# OSPF路由项欺骗攻击与防御策略

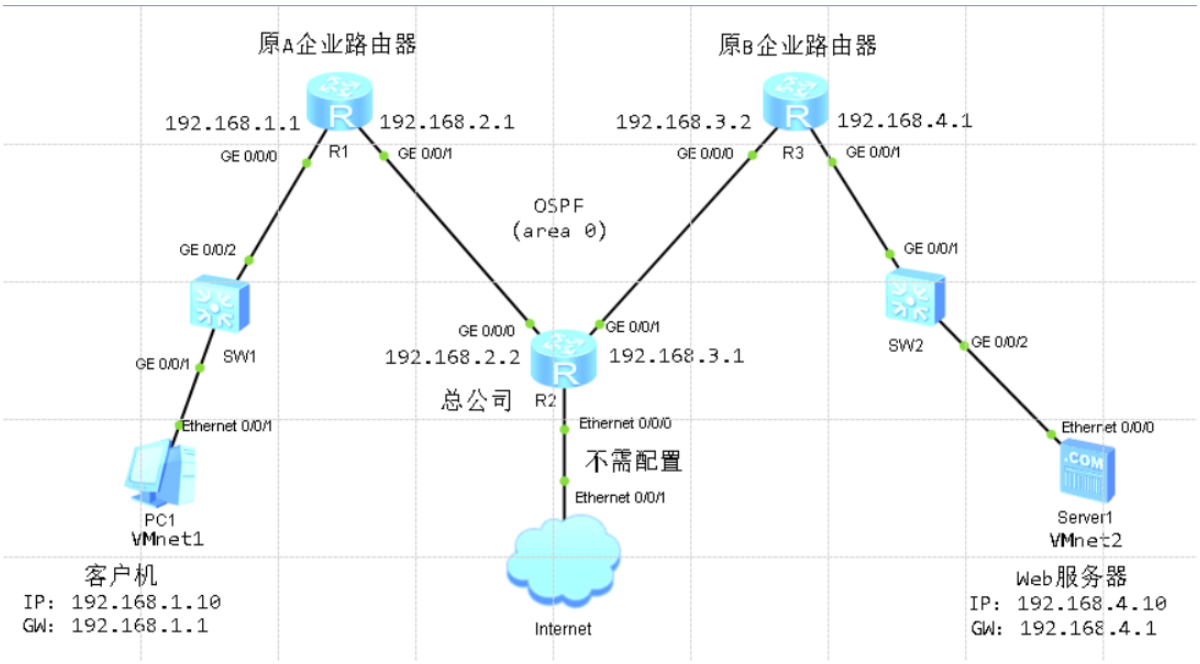
## 任务目的

掌握OSPF路由项欺骗攻击和OSPF源端鉴别的配置方法。

## 任务设备、设施

Win 华为ENSP Vmare

## 拓扑




## 基本配置

### 路由器配置

R1

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]undo info en
Info: Information center is disabled.
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24
[R1-GigabitEthernet0/0/0]q
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 192.168.2.1 24
[R1-GigabitEthernet0/0/1]q
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]q
[R1-ospf-1]q
```

