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	电子与信息工程学院	班 级	通信工程 1 班	组长	刘渤
学号	16308073	16308161	16308091	16308015	
学生	刘渤	邹紫婧	彭肖文	陈瑞佳	
实验分工					
刘渤	访问控制列表（ACL）模块 贡献：25%		邹紫婧	访问控制列表（ACL）模块 贡献：25%	
彭肖文	访问控制列表（ACL）模块 贡献：25%		陈瑞佳	访问控制列表（ACL）模块 贡献：25%	

【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】

第二版：

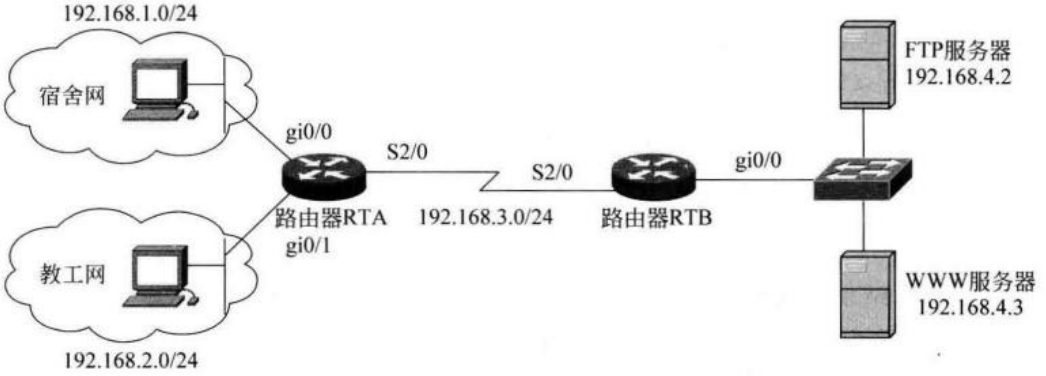
1. 完成实验 8.2 配置扩展 IP ACL（P288），在步骤 1 之前，请设计步骤 0（即实验前的情况，包括安装与建立 FTP、WEB），要求写出详细的步骤；

2. 完成步骤 8 的验证测试。

一、访问控制列表（ACL）实验

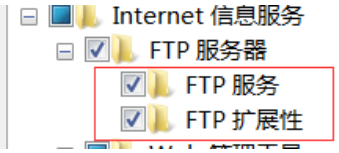
步骤 0、1：按照拓扑图上的标示，配置实验主机的 IP 地址、子网掩码、网关，并且测试它们的连通性。

