计算机网络实验报告

警

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	计科（2）班	组长	郑梓霖
学号	21307077				
学生	凌国明				

基于时间的 ACL

【实验目的】

使用基于时间的 ACL 实现基于时间段的高级访问控制

【实验原理】

本实验采用基于时间的访问控制列表（ACL）来实现网络中的高级访问控制。ACL 是一种用于定义哪些用户或系统可以访问或使用网络资源的规则列表。基于时间的 ACL 允许根据时间段来定义这些规则。本实验的关键是创建和应用这些基于时间的规则来控制网络流量。

实验涉及两个主要部分：首先，定义时间范围对象，指定允许或拒绝访问的具体时间段；其次，创建 ACL 规则，使用这些时间范围对象来限制不同子网内的主机在特定时间访问特定服务器。

【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 19216810/24 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 10.1.10/24 为公司服务器网段,其中有 2 台服务器 1 台 www 服务器(10.11100/24)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

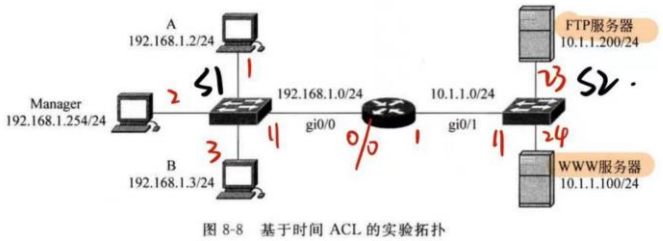


图 8-8 基于时间 ACL 的实验拓扑

【实验设备】

路由器 1 台，计算机 5 台（其中 2 台作为 WWW Server 和 FTP Server）

【实验步骤】

1. 基本的环境配置

1) 配置 3 台计算机（员工 AB 和 Manager）的 IP 地址，子网掩码，网关

```
C:\Windows\system32>netsh interface ip set address "实验网" static 192.168.1.3 255.255.255.0 192.168.1.1

C:\Windows\system32>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::57cb:e9dc:a5e4:6a07%14
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.3
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.1.1

无线局域网适配器 WLAN:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 校园网:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2001:250:3002:4b98:b674:5c1d:a5b0:6980
   临时 IPv6 地址. . . . . . . . . . : 2001:250:3002:4b98:95c5:807c:65f4:cb65
   本地链接 IPv6 地址. . . . . . . . : fe80::6d79:9dad:f23f:abe%9
   IPv4 地址 . . . . . . . . . . . . : 172.16.17.3
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . : fe80::5ee8:83ff:fec4:ece4%9
                                       172.16.0.1
```

2) 检查计算机和服务器的连通性

```
C:\Windows\system32>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 = 0ms, 平均 = 0ms

C:\Windows\system32>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<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 = 2ms, 平均 = 0ms
```

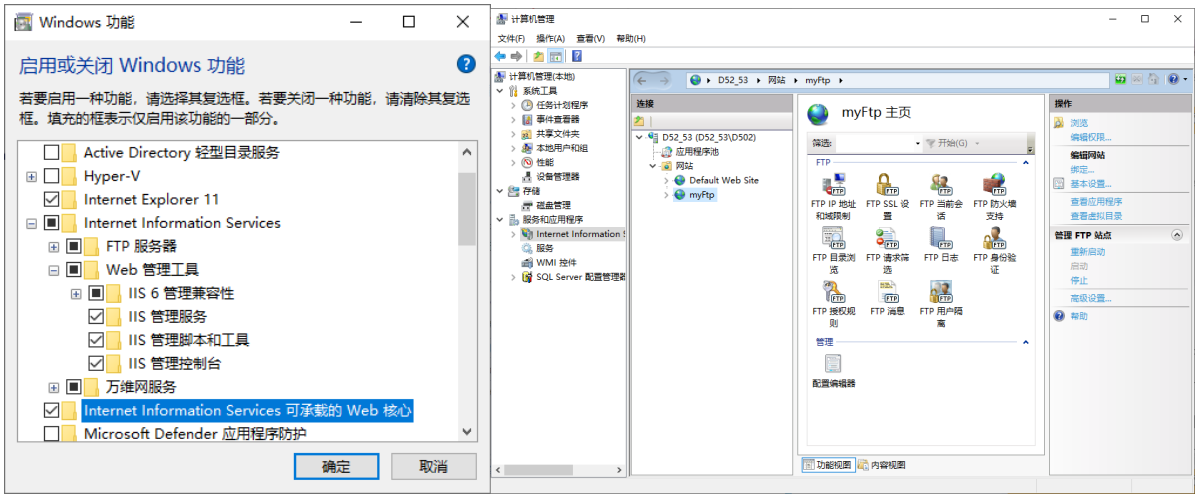
3) 在一台计算机中配置 FTP Server，在另一台计算机中配置 WWW Server