```
[R1]
```

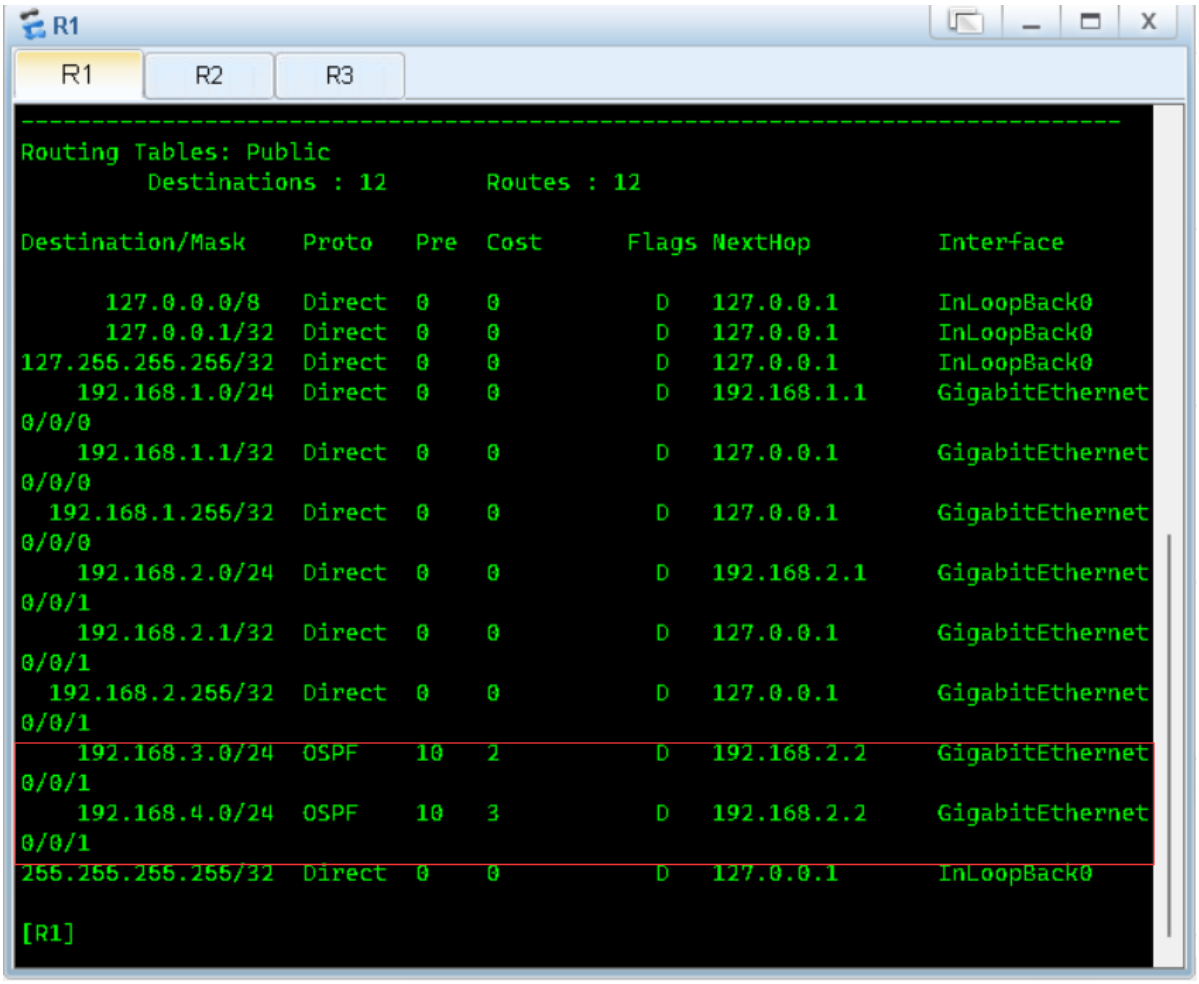
R2

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]undo info en
Info: Information center is disabled.
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 192.168.2.2 24
[R2-GigabitEthernet0/0/0]q
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 192.168.3.1 24
[R2-GigabitEthernet0/0/1]q
[R2]ospf 1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]q
[R2-ospf-1]q
[R2]
```

