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	1 班 + 保密	组长	马岱
学号	22336180		22336090		
姓名	马岱		黄集瑞		

实验分工

姓名	分工	在本次中的占比
马岱	合作完成实验	50%
黄集瑞	合作完成实验	50%

【实验题目】**扩展访问控制列表实验。**

【实验目的】

1. 掌握扩展访问列表规则及配置。
2. 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 P300【习题 8】，可配置静态路由或 OSPF 路由协议（可加分）

【实验拓扑】

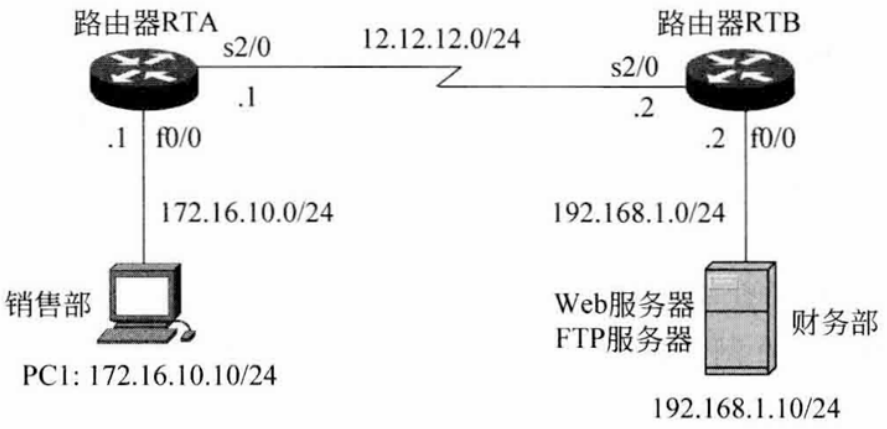


图 8-11　第 8 题实验拓扑

【实验记录】

重要信息需给出截图，**注意实验步骤的前后对比。**

1. 记录配置访问列表前的结果
2. 记录配置访问列表后的结果
3. 记录路由器的路由表，体现静态路由或 OSPF 路由

【实验步骤】

在本次实验中，我们不仅完成了静态路由的配置同时也完成了 OSPF 路由的配置，以下是详细的配置过程：

- 步骤一：

（1） 按拓扑图上的标示，配置 PC1 和 PC2 的 IP 地址、子网掩码、网关，，具体配置过程如下：

我们根据上面的拓扑图，分别将 PC1 和 PC2 的 IP 地址配置成 172.16.10.10 以及 192.168.1.10; 同时将网关分别设置成第一跳路由器的 IP 地址为 172.16.10.1 以及 192.168.1.2。

（2） 按照以上拓扑图，分别在路由器 RTA 和 RTB 处配置端口的 IP 地址，具体配置过程如下：

```
14-RSR20-1(config)#interface gigabitethernet 0/1
14-RSR20-1(config-if-GigabitEthernet 0/1)#$2.16.10.1 255.255.255.0
14-RSR20-1(config-if-GigabitEthernet 0/1)#no shutdown
14-RSR20-1(config-if-GigabitEthernet 0/1)#exit
14-RSR20-1(config)#interface serial 2/0
14-RSR20-1(config-if-Serial 2/0)#ip address 12.12.12.1 255.255.255.0
14-RSR20-1(config-if-Serial 2/0)#no shutdown
14-RSR20-1(config-if-Serial 2/0)#exit
14-RSR20-2(config)#interface gigabitethernet 0/0
14-RSR20-2(config-if-GigabitEthernet 0/0)#$2.168.1.2 255.255.255.0
14-RSR20-2(config-if-GigabitEthernet 0/0)#no shutdown
14-RSR20-2(config-if-GigabitEthernet 0/0)#exit
14-RSR20-2(config)#interface serial 2/0
14-RSR20-2(config-if-Serial 2/0)#ip address 12.12.12.2 255.255.255.0
14-RSR20-2(config-if-Serial 2/0)#no shutdown
14-RSR20-2(config-if-Serial 2/0)#exit
```

