RIP路由项欺骗攻击与防御策略

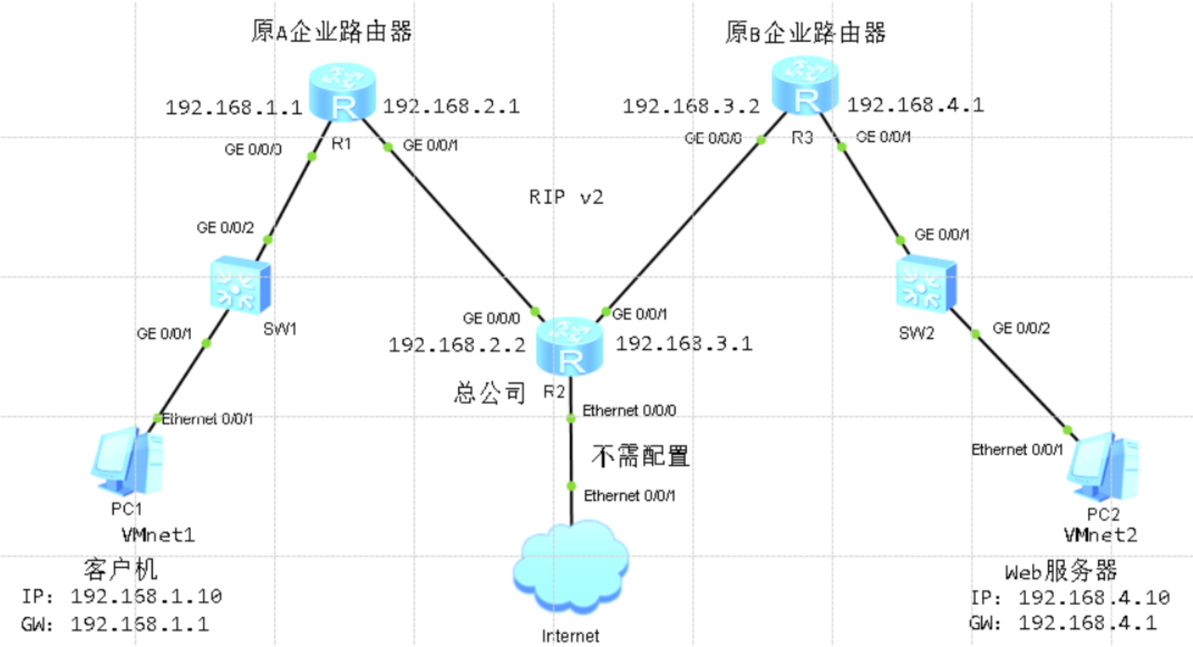
任务目的

掌握基于RIP路由项欺骗攻击过程与RIP源端鉴别的配置方法。

任务设备、设施

win10、华为eNSP、vmvare、win7

任务拓扑结构图



基本配置

路由器R1接口IP与RIP路由配置

```
<Huawei>sys
[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]rip 1
[R1-rip-1]version 2
[R1-rip-1]network 192.168.1.0
[R1-rip-1]network 192.168.2.0
[R1-rip-1]q
[R1]
```