按照下图的拓扑结构进行连接，宿舍网以及教工网通过路由器 R1，经由路由器 R2 连接到交换机后分别接到两个服务器上去。



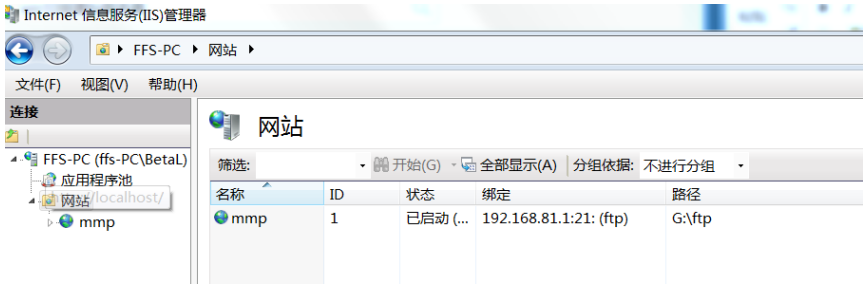
实验拓扑图

对于 FTP 服务器的建立，首先要在控制面板的程序界面找到 windows 功能一项，然后将 FTP 服务以及 FTP 扩展性两项功能打开。如下图：



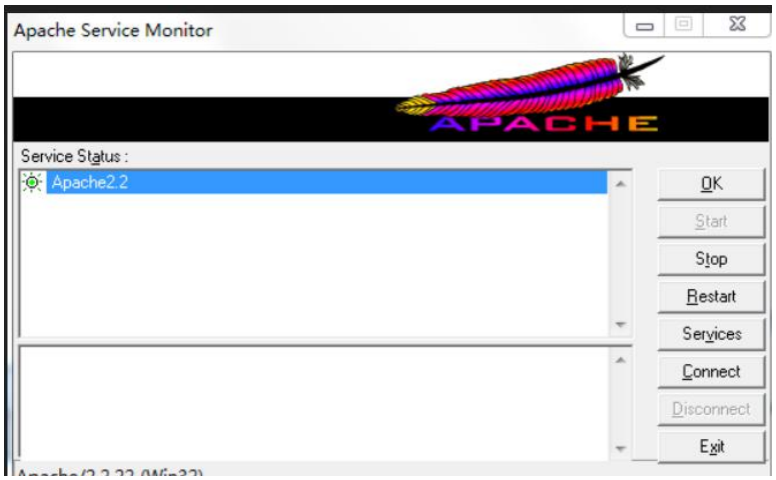
开启服务图

然后进行 IIS 管理器的配置，通过在网站一处添加 FTP 站点，设置好用户名后配置成功：



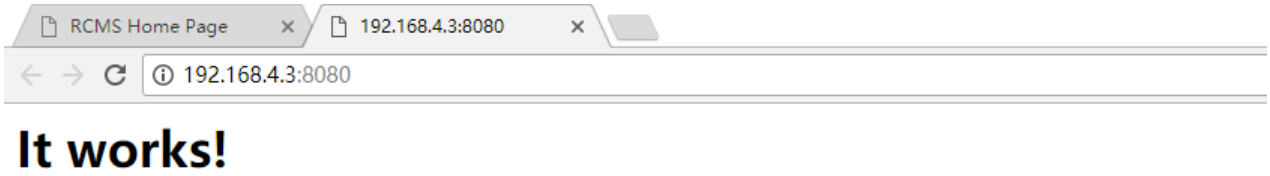
配置成功后用户图

对于 WWW 服务器的开通，使用 Apache Server 进行配置，按照指导文件进行配置后：



配置图

可以看到我们工作的页面：



www 服务器配置图

① 查连通性

根据拓扑图上对于每一台主机或者服务器进行 IP 地址的配置以及子网掩码、还有网关的设置后进行 PING 操作，可以看到我们此时是不通的。

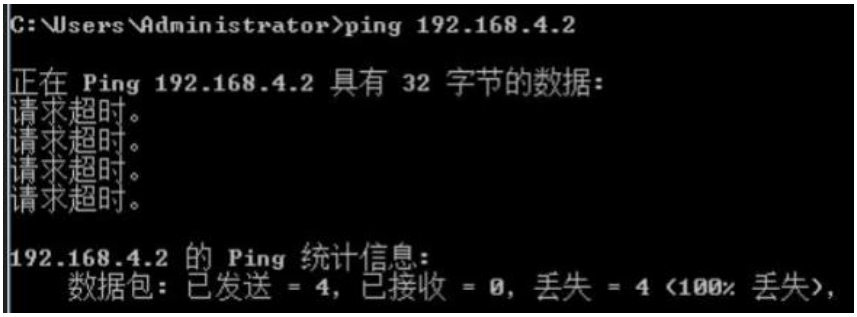


图 1-2 实验前 互不连通

在实验前，因为路由没有邻居路由和交换机的信息，不知道其他子网的信息，所以 ping 不通。同时 FTP 以及 WWW 的访问也无法接通。

步骤 2~4：配置路由器 RTA 以及 RTB，并且查看它们的端口状态。

根据指令进行配置后，使用 show ip interface brief 进行查看各端口的状态。

```
22-RSR20-1(config)#show ip interface brief
Interface                  IP-Address(Pri)      IP-Address(Sec)      Statu
s                Protocol
Serial 2/0                 192.168.3.1/24       no address           up
                 up
SIC-3G-WCDMA 3/0           no address           no address           up
                 down
GigabitEthernet 0/0        192.168.1.1/24       no address           up
                 up
GigabitEthernet 0/1        192.168.2.1/24       no address           down
                 down
VLAN 1                     no address           no address           up
                 down
```

路由器 RTA 的端口状态

可以看到 2/0 端口接到路由器 RTB，而 0/0 端口与 0/1 端口分别对应于宿舍网与教工网。

```
22-RSR20-2(config)#show ip interface brief
Interface                  IP-Address(Pri)      IP-Address(Sec)      Statu
s                Protocol
Serial 2/0                 192.168.3.2/24       no address           up
                 up
Serial 3/0                 no address           no address           down
                 down
GigabitEthernet 0/0        192.168.4.1/24       no address           up
                 up
GigabitEthernet 0/1        no address           no address           down
                 down
VLAN 1                     no address           no address           up
                 down
```

