

## 《HCIP – Datacom Core 实验手册》目录

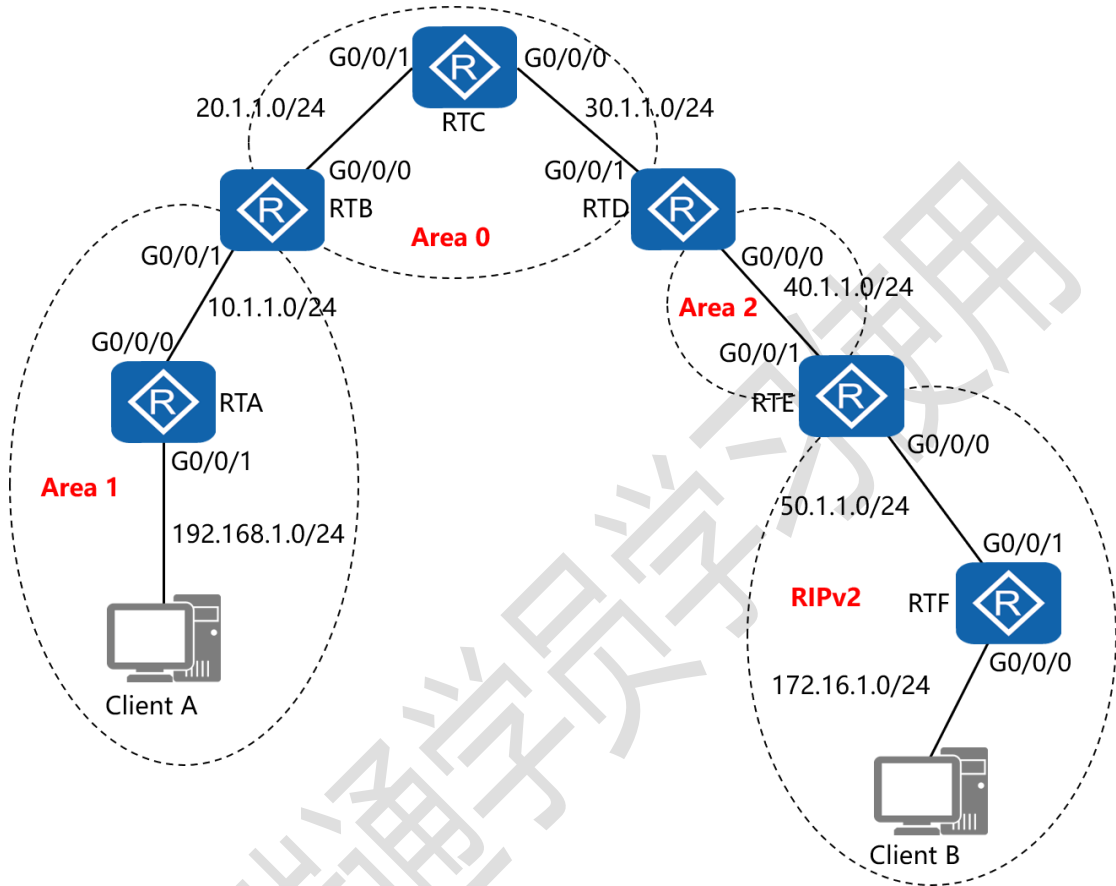
01、配置 OSPF 多区域实验组网	004
02、OSPF 高级配置实验组网	010
03、配置 VRRP 实验组网	016
04、配置静默接口实验组网	019
05、配置通过 filter-policy 控制路由实验组网	022
06、配置协议优先级实验组网(一)	026
07、配置协议优先级实验组网(二)	030
08、配置 IS-IS 单区域实验组网	034
09、配置 IS-IS 多区域实验组网	036
10、配置 IS-IS 路由验证及聚合实验组网	040
11、配置 IS-IS 路由渗透实验组网	045
12、配置 RIPng 实验组网	050
13、配置 OSPFv3 实验组网	053
14、配置 IPv6 各类地址实验组网	056
15、配置 IBGP 与 EBGP 会话实验组网	061
16、配置通过 AS-Path 属性移除私有 AS 号实验组网	069
17、配置 BGP 原子汇总实验组网	077
18、配置 BGP 汇总子实验组网	086
19、配置 BGP 本地优先级实验组网	095
20、配置 BGP 多出口鉴别实验组网	104

21、配置 BGP 优先级值实验组网	-----	113
22、配置 BGP filter-policy 实验组网	-----	120
23、配置 BGP ip ip-prefix 实验组网	-----	126
24、配置 BGP 双向重发布实验组网	-----	132
25、配置 RSTP 实验组网	-----	136
26、配置 STP 边缘端口实验组网	-----	139
27、配置 STP 根保护实验组网	-----	142
28、配置 STP BPDU 保护实验组网	-----	145
29、配置 STP 环路保护实验组网	-----	148
30、配置 MSTP 实验组网	-----	151
31、配置三层交换实验组网	-----	156
32、配置 DHCP 接口地址池实验组网	-----	158
33、配置 DHCP 全局地址池实验组网	-----	160
34、配置 DHCP 中继代理实验组网	-----	164
35、配置 DHCP Snooping 实验组网	-----	170
36、配置端口安全实验组网	-----	173
37、配置二层隔离三层互通的端口隔离实验组网	-----	177
38、配置二层三层均隔离的端口隔离实验组网	-----	183
39、配置 MUX VLAN 实验组网	-----	189
40、配置 BFD 与 OSPF 联动实验组网	-----	199
41、配置 BFD 与 VRRP 联动实验组网	-----	201
42、配置 BFD 与静态路由联动实验组网	-----	207

43、配置 BFD 与 BGP 联动实验组网	-----	213
44、配置 BFD 单臂回声实验组网	-----	217
45、配置端口镜像实验组网	-----	219
46、配置组播综合实验组网	-----	223
47、配置 IKE 方式的 IPSec VPN 实验组网	-----	230
48、配置手动方式的 IPSec VPN 实验组网	-----	234
49、配置 GRE VPN 实验组网 (一)	-----	238
50、配置 GRE VPN 实验组网 (二)	-----	241
51、配置 GRE over IPSec VPN 实验组网	-----	245
52、配置 L2TP VPN 实验组网	-----	251
53、配置 MBGP MPLS VPN 实验组网	-----	260

# 一、配置 OSPF 多区域实验组网

## 一、实验拓扑：



## 二、实验目的：

通过 OSPF 多区域和双向重发布的配置，令 Client A 能够与 Client B 正常通讯

## 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

```
interface G0/0/0    #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface Loopback0    #创建环回接口 0
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
器 ID
area 1    #创建 OSPF 区域 1
network 10.1.1.0 0.0.0.255    #通告其直连网段
network 192.168.1.0 0.0.0.255    #通告其直连网段

RTB:
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
```

```
area 1
network 10.1.1.0 0.0.0.255
area 0
network 20.1.1.0 0.0.0.255
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
area 0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
```

RTD:

```
system-view
sysname RTD
```

```
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
interface Loopback0
ip address 4.4.4.4 32
ospf 1 router-id 4.4.4.4
area 0
network 30.1.1.0 0.0.0.255
area 2
network 40.1.1.0 0.0.0.255
```

RTE:

```
system-view
sysname RTE
interface G0/0/0
ip address 50.1.1.1 24
interface G0/0/1
ip address 40.1.1.2 24
interface Loopback0
ip address 5.5.5.5 32
ospf 1 router-id 5.5.5.5
```

```

import-route rip 1      #将 RIP1 的路由条目重发布进
OSPF1 的进程中
area 2
network 40.1.1.0 0.0.0.255
rip 1      #进入 RIP 进程 1
version 2   #指定使用版本 2
network 50.0.0.0    #通告其直连的网段
undo summary      #关闭自动汇总
import-route ospf 1    #将 OSPF1 的路由条目重发布进 RIP1
的进程中

```

RTF:

```

system-view
sysname RTF
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
ip address 50.1.1.2 24
rip 1
version 2
network 50.0.0.0
network 172.16.0.0

```

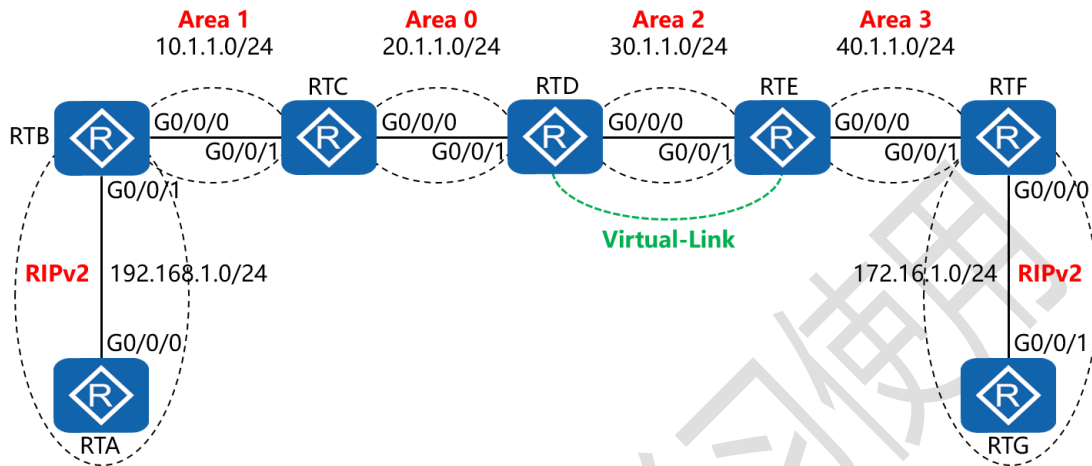


undo summary

仅供瑞通学员学习使用

## 二、OSPF 高级配置实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 OSPF 多区域、虚链路以及双向重发布的配置，令全网全通

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
rip 1               #进入 RIP 进程 1
version 2           #指定使用版本 2
network 192.168.1.0   #通告其直连的网段
undo summary        #关闭自动汇总
    
```

```

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 10.1.1.1 24

interface G0/0/1

ip address 192.168.1.2 24

interface Loopback0

ip address 2.2.2.2 32

ospf 1 router-id 2.2.2.2    #进入 OSPF 进程 1, 并指定其路
由器 ID

import-route rip 1    #将 RIP1 的路由条目重发布进
OSPF1 的进程中

area 1    #创建 OSPF 区域 1

network 10.1.1.0 0.0.0.255    #通告其直连网段

rip 1

version 2

network 192.168.1.0

undo summary

import-route ospf 1    #将 OSPF1 的路由条目重发布进 RIP1
的进程中
    
```

RTC:

```
system-view
```

```
sysname RTC
```

```
interface G0/0/0
```

```
ip address 20.1.1.1 24
```

```
interface G0/0/1
```

```
ip address 10.1.1.2 24
```

```
interface Loopback0
```

```
ip address 3.3.3.3 32
```

```
ospf 1 router-id 3.3.3.3
```

```
area 0
```

```
network 20.1.1.0 0.0.0.255
```

```
area 1
```

```
network 10.1.1.0 0.0.0.255
```

RTD:

```
system-view
```

```
sysname RTD
```

```
interface G0/0/0
```

```
ip address 30.1.1.1 24
```

```
interface G0/0/1
```

```
ip address 20.1.1.2 24
```

```
interface Loopback0
ip address 4.4.4.4 32
ospf 1 router-id 4.4.4.4
area 0
network 20.1.1.0 0.0.0.255
area 2
network 30.1.1.0 0.0.0.255
vlink-peer 5.5.5.5    #与对端设备 5.5.5.5 在区域 2 中配置虚
链路
```