https://blog.csdn.net/qq_43442524/article/details/103817226 配置 ftp 服务器

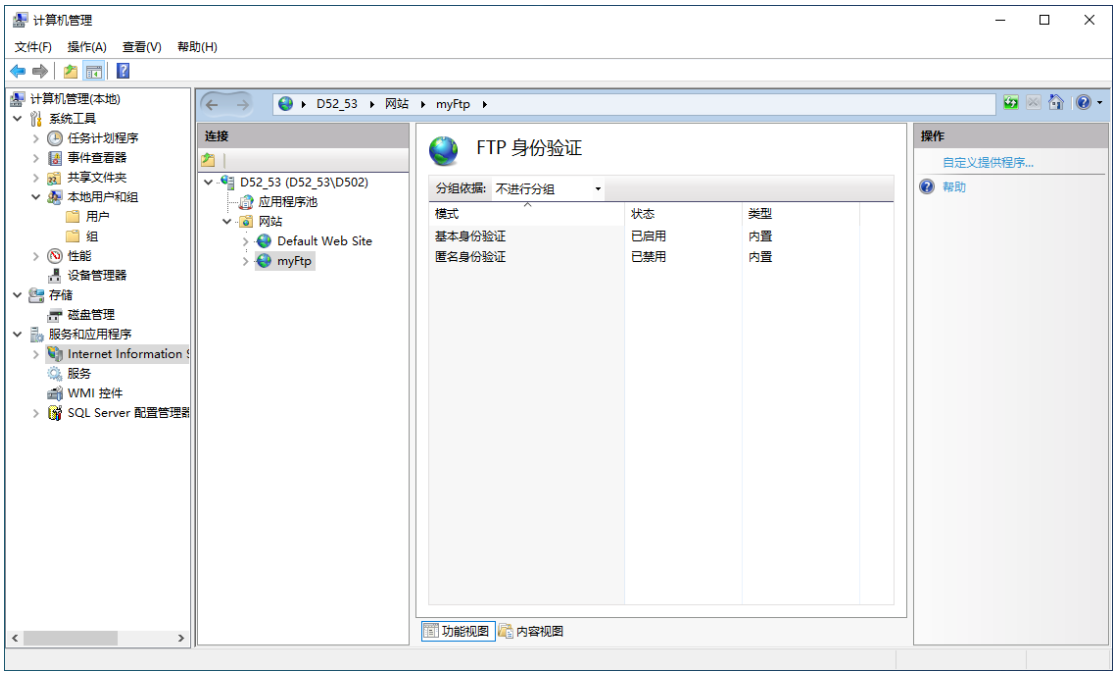
https://blog.csdn.net/zhj_1121/article/details/85344185 创建用户并认证

