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	计算机学院	班 级	行政 4 班	组长	李钰
学号	19335112	19335134	19335156		
学生	李钰	林雁纯	毛羽翎		
实验分工					
李钰	负责路由器的配置以及 ftp 服务器的搭建	林雁纯	负责 www 服务器的搭建以及操作三台主机		
毛羽翎	负责 www 服务器的搭建，查找资料				

【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 8-4　配置基于时间的 ACL

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图 8-8 所示。

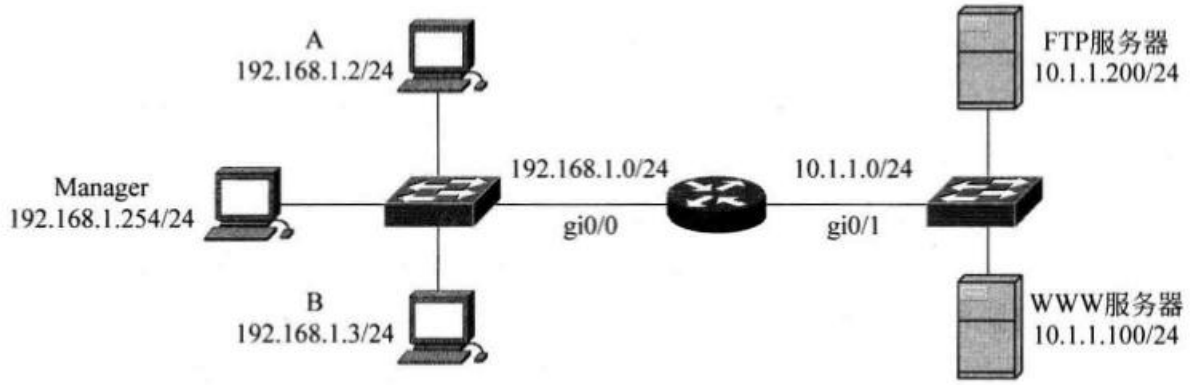


图 8-8　基于时间 ACL 的实验拓扑

计算机网络实验报告

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)

实验步骤

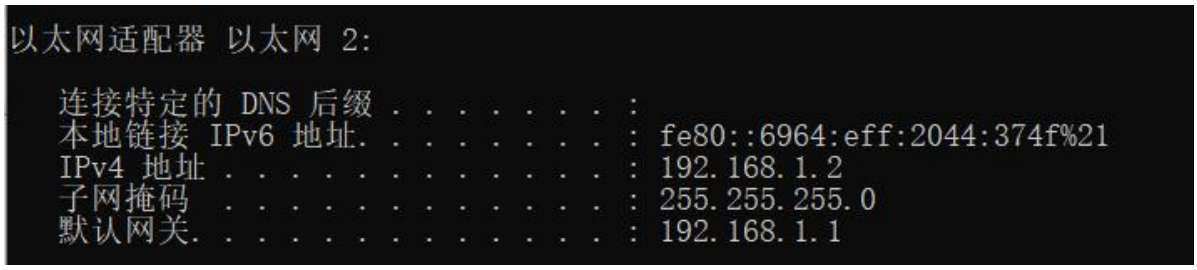
分析：（根据理解自行写出）

步骤 1:

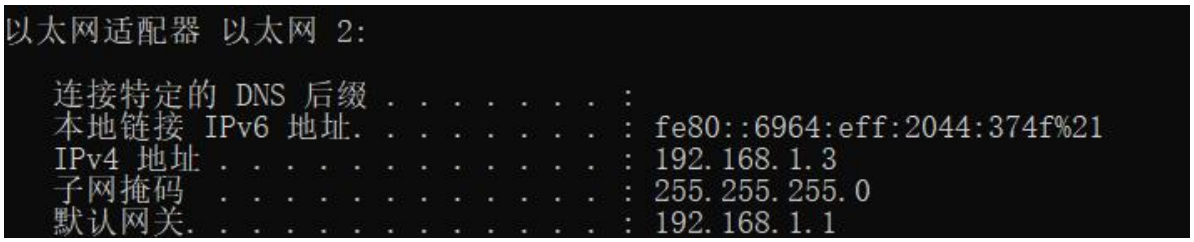
(1) 配置 3 台计算机(A、B 和 Manager)以及两台服务器的 IP 地址、子网掩码、网关。