```
RTE:
system-view
sysname RTE
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
interface Loopback0
ip address 5.5.5.5 32
ospf 1 router-id 5.5.5.5
area 2
network 30.1.1.0 0.0.0.255
```

```
vlink-peer 4.4.4.4  
area 3  
network 40.1.1.0 0.0.0.255
```

RTF:

```
system-view  
sysname RTF  
interface G0/0/0  
ip address 172.16.1.1 24  
interface G0/0/1  
ip address 40.1.1.2 24  
interface Loopback0  
ip address 6.6.6.6 32  
ospf 1 router-id 6.6.6.6  
import-route rip 1  
area 3  
network 40.1.1.0 0.0.0.255  
rip 1  
version 2  
network 172.16.0.0  
undo summary  
import-route ospf 1
```

RTG:

system-view

sysname RTG

interface G0/0/1

ip address 172.16.1.2 24

rip 1

version 2

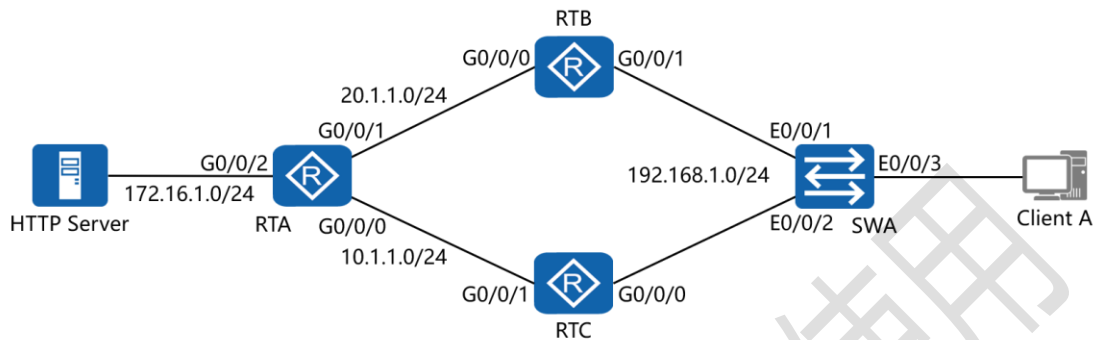
network 172.16.0.0

undo summary

仅供瑞通学员学习使用

## 三、配置 VRRP 实验组网

### 一、实验拓扑：



### 二、实验目的：

令 Client A 访问 HTTP Server，默认从 RTB 到达，之后 down 掉 RTB 的 G0/0/0 接口，使 RTC 自动接替转发工作，并且在 RTB 的 E0/0/0 接口正常工作之后从 RTC 抢夺转发权，同时 RTB、RTC 都实现端口跟踪

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24 #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 20.1.1.1 24 #配置 IP 地址及子网掩码
interface G0/0/2     #进入相应接口
    
```



```

ip address 172.16.1.1 24      #配置 IP 地址及子网掩码
rip 1      #进入 RIP 进程 1
version 2      #指定使用版本 2
network 172.16.0.0      #通告其直连的网段
network 10.0.0.0      #通告其直连的网段
network 20.0.0.0      #通告其直连的网段
undo summary      #关闭自动汇总

RTB:
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.2 24
interface G0/0/1
ip address 192.168.1.1 24
vrrp vrid 47 virtual-ip 192.168.1.254      #创建 VRRP 组,
指定组号与虚拟 IP 地址
vrrp vrid 47 priority 200      #配置当前路由器的 VRRP 优
先级
vrrp vrid 47 track interface G0/0/0 reduced 60      #配置
VRRP 端口跟踪, 并指定在被跟踪的接口失效时, 令当前
VRRP 路由器的优先级降低 60

```

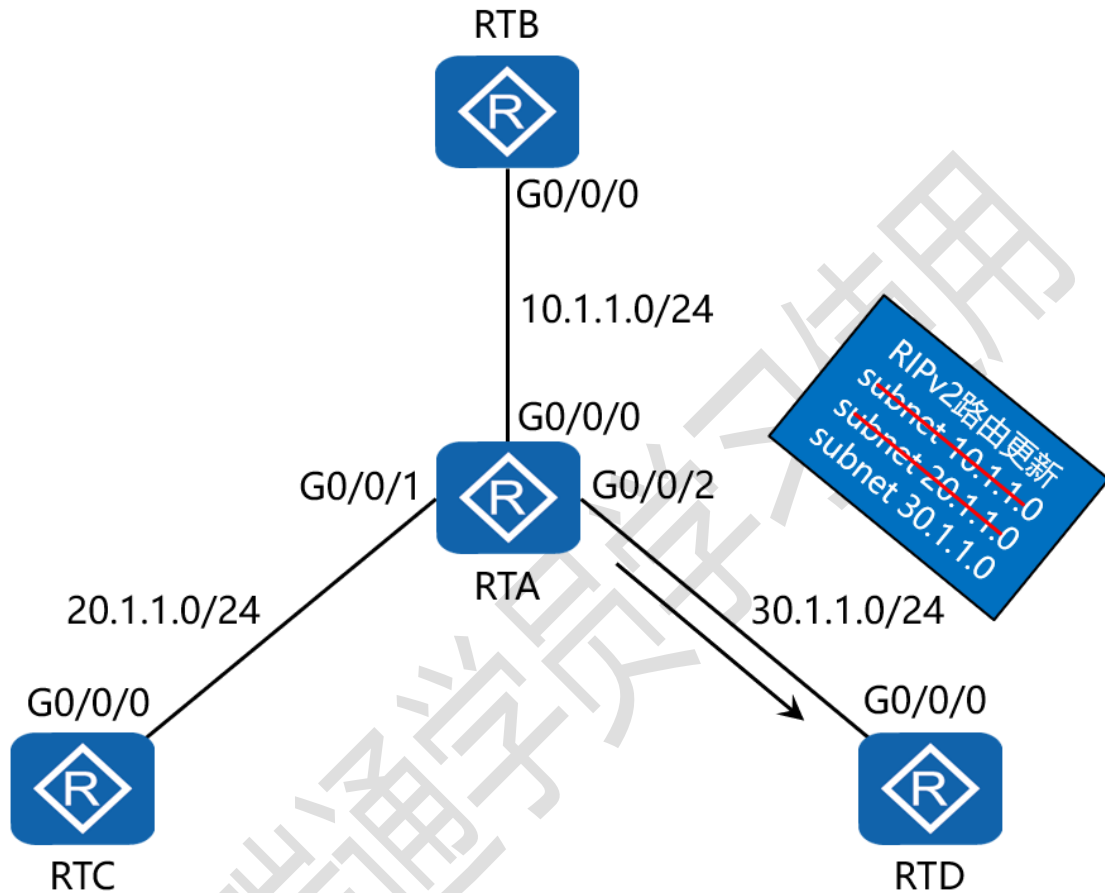
```
rip 1  
version 2  
network 192.168.1.0  
network 20.0.0.0  
undo summary
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 192.168.1.2 24  
vrrp vrid 47 virtual-ip 192.168.1.254  
vrrp vrid 47 priority 150  
vrrp vrid 47 track interface G0/0/1 reduced 60  
interface G0/0/1  
ip address 10.1.1.2 24  
rip 1  
version 2  
network 192.168.1.0  
network 10.0.0.0  
undo summary
```

## 四、配置静默接口实验组网

### 一、实验拓扑：



### 二、实验目的：

4 台路由器运行 RIPv2，通过将 RTA 的 G0/0/2 配置为静默接口，令 RTA 不再向 RTD 通告 RIP 路由信息，但从 RTD 接收路由信息

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

```

sysname RTA      #给设备命名
interface G0/0/0  #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1  #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/2  #进入相应接口
ip address 30.1.1.1 24    #配置 IP 地址及子网掩码
rip 1            #进入 RIP 进程 1
version 2        #配置使用版本 2
network 10.0.0.0  #通告其直连网段
network 20.0.0.0  #通告其直连网段
network 30.0.0.0  #通告其直连网段
silent-interface G0/0/0  #将 G0/0/0 配置为静默接口
undo summary     #关闭自动汇总

```

```

RTB:
system-view
sysname RTB
interface G0/0/0
ip address 10.1.1.2 24
rip 1
version 2

```

---

```
network 10.0.0.0
```

```
undo summary
```

```
RTC:
```

```
system-view
```

```
sysname RTC
```

```
interface G0/0/0
```

```
ip address 20.1.1.2 24
```

```
rip 1
```

```
version 2
```

```
network 20.0.0.0
```

```
undo summary
```

```
RTD:
```

```
system-view
```

```
sysname RTD
```

```
interface G0/0/0
```

```
ip address 30.1.1.2 24
```

```
rip 1
```

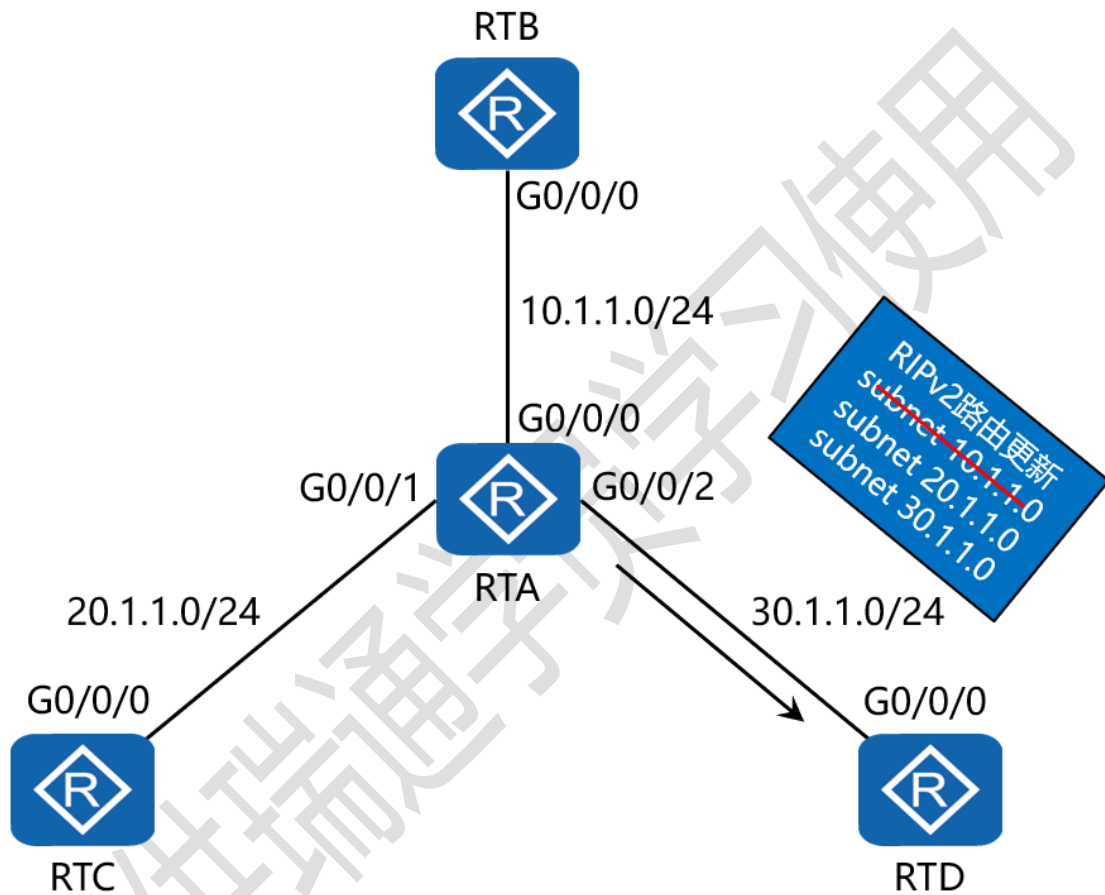
```
version 2
```

```
network 30.0.0.0
```

```
undo summary
```