- RTA 先配置千兆以太网口 0/0 将其的地址配置为 172.16.10.1，子网掩码为 255.255.255.0，配置完毕后，设置其状态为 no shutdown 打开此端口；然后我们再配置路由串口 2/0 的 IP 地址为 12.12.12.1，子网掩码对应为 255.255.255.0；同样的，配置完成后设置该端口的状态为 no shutdown 来保持连接。
- RTB 先配置千兆以太网口 0/0 将其的地址配置为 192.168.1.2，子网掩码为 255.255.255.0，配置完毕后，设置其状态为 no shutdown 打开此端口；然后我们再配置路由串口 2/0 的 IP 地址为 12.12.12.2，子网掩码对应为 255.255.255.0；同样的，配置完成后设置该端口的状态为 no shutdown 来保持连接。

（3） 先配置静态路由，完成基础任务，具体配置过程如下：

```
14-RSR20-1(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.2

14-RSR20-2(config)#ip route 172.16.10.0 255.255.255.0 12.12.12.1
```

最后，我们设置路由器 RTA 和 RTB 的静态路由，分别使得发往 192.168.1.0 的消息都通过 12.12.12.2 端口和发往 172.16.10.0 的消息都通过 12.12.12.1 端口。

配置结果如下所示：

```
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    12.12.12.0/24 is directly connected, Serial 2/0
C    12.12.12.1/32 is local host.
C    172.16.10.0/24 is directly connected, GigabitEthernet 0/1
C    172.16.10.1/32 is local host.
S    192.168.1.0/24 [1/0] via 12.12.12.2
14-RSR20-1(config)#
```

```
14-RSR20-2(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    12.12.12.0/24 is directly connected, Serial 2/0
C    12.12.12.2/32 is local host.
S    172.16.10.0/24 [1/0] via 12.12.12.1
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.2/32 is local host.
```

可以看到此时两个路由表中都出现了“S”条目，即静态路由的条目，该条目的设置与我们的期望相一致。

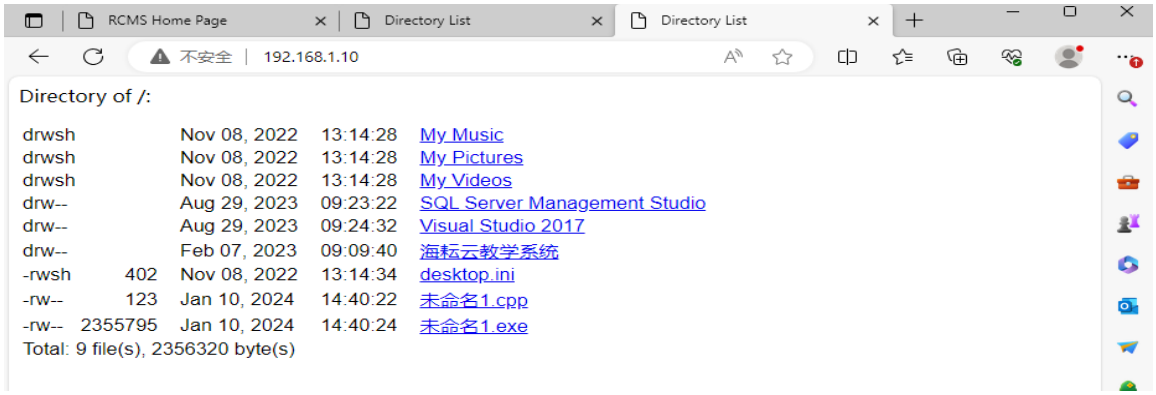
```
14-RSR20-1(config)#show ip interface brief
Interface                  IP-Address(Pri)      IP-Address(Sec)      Statu
s                Protocol
Serial 2/0                 12.12.12.1/24        no address           up
                 up
SIC-3G-WCDMA 3/0           no address           no address           up
                 down
GigabitEthernet 0/0        192.168.1.1/24       no address           down
                 down
GigabitEthernet 0/1        172.16.10.1/24       no address           up
                 up
VLAN 1                     no address           no address           up
                 down
```

```
14-RSR20-2(config)#show ip interface brief
Interface                  IP-Address(Pri)      IP-Address(Sec)      Statu
s                Protocol
Serial 2/0                 12.12.12.2/24        no address           up
                 up
Serial 3/0                 no address           no address           down
                 down
GigabitEthernet 0/0        192.168.1.2/24       no address           up
                 up
GigabitEthernet 0/1        no address           no address           down
                 down
VLAN 1                     no address           no address           up
                 down
```