主机/服务器	IP 地址	子网掩码	网关
A	192.168.1.2	255.255.255.0	192.168.1.1
B	192.168.1.254	255.255.255.0	192.168.1.1
Manager	192.168.1.3	255.255.255.0	192.168.1.1
ftp 服务器	10.1.1.200	255.255.255.0	10.1.1.1
www 服务器	10.1.1.100	255.255.255.0	10.1.1.1

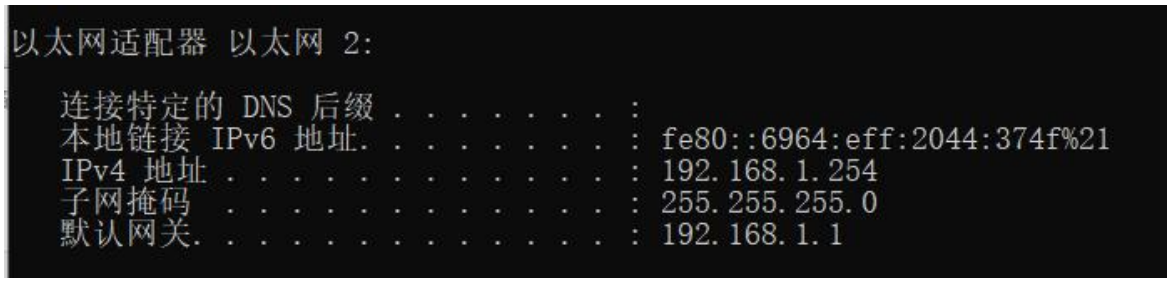
A



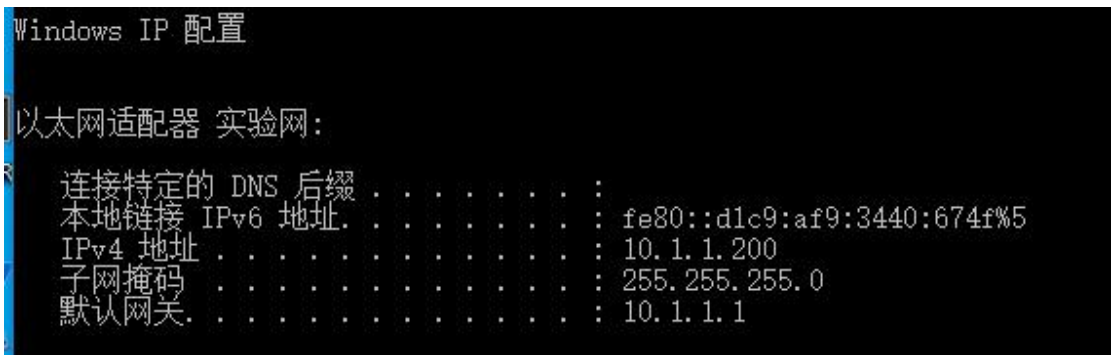
B



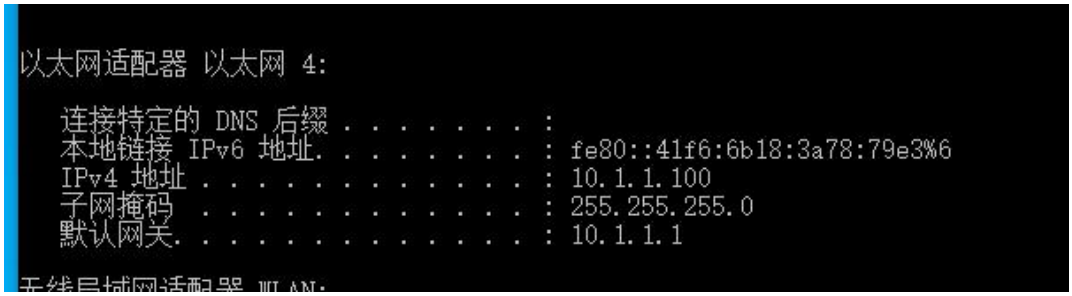