## 五、配置通过 filter-policy 控制路由实验组网

### 一、实验拓扑：



### 二、实验目的：

4 台路由器运行 OSPF，通过在 RTD 上配置 filter-policy，令其过滤掉 RTA 通告过来的路由中的网络 10.1.1.0/24

### 三、实验步骤:

RTA:

```

system-view      #进入系统视图模式
sysname RTA     #给设备命名
interface G0/0/0  #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1  #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/2  #进入相应接口
ip address 30.1.1.1 24    #配置 IP 地址及子网掩码
interface Loopback0  #创建环回接口 0
ip address 1.1.1.1 32     #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1 #进入 OSPF 进程 1, 并指定其路由
                        #器 ID
area 0            #创建 OSPF 区域 1
network 10.1.1.0 0.0.0.255 #通告其直连网段
network 20.1.1.0 0.0.0.255 #通告其直连网段
network 30.1.1.0 0.0.0.255 #通告其直连网段

```

RTB:

```

system-view
sysname RTB

```

```
interface G0/0/0
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 10.1.1.0 0.0.0.255
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 20.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
area 0
network 20.1.1.0 0.0.0.255
```

RTD:

```
system-view
sysname RTD
```



```
interface G0/0/0
ip address 30.1.1.2 24

interface Loopback0
ip address 4.4.4.4 32

acl 2001    #配置基本 ACL

rule deny source 10.1.1.0 0.0.0.255    #拒绝来自
10.1.1.0/24 的路由条目

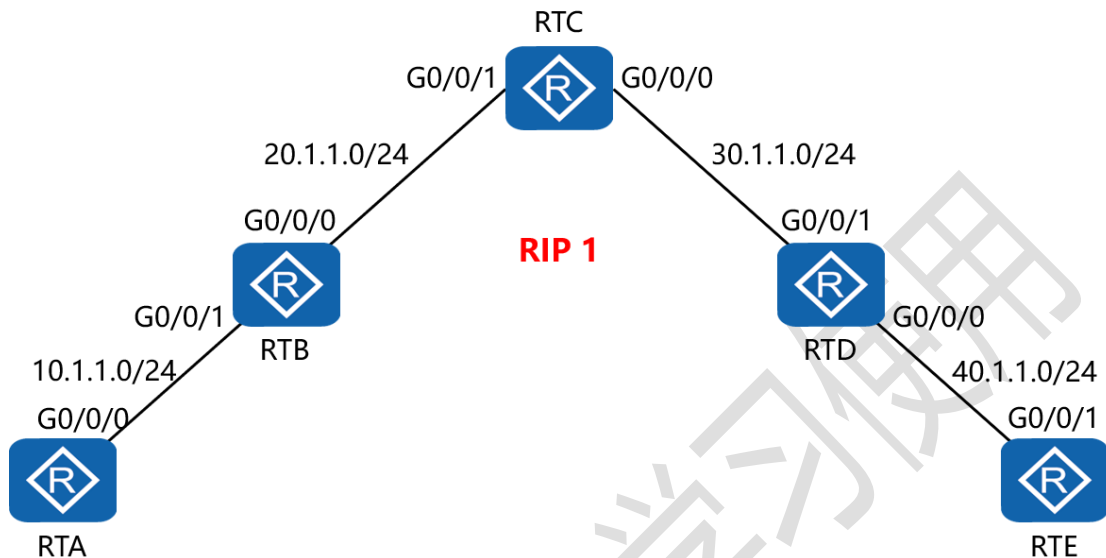
rule permit source any    #允许来自其它任意网段的路由条
目

ospf 1 router-id 4.4.4.4
filter-policy 2001 import    #使用过滤策略调用 ACL
2001, 并应用在入方向上

area 0
network 30.1.1.0 0.0.0.255
```

## 六、配置协议优先级实验组网（一）

### 一、实验拓扑：



### 二、实验目的：

5 台路由器运行 RIPv2，通过更改协议优先级，令 RTC 学到的所有路由条目的协议优先级值均变为 98

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

rip 1 #进入 RIP 进程 1

version 2 #配置使用版本 2

```
network 10.0.0.0    #通告其直连网段  
undo summary      #关闭自动汇总
```

RTB:

```
system-view  
sysname RTB  
interface G0/0/0  
ip address 20.1.1.1 24  
interface G0/0/1  
ip address 10.1.1.2 24  
rip 1  
version 2  
network 10.0.0.0  
network 20.0.0.0  
undo summary
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1
```

```
ip address 20.1.1.2 24
rip 1
version 2
network 20.0.0.0
network 30.0.0.0
undo summary
preference 98 #配置协议优先级为 98
```

```
RTD:
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
rip 1
version 2
network 30.0.0.0
network 40.0.0.0
undo summary
```

RTE:

system-view

sysname RTE

interface G0/0/1

ip address 40.1.1.2 24

rip 1

version 2

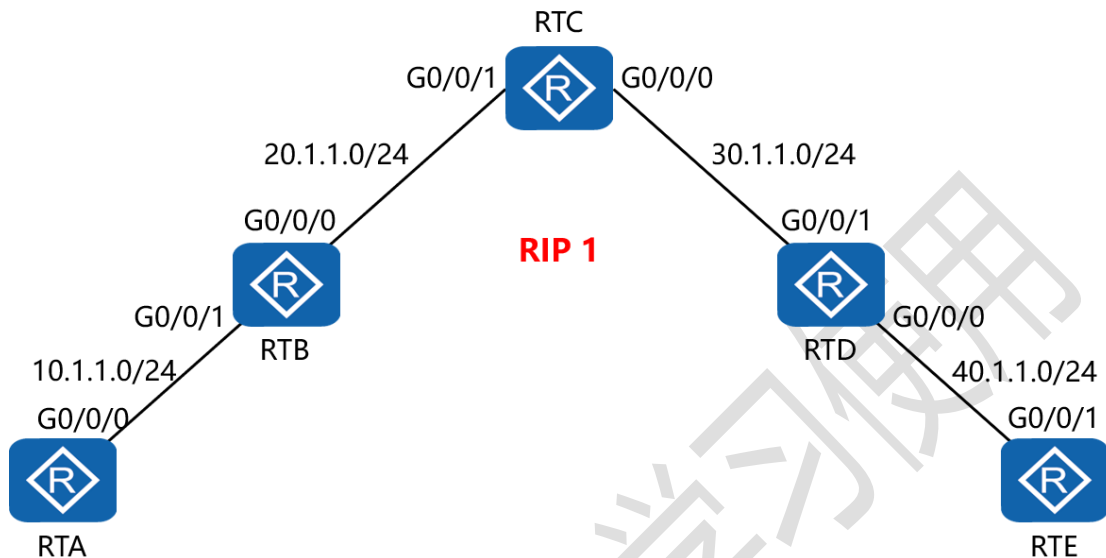
network 40.0.0.0

undo summary

仅供瑞通学员学习使用

## 七、配置协议优先级实验组网（二）

### 一、实验拓扑：



### 二、实验目的：

5 台路由器运行 RIPv2，通过更改协议优先级，令 RTC 从 RTD 学到的 RIP 的路由条目的协议优先级值变为 98，而从 RTB 学到的 RIP 的路由条目的协议优先级值保持不变

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

rip 1 #进入 RIP 进程 1

```
version 2      #配置使用版本 2
network 10.0.0.0  #通告其直连网段
undo summary   #关闭自动汇总
```

RTB:

```
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
rip 1
version 2
network 10.0.0.0
network 20.0.0.0
undo summary
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 30.1.1.1 24
```

```

interface G0/0/1
ip address 20.1.1.2 24
acl 2001    #配置基本 ACL
rule permit source 30.1.1.2 0    #匹配源主机地址 30.1.1.2
rule deny source any    #拒绝任何其它信源
route-policy 1 permit node 10    #创建路由策略 1
if-match ip next-hop acl 2001    #若下一跳 IP 地址匹配
ACL 2001
apply preference 98    #设置其协议优先级值为 98
rip 1
version 2
network 20.0.0.0
network 30.0.0.0
undo summary
preference route-policy 1    #按路由策略 1 定义协议优先级
值
RTD:
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24

```



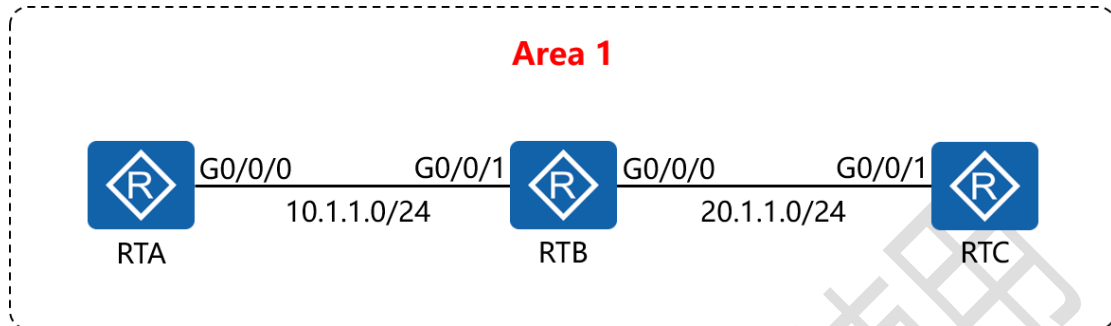
```
interface G0/0/1
ip address 30.1.1.2 24
rip 1
version 2
network 30.0.0.0
network 40.0.0.0
undo summary
```

RTE:

```
system-view
sysname RTE
interface G0/0/1
ip address 40.1.1.2 24
rip 1
version 2
network 40.0.0.0
undo summary
```

## 八、配置 IS-IS 单区域实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 IS-IS 单区域的配置，令 RTA 与 RTC 可相互访问

### 三、实验步骤：

RTA:

```

system-view      #进入系统视图模式
sysname RTA     #给设备命名
interface G0/0/0 #进入相应的接口
ip address 10.1.1.1 24 #配置 IP 地址及子网掩码
isis enable 1   #在指定接口上启用 IS-IS
isis 1         #开启 IS-IS 路由功能
is-level level-1 #配置 IS-IS 路由器类型为层 1 路由
network-entity 01.0010.0100.1001.00 #配置 IS-IS 的网络实体名称
  