https://blog.csdn.net/farmwang/article/details/71159327 认证用户授权

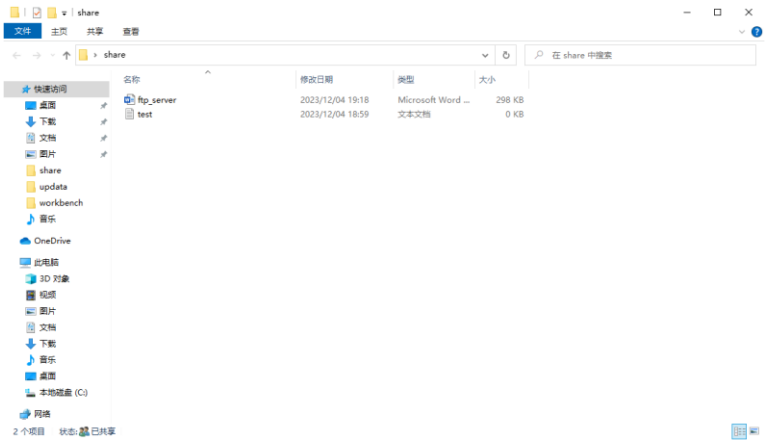
根据第一个教程，利用 windows 相关设置和 IIS，配置 ftp 服务器



根据第二个教程，创建用户并认证

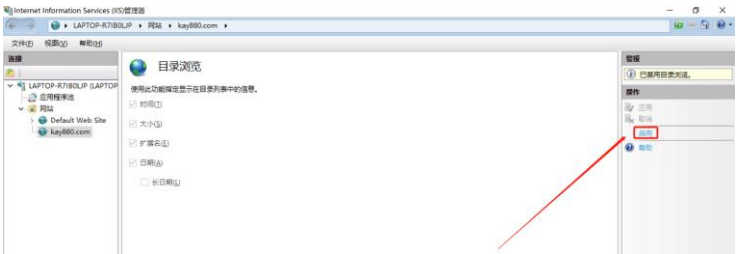


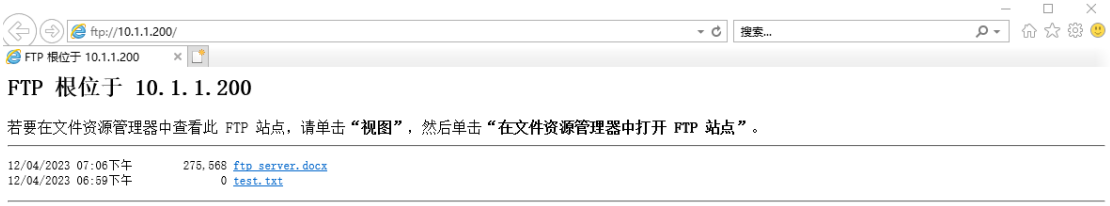
然后进行配置的验证，由下图可知本机可以访问本机的 ftp server



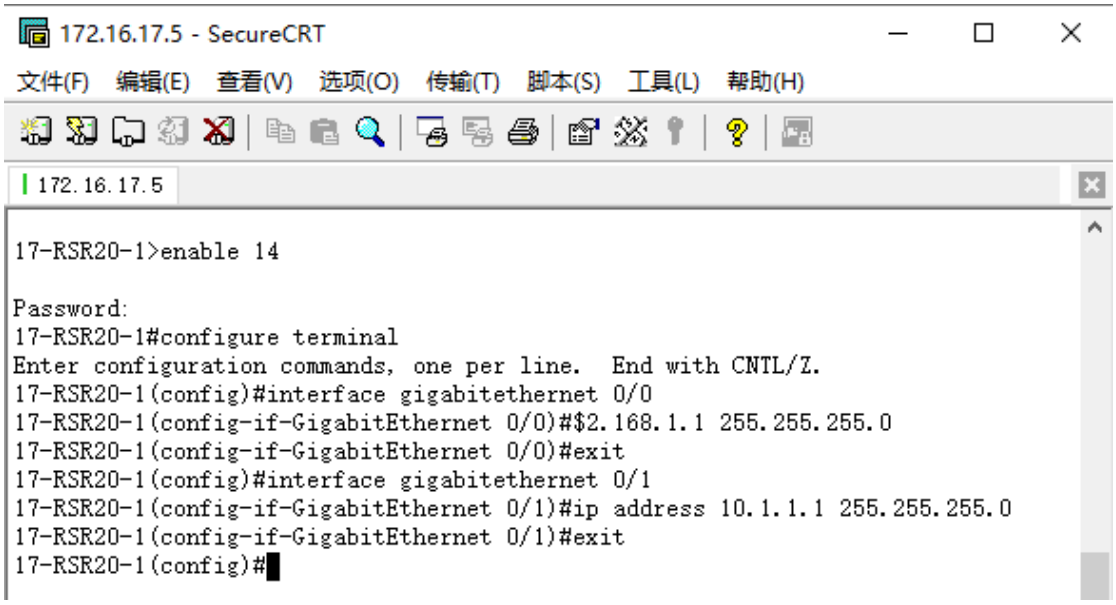
ftp 服务器访问成功

再配置 WWW 服务器



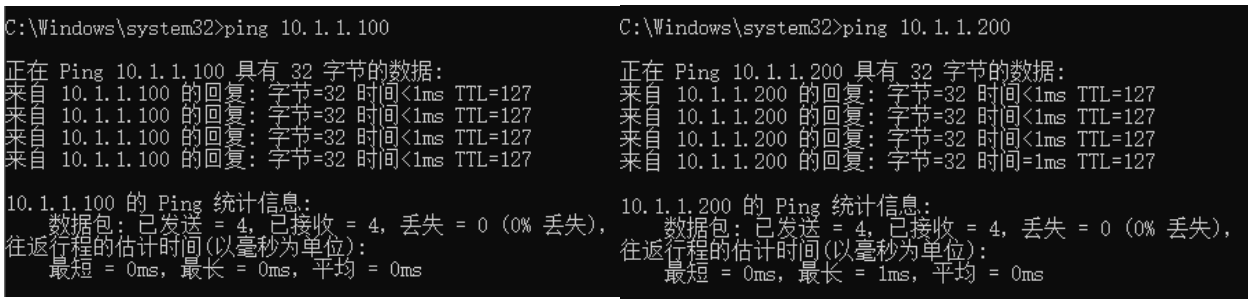


2. 路由器的基本配置

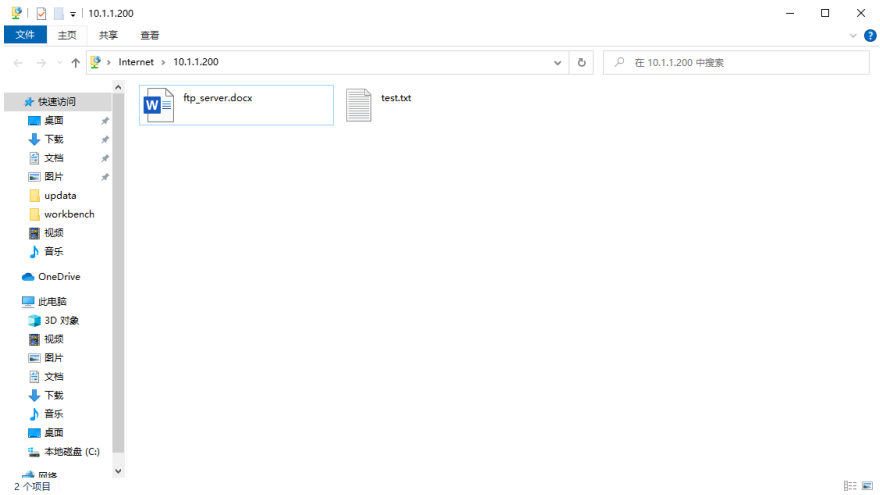


3. 验证当前的配置

1) 验证主机和服务器的连通性



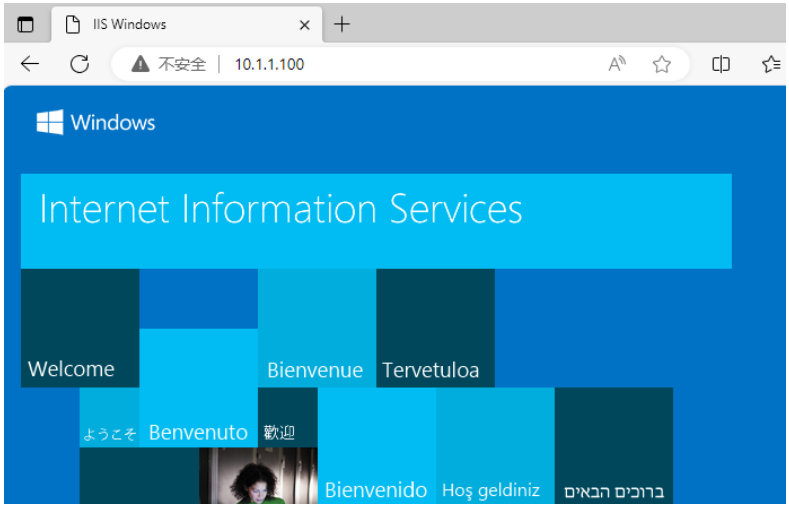
2) 经理机和员工机能否登录 FTP 服务器？能否达到预期目标？原因？