Manager



ftp 服务器

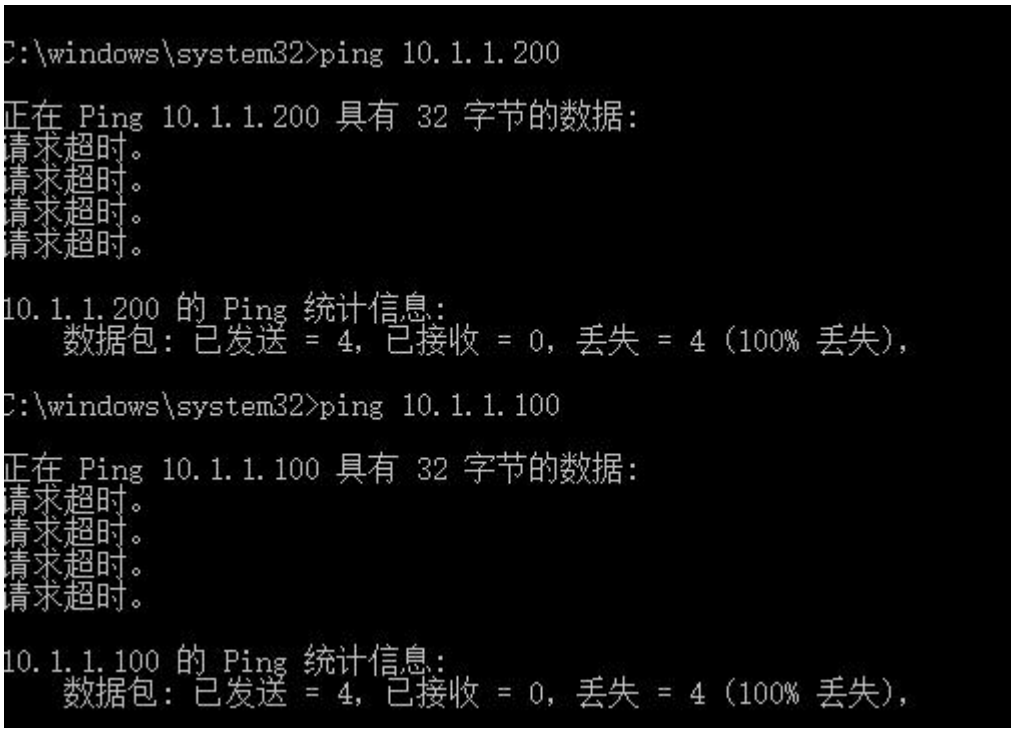


www:



(2) 检查计算机与服务器的连通性。

此时还没有进行相应配置，所以主机与服务器之间无法联通



(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。

ly 12345

A. 关于 ftp 服务器的搭建

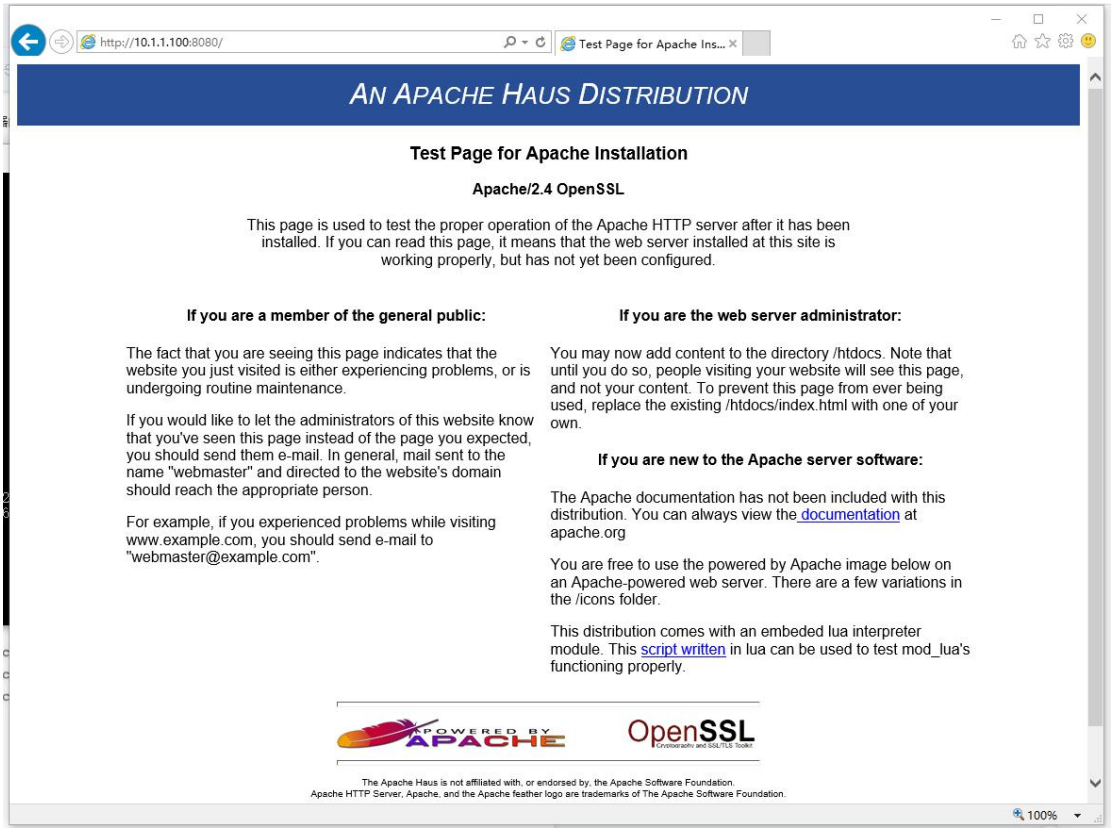
这里我们下载了 FileZilla 软件用于搭建一个 ftp 服务器，参照教程进行配置。（https://jingyan.baidu.com/article/63f236286ca3d60208ab3d23.html）