```

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 20.1.1.1 24

isis enable 1

interface G0/0/1

ip address 10.1.1.2 24

isis enable 1

isis 1

is-level level-1

network-entity 01.0020.0200.2002.00

RTC:

system-view

sysname RTC

interface G0/0/1

ip address 20.1.1.2 24

isis enable 1

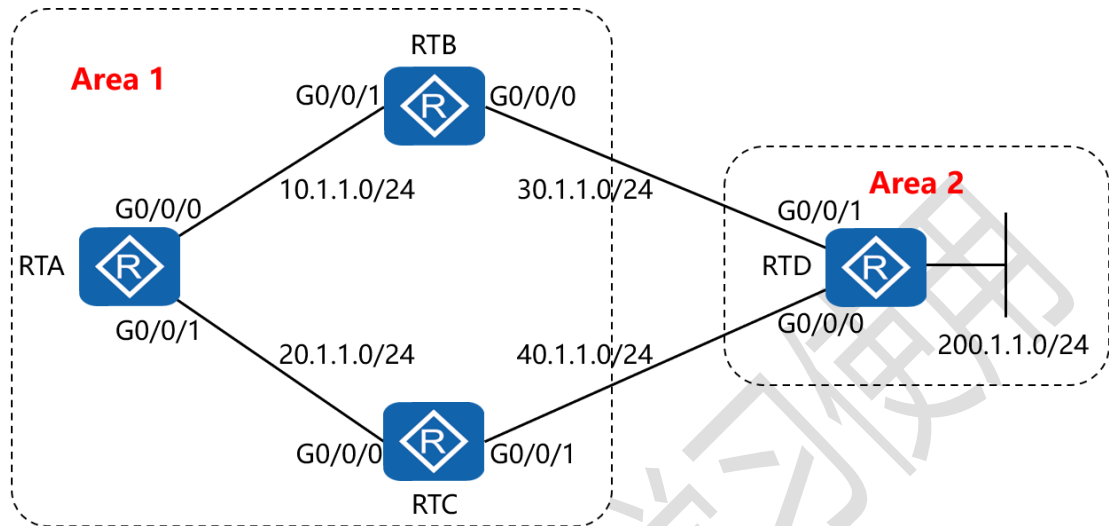
isis 1

is-level level-1

network-entity 01.0030.0300.3003.00

## 九、配置 IS-IS 多区域实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 IS-IS 多区域的配置，令全网全通，并令 RTA 到达 RTD 的 200.1.1.0/24 网络优选经过 RTB

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应的接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
isis enable 1       #在指定接口上启用 IS-IS
isis cost 10        #配置 IS-IS 接口的链路开销值
interface G0/0/1     #进入相应的接口
    
```

```
ip address 20.1.1.1 24      #配置 IP 地址及子网掩码
isis enable 1              #在指定接口上启用 IS-IS
isis cost 20              #配置 IS-IS 接口的链路开销值
isis 1                    #开启 IS-IS 路由功能
is-level level-1          #配置 IS-IS 路由器类型为层 1 路由
network-entity 01.0010.0100.1001.00  #配置 IS-IS 的网络实体名称
```

RTB:

```
system-view
```

```
sysname RTB
```

```
interface G0/0/0
```

```
ip address 30.1.1.1 24
```

```
isis enable 1
```

```
interface G0/0/1
```

```
ip address 10.1.1.2 24
```

```
isis enable 1
```

```
isis 1
```

```
is-level level-1-2
```

```
network-entity 01.0020.0200.2002.00
```

RTC:

system-view

sysname RTC

interface G0/0/0

ip address 20.1.1.2 24

isis enable 1

interface G0/0/1

ip address 40.1.1.1 24

isis enable 1

isis 1

is-level level-1-2

network-entity 01.0030.0300.3003.00

RTD:

system-view

sysname RTD

interface G0/0/0

ip address 40.1.1.2 24

isis enable 1

interface G0/0/1

ip address 30.1.1.2 24

isis enable 1

```
interface Loopback0
ip address 200.1.1.1 24
isis enable 1
isis 1
is-level level-2
network-entity 02.0040.0400.4004.00
```

测试:

在 RTA 上 ping RTD 的 200.1.1.1:

```
[RTA]ping 200.1.1.1
  PING 200.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 200.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/28/30 ms

[RTA]
```

在 RTA 上检测到达网络 200.1.1.1 所使用的路径:

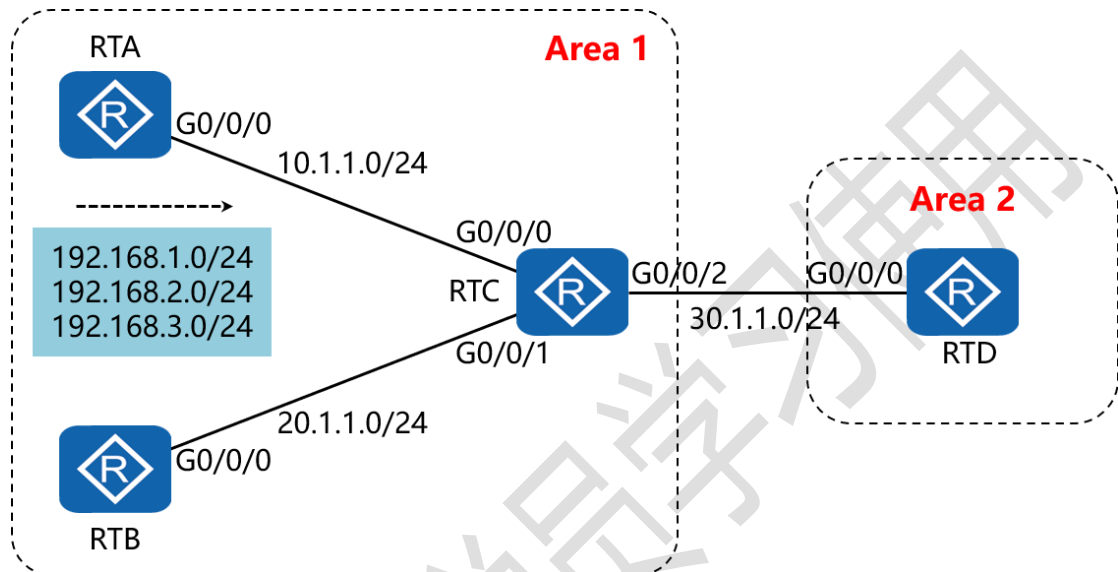
```
[RTA]tracert 200.1.1.1
  traceroute to 200.1.1.1(200.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C to break
  1 10.1.1.2 20 ms  20 ms  20 ms
  2 30.1.1.2 30 ms  10 ms  20 ms

[RTA]
```

# 十、配置 IS-IS 路由验证及聚合实验组

## 网

### 一、实验拓扑：



### 二、实验目的：

在 4 台路由器上配置认证, 同时在 RTC 上配置路由聚合, 令 RTD 只学习聚合后的路由 192.168.0.0/16

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应的接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

isis enable 1 #在指定接口上启用 IS-IS



isis authentication-mode md5 cipher *huawei* #配置邻

居关系验证方式及验证密码

interface Loopback0 #创建并进入环回接口 0

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

isis enable 1 #在指定接口上启用 IS-IS

interface Loopback1 #创建并进入环回接口 1

ip address 192.168.2.1 24 #配置 IP 地址及子网掩码

isis enable 1 #在指定接口上启用 IS-IS

interface Loopback2 #创建并进入环回接口 2

ip address 192.168.3.1 24 #配置 IP 地址及子网掩码

isis enable 1 #在指定接口上启用 IS-IS

isis 1 #开启 IS-IS 路由功能

is-level level-1 #配置 IS-IS 路由器类型为层 1 路由

network-entity 01.0010.0100.1001.00 #配置 IS-IS 的网

络实体名称

area-authentication-mode md5 cipher *atnet* #配置区

域验证方式及验证密码

RTB:

system-view

sysname RTB

interface G0/0/0

```
ip address 20.1.1.1 24
isis enable 1
isis authentication-mode md5 cipher huawei
isis 1
is-level level-1
network-entity 01.0020.0200.2002.00
area-authentication-mode md5 cipher atnet
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 10.1.1.2 24
isis enable 1
isis authentication-mode md5 cipher huawei
interface G0/0/1
ip address 20.1.1.2 24
isis enable 1
isis authentication-mode md5 cipher huawei
interface G0/0/2
ip address 30.1.1.1 24
isis enable 1
```

```
isis authentication-mode md5 cipher huawei
isis 1
is-level level-1-2
network-entity 01.0030.0300.3003.00
area-authentication-mode md5 cipher atnet
domain-authentication-mode md5 cipher hcip #配置路由域验证方式及验证密码
summary 192.168.0.0 255.255.0.0 level-2 #配置仅对引入到层 2 的路由进行聚合

RTD:
system-view
sysname RTD
interface G0/0/0
ip address 30.1.1.2 24
isis enable 1
isis authentication-mode md5 cipher huawei
isis 1
is-level level-2
network-entity 02.0040.0400.4004.00
domain-authentication-mode md5 cipher hcip
```

测试：

查看 RTD 的 IS-IS 路由表，发现只有聚合路由条目：

```
[RTD]display isis route

Route information for ISIS(1)
-----

ISIS(1) Level-2 Forwarding Table
-----

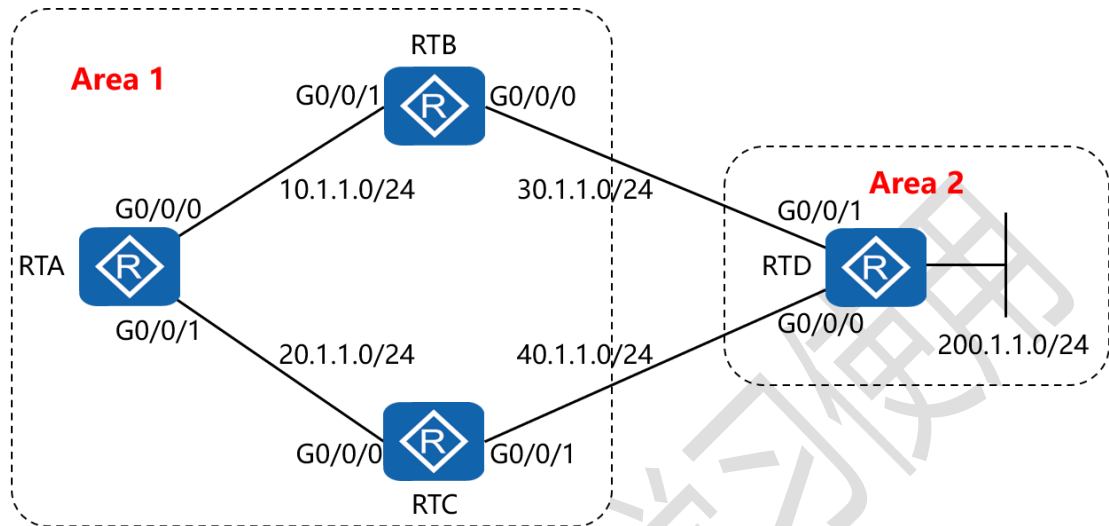
IPV4 Destination      IntCost    ExtCost  ExitInterface  NextHop      Flags
-----
192.168.0.0/16        20         NULL    GE0/0/0        30.1.1.1     A/-/-/-
10.1.1.0/24           20         NULL    GE0/0/0        30.1.1.1     A/-/-/-
20.1.1.0/24           20         NULL    GE0/0/0        30.1.1.1     A/-/-/-
30.1.1.0/24           10         NULL    GE0/0/0        Direct       D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
       U-Up/Down Bit Set

[RTD]
```



# 十一、配置 IS-IS 路由渗透实验组网

## 一、实验拓扑：



## 二、实验目的：

配置 RTB 与 RTC，令其将从层 2 学习到的路由条目渗透给层 1 的路由器

## 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应的接口
ip address 10.1.1.1 24 #配置 IP 地址及子网掩码
isis enable 1       #在指定接口上启用 IS-IS
interface G0/0/1     #进入相应的接口
ip address 20.1.1.1 24 #配置 IP 地址及子网掩码
    
```

```
isis enable 1      #在指定接口上启用 IS-IS  
isis 1            #开启 IS-IS 路由功能  
is-level level-1  #配置 IS-IS 路由器类型为层 1 路由  
network-entity 01.0010.0100.1001.00  #配置 IS-IS 的网络实体名称
```