如上图，经理机和员工机都能登录 FTP 服务器，因为他们之间本就是相互连通的，且还没有设置 ACL 的过滤规则。这种现象符合我们的预期

3) 经理机和员工机能否登录 WWW 服务器？能否达到预期目标？原因？

员工机：



经理机：

如上图，经理机和员工机都能登录 WWW 服务器，因为他们之间本就是相互连通的，且还没有设置 ACL 的过滤规则。这种现象符合我们的预期

4. 配置时间段

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

配置工作时间，为配置 ACL 做铺垫

5. 配置 ACL

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

就绪 Telnet 24, 20 24 行, 80 列 VT100 数字

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

6. 应用 ACL

```
17-RSR20-1(config)#interface gigabitethernet 0/0
17-RSR20-1(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
17-RSR20-1(config-if-GigabitEthernet 0/0)#end
17-RSR20-1#*Dec  4 10:24:28: %SYS-5-CONFIG_I: Configured from console by console

17-RSR20-1#
```

将 ACL 规则应用于我们的子网

7. 验证测试

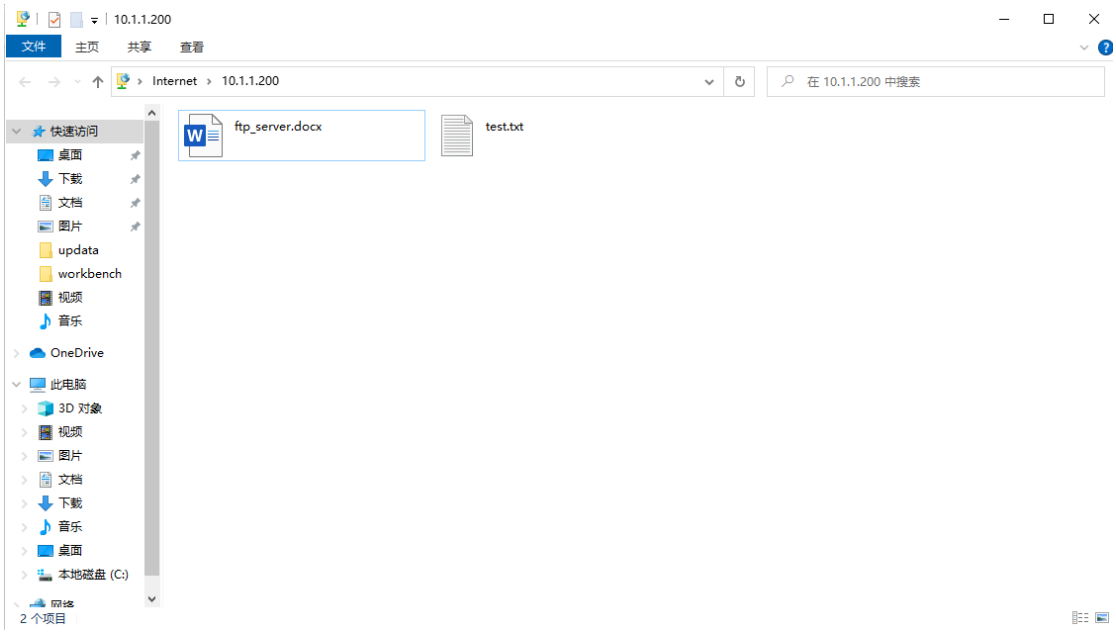
1) 查看路由器的系统时间:使用 showclock 命令判断当前时间段

```
17-RSR20-1#show clock
10:25:14 UTC Mon, Dec 4, 2023
```

位于工作时间，预期员工机只能访问 FTP 不能访问 WWW，经理机都可以访问。

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?

上班时间，经理机登录 FTP 服务器：



上班时间，经理机登录 WWW 服务器：

如上图，经理机可以访问 FTP 和 WWW，符合 ACL 规则，符合预期。

3) 普通员工主机 AB 分别使用步骤 1 建立的用户名登录 FTP 服务器并通过 http://10.1.1.100 访问 WW 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)?