在 ftp 服务器上创建了一个共享文件 hahaha.txt。创建了一个用户‘ly’，其密码为 12345.最后搭建成功后，在本机浏览器页面中输入 ftp://10.1.1.200 可以访问成功，如下图所示。

B. 关于 www 服务器的搭建

这里我们下载了 Apache 软件，参照的教程是这篇博客（https://www.cnblogs.com/wcwnina/p/8044353.html），之后进行了 www 服务器的搭建，最后在本机浏览器中输入 http://10.1.1.100:8080/可以访问成功。

这里要注意的是我们在搭建过程中更改了端口号，访问时输入的网址后面要标明，不然访问不成功。最后成功访问 www 服务器。



步骤 2：路由器的基本配置

该步骤为路由器与交换机相连的两个端口设置了 IP 地址

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

步骤 3:验证当前配置。

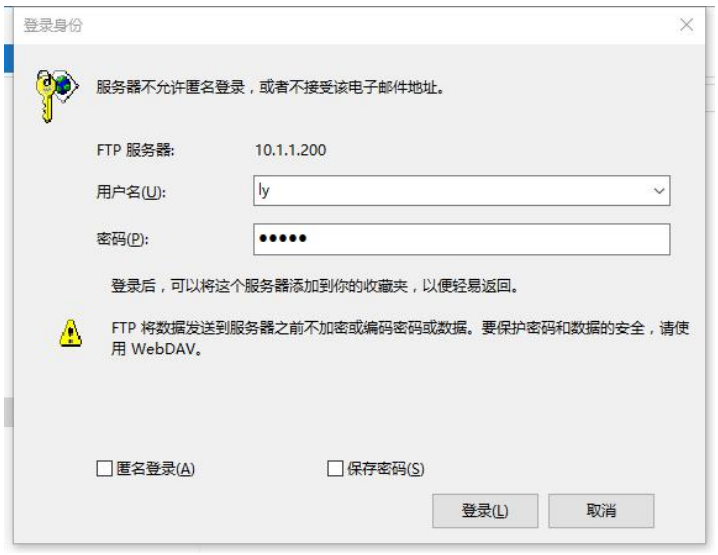
(1) 验证主机与服务器的连通性。

此时路由器的配置已经完成，ftp 和 www 服务器也已搭建完成，这时三台 PC 机都可以连通服务器。这里以 Manager 为例

```
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<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:\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=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
```

(2) 经理机和员工机能否登录 FTP 服务器?通过 http://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。

经理机和员工机都可以登录 ftp 服务器。如下图，在本机网络中搜索 ftp://1.1.1.200，输入正确的用户名 ly 和正确的密码 12345 即可登录 ftp



同时，经理机和员工机也都可以访问 http://10. 1. 1. 100，如下图。

步骤 4:配置时间段。

定义正常上班的时间段，将其设置为上午 9 点到下午 6 点

```
                down
26-RSR20-1(config)#time-range work-time
26-RSR20-1(config-time-range)#periodic weekdays 09:00 to 18:00
26-RSR20-1(config-time-range)#exit
26-RSR20-1(config)#
```

步骤 5：配置 ACL

配置 ACL 并应用时间段，通过 permit 和 deny 指令，实现需求中基于时间段的访问控制

```
26-RSR20-1(config)#ip access-list extended accessctrl
26-RSR20-1(config-ext-nacl)#$255 host 10.1.1.200 eq ftp time-range work-time
permit ip host 192.168.1.0 0.0.0.255 host 10.1.1.200 eq ftp time-range work-t
ime                                  ^
% Invalid input detected at '^' marker.

26-RSR20-1(config-ext-nacl)#permit ip host 192.168.1.254 10.1.1.0 0.0.0.255
26-RSR20-1(config-ext-nacl)#$host 10.1.1.200 eq ftp time-range work-time
26-RSR20-1(config-ext-nacl)#$1.200 eq ftp-data time-range work-time
26-RSR20-1(config-ext-nacl)#$st 10.1.1.100 eq www time-range work-time
26-RSR20-1(config-ext-nacl)#$8.1.0 0.0.0.255 host 10.1.1.100 eq www
26-RSR20-1(config-ext-nacl)#exit
26-RSR20-1(config)#
```

