192.168.1.3	10.1.1.200	TCP	66	[TCP Retransmission] 1290 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
11	10.110841	192.168.1.3	10.1.1.200	TCP	62	[TCP Retransmission] 1290 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
12	10.508302	192.168.1.3	192.168.1.255	UDP	1482	55236 → 1689 Len=1440
13	14.688472	Shenzhen_0e:ab:7d	RuijieNe_27:b8:1d	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
14	14.694802	RuijieNe_27:b8:1d	Shenzhen_0e:ab:7d	ARP	64	192.168.1.1 is at 58:69:6c:27:b8:1d

图 23-员工尝试访问 FTP 服务器的数据包



分析：如图，员工接受不到来自 FTP 服务的数据包，不能访问。

下面测试员工能否访问 WWW 服务器。

No.	Time	Source	Destination	Protocol	Length	Info
23	18.539029	192.168.1.3	10.1.1.100	TCP	54	1136 → 80 [A
24	23.097245	192.168.1.3	10.1.1.100	HTTP	589	GET / HTTP/1
25	23.098185	10.1.1.100	192.168.1.3	HTTP	238	HTTP/1.1 304
26	23.148491	192.168.1.3	10.1.1.100	TCP	54	1136 → 80 [A
27	25.596522	192.168.1.3	192.168.1.255	UDP	1482	55236 → 1689

图 24-员工访问 WWW 服务器接受到数据包

根据抓包，可以接收到来自 WWW 服务器的数据包，员工此时可以访问 WWW 服务器。

综上，本次实验中使用 ACL 控制策略，使得员工在上班时间可以访问 FTP 服务器不允许访问 WWW 服务器，下班时间不允许访问 FTP 服务器，允许访问 WWW 服务器，而经理任何时间段均可以访问。

【实验感想】

本次实验是使用 ACL 控制策略完整针对特定数据包的控制方法，完成对特定服务器在特定时间段内访问特定服务器限制的目的。不过这种限制方法也有缺点，对 WWW 服务器和 FTP 服务器的限制是通过对特定端口的访问控制来是实现的，若用户与服务器协商，使用一个非标准的端口进行通信，则原来的限制会失效。

同时在实验中，在设置了 ACL 策略之后一开始使用 ping 测试主机之间的连通性，ping 不通但是机器之间可以互相访问。经过测试发现 ACL 策略默认情况下 icmp 包也被丢弃，因此不能 ping 通，加入了 permit icmp any any 之后即可访问。

```
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
60 permit icmp any any
14-RSR20-1(config-ext-nacl)#
```

图 24-permit icmp 后 ping 通