AB 访问服务器时是等效的，所以我们仅研究一台员工机即可

上班时间，员工机访问 FTP 服务器：

上班时间，员工机访问 WWW 服务器

如上图，上班时间员工机只能访问 FTP，不能访问 WWW，符合 ACL 规则，符合预期

上班时间员工机访问 WWW 的报文如下

90	78.018261	192.168.1.2	10.1.1.100	TCP	66 57022 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
91	78.022209	192.168.1.2	10.1.1.100	TCP	66 57023 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
92	78.283412	192.168.1.2	10.1.1.100	TCP	66 57024 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
93	78.569304	192.168.1.3	192.168.1.255	UDP	1486 59106 → 1689 Len=1440
94	79.019016	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57022 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
95	79.033953	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57023 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
96	79.285670	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57024 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
97	80.516650	192.168.1.254	239.255.255.250	SSDP	221 M-SEARCH * HTTP/1.1
98	80.516805	192.168.1.254	239.255.255.250	SSDP	221 M-SEARCH * HTTP/1.1
99	80.578745	192.168.1.254	192.168.1.255	UDP	1486 51996 → 1689 Len=1440
100	81.023411	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57022 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
101	81.038742	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57023 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
102	81.286446	192.168.1.2	10.1.1.100	TCP	66 [TCP Retransmission] 57024 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

捕获的数据包中，我们看到多个 TCP 的 SYN 包，这表明客户端（员工机）试图与 WWW 服务器（IP 地址 10.1.1.100）建立 TCP 连接。然而，没有看到对应的 SYN-ACK 回应，表示服务器未响应或响应被阻止。

TCP 重传尝试：标记为“TCP Retransmission”的数据包表明，客户端尝试重新发送 SYN 包，以期望收到来自服务器的响应。这些重传尝试表明之前的连接请求没有成功。

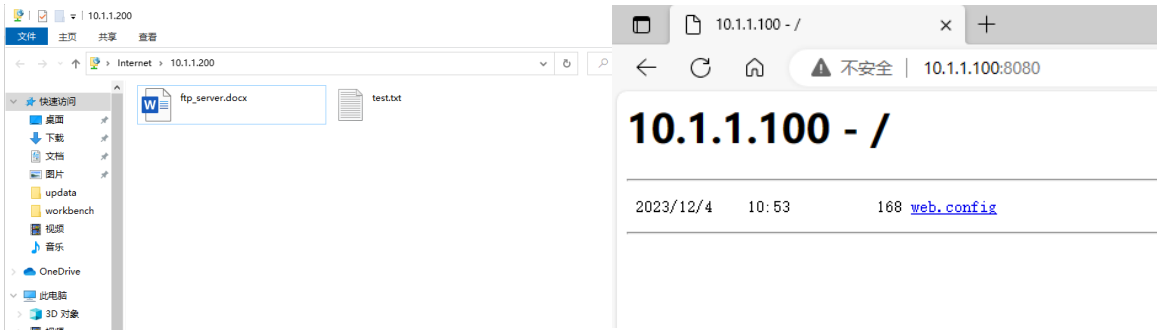
4) 改变路由器系统时间段,在其他时间段执行(2)~(3)的测试

```
17-RSR20-1#clock set 18:23:06 1 2 2023
17-RSR20-1#*Jan  2 18:23:06: %SYS-6-CLOCKUPDATE: System clock has been updated t
o 18:23:06 UTC Mon Jan  2 2023.
```

位于下班时间，预期员工机只能访问 WWW 不能访问 FTP，经理机都可以访问。

我们先分析经理机，预期访问结果不会发生改变。

下班时间，经理机登录 FTP 服务器和 WWW 服务器：



如上图，下班时间，经理机可以访问 FTP 和 WWW，符合 ACL 规则，符合预期。

经理机访问 WWW 服务器的 TCP 包和 HTTP 包如下，可见确实建立了 TCP 和 HTTP 连接

292	97.258233	192.168.1.254	10.1.1.100	TCP	66 58131 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
293	97.259085	10.1.1.100	192.168.1.254	TCP	66 80 → 58131 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
294	97.259123	192.168.1.254	10.1.1.100	TCP	54 58131 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
295	97.262154	192.168.1.254	10.1.1.100	HTTP	627 GET / HTTP/1.1
312	99.384970	192.168.1.254	10.1.1.100	HTTP	627 GET / HTTP/1.1
313	99.388349	10.1.1.100	192.168.1.254	HTTP	197 HTTP/1.1 304 Not Modified
314	99.436163	192.168.1.254	10.1.1.100	TCP	54 58131 → 80 [ACK] Seq=1634 Ack=430 Win=2101760 Len=0