步骤 6:

应用 ACL.,将 ACL 应用到端口 0/0 的输入方向。

```
26-RSR20-1(config)#interface gigabitethernet 0/0
26-RSR20-1(config-if-GigabitEthernet 0/0)#ip access-group accessctrl in
26-RSR20-1(config-if-GigabitEthernet 0/0)#end
26-RSR20-1#*Jun  7 18:15:07: %SYS-5-CONFIG_I: Configured from console by console
```

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实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,

```
26-RSR20-1#show clock
18:16:16 UTC Mon, Jun 7, 2021
26-RSR20-1#
```

(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?

(3)

在 18：16 是下班时间 或是将时间设置为 12：00（上班时间），经理机都可以访问到 ftp 和 www

```
26-RSR20-1#show clock
18:16:16 UTC Mon, Jun 7, 2021
26-RSR20-1#
```

```
26-RSR20-1#clock set 12:00:00 6 9 2021
26-RSR20-1#*Jun  9 12:00:00: %SYS-6-CLOCKUPDATE: Syste
o 12:00:00 UTC Wed Jun  9 2021.

26-RSR20-1#ahow clock
% Unknown command.

26-RSR20-1#show clock
12:00:12 UTC Wed, Jun 9, 2021
26-RSR20-1#
```

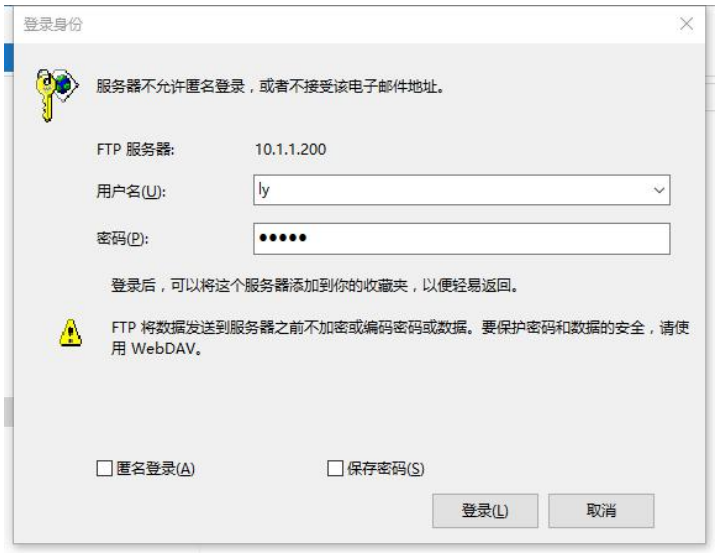
(4) 普通员工主机 A,B 分别使用步骤 1 建立的用户名登录 FTP 服务器,并通过 http://10. 1.1. 100 访问 www 服务器,在设定时间段内是否能登录和访问(登录 FTP 时分别通过 DOS 命令与浏览器方式,结合捕获报文分析)?

将时间设置为

2021 年 6 月 9 日 星期三中午十二点，是上班时间

```
26-RSR20-1#clock set 12:00:00 6 9 2021
26-RSR20-1#*Jun  9 12:00:00: %SYS-6-CLOCKUPDATE: Syste
o 12:00:00 UTC Wed Jun  9 2021.

26-RSR20-1#ahow clock
% Unknown command.

26-RSR20-1#show clock
12:00:12 UTC Wed, Jun 9, 2021
26-RSR20-1#
```

员工及在上班时间可以访问到 ftp 但是访问不了 www 服务器



通过 DOS 命令登录 ftp

```
C:\windows\system32>ftp
ftp> open 10.1.1.200
连接到 10.1.1.200。
220-FileZilla Server version 0.9.43 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit http://sourceforge.net/projects/filezilla/
530 Please log in with USER and PASS first.
用户(10.1.1.200:(none)): ly
331 Password required for ly
密码:
230 Logged on
ftp>
```