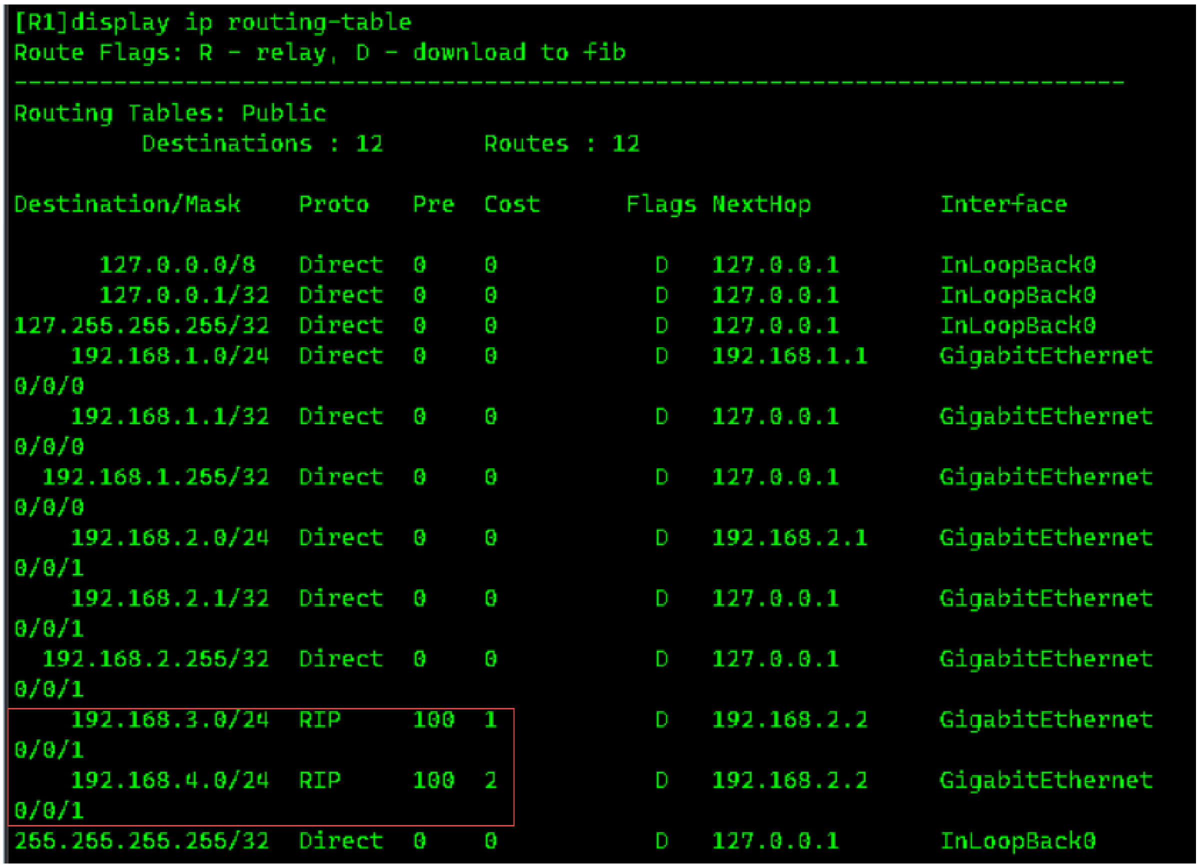
路由器R2接口接口IP与RIP路由配置

```
<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]rip 2
[R2-rip-2]version 2
[R2-rip-2]network 192.168.2.0
[R2-rip-2]network 192.168.3.0
[R2-rip-2]q
[R2]
```

路由R3接口IP与RIP路由配置

```
<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]rip 3
[R3-rip-3]version 2
[R3-rip-3]network 192.168.3.0
[R3-rip-3]network 192.168.4.0
[R3-rip-3]q
[R3]
```