R3

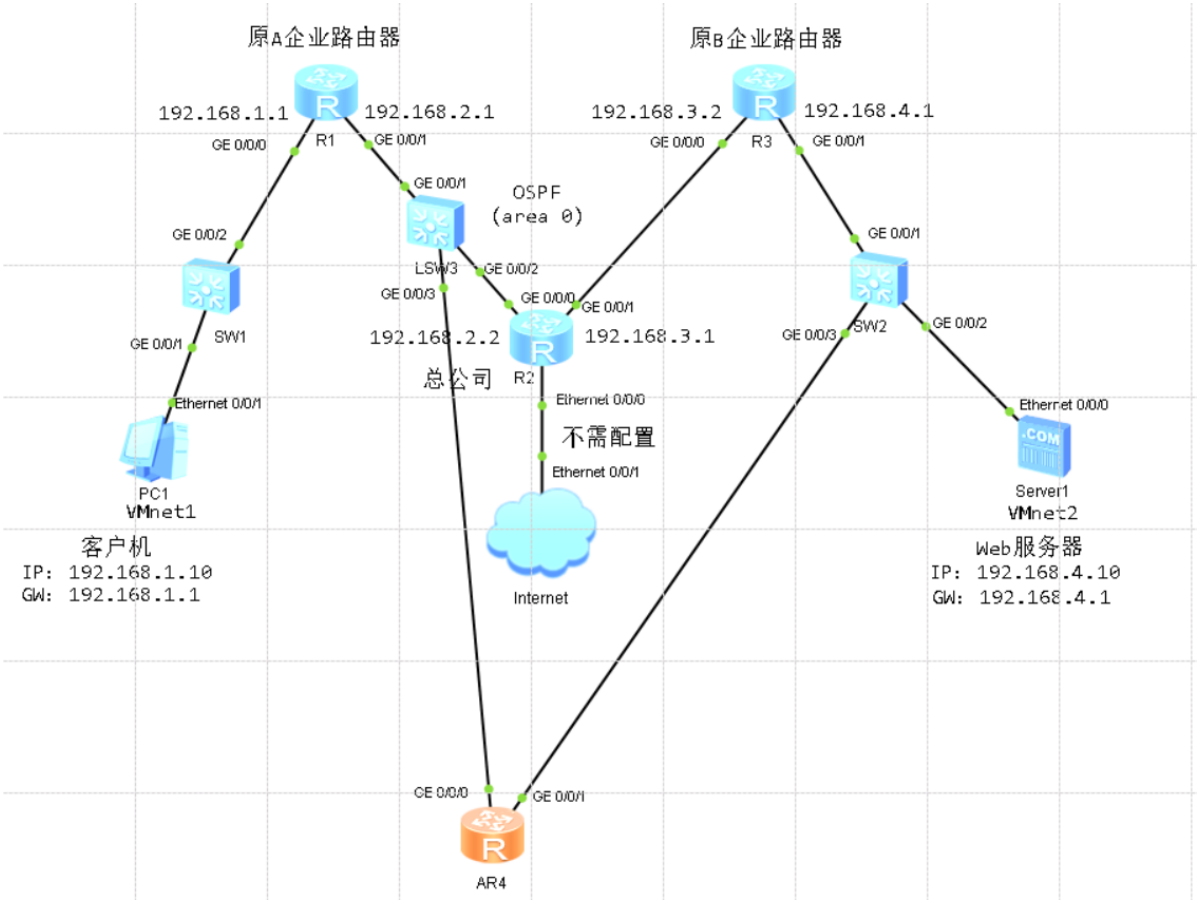
```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R3
[R3]undo info en
Info: Information center is disabled.
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ip add 192.168.3.2 24
[R3-GigabitEthernet0/0/0]q
[R3]int g0/0/1
[R3-GigabitEthernet0/0/1]ip add 192.168.4.1 24
[R3-GigabitEthernet0/0/1]q
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]q
[R3-ospf-1]q
[R3]
```

查看路由器R1路由器表



```
R1
R1   R2   R3
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet
0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   2           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   3           D   192.168.2.2     GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R1]
```

# 入侵实战




R4伪造OSPF路由表

```
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R4
[R4]undo info en
Info: Information center is disabled.
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]ip add 192.168.2.3 24
[R4-GigabitEthernet0/0/0]q
[R4]int g0/0/1
[R4-GigabitEthernet0/0/1]ip add 192.168.4.2 24
[R4-GigabitEthernet0/0/1]q
[R4]ospf 1
[R4-ospf-1]area 0
[R4-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[R4-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[R4-ospf-1-area-0.0.0.0]q
[R4-ospf-1]
```

路由表信息

R1路由表

```
[R1]disp ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet
0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   2           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   2           D   192.168.2.3     GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

R2路由表

```
[R2]disp ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   2           D   192.168.2.1     GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.2     GigabitEthernet
0/0/0
    192.168.2.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet
0/0/1
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
  192.168.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   2           D   192.168.3.2     GigabitEthernet
0/0/1
                    OSPF    10   2           D   192.168.2.3     GigabitEthernet
0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