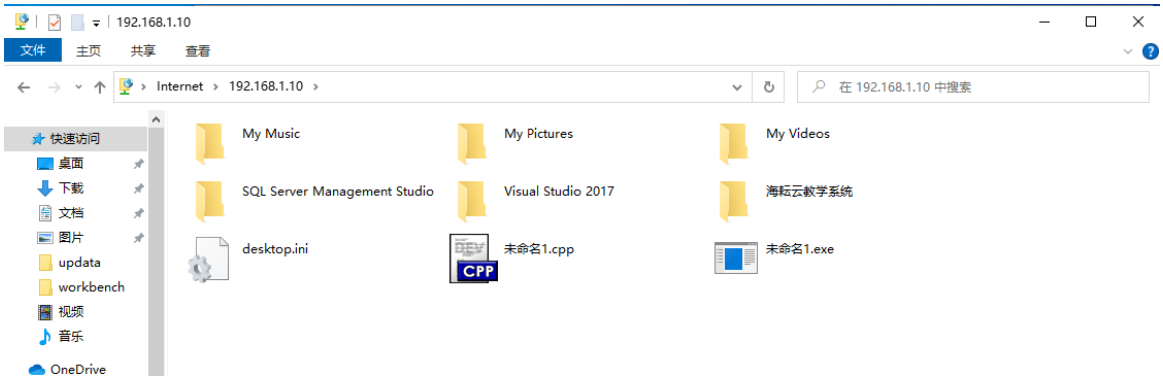
在这里我们可以看到，我们所配置的端口以及 IP 地址均正确，说明我们静态路由配置完成。