在 Wire Shark 上可以捕捉到 ftp 的报文，可以看到相应的用户名和密码

```
240 467.581298   10.1.1.200      192.168.1.2     FTP      96 Response: 220-FileZilla Server version 0.9.43 beta
241 467.581348   10.1.1.200      192.168.1.2     FTP     114 Response: 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
242 467.581378   10.1.1.200      192.168.1.2     FTP     115 Response: 220 Please visit http://sourceforge.net/projects/filezilla/
244 467.589617   192.168.1.2     10.1.1.200      FTP      68 Request: OPTS UTF8 ON
245 467.589841   10.1.1.200      192.168.1.2     FTP      99 Response: 530 Please log in with USER and PASS first.
261 476.954679   192.168.1.2     10.1.1.200      FTP      63 Request: USER ly
262 476.955034   10.1.1.200      192.168.1.2     FTP      84 Response: 331 Password required for ly
265 479.891351   192.168.1.2     10.1.1.200      FTP      66 Request: PASS 12345
266 479.891671   10.1.1.200      192.168.1.2     FTP      69 Response: 230 Logged on
```

(5) 改变路由器系统时间段,在其他时间段执行(2)~(3)的测试。

在时间为 2021 年 7 月 7 日 星期一 18：16 即下班时间时

```
26-RSR20-1#show clock
18:16:16 UTC Mon, Jun 7, 2021
26-RSR20-1#
```

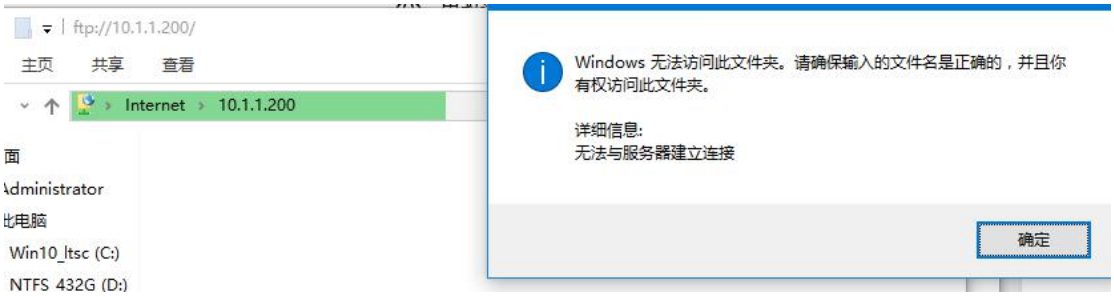
在下班时间访问不了 ftp 但是可以访问到 www 服务器

员工机访问 ftp 失败

无法显示此页

- 确保 Web 地址 ftp://10.1.1.200 正确。
- 使用搜索引擎查找页面。
- 请过几分钟后刷新页面。

修复连接问题



访问 www 服务器成功

(6) 捕获主机访问服务器时的数据包,并进行分析。ACL 应用广泛,例如在 NAT,IPv4-1Pv6 地址翻译、VPN 技术、Qos 中都使用了 ACL.因此需要熟练掌握。

对 manager 访问 web 时进行抓包

24	6.487068	192.168.1.254	10.1.1.100	TCP	66 2006 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
25	6.487185	192.168.1.254	10.1.1.100	TCP	66 2007 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	6.487542	10.1.1.100	192.168.1.254	TCP	66 8080 → 2006 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
27	6.487543	10.1.1.100	192.168.1.254	TCP	66 8080 → 2007 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
28	6.487617	192.168.1.254	10.1.1.100	TCP	54 2006 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
29	6.487624	192.168.1.254	10.1.1.100	TCP	54 2007 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
30	6.488323	192.168.1.254	10.1.1.100	HTTP	543 GET / HTTP/1.1
31	6.491238	10.1.1.100	192.168.1.254	HTTP	264 HTTP/1.1 304 Not Modified
32	6.688659	192.168.1.254	10.1.1.100	TCP	54 1999 → 8080 [ACK] Seq=490 Ack=211 Win=63820 Len=0