# 防御策略

路由器R1接口开启OSPF路由项源鉴别功能

```
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]ospf authentication-mode hmac-md5 1 cipher huawei
[R1-GigabitEthernet0/0/1]q
[R1]
```

路由器R2接口开启OSPF路由项源鉴别功能

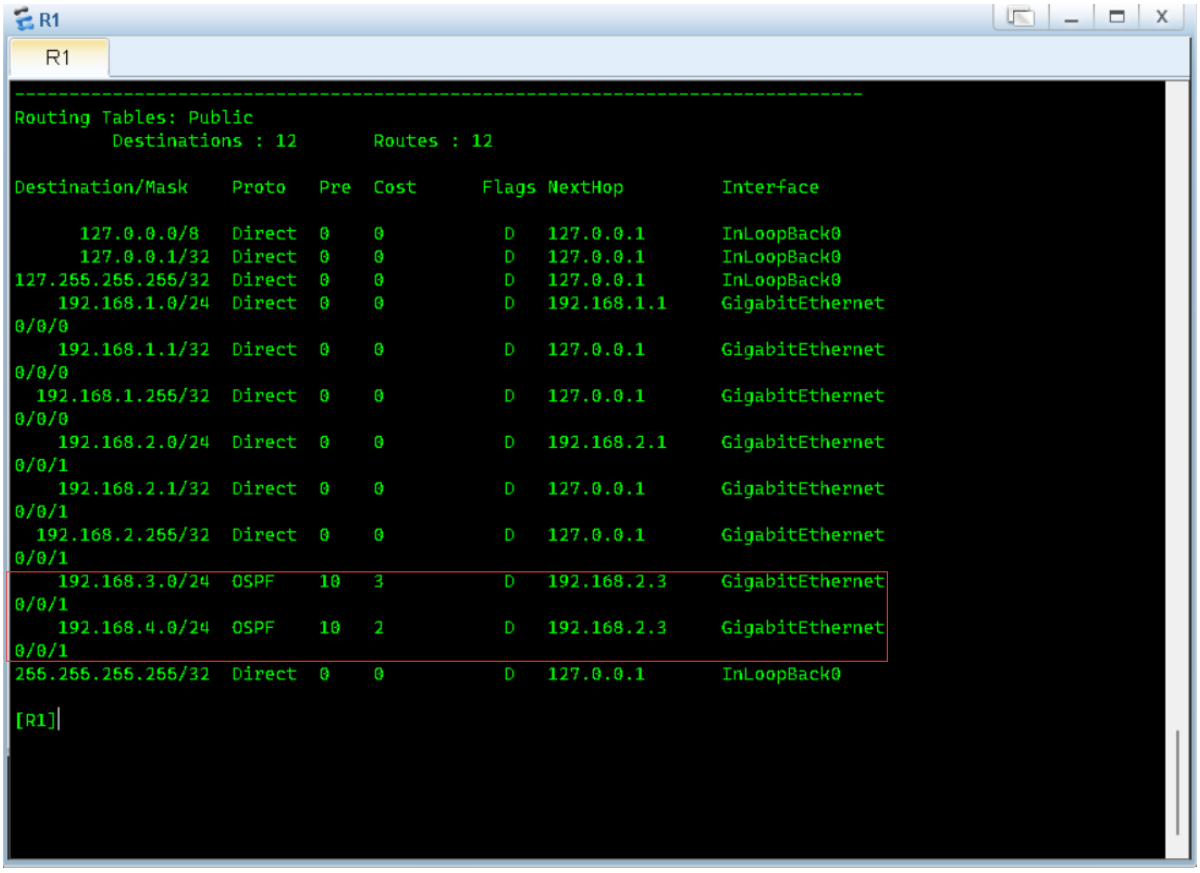
```
<R2>sys
Enter system view, return user view with Ctrl+Z.
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ospf authentication-mode hmac-md5 1 ciph huawei
[R2-GigabitEthernet0/0/0]q

[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ospf authentication-mode hmac-md5 1 cipher bbbb
[R2-GigabitEthernet0/0/1]q
[R2]
```