（4） 在配置扩展 ACL 之前先检查连通性

1. 允许 172.16.10.0 的主机访问 www 服务器 192.168.1.10（此时访问成功）

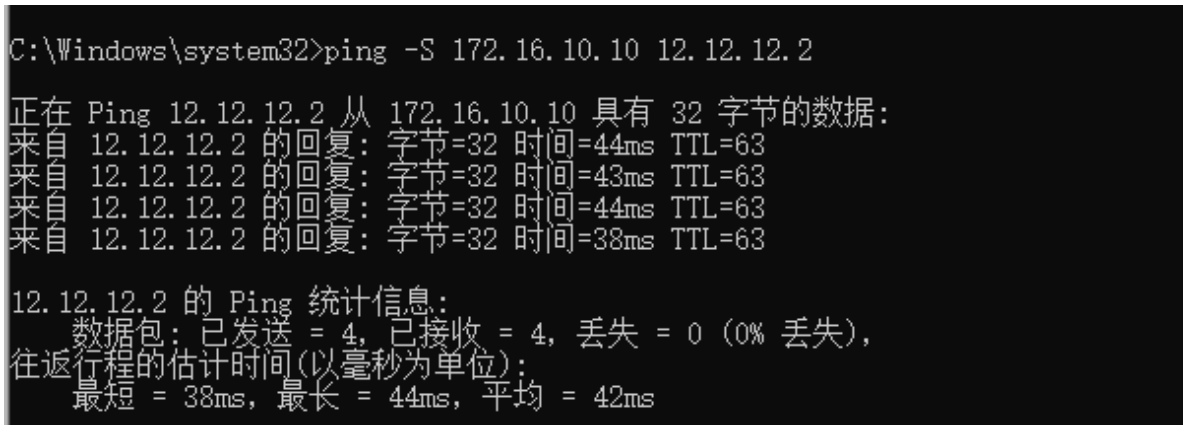


2. 允许 172.16.10.0 的主机访问 FTP 服务器 192.168.1.10（此时访问成功）



3. 允许 172.16.10.0 的主机 Telnet 路由器 RTB（此时访问成功）

4. 允许 172.16.10.0 的主机 ping 路由器 RTB（此时访问成功）



（5） 配置扩展 ACL

```
l4-KSR2U-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
l4-RSR20-1(config)#$it tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq 80
l4-RSR20-1(config)#$ tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq 21
l4-RSR20-1(config)#$ tcp 172.16.10.0 0.0.0.255 host 12.12.12.2 eq 23
l4-RSR20-1(config)#$eny icmp host 172.16.10.10 host 12.12.12.2 echo
no access-list 100 deny icmp host 172.16.10.10 host 12.12.12.2 echo
                   ^
% Invalid input detected at '^' marker.

l4-RSR20-1(config)#$ icmp host 172.16.10.10 host 12.12.12.2 echo
l4-RSR20-1(config)#access-list 100 permit ip any any
l4-RSR20-1(config)#interface f0/0
                           ^
% Invalid input detected at '^' marker.

l4-RSR20-1(config)#interface gigabitethernet 0/1
l4-RSR20-1(config-if-GigabitEthernet 0/1)# ip access-group 100 in
l4-RSR20-1(config-if-GigabitEthernet 0/1)#
```

根据实验要求我们在 RTA 上配置扩展 ACL，这里注意不能配置到 RTB 上，扩展 ACL 建议放在接近流量源的位置，因为可以基于多个条件过滤数据包，可以更早地过滤掉不必要的数据流。我们通过配置 ACL 实现以下 4 个功能：

- access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq 80 允许销售部网络 172.16.10.0 的主机访问 WWW Server 192.168.1.10；80 端口（HTTP 协议，即 WWW 服务）
- access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq 21 拒绝销售部网络 172.16.10.0 的主机访问 FTP Server 192.168.1.10；21 端口（FTP 协议）
- access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 12.12.12.2 eq 23 拒绝销售部网络 172.16.10.0 的主机 Telnet 路由器 RTB；23 端口（Telnet）
- access-list 100 deny icmp host 172.16.10.10 host 12.12.12.2 echo 拒绝销售部主机 172.16.10.10 Ping 路由器 RTB。
- access-list 100 permit ip any any 同时允许其他 ip 地址访问（注意 ospf 必须配置此项）

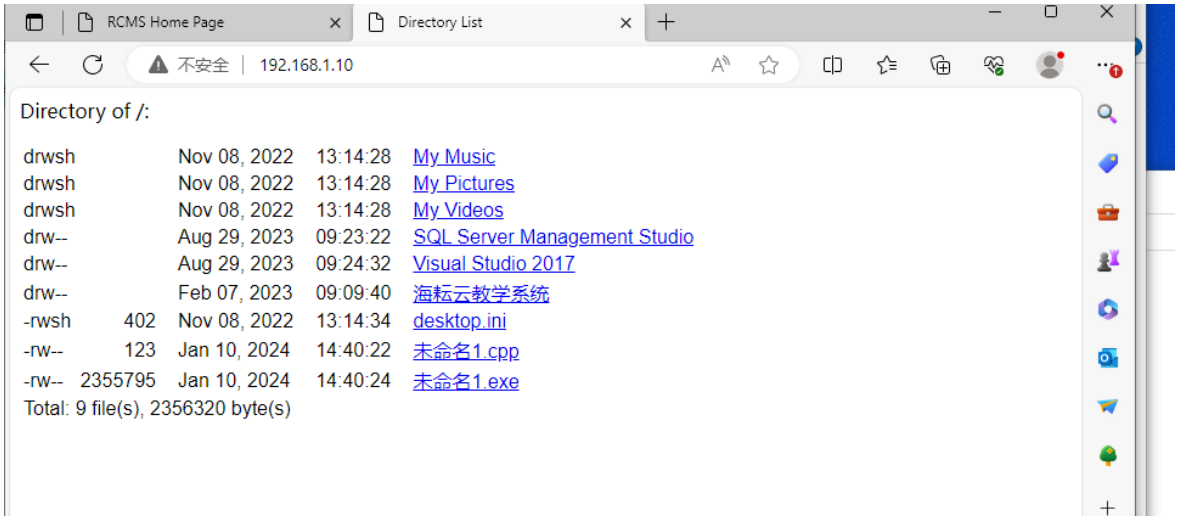
完成 ACL 配置后，需要将其应用到 RTA 的相应接口上，在进入方向配置 interface f0/0 和 ip access-group 100 in 这样就能确保所有来自 172.16.10.0/24 网段的流量按照上述规则进行过滤。通过这些配置，可以精细地控制销售部网络的访问权限，确保符合实验要求