RTB:

```
system-view  
sysname RTB  
interface G0/0/0  
ip address 30.1.1.1 24  
isis enable 1  
interface G0/0/1  
ip address 10.1.1.2 24  
isis enable 1  
isis 1  
is-level level-1-2  
network-entity 01.0020.0200.2002.00
```

RTC:

```
system-view  
sysname RTC
```

```
interface G0/0/0
ip address 20.1.1.2 24
isis enable 1
interface G0/0/1
ip address 40.1.1.1 24
isis enable 1
isis 1
is-level level-1-2
network-entity 01.0030.0300.3003.00
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.2 24
isis enable 1
interface G0/0/1
ip address 30.1.1.2 24
isis enable 1
interface Loopback0
ip address 200.1.1.1 24
isis enable 1
```

isis 1

is-level level-2

network-entity 02.0040.0400.4004.00

测试:

完成上述配置后, 在 RTA 上 ping RTD 的 200.1.1.1:

```
[RTA]ping 200.1.1.1
  PING 200.1.1.1: 56 data bytes, press CTRL C to break
    Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=254 time=20 ms
    Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 200.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/30/40 ms

[RTA]
```

再在 RTA 上查看 IS-IS 的路由表:

```
[RTA]display isis route

      Route information for ISIS(1)
      -----
      ISIS(1) Level-1 Forwarding Table
      -----

IPV4 Destination    IntCost    ExtCost    ExitInterface    NextHop        Flags
-----
0.0.0.0/0           10         NULL       GE0/0/1          20.1.1.2       A/-/-/-
10.1.1.0/24         10         NULL       GE0/0/0          10.1.1.2       D/-/L/-
20.1.1.0/24         10         NULL       GE0/0/1          Direct         D/-/L/-
30.1.1.0/24         20         NULL       GE0/0/0          10.1.1.2       A/-/-/-
40.1.1.0/24         20         NULL       GE0/0/1          20.1.1.2       A/-/-/-

      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
            U-Up/Down Bit Set

[RTA]
```

发现 RTA 的 IS-IS 路由表中并没有关于 200.1.1.0 网络的路由  
条目



此时，需要在 RTB 及 RTC 上做如下配置：

RTB:

isis 1

import-route isis level-2 into level-1

RTC:

isis 1

import-route isis level-2 into level-1

再次查看 RTA 的 IS-IS 路由表：

```
[RTA]display isis route

Route information for ISIS(1)
-----

ISIS(1) Level-1 Forwarding Table
-----

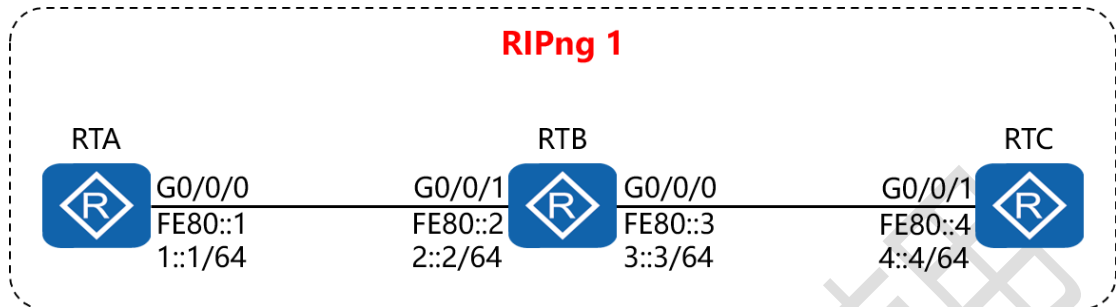
IPV4 Destination      IntCost    ExtCost    ExitInterface    NextHop        Flags
-----
0.0.0.0/0             10         NULL       GE0/0/1          20.1.1.2       A/-/-/-
                    10         NULL       GE0/0/0          10.1.1.2
10.1.1.0/24          10         NULL       GE0/0/0          Direct         D-/L/-
20.1.1.0/24          10         NULL       GE0/0/1          Direct         D-/L/-
30.1.1.0/24          20         NULL       GE0/0/0          10.1.1.2       A/-/-/-
40.1.1.0/24          20         NULL       GE0/0/1          20.1.1.2       A/-/-/-
200.1.1.0/24         20         NULL       GE0/0/0          10.1.1.2       A/-/-/U
                    20         NULL       GE0/0/1          20.1.1.2

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
       U-Up/Down Bit Set

[RTA]
```

## 十二、配置 RIPng 实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 RIPng 的配置，令 RTA 可以学习到 RTC 的路由条目，并与之通讯

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

ipv6 #开启设备的 IPv6 功能

ripng #开启并进入 RIPng 进程

interface G0/0/0 #进入相应接口

ipv6 enable #在接口下开启 IPv6 功能

ipv6 address FE80::1 link-local #配置该接口的链路本地地址

ipv6 address 1::1/64 #配置该接口的通讯地址

ripng 1 enable #在该接口上开启 RIPng 进程

RTB:

system-view

sysname RTB

ipv6

ripng

interface G0/0/1

ipv6 enable

ipv6 address FE80::2 link-local

ipv6 address 2::2/64

ripng 1 enable

interface G0/0/0

ipv6 enable

ipv6 address FE80::3 link-local

ipv6 address 3::3/64

ripng 1 enable

RTC:

system-view

sysname RTC

ipv6

```
ripng  
interface G0/0/1  
ipv6 enable  
ipv6 address FE80::4 link-local  
ipv6 address 4::4/64  
ripng 1 enable
```

仅供瑞通学员学习使用



## 地址

ipv6 address 1::1/64 #配置该接口的通讯地址  
ospfv3 1 area 0.0.0.0 #在该接口上开启 OSPFv3 进程，并指定其所属区域

RTB:

```
system-view
sysname RTB
interface Loopback0
ip address 2.2.2.2 32
ipv6
ospfv3
router-id 2.2.2.2
interface G0/0/1
ipv6 enable
ipv6 address FE80::2 link-local
ipv6 address 2::2/64
ospfv3 1 area 0.0.0.0
interface G0/0/0
ipv6 enable
ipv6 address FE80::3 link-local
ipv6 address 3::3/64
```

---

```
ospfv3 1 area 0.0.0.0
```

```
RTC:
```

```
system-view
```

```
sysname RTC
```

```
interface Loopback0
```

```
ip address 3.3.3.3 32
```

```
ipv6
```

```
ospfv3
```

```
router-id 3.3.3.3
```

```
interface G0/0/1
```

```
ipv6 enable
```

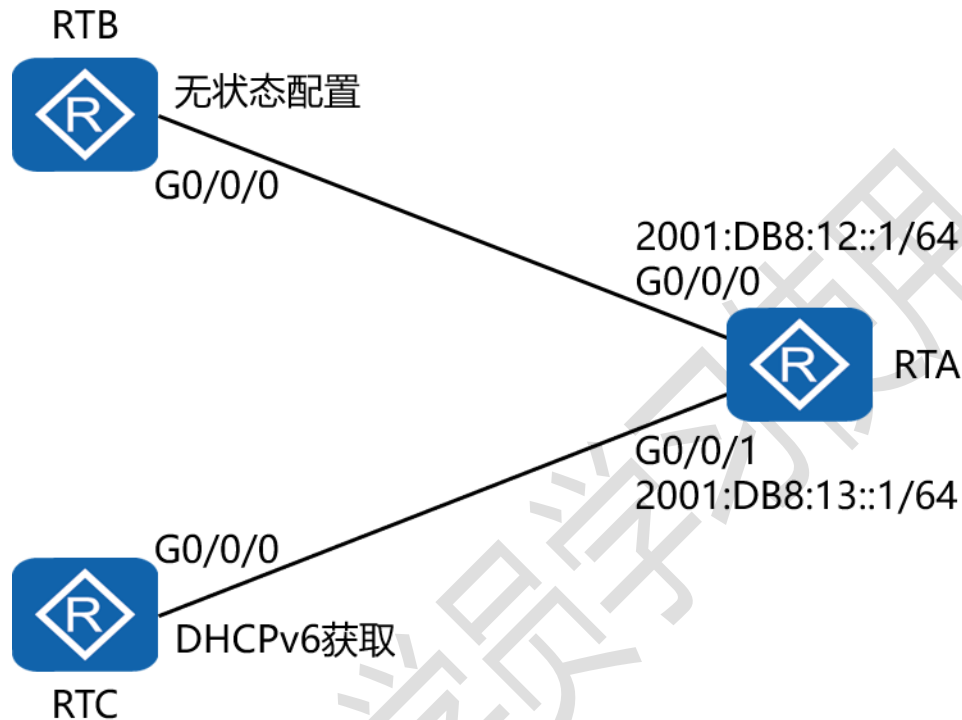
```
ipv6 address FE80::4 link-local
```

```
ipv6 address 4::4/64
```

```
ospfv3 1 area 0.0.0.0
```

## 十四、配置 IPv6 各类地址实验组网

### 一、实验拓扑：



### 二、实验目的：

RTA 的 G0/0/0 与 G0/0/1 接口采用手工方式配置 IPv6 地址；  
RTB 的 G0/0/0 接口通过无状态地址自动配置的方式获取 IPv6 地址；  
RTC 的 G0/0/0 接口通过 DHCPv6 的方式获取 IPv6 地址

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

ipv6 #开启设备的 IPv6 功能



```

dhcp enable          #开启 DHCP 功能
dhcpv6 pool easthome #创建 DHCPv6 地址池并命名
address prefix 2001:DB8:13::/64 #指定分配的网段及掩码
excluded-address 2001:DB8:13::1 #排除不分配的地址
interface G0/0/0    #进入相应的接口
ipv6 enable        #在接口下开启 IPv6 功能
ipv6 address auto link-local #令接口自动生成链路本地地址
ipv6 address 2001:DB8:12::1 64 #配置该接口的通讯地址
undo ipv6 nd ra halt #开启发布 RA 报文的功能
interface G0/0/1
ipv6 enable
ipv6 address auto link-local
ipv6 address 2001:DB8:13::1 64
dhcpv6 server easthome

RTB:
system-view
sysname RTB
ipv6
interface G0/0/0
ipv6 enable

```

ipv6 address auto link-local

ipv6 address auto global #令该接口通过无状态地址自动配置的方式获取 IPv6 地址

RTC:

system-view

sysname RTC

ipv6

dhcp enable

interface G0/0/0

ipv6 enable

ipv6 address auto link-local

ipv6 address auto dhcp #令该接口通过 DHCPv6 的方式获取 IPv6 地址

测试:

在 RTB 上查看其接口的 IPv6 地址

```
[RTB]display ipv6 interface g0/0/0
GigabitEthernet0/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE13:36C5
Global unicast address(es):
  2001:DB8:12:0:2E0:FCFF:FE13:36C5,
  subnet is 2001:DB8:12::/64 [SLAAC 1970-01-01 00:05:25 2592000S]
Joined group address(es):
  FF02::1:FF13:36C5
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
[RTB]
```