查看路由器R1路由表



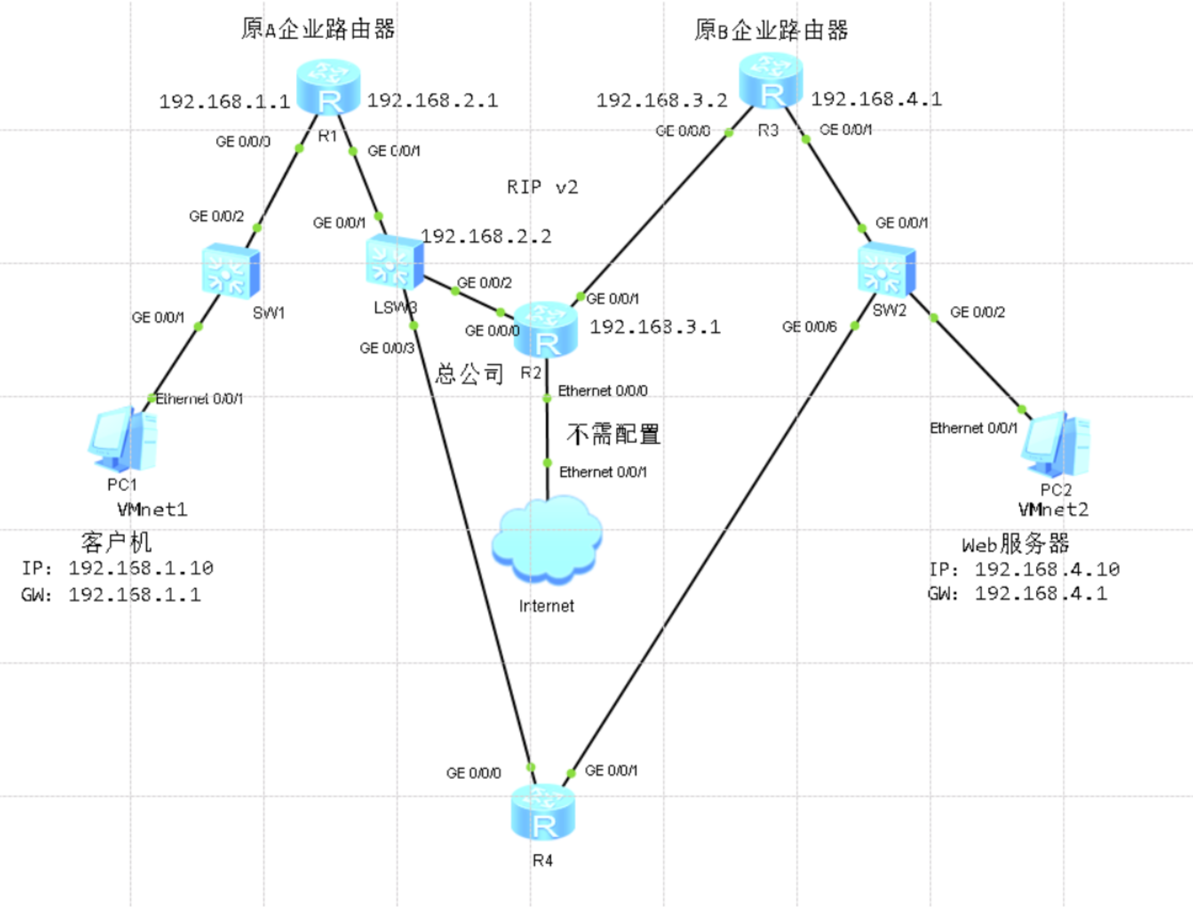
```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

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  RIP     100  1           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.4.0/24  RIP     100  2           D   192.168.2.2     GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

入侵实战

网络拓扑

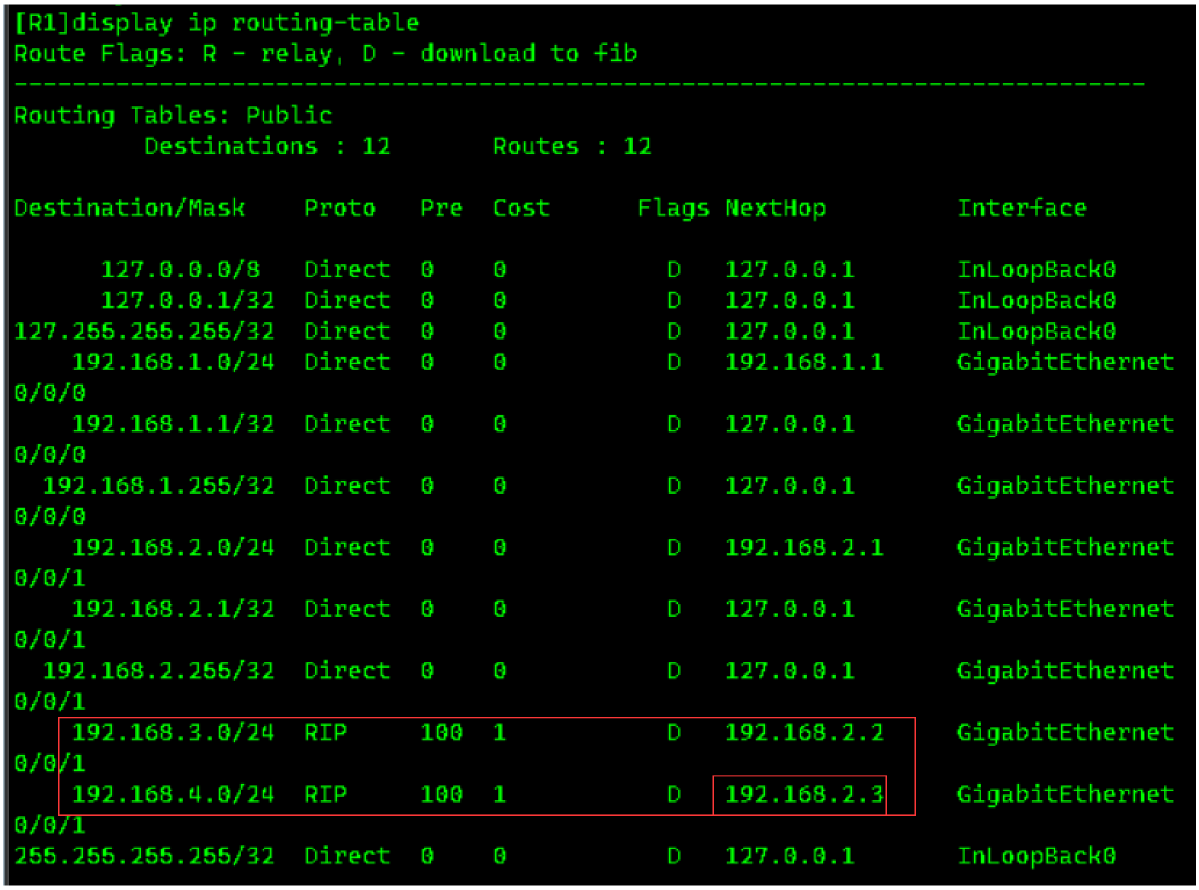


路由器R4接口IP与RIP路由配置