会先进行 tcp 的三次握手

可以看到 30：HTTP 请求以及 31：HTTP 响应

- HTTP 请求消息头

1〉Accept：call 服务器，可以接收文件、网页和图片。

2〉Accept-Charset：所接收的字符编码。

3〉Accept-Encoding：可接收（）压缩后的数据。

4〉Accept-Language：Browser 支持中、英文。

5〉Host：要找的主机是。

6〉If-Modified-Since：告诉服务器我们的缓冲中有这个资源文件，该文件的时间是，,

7〉Referer：告诉服务器，我来自哪里。

8〉User-Agent：告诉服务器，Browser 内核。

9〉Cookie：

10〉Connection：保持连续发完信息后，我不关闭连接。

11〉Date：Browser 发送时间。

可以看到 http 请求报头

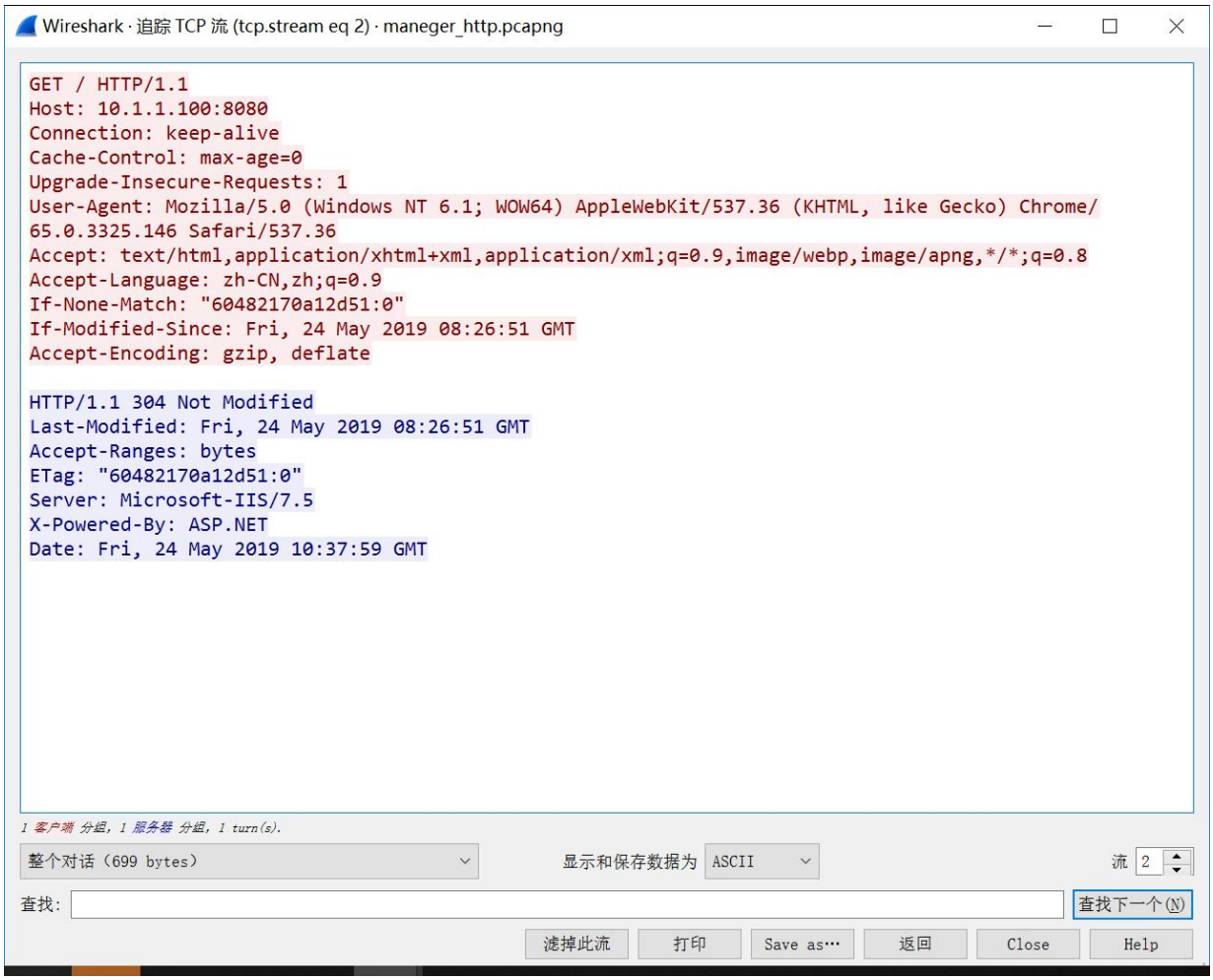
```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: 10.1.1.100:8080\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Language: zh-CN,zh;q=0.9\r\n
  If-None-Match: "60482170a12d51:0"\r\n
  If-Modified-Since: Fri, 24 May 2019 08:26:51 GMT\r\n
  Accept-Encoding: gzip, deflate\r\n
  \r\n
  [Full request URI: http://10.1.1.100:8080/]
  [HTTP request 1/1]
  [Response in frame: 31]
```