路由器R3接口开启OSPF路由项源鉴别功能

```
<R3>sys
Enter system view, return user view with Ctrl+Z.
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ospf authentication-mode hmac-md5 1 cipher bbbb
[R3-GigabitEthernet0/0/0]q
[R3]
```

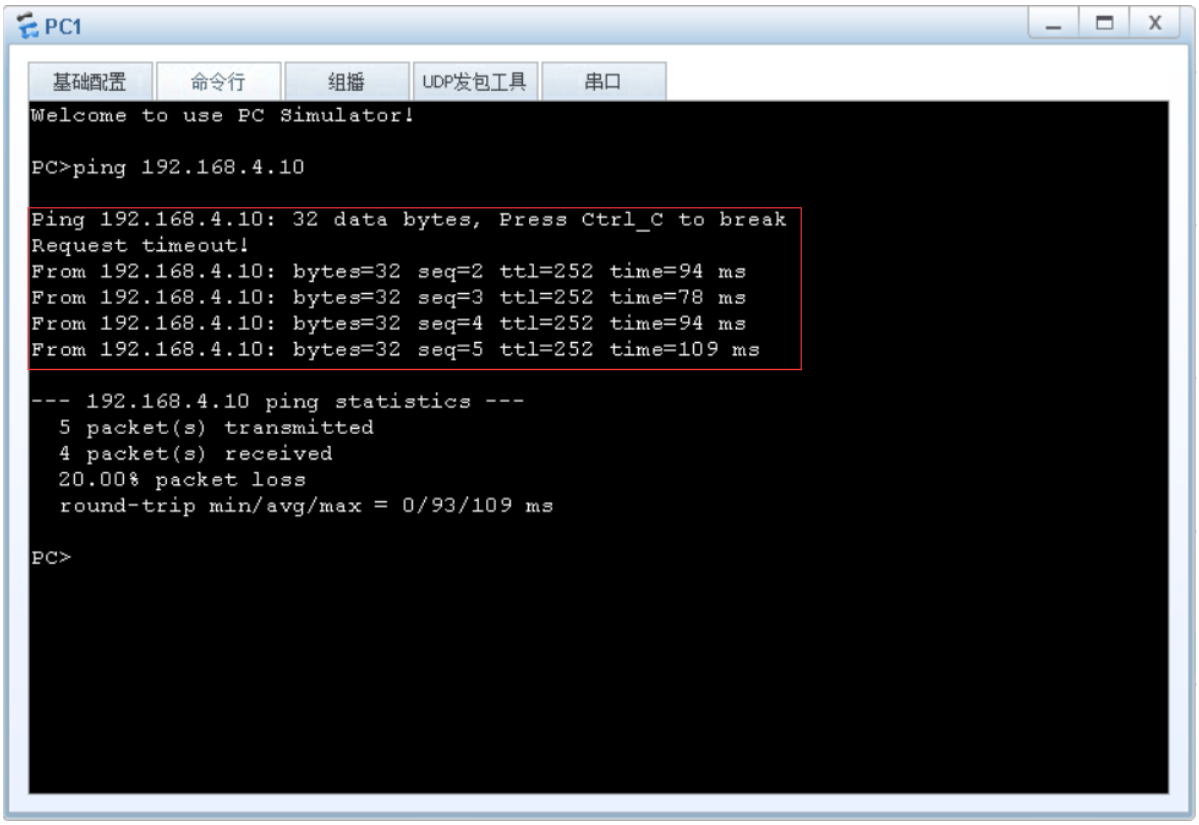
# 验证

R1路由表



```
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet
0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   3           D   192.168.2.3     GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   2           D   192.168.2.3     GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R1]
```

PC1 ping web服务结果




# 任务总结

1.在配置OSPF路由项源端鉴别时，相邻路由器之间接口必须采用相同得鉴别方式(如Hmac-md5)、相同得鉴别密码(密钥存储方式可以不同,如cipher或者plain)和相同得密钥标识符,否则不能建立邻居关系

2.对于交换机SW2而言，去往目的IP地址192.168.4.1时,可能通过GE0/0/1接口(客户机与Web服务器通信时去跟回走不同路径),也可能通过GE0/0/3接口(客户机与Web服务器通信时去跟回走相同路径),由SW2端口映射表更新状态决定,无法人为指定.