```
<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 192.168.4.1 24
[R4-GigabitEthernet0/0/1]q
[R4]rip 4
[R4-rip-4]version 2
[R4-rip-4]network 192.168.2.0
[R4-rip-4]network 192.168.4.0
[R4-rip-4]q
[R4]
```

R4伪造后查看R1路由表

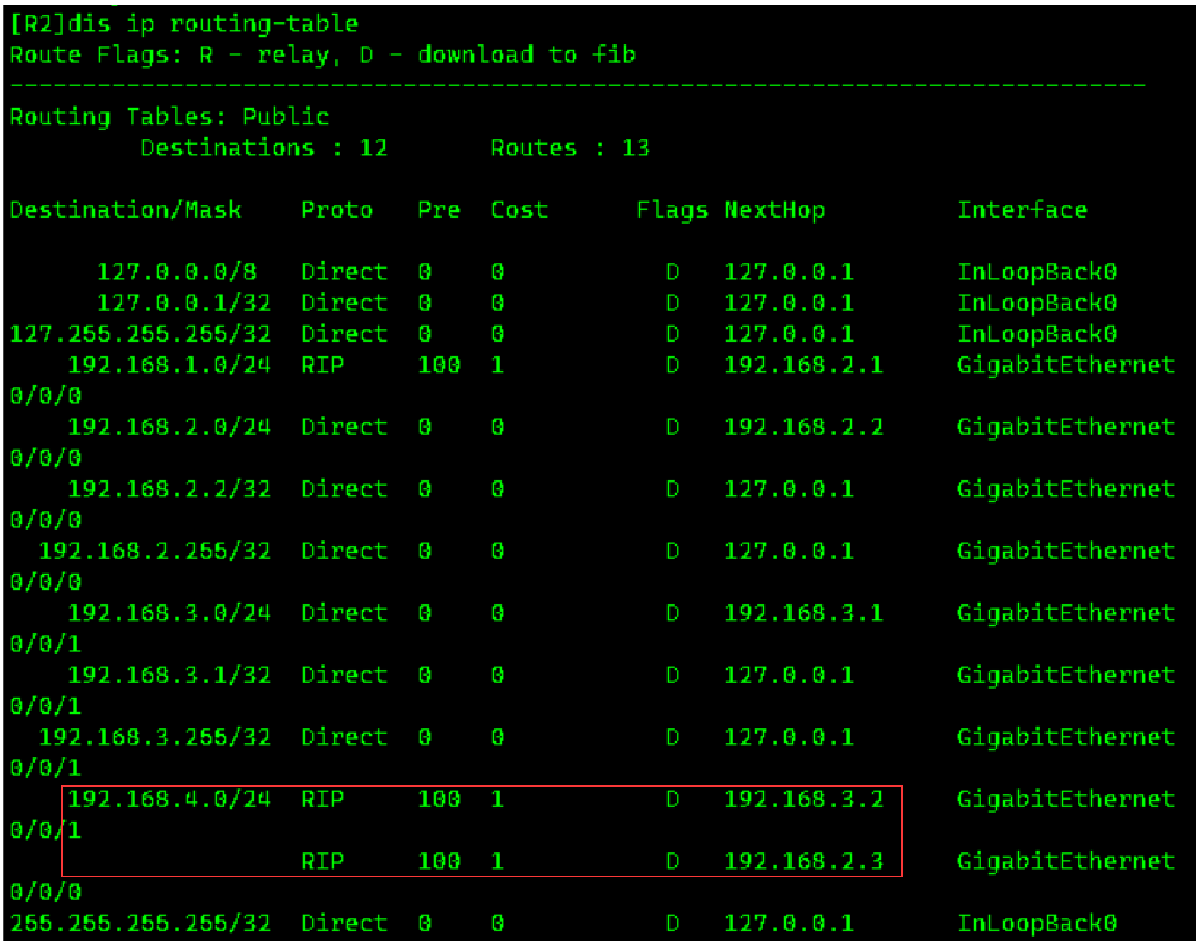