再在 RTB 上查看其接口 G0/0/0 的 MAC 地址，确认其 IPv6 地址是使用其自身的接口 MAC 地址自动生成的

```
[RTB]display interface g0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, GigabitEthernet0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc13-36c5
Last physical up time : 2021-06-10 12:14:25 UTC-08:00
Last physical down time : 2021-06-10 12:14:16 UTC-08:00
Current system time: 2021-06-10 12:25:21-08:00
Port Mode: FORCE COPPER
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 176 bits/sec,Record time: 2021-06-10 12:18:28
Output peak rate 232 bits/sec,Record time: 2021-06-10 12:19:38

Input: 8 packets, 816 bytes
  Unicast: 0, Multicast: 8
  Broadcast: 0, Jumbo: 0
  Discard: 0, Total Error: 0

CRC: 0, Giants: 0
---- More ----
```

在 RTC 上查看其接口的 IPv6 地址

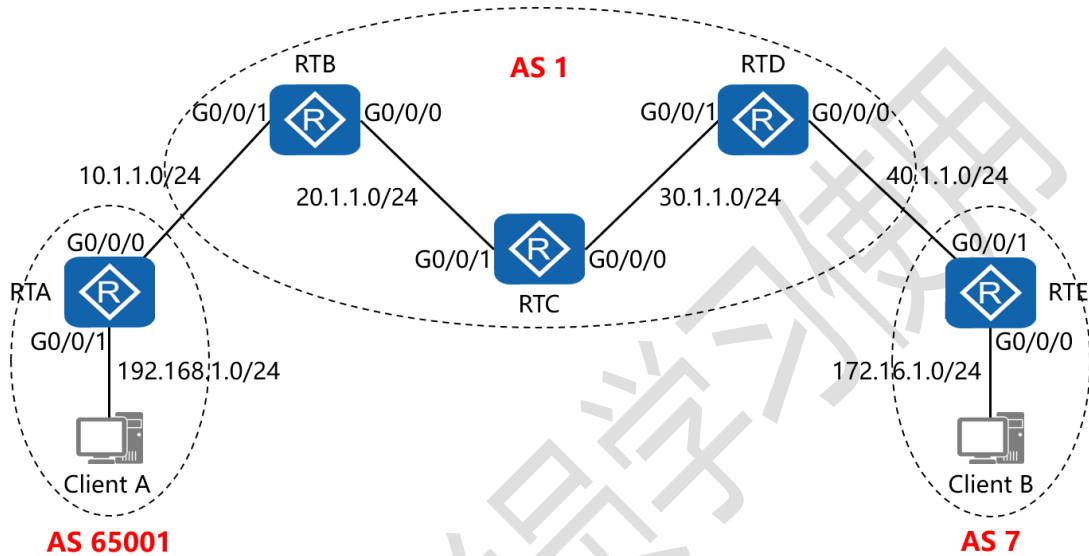
```
[RTC]display dhcpv6 client
GigabitEthernet0/0/0 is in stateful DHCPv6 client mode.
State is BOUND.
Preferred server DUID    : 0003000100E0FC1B6A14
  Reachable via address  : FE80::2E0:FCFF:FE1B:6A15
IA NA IA ID 0x00000031 T1 43200 T2 69120
  Obtained               : 2021-06-10 12:20:02
  Renews                 : 2021-06-11 00:20:02
  Rebinds                : 2021-06-11 07:32:02
  Address                : 2001:DB8:13::2
  Lifetime valid 172800 seconds, preferred 86400 seconds
  Expires at 2021-06-12 12:20:02 (172265 seconds left)

[RTC]
```

# 十五、配置 IBGP 与 EBGP 会话实验组

## 网

### 一、实验拓扑：



### 二、实验目的：

通过 IBGP 与 EBGP 之间会话的配置，令 2 台客户端能够正常通讯

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```

ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0    #进入相应接口
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
bgp 65001    #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID，以及
#远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
#EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
#与对等体之间用哪个接口来承载更新
network 192.168.1.0    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总
ip route-static 2.2.2.2 255.255.255.255 10.1.1.2    #配置静
#态路由（对等体路由器 ID+对等体路由器 ID 的子网掩码+下一
#跳接口地址）

RTB:
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24

```

```
interface G0/0/1
ip address 10.1.1.2 24

interface LoopBack0
ip address 2.2.2.2 32

bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 24
network 20.1.1.0 24
network 30.1.1.0 24
peer 3.3.3.3 next-hop-local      #告知对等体, 自己为其访问
EBGP 的下一跳路由器
peer 4.4.4.4 next-hop-local

rip 1
version 2
network 2.0.0.0
```

```
network 20.0.0.0  
undo summary  
ip route-static 1.1.1.1 255.255.255.255 10.1.1.1
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
interface LoopBack0  
ip address 3.3.3.3 32  
bgp 1  
router-id 3.3.3.3  
peer 2.2.2.2 as-number 1  
peer 2.2.2.2 connect-interface LoopBack0  
peer 4.4.4.4 as-number 1  
peer 4.4.4.4 connect-interface LoopBack0  
network 20.1.1.0 24  
network 30.1.1.0 24  
rip 1
```



```
version 2
network 20.0.0.0
network 30.0.0.0
network 3.0.0.0
undo summary
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
bgp 1
router-id 4.4.4.4
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 5.5.5.5 as-number 7
```

```
peer 5.5.5.5 ebgp-max-hop 2
peer 5.5.5.5 connect-interface LoopBack0
network 20.1.1.0 24
network 30.1.1.0 24
network 40.1.1.0 24
peer 2.2.2.2 next-hop-local
peer 3.3.3.3 next-hop-local
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
undo summary
ip route-static 5.5.5.5 255.255.255.255 40.1.1.2
```

RTE:

```
system-view
sysname RTE
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
ip address 40.1.1.2 24
interface LoopBack0
```

```
ip address 5.5.5.5 32
bgp 7
router-id 5.5.5.5
peer 4.4.4.4 as-number 1
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 172.16.1.0 24
ip route-static 4.4.4.4 255.255.255.255 40.1.1.1
```

测试:

分别在 RTA 与 RTE 上查看路由表:

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 16          Routes : 16

Destination/Mask    Proto    Pre  Cost           Flags NextHop           Interface
-----
      1.1.1.1/32     Direct   0    0              D    127.0.0.1           LoopBack0
      2.2.2.2/32     Static   60   0              RD   10.1.1.2            GigabitEthernet
0/0/0
      10.1.1.0/24    Direct   0    0              D    10.1.1.1            GigabitEthernet
0/0/0
      10.1.1.1/32    Direct   0    0              D    127.0.0.1            GigabitEthernet
0/0/0
      10.1.1.255/32  Direct   0    0              D    127.0.0.1            GigabitEthernet
0/0/0
      20.1.1.0/24    EBGP     255  0              RD   2.2.2.2             GigabitEthernet
0/0/0
      30.1.1.0/24    EBGP     255  1              RD   2.2.2.2             GigabitEthernet
0/0/0
      40.1.1.0/24    EBGP     255  0              RD   2.2.2.2             GigabitEthernet
0/0/0
      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
      172.16.1.0/24  EBGP     255  0              RD   2.2.2.2             GigabitEthernet
0/0/0
      192.168.1.0/24 Direct   0    0              D    192.168.1.1         GigabitEthernet
0/0/1
      192.168.1.1/32 Direct   0    0              D    127.0.0.1            GigabitEthernet
0/0/1
      192.168.1.255/32 Direct   0    0              D    127.0.0.1            GigabitEthernet
0/0/1
255.255.255.255/32 Direct   0    0              D    127.0.0.1            InLoopBack0
[RTA]
```

```
[RTE]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 16          Routes : 16

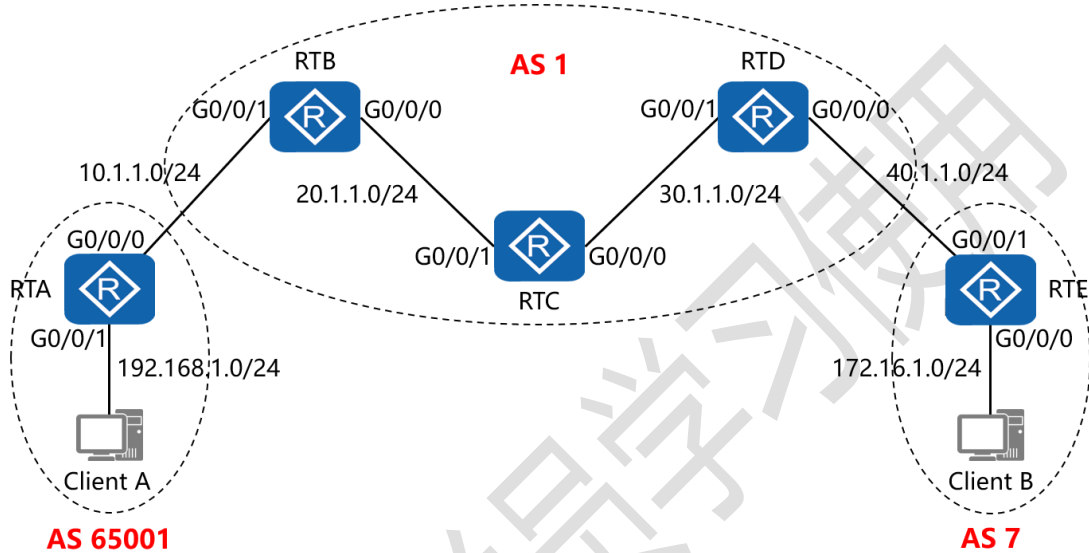
Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
0/0/1               4.4.4.4/32 Static   60   0              RD   40.1.1.1          GigabitEthernet
0/0/1               5.5.5.5/32 Direct   0    0              D    127.0.0.1         LoopBack0
0/0/1               10.1.1.0/24 EBGP     255  0              RD   4.4.4.4           GigabitEthernet
0/0/1               20.1.1.0/24 EBGP     255  1              RD   4.4.4.4           GigabitEthernet
0/0/1               30.1.1.0/24 EBGP     255  0              RD   4.4.4.4           GigabitEthernet
0/0/1               40.1.1.0/24 Direct   0    0              D    40.1.1.2          GigabitEthernet
0/0/1               40.1.1.2/32 Direct   0    0              D    127.0.0.1         GigabitEthernet
0/0/1               40.1.1.255/32 Direct  0    0              D    127.0.0.1         GigabitEthernet
0/0/1               127.0.0.0/8 Direct   0    0              D    127.0.0.1         InLoopBack0
0/0/1               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
0/0/0               172.16.1.0/24 Direct  0    0              D    172.16.1.1       GigabitEthernet
0/0/0               172.16.1.1/32 Direct  0    0              D    127.0.0.1         GigabitEthernet
0/0/0               172.16.1.255/32 Direct  0    0              D    127.0.0.1         GigabitEthernet
0/0/0               192.168.1.0/24 EBGP     255  0              RD   4.4.4.4           GigabitEthernet
0/0/1               255.255.255.255/32 Direct  0    0              D    127.0.0.1         InLoopBack0

[RTE]
```



# 十六、配置通过 AS-Path 属性移除私有 AS 号实验组网

## 一、实验拓扑：



## 二、实验目的：

通过 IBGP 与 EBGP 之间会话的配置，令 2 台客户端能够正常通讯，之后在 RTD 上配置 AS-Path 属性，令其在将网络 192.168.1.0/24 发送给 RTE 时，移除其所属的私有 AS 号码