（6） 配置完扩展 ACL，检测实验结果

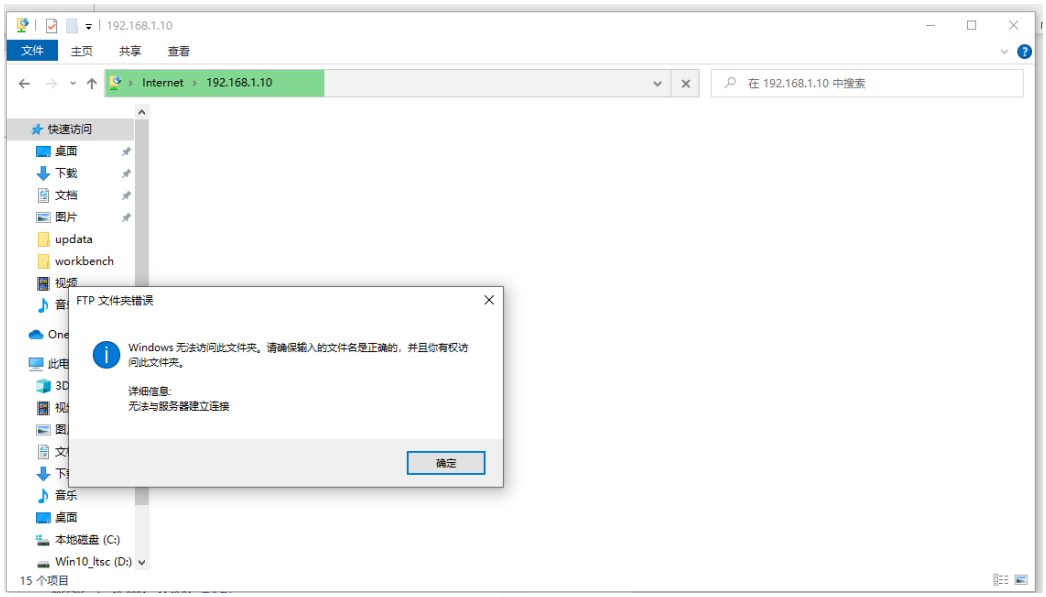
```
ip access-list extended 100
 10 permit tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq www
 20 deny tcp 172.16.10.0 0.0.0.255 host 192.168.1.10 eq ftp
 30 deny tcp 172.16.10.0 0.0.0.255 host 12.12.12.2 eq telnet
 40 deny icmp host 172.16.10.10 host 12.12.12.2 echo
 50 permit ip any any
l4-RSR20-1(config-if-GigabitEthernet 0/1)#
```