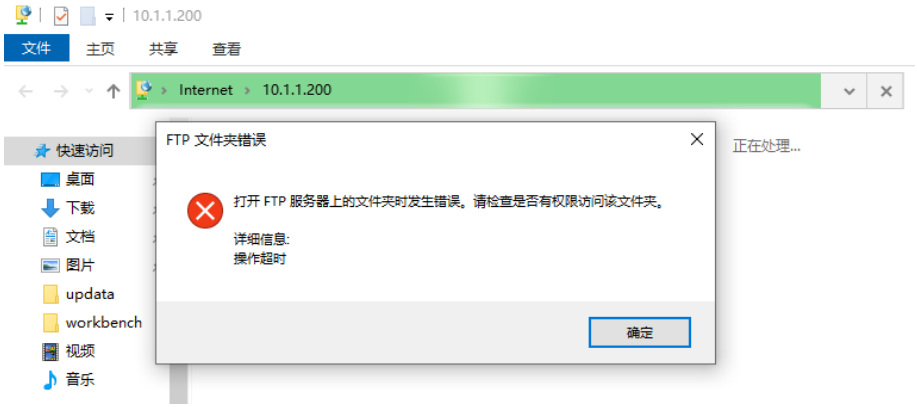
经理机通过 DOS 命令登录 FTP 服务器的包如下，可见确实与 FTP 服务器建立了 TCP 连接

267	92.202737	192.168.1.254	10.1.1.200	TCP	66 58130 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
268	92.204513	10.1.1.200	192.168.1.254	TCP	66 7680 → 58130 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
269	92.204564	192.168.1.254	10.1.1.200	TCP	54 58130 → 7680 [ACK] Seq=1 Ack=1 Win=262656 Len=0
270	92.204725	192.168.1.254	10.1.1.200	TCP	129 58130 → 7680 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=75
271	92.205394	10.1.1.200	192.168.1.254	TCP	129 7680 → 58130 [PSH, ACK] Seq=1 Ack=76 Win=2102272 Len=75
272	92.205643	192.168.1.254	10.1.1.200	TCP	80 58130 → 7680 [PSH, ACK] Seq=76 Ack=76 Win=262656 Len=26
273	92.206076	10.1.1.200	192.168.1.254	TCP	80 7680 → 58130 [PSH, ACK] Seq=76 Ack=102 Win=2102272 Len=26
274	92.206076	10.1.1.200	192.168.1.254	TCP	60 7680 → 58130 [FIN, ACK] Seq=102 Ack=102 Win=2102272 Len=0
275	92.206117	192.168.1.254	10.1.1.200	TCP	54 58130 → 7680 [ACK] Seq=102 Ack=103 Win=262656 Len=0
276	92.206267	192.168.1.254	10.1.1.200	TCP	54 58130 → 7680 [FIN, ACK] Seq=102 Ack=103 Win=262656 Len=0
277	92.206867	10.1.1.200	192.168.1.254	TCP	60 7680 → 58130 [ACK] Seq=103 Ack=103 Win=2102272 Len=0