## 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

```

interface G0/0/1    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0    #进入相应接口
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
bgp 65001    #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID，以及
远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
与对等体之间用哪个接口来承载更新
network 192.168.1.0    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总
ip route-static 2.2.2.2 255.255.255.255 10.1.1.2    #配置静
态路由（对等体路由器 ID+对等体路由器 ID 的子网掩码+下一
跳接口地址）

```

RTB:

```

system-view
sysname RTB
interface G0/0/0

```

```
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface LoopBack0
ip address 2.2.2.2 32
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 24
network 20.1.1.0 24
network 30.1.1.0 24
peer 3.3.3.3 next-hop-local
peer 4.4.4.4 next-hop-local
rip 1
version 2
network 2.0.0.0
```

```
network 20.0.0.0  
undo summary  
ip route-static 1.1.1.1 255.255.255.255 10.1.1.1
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
interface LoopBack0  
ip address 3.3.3.3 32  
bgp 1  
router-id 3.3.3.3  
peer 2.2.2.2 as-number 1  
peer 2.2.2.2 connect-interface LoopBack0  
peer 4.4.4.4 as-number 1  
peer 4.4.4.4 connect-interface LoopBack0  
network 20.1.1.0 24  
network 30.1.1.0 24  
rip 1
```



```
version 2
network 20.0.0.0
network 30.0.0.0
network 3.0.0.0
undo summary
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
bgp 1
router-id 4.4.4.4
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 5.5.5.5 as-number 7
```

```
peer 5.5.5.5 ebgp-max-hop 2
peer 5.5.5.5 connect-interface LoopBack0
peer 5.5.5.5 public-as-only      #移除私有 AS 号码, 仅保留
公有 AS 号码
network 20.1.1.0 24
network 30.1.1.0 24
network 40.1.1.0 24
peer 2.2.2.2 next-hop-local
peer 3.3.3.3 next-hop-local
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
undo summary
ip route-static 5.5.5.5 255.255.255.255 40.1.1.2

RTE:
system-view
sysname RTE
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
```

```
ip address 40.1.1.2 24
interface LoopBack0
ip address 5.5.5.5 32
bgp 7
router-id 5.5.5.5
peer 4.4.4.4 as-number 1
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 172.16.1.0 24
ip route-static 4.4.4.4 255.255.255.255 40.1.1.1
```

测试:

在 RTD 上未应用 public-as-only 参数时, RTE 的 BGP 表项为:

```
[RTE]dis bgp routing-table

BGP Local router ID is 5.5.5.5
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6
   Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
*> 10.1.1.0/24      4.4.4.4          0             0               0       1i
*> 20.1.1.0/24      4.4.4.4          1             0               0       1i
*> 30.1.1.0/24      4.4.4.4          0             0               0       1i
*> 40.1.1.0/24      4.4.4.4          0             0               0       1i
*> 172.16.1.0/24    0.0.0.0          0             0               0       i
*> 192.168.1.0     4.4.4.4          0             0               1       65001i
[RTE]
```

在 RTD 上应用 public-as-only 参数后, RTE 的 BGP 表项为:

```
[RTE]dis bgp routing-table

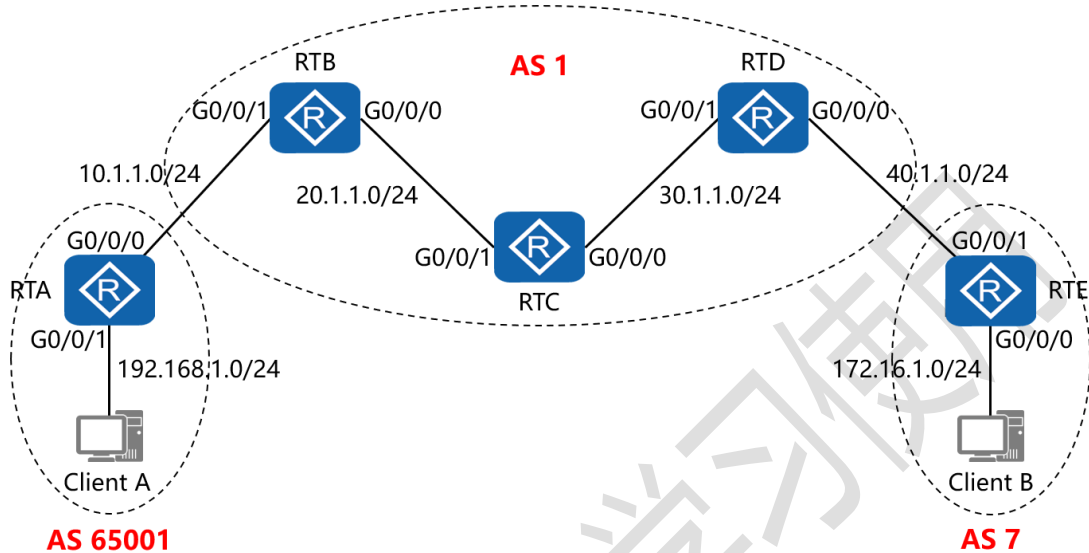
BGP Local router ID is 5.5.5.5
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6
  Network          NextHop      MED      LocPrf    PrefVal Path/Ogn
* > 10.1.1.0/24    4.4.4.4
* > 20.1.1.0/24    4.4.4.4      1
* > 30.1.1.0/24    4.4.4.4      0
* > 40.1.1.0/24    4.4.4.4      0
* > 172.16.1.0/24  0.0.0.0      0
* > 192.168.1.0    4.4.4.4      0
```



## 十七、配置 BGP 原子汇总实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 IBGP 与 EBGP 之间会话的配置，令 2 台客户端能够正常通讯，之后在 RTD 上配置原子汇总，将其网络 192.168.1.0/24 汇总为 192.168.0.0/16 通告给 RTE，而 192.168.1.0/24 的明晰路由则不再通告

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

```

interface G0/0/1    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0    #进入相应接口
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
bgp 65001    #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID，以及
#远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
#EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
#与对等体之间用哪个接口来承载更新
network 192.168.1.0    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总
ip route-static 2.2.2.2 255.255.255.255 10.1.1.2    #配置静
#态路由（对等体路由器 ID+对等体路由器 ID 的子网掩码+下一
#跳接口地址）

```

RTB:

system-view

sysname RTB

interface G0/0/0

```
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface LoopBack0
ip address 2.2.2.2 32
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 24
network 20.1.1.0 24
network 30.1.1.0 24
peer 3.3.3.3 next-hop-local
peer 4.4.4.4 next-hop-local
rip 1
version 2
network 2.0.0.0
```

```
network 20.0.0.0  
undo summary  
ip route-static 1.1.1.1 255.255.255.255 10.1.1.1
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
interface LoopBack0  
ip address 3.3.3.3 32  
bgp 1  
router-id 3.3.3.3  
peer 2.2.2.2 as-number 1  
peer 2.2.2.2 connect-interface LoopBack0  
peer 4.4.4.4 as-number 1  
peer 4.4.4.4 connect-interface LoopBack0  
network 20.1.1.0 24  
network 30.1.1.0 24  
rip 1
```



```
version 2  
network 20.0.0.0  
network 30.0.0.0  
network 3.0.0.0  
undo summary
```

RTD:

```
system-view  
sysname RTD  
interface G0/0/0  
ip address 40.1.1.1 24  
interface G0/0/1  
ip address 30.1.1.2 24  
interface LoopBack0  
ip address 4.4.4.4 32  
bgp 1  
router-id 4.4.4.4  
peer 2.2.2.2 as-number 1  
peer 2.2.2.2 connect-interface LoopBack0  
peer 3.3.3.3 as-number 1  
peer 3.3.3.3 connect-interface LoopBack0  
peer 5.5.5.5 as-number 7
```

```
peer 5.5.5.5 ebgp-max-hop 2
peer 5.5.5.5 connect-interface LoopBack0
network 20.1.1.0 24
network 30.1.1.0 24
network 40.1.1.0 24
aggregate 192.168.0.0 16 detail-suppressed #进行路由
汇总, 并拒绝明晰路由
peer 2.2.2.2 next-hop-local
peer 3.3.3.3 next-hop-local
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
undo summary
ip route-static 5.5.5.5 255.255.255.255 40.1.1.2

RTE:
system-view
sysname RTE
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
```

```
ip address 40.1.1.2 24
interface LoopBack0
ip address 5.5.5.5 32
bgp 7
router-id 5.5.5.5
peer 4.4.4.4 as-number 1
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 172.16.1.0 24
ip route-static 4.4.4.4 255.255.255.255 40.1.1.1
```

测试：

在 RTD 上没有配置原子汇总时，查看 RTE 的路由表：

```
[RTE]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 16          Routes : 16

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
0/0/1      4.4.4.4/32  Static  60   0             RD   40.1.1.1         GigabitEthernet
0/0/1      5.5.5.5/32  Direct   0   0             D    127.0.0.1        LoopBack0
0/0/1      10.1.1.0/24 EBGP     255  0             RD   4.4.4.4          GigabitEthernet
0/0/1      20.1.1.0/24 EBGP     255  1             RD   4.4.4.4          GigabitEthernet
0/0/1      30.1.1.0/24 EBGP     255  0             RD   4.4.4.4          GigabitEthernet
0/0/1      40.1.1.0/24 Direct   0   0             D    40.1.1.2         GigabitEthernet
0/0/1      40.1.1.2/32 Direct   0   0             D    127.0.0.1        GigabitEthernet
0/0/1      40.1.1.255/32 Direct  0   0             D    127.0.0.1        GigabitEthernet
0/0/1      127.0.0.0/8 Direct   0   0             D    127.0.0.1        InLoopBack0
0/0/1      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
0/0/0      172.16.1.0/24 Direct  0   0             D    172.16.1.1       GigabitEthernet
0/0/0      172.16.1.1/32 Direct  0   0             D    127.0.0.1        GigabitEthernet
0/0/0      172.16.1.255/32 Direct  0   0             D    127.0.0.1        GigabitEthernet
0/0/0      192.168.1.0/24 EBGP     255  0             RD   4.4.4.4          GigabitEthernet
0/0/1      255.255.255.255/32 Direct  0   0             D    127.0.0.1        InLoopBack0

[RTE]
```