```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

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  RIP     100  1           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.4.0/24  RIP     100  1           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

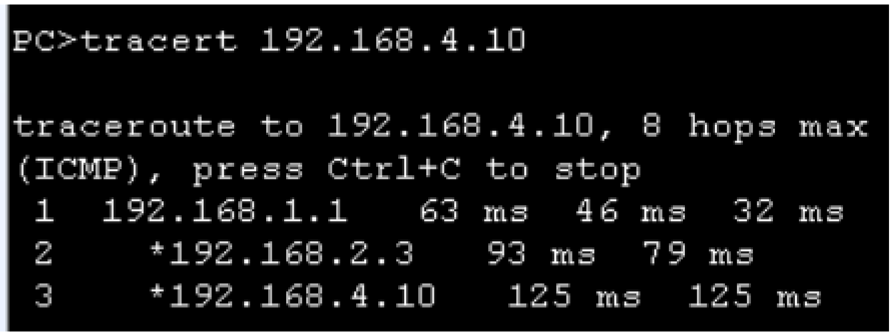


```
[R2]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 13

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  RIP     100  1           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  RIP     100  1           D   192.168.3.2     GigabitEthernet
0/0/1
                    RIP     100  1           D   192.168.2.3     GigabitEthernet
0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

查看tracert测试结果



```
PC>tracert 192.168.4.10

traceroute to 192.168.4.10, 8 hops max
(ICMP), press Ctrl+C to stop
 1  192.168.1.1    63 ms  46 ms  32 ms
 2    *192.168.2.3    93 ms  79 ms
 3    *192.168.4.10    125 ms  125 ms
```

防御策略

在路由器R1接口开启RIP路由项源端鉴别功能