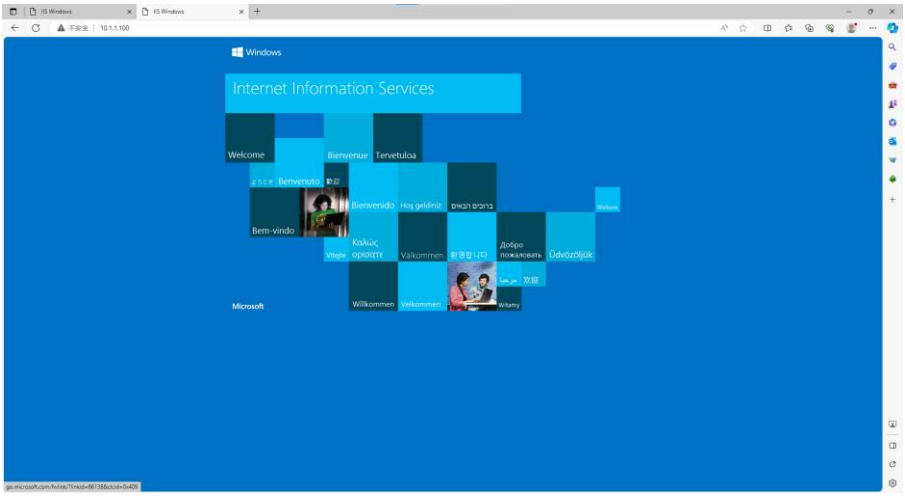
接着我们研究员工机在下班时间对两台服务器的访问

员工机 AB 访问服务器时是等效的，所以我们仅研究一台员工机即可

下班时间，员工机访问 FTP 服务器：



下班时间，员工机访问 WWW 服务器



如上图，下班时间员工机只能访问 WWW，不能访问 FTP，符合 ACL 规则，符合预期

下班时间员工机访问 FTP 的报文如下

52	32.436200	10.1.1.200	192.168.1.3	TCP	66 52839 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	32.436286	192.168.1.3	10.1.1.200	TCP	66 7680 → 52839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
54	33.447712	10.1.1.200	192.168.1.3	TCP	66 [TCP Retransmission] 52839 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
55	33.448538	192.168.1.3	10.1.1.200	TCP	66 [TCP Retransmission] 7680 → 52839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

出现了“TCP Retransmission”，这表明 SYN 包或[SYN,ACK]需要重新发送，这是因为员工机和服务器都没有收到对方发生的数据包。**这个过程中，员工机和服务器之间的传输要通过路由器，而路由器设置了 ACL 规则，且路由器时间是下班时间，所以路由器过滤了员工机和 FTP 服务器的数据包，使得这些数据包不能到达 dst**

5) 捕获主机访问服务器时的数据包，并进行分析。

员工机 192.168.1.3 访问 FTP 服务器 10.1.1.200 时，进行 wireshark 抓包

上班时间，员工机访问 FTP 服务器，分析数据包

首先，三次挥手建立 TCP 连接

No.	Time	Source	Destination	Protocol	Length	Info
596	177.540851	192.168.1.3	10.1.1.200	TCP	66	64473 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
597	177.541039	10.1.1.200	192.168.1.3	TCP	66	21 → 64473 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
598	177.541625	192.168.1.3	10.1.1.200	TCP	60	64473 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0

然后，FTP 用户登录

No.	Time	Source	Destination	Protocol	Length	Info
599	177.542191	10.1.1.200	192.168.1.3	FTP	81	Response: 220 Microsoft FTP Service
601	177.542647	192.168.1.3	10.1.1.200	FTP	70	Request: USER anonymous
602	177.542874	10.1.1.200	192.168.1.3	FTP	77	Response: 331 Password required
604	177.543332	192.168.1.3	10.1.1.200	FTP	68	Request: PASS IEUser@
605	177.543590	10.1.1.200	192.168.1.3	FTP	79	Response: 530 User cannot log in.
614	177.547885	10.1.1.200	192.168.1.3	FTP	81	Response: 220 Microsoft FTP Service
616	177.548264	192.168.1.3	10.1.1.200	FTP	65	Request: USER user
617	177.548491	10.1.1.200	192.168.1.3	FTP	77	Response: 331 Password required
619	177.550876	192.168.1.3	10.1.1.200	FTP	67	Request: PASS 123456
620	177.551678	10.1.1.200	192.168.1.3	FTP	75	Response: 230 User logged in.
622	177.552230	192.168.1.3	10.1.1.200	FTP	68	Request: opts utf8 on
623	177.552458	10.1.1.200	192.168.1.3	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON

通过以上抓包分析，认为上班时间员工机访问 FTP 服务器正常，符合 ACL 规则。此时的网络表现和【没有设置 ACL 规则】时是一样的，符合我们的预期。

下班时间员工机访问 FTP 的报文如下

52	32.436200	10.1.1.200	192.168.1.3	TCP	66 52839 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	32.436286	192.168.1.3	10.1.1.200	TCP	66 7680 → 52839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
54	33.447712	10.1.1.200	192.168.1.3	TCP	66 [TCP Retransmission] 52839 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
55	33.448538	192.168.1.3	10.1.1.200	TCP	66 [TCP Retransmission] 7680 → 52839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

出现了“TCP Retransmission”，这表明 SYN 包或[SYN,ACK]需要重新发送，这是因为员工机和服务器都没有收到对方发生的数据包。**这个过程中，员工机和服务器之间的传输要通过路由器，而路由器设置了 ACL 规则，且路由器时间是下班时间，所以路由器过滤了员工机和 FTP 服务器的数据包，使得这些数据包不能到达 dst**

“Retransmission”是由 ACL 导致。如果 ACL 阻止了数据包的传递，那么发送方（员工机）不会收到期待的回应，因此会触发重传机制，尝试重新发送数据包

抓包分析符合预期。