路由器 RTB 端口配置

而路由器 RTB 对应于 2/0 端口连接路由器 RTA，同时连接到 4.0 网段的交换机上去。

步骤 5~6：配置静态路由之后验证主机与服务器的连通性。

对于配置之后宿舍网与教工网对于服务器的访问理论上都是可以的，因为我们的链路已经打通，同时没有任何的限制，所以都可以连通。

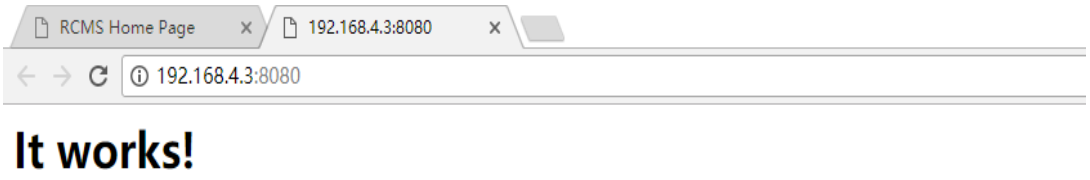
www 访问图如下：

```
C:\Users\Administrator>ping 192.168.4.3

正在 Ping 192.168.4.3 具有 32 字节的数据:
来自 192.168.4.3 的回复: 字节=32 时间=35ms TTL=126
来自 192.168.4.3 的回复: 字节=32 时间=41ms TTL=126
来自 192.168.4.3 的回复: 字节=32 时间=37ms TTL=126
来自 192.168.4.3 的回复: 字节=32 时间=38ms TTL=126

192.168.4.3 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 = 35ms, 最长 = 41ms, 平均 = 37ms
```

www 范问图



www 登录界面

对于 ftp，根据老师的讲法，是无法 ping 到的，因为我们没有允许它进行 ping，所以只能通过登录来实现检查互连，下图：

ftp 登录界面

根据我们所要配置的目的以及对应的效果可以看到我们达到了实验的预处理效果。

步骤 7：配置扩展 ACL 检验连通性（对于教工网与宿舍网的配置，我们将其 IP 地址相反过来配置）。

① 经过 ACL 之后，教工网对于 FTP 以及 WWW 都是可以访问的，因为访问的截图与前面一模一样，此处省略，直接看访问报文：

因为我们已经允许教工网进行范问 FTP 以及 WWW：

```
RTA (config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.4.2 eq
ftp-data
                !允许来自教工网 192.168.2.0/24 子网的到达 FTP 服务器(192.168.4.2)的流量
RTA (config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.4.3
eq www
                !允许来自教工网 192.168.2.0/24 子网的到达 WWW 服务器(192.168.4.3)的流量
```

配置图

因此我们可以看到访问 WWW 的报文

3	0.000333	192.168.2.2	192.168.4.3	TCP	66 3859 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	0.056075	192.168.4.3	192.168.2.2	TCP	66 8080 → 3859 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	0.056127	192.168.2.2	192.168.4.3	TCP	54 3859 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
11	0.056557	192.168.2.2	192.168.4.3	HTTP	558 GET / HTTP/1.1
14	0.185982	192.168.4.3	192.168.2.2	HTTP	247 HTTP/1.1 304 Not Modified
15	0.227064	192.168.2.2	192.168.4.3	TCP	54 3859 → 8080 [ACK] Seq=505 Ack=194 Win=65280 Len=0
16	1.529615	192.168.2.2	192.168.4.3	HTTP	558 GET / HTTP/1.1
17	1.649919	192.168.4.3	192.168.2.2	HTTP	246 HTTP/1.1 304 Not Modified
18	1.690855	192.168.2.2	192.168.4.3	TCP	54 3859 → 8080 [ACK] Seq=1009 Ack=386 Win=65280 Len=0
46	6.622930	192.168.4.3	192.168.2.2	TCP	60 8080 → 3859 [FIN, ACK] Seq=386 Ack=1009 Win=64512 Len=0
47	6.622989	192.168.2.2	192.168.4.3	TCP	54 3859 → 8080 [ACK] Seq=1009 Ack=387 Win=65280 Len=0