```
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]rip version 2 multicast
[R1-GigabitEthernet0/0/1]rip authentication-mode hmac-sha256 cipher huawei 100
[R1-GigabitEthernet0/0/1]q
```

在路由器R2接口开启RIP路由项端鉴别功能

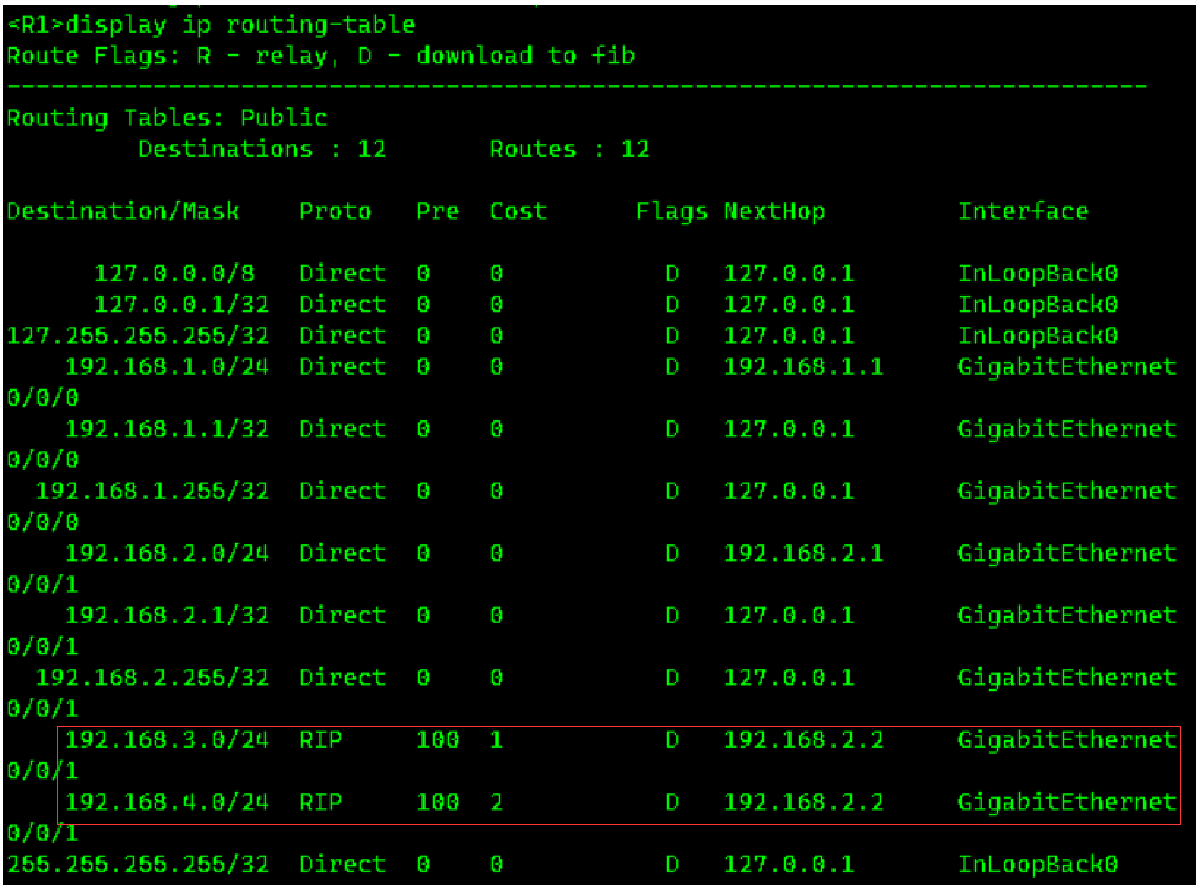
```
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]rip version 2 multicast
[R2-GigabitEthernet0/0/0]rip authentication-mode hmac-sha256 cipher huawei 100
[R2-GigabitEthernet0/0/0]q
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]rip version 2 multicast
[R2-GigabitEthernet0/0/1]rip authentication-mode hmac-sha256 cipher huawei 100
[R2-GigabitEthernet0/0/1]q
[R2]
```

在路由器R3接口开启RIP路由项源端鉴别功能

```
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]rip version 2 multicast
[R3-GigabitEthernet0/0/0]rip authentication-mode hmac-sha256 cipher huawei 100
[R3-GigabitEthernet0/0/0]q
[R3]
```

任务验证

查看AR1路由表

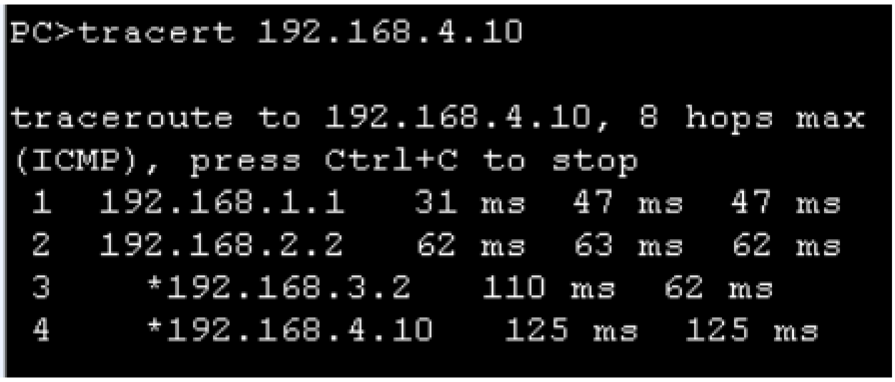


```
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

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  RIP     100  1           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.4.0/24  RIP     100  2           D   192.168.2.2     GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

查看tracert结果



```
PC>tracert 192.168.4.10

traceroute to 192.168.4.10, 8 hops max
(ICMP), press Ctrl+C to stop
 1  192.168.1.1    31 ms   47 ms   47 ms
 2  192.168.2.2    62 ms   63 ms   62 ms
 3    *192.168.3.2    110 ms   62 ms
 4    *192.168.4.10    125 ms   125 ms
```

任务总结

1.在配置RIP路由项源端鉴别时，相邻路由器之间接口必须使用相同摘要算法(如Hmac-SHA256)、相同的共享密钥(密钥存储方式可以不同,如cipher或者plain)和相同的密钥标识符,否则不能建立RIP邻居关系。

2.对于交换机SW2而言,去往IP地址为192.168.4.1的目的地时可能通过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GE 0/0/3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。