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Last-Modified: Fri, 24 May 2019 08:26:51 GMT\r\n
  Accept-Ranges: bytes\r\n
  ETag: "60482170a12d51:0"\r\n
  Server: Microsoft-IIS/7.5\r\n
  X-Powered-By: ASP.NET\r\n
  Date: Fri, 24 May 2019 10:37:59 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.002915000 seconds]
  [Request in frame: 30]
  [Request URI: http://10.1.1.100:8080/]
```

计算机网络实验报告

http 响应数据包报头分析

追踪 tcp 流



【实验结果】

1.无论何时 Manager 都可以访问两个服务器

2.员工只能在 weekdays work-time 访问 FTP

3.员工只能在 weekdays work-time 以外时间访问 WWW

【实验心得】

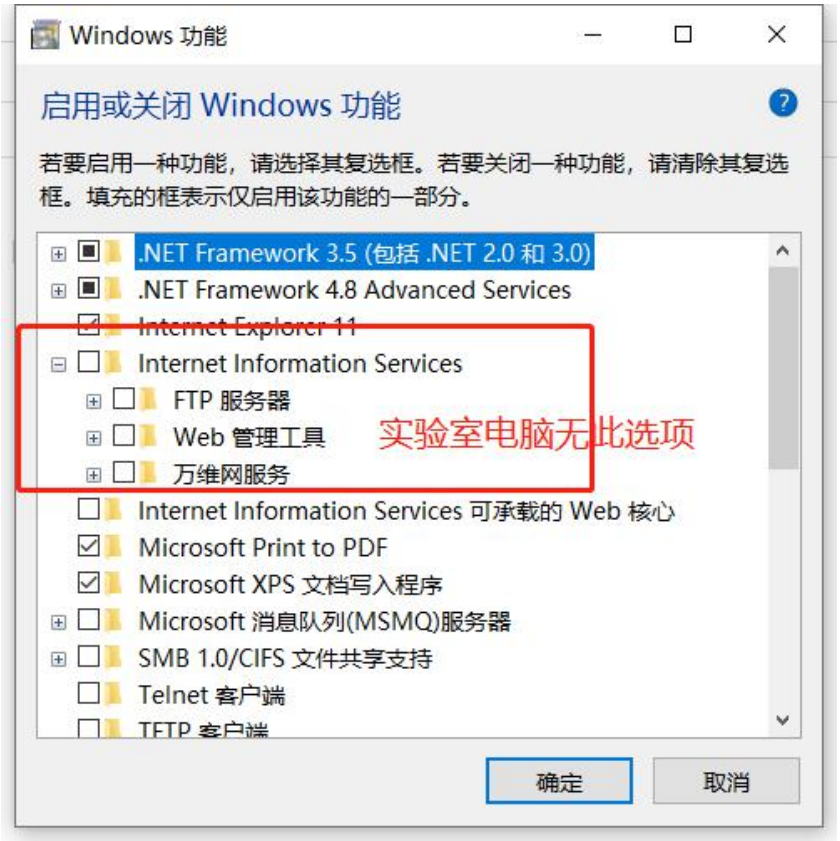
这次实验主要学习了 ACL，访问控制表，掌握标准访问列表规则及配置。 主要是要特别注意指令的顺序。掌握扩展访问列表规则及配置，扩展访问增加了一些指令。

了解标准访问列表和扩展访问列表的区别。访问控制列表(ACL)是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪能些数据包可以收、哪能数据包需要拒绝。至于数据包是被接收还是拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来决定。扩展访问控制列表其中重要的一种是 IP 访问控制列表。扩展 IP 访问控制列表比标准 IP 访问控制列表具有更多的匹配项，包括协议类型、源地址、目的地址、源端口、目的端口、建立连接的和 IP 优先级等。编号范围是从 100 到 199 的访问控制列表是扩展 IP 访问控制列表。

实验过程中遇到的困难：

1. 首先不确定主机和服务器的网管是多少，后来看了实验指导书上的参考代码发现在设置路由器的时候指令中有涉及。

2. 一开始老师给出了搭建 ftp 服务器和 www 服务器的方法，但是因为实验室的电脑没有相应配置选项，如下图



所以我们搜索了其他解决方案。在网上查找到可通过 File Zilla 软件搭建一个 ftp 服务器，Apache 软件搭建 www 服务器，按照教程，完成了相关配置。

3. 接着在配置完路由器之后验证主机和服务器的连通性时，也是需要断开校园网连接的。

【自评】

学号	学生	自评分
19335112	李钰	99
19335134	林雁纯	99
19335156	毛羽翎	99