www 访问报文

从表中我们可以看到：TCP 的三次握手之后进行 HTTP 的访问，包括释放完成则是四次握手，在这个报文里，出现了请求报文，说明我们也成功进行了访问。

对于 FTP 的访问，则可以看到：

26	5.038984	192.168.2.2	192.168.4.2	TCP	66 3864 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	5.081164	192.168.4.2	192.168.2.2	TCP	66 21 → 3864 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
31	5.081240	192.168.2.2	192.168.4.2	TCP	54 3864 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
32	5.117093	192.168.4.2	192.168.2.2	FTP	81 Response: 220 Microsoft FTP Service
33	5.117256	192.168.2.2	192.168.4.2	FTP	64 Request: AUTH TLS
34	5.162362	192.168.4.2	192.168.2.2	FTP	121 Response: 534 Local policy on server does not allow TLS secure connections.
35	5.162565	192.168.2.2	192.168.4.2	FTP	64 Request: AUTH SSL
36	5.202445	192.168.4.2	192.168.2.2	FTP	121 Response: 534 Local policy on server does not allow TLS secure connections.
37	5.202638	192.168.2.2	192.168.4.2	FTP	70 Request: USER anonymous
38	5.246992	192.168.4.2	192.168.2.2	FTP	126 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
39	5.247149	192.168.2.2	192.168.4.2	FTP	75 Request: PASS anon@localhost
40	5.284679	192.168.4.2	192.168.2.2	FTP	75 Response: 230 User logged in.
41	5.284836	192.168.2.2	192.168.4.2	FTP	68 Request: OPTS UTF8 ON
42	5.329245	192.168.4.2	192.168.2.2	FTP	112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
43	5.330598	192.168.2.2	192.168.4.2	FTP	59 Request: PWD
44	5.365632	192.168.4.2	192.168.2.2	FTP	85 Response: 257 "/" is current directory.
45	5.408340	192.168.2.2	192.168.4.2	TCP	54 3864 → 21 [ACK] Seq=77 Ack=344 Win=65280 Len=0

ftp 范问报文

同样可以看到经过三次握手之后，进行 FTP 协商，应为我们的用户设置为匿名登录，可以看到 USER anonymous 的格式，表示匿名登录，然后是找到了“/”文件夹，说明我们访问成功了。

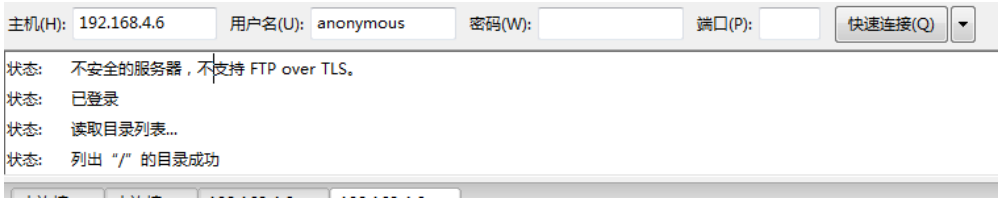
② 对于宿舍网的访问：

因为我们经过了一定的 ACL 配置后，使得宿舍网只能访问 FTP 而不能访问 WWW，经过的配置图如下：

```
RTA (config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.4.2
eq ftp
RTA (config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.4.2 eq
ftp-data
                !允许来自宿舍网 192.168.1.0/24 子网的到达 FTP 服务器(192.168.4.2)的流量
RTA (config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.4.2
eq ftp
```

宿舍网的 ACL 配置

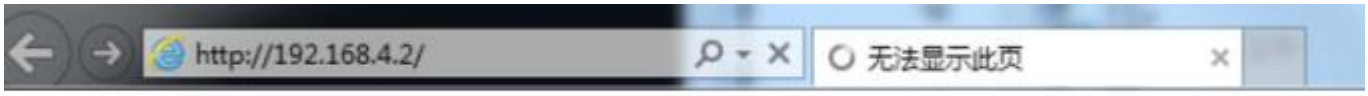
经过配置之后，可以看到对于 FTP 的访问还是可以的，但是对于 WWW 的访问是受限的。



ftp 登录图

因为主机登录 ftp 的模式与教工网一模一样，因此此处的报文与上面的报文分析一样。

而对于 WWW 的访问，则不通，达到实验目的：



www 访问图

对于扩展 ACL 的实验中，可以额对数据包中的源 IP 地址、目的地址以及协议、源端口还有目的端口进行检查，实现更加精确的流量控制，同时这种更加多选项的数据包检查，对于高级复杂的访问更加有控制效果，提高了网络的安全性。

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
16308073	刘渤	100
16308161	邹紫婧	100
16308091	彭肖文	100
16308015	陈瑞佳	100

【交实验报告】

上传实验报告：ftp://222.200.181.161/　　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！