可见，我们已经配置 ACL 配置成功，5 条限制已经全部显示在上图。

1. 允许 172.16.10.0 的主机访问 www 服务器 192.168.1.10（此时访问成功）

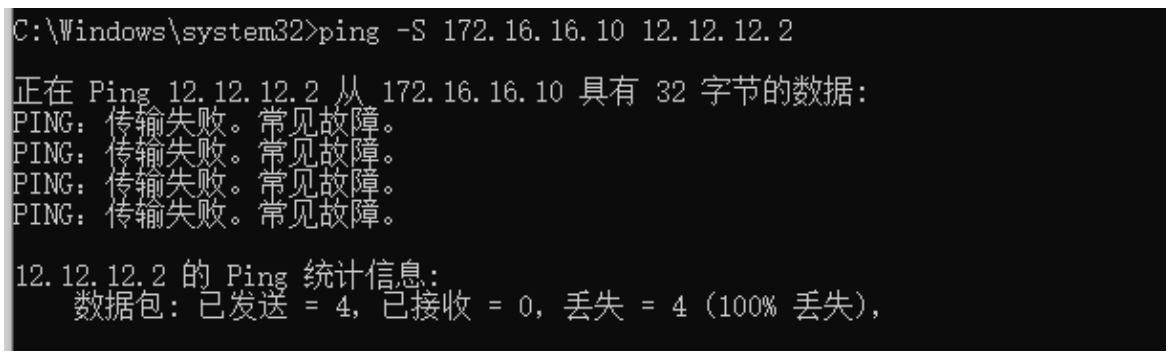


2. 拒绝 172.16.10.0 的主机访问 FTP 服务器 192.168.1.10（此时访问失败）



3. 拒绝 172.16.10.0 的主机 Telnet 路由器 RTB（此时访问失败）

4. 拒绝 172.16.10.0 的主机 ping 路由器 RTB（此时访问失败）



可以看到实验结果完全符合要求，至基于静态路由的扩展 ACL 配置成功。

- 步骤二：实现 OSPF 路由协议

（1） 按照拓扑图来配置 OSPF 协议，具体过程如下所示：

```
14-RSR20-1(config)#route ospf 1
14-RSR20-1(config-router)#network 172.16.10.0 0.0.0.255 area 0
14-RSR20-1(config-router)#network 12.12.12.0 0.0.0.255 area 0
14-RSR20-1(config-router)#*Jan  1 01:47:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.1
68.1.2-Serial 2/0 from Down to Init, HelloReceived.
*Jan  1 01:47:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2-Serial 2/0 from Loa
```

```
14-RSR20-2(config)#route ospf 1
14-RSR20-2(config-router)#network 192.168.1
14-RSR20-2(config-network-region)#exit
14-RSR20-2(config)#route ospf 1
14-RSR20-2(config-router)#network 192.168.1.0 0.0.0.255 area 0
14-RSR20-2(config-router)#network 12.12.12.0 0.0.0.255 area 0
```

我们按照拓扑图上的要求来配置 OSPF 协议，我们将 RTA 和 RTB 路由的区域设置为 area 0。

具体结果如下所示：

```
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    12.12.12.0/24 is directly connected, Serial 2/0
C    12.12.12.1/32 is local host.
C    172.16.10.0/24 is directly connected, GigabitEthernet 0/1
C    172.16.10.1/32 is local host.
O    192.168.1.0/24 [110/51] via 12.12.12.2, 00:00:18, Serial 2/0
```

```
14-RSR20-2(config-router)#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    12.12.12.0/24 is directly connected, Serial 2/0
C    12.12.12.2/32 is local host.
O    172.16.10.0/24 [110/51] via 12.12.12.1, 00:00:04, Serial 2/0
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.2/32 is local host.
```

可以看到，我们此时的路由表中出现了“O”条目，这个就是路由器 RTB 通过 OSPF 学习而来的路由条目，该条目的含义是发往 172.16.10.0 网段的消息都要经过 12.12.12.1 端口（即路由器 RTA 的 IP 地址），可见这个协议是符合我们要求的。RTA 同理。

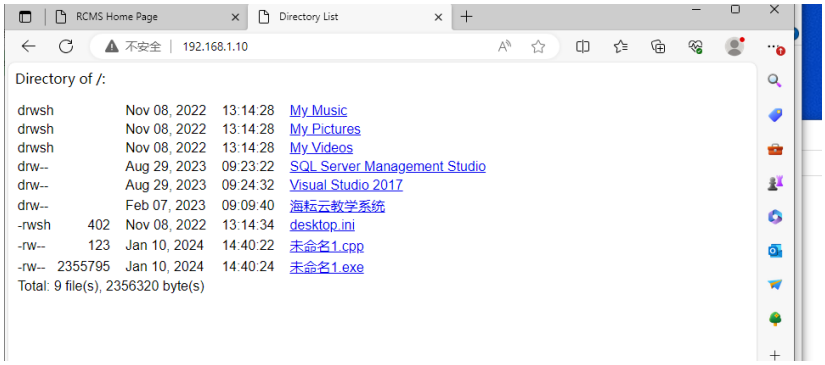
（2） 配置扩展 ACL，配置过程与上面相同，但是有一点需要注意。

```
4-RSR20-1(config)#access-list 100 permit ip any any
```

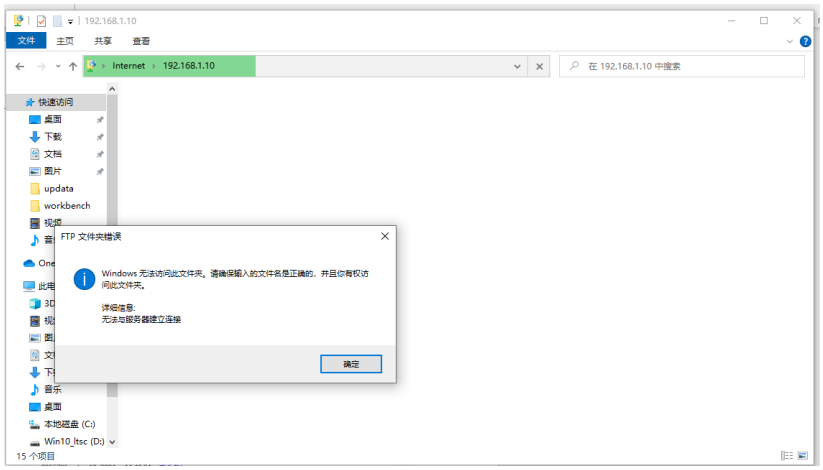
配置 ospf 必须加上此条，由于我们小组最初在配静态路由的时候就加上了该条指令，因此在配置 ospf 的时候很顺利，没有发生错误，后来在与其他小组交流的时候，才发现他们由于未加该指令导致一直无法运行成功。由于 OSPF 默认使用协议号 89，并且在发送和接收 OSPF Hello 数据包时需要通过 IP 协议传输。如果在配置 ACL 时没有显式允许该协议流量，则会被 ACL 阻止，从而导致 OSPF 的邻接关系无法建立。

（3） 配置完扩展 ACL，检测实验结果

5. 允许 172.16.10.0 的主机访问 www 服务器 192.168.1.10（此时访问成功）



6. 拒绝 172.16.10.0 的主机访问 FTP 服务器 192.168.1.10（此时访问失败）



7. 拒绝 172.16.10.0 的主机 Telnet 路由器 RTB（此时访问失败）

```
C:\Windows\system32>Telnet 12.12.12.2
正在连接12.12.12.2...无法打开到主机的连接。 在端口 23: 连接失败
```

8. 拒绝 172.16.10.0 的主机 ping 路由器 RTB（此时访问失败）

```
C:\Windows\system32>ping -S 172.16.16.10 12.12.12.2

正在 Ping 12.12.12.2 从 172.16.16.10 具有 32 字节的数据:
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。

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

可以看到实验结果完全符合要求，至此基于 OSPF 协议的扩展 ACL 配置成功。