在 RTD 上配置了原子汇总后，查看 RTE 的路由表：

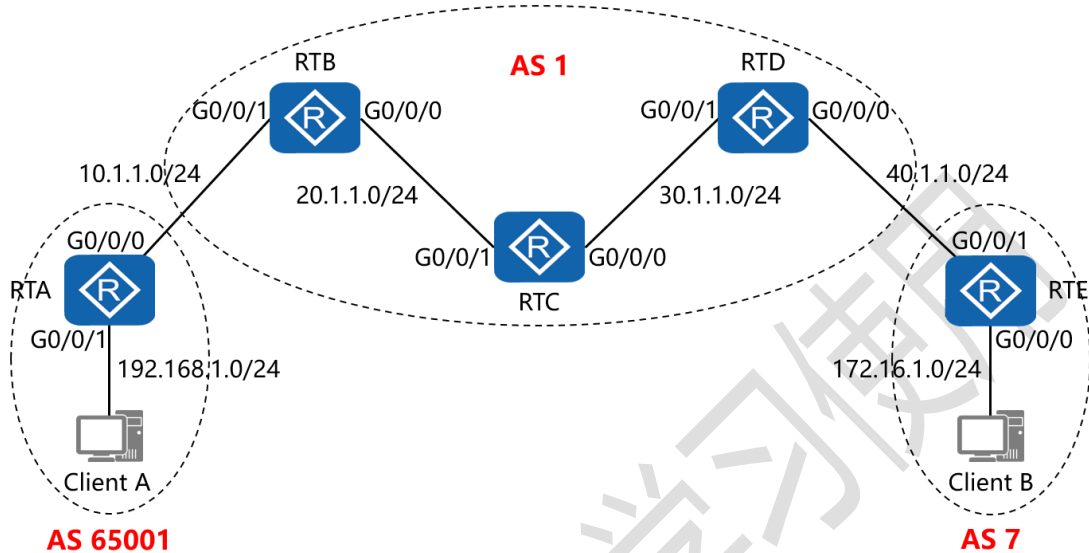
```
[RTE]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 16          Routes : 16

Destination/Mask    Proto    Pre  Cost    Flags NextHop         Interface
-----
0/0/1      4.4.4.4/32  Static  60    0        RD  40.1.1.1         GigabitEthernet
5.5.5.5/32  Direct    0     0         D  127.0.0.1        LoopBack0
10.1.1.0/24 EBGP      255   0         RD  4.4.4.4          GigabitEthernet
0/0/1
20.1.1.0/24 EBGP      255   1         RD  4.4.4.4          GigabitEthernet
0/0/1
30.1.1.0/24 EBGP      255   0         RD  4.4.4.4          GigabitEthernet
0/0/1
40.1.1.0/24 Direct    0     0         D  40.1.1.2         GigabitEthernet
0/0/1
40.1.1.2/32 Direct    0     0         D  127.0.0.1        GigabitEthernet
0/0/1
40.1.1.255/32 Direct    0     0         D  127.0.0.1        GigabitEthernet
0/0/1
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
172.16.1.0/24 Direct    0     0         D  172.16.1.1       GigabitEthernet
0/0/0
172.16.1.1/32 Direct    0     0         D  127.0.0.1        GigabitEthernet
0/0/0
172.16.1.255/32 Direct    0     0         D  127.0.0.1        GigabitEthernet
0/0/0
192.168.0.0/16 EBGP      255   0         RD  4.4.4.4          GigabitEthernet
0/0/1
255.255.255.255/32 Direct    0     0         D  127.0.0.1        InLoopBack0
[RTE]
```



## 十八、配置 BGP 汇总子实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 IBGP 与 EBGP 之间会话的配置，令 2 台客户端能够正常通讯，之后在 RTD 上配置汇总子，将其网络 192.168.1.0/24 汇总为 192.168.0.0/16 通告给 RTE，并在 RTE 上查看网络 192.168.0.0/16 的明细信息

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

```

interface G0/0/1    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0    #进入相应接口
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
bgp 65001    #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID，以及
#远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
#EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
#与对等体之间用哪个接口来承载更新
network 192.168.1.0    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总
ip route-static 2.2.2.2 255.255.255.255 10.1.1.2    #配置静
#态路由（对等体路由器 ID+对等体路由器 ID 的子网掩码+下一
#跳接口地址）

```

RTB:

```

system-view
sysname RTB
interface G0/0/0

```

```
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface LoopBack0
ip address 2.2.2.2 32
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 24
network 20.1.1.0 24
network 30.1.1.0 24
peer 3.3.3.3 next-hop-local
peer 4.4.4.4 next-hop-local
rip 1
version 2
network 2.0.0.0
```



```
network 20.0.0.0  
undo summary  
ip route-static 1.1.1.1 255.255.255.255 10.1.1.1
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
interface LoopBack0  
ip address 3.3.3.3 32  
bgp 1  
router-id 3.3.3.3  
peer 2.2.2.2 as-number 1  
peer 2.2.2.2 connect-interface LoopBack0  
peer 4.4.4.4 as-number 1  
peer 4.4.4.4 connect-interface LoopBack0  
network 20.1.1.0 24  
network 30.1.1.0 24  
rip 1
```

```
version 2
network 20.0.0.0
network 30.0.0.0
network 3.0.0.0
undo summary
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
bgp 1
router-id 4.4.4.4
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 5.5.5.5 as-number 7
```

```
peer 5.5.5.5 ebgp-max-hop 2
peer 5.5.5.5 connect-interface LoopBack0
network 20.1.1.0 24
network 30.1.1.0 24
network 40.1.1.0 24
aggregate 192.168.0.0 16 detail-suppressed as-set #
在原子汇总的基础上配置汇总子
peer 2.2.2.2 next-hop-local
peer 3.3.3.3 next-hop-local
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
undo summary
ip route-static 5.5.5.5 255.255.255.255 40.1.1.2

RTE:
system-view
sysname RTE
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
```

```

ip address 40.1.1.2 24
interface LoopBack0
ip address 5.5.5.5 32
bgp 7
router-id 5.5.5.5
peer 4.4.4.4 as-number 1
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 172.16.1.0 24
ip route-static 4.4.4.4 255.255.255.255 40.1.1.1
    
```

测试:

在 RTD 上仅配置了原子汇总, 而没有配置汇总子时, 查看 RTE 的 BGP 表:

```

[RTE]dis bgp routing-table

BGP Local router ID is 5.5.5.5
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6
   Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
*> 10.1.1.0/24      4.4.4.4          0             0               0       li
*> 20.1.1.0/24      4.4.4.4          1             0               0       li
*> 30.1.1.0/24      4.4.4.4          0             0               0       li
*> 40.1.1.0/24      4.4.4.4          0             0               0       li
*> 172.16.1.0/24    0.0.0.0          0             0               0       i
*> 192.168.0.0/16  4.4.4.4          0             0               0       li
[RTE]
    
```

在 RTE 的 BGP 表中具体查看网络 192.168.0.0 的明细内容:

```
[RTE]display bgp routing-table 192.168.0.0

BGP local router ID : 5.5.5.5
Local AS number : 7
Paths: 1 available, 1 best, 1 select
BGP routing table entry information of 192.168.0.0/16:
From: 4.4.4.4 (4.4.4.4)
Route Duration: 00h03m29s
Relay IP Nexthop: 40.1.1.1
Relay IP Out-Interface: GigabitEthernet0/0/1
Original nexthop: 4.4.4.4
Qos information : 0x0
AS-path 1, origin igp, pref-val 0, valid, external, best, select, active, pre 2
55
Aggregator: AS 1, Aggregator ID 4.4.4.4, Atomic-aggregate
Not advertised to any peer yet

[RTE]
```

在 RTD 上配置完原子汇总, 再配置上汇总子后, 查看 RTE 的 BGP 表:

```
[RTE]dis bgp routing-table

BGP Local router ID is 5.5.5.5
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6
  Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
* > 10.1.1.0/24    4.4.4.4          0             0               0       1i
* > 20.1.1.0/24    4.4.4.4          1             0               0       1i
* > 30.1.1.0/24    4.4.4.4          0             0               0       1i
* > 40.1.1.0/24    4.4.4.4          0             0               0       1i
* > 172.16.1.0/24  0.0.0.0          0             0               0       i
* > 192.168.0.0/16 4.4.4.4          0             0               0       1 65001i
[RTE]
```



在 RTE 的 BGP 表中具体查看网络 192.168.0.0 的明细内容：

```
[RTE]display bgp routing-table 192.168.0.0

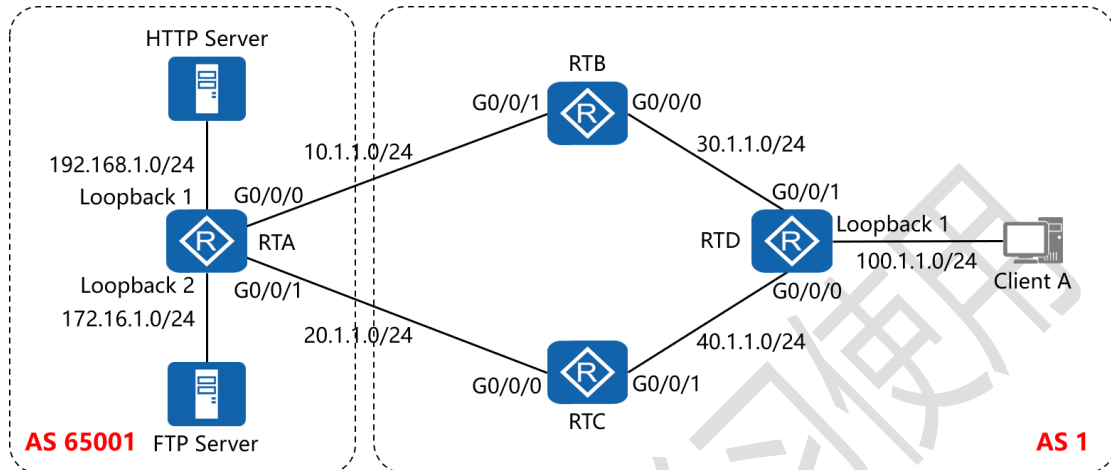
BGP local router ID : 5.5.5.5
Local AS number : 7
Paths: 1 available, 1 best, 1 select
BGP routing table entry information of 192.168.0.0/16:
From: 4.4.4.4 (4.4.4.4)
Route Duration: 00h00m08s
Relay IP Nexthop: 40.1.1.1
Relay IP Out-Interface: GigabitEthernet0/0/1
Original nexthop: 4.4.4.4
Qos information : 0x0
AS-path 1 65001, origin igp, pref-val 0, valid, external, best, select, active,
pre 255
Aggregator: AS 1, Aggregator ID 4.4.4.4, Atomic-aggregate
Not advertised to any peer yet

[RTE]
```

仅供瑞通学员学习使用

## 十九、配置 BGP 本地优先级实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 BGP 本地优先级的配置，令 Client A 访问 HTTP Server 经过 RTB，Client A 访问 FTP Server 经过 RTC

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0  #进入相应接口
    
```

```

ip address 1.1.1.1 32      #配置 IP 地址及子网掩码
interface LoopBack1      #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
interface LoopBack2      #进入相应接口
ip address 172.16.1.1 24  #配置 IP 地址及子网掩码
bgp 65001                 #开启 BGP 路由功能, 并配置其 AS 号
router-id 1.1.1.1         #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1  #指定对等体的路由器 ID, 以及
                           远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2 #指定自身与对等体为
                           EBGP 关系, 并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0 #指定自身
                           与对等体之间用哪个接口来承载更新
peer 3.3.3.3 as-number 1  #指定对等体的路由器 ID, 以及
                           远程自治系统号码
peer 3.3.3.3 ebgp-max-hop 2 #指定自身与对等体为
                           EBGP 关系, 并指出到对等体所跨越的跳数
peer 3.3.3.3 connect-interface LoopBack0 #指定自身
                           与对等体之间用哪个接口来承载更新
network 192.168.1.0 24    #通告自己的网段及子网掩码
network 172.16.1.0 24    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总

```



ip route-static 2.2.2.2 32 10.1.1.2 #配置静态路由 (对等  
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

ip route-static 3.3.3.3 32 20.1.1.2 #配置静态路由 (对等  
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 30.1.1.1 24

interface G0/0/1

ip address 10.1.1.2 24

interface LoopBack0

ip address 2.2.2.2 32

acl number 2001 #创建基本 ACL 2001

rule 5 permit source 192.168.1.0 0.0.0.255 #匹配源网  
段, 并定义为允许转发

acl number 2002 #创建基本 ACL 2002

rule 5 permit source 172.16.1.0 0.0.0.255 #匹配源网段,  
并定义为允许转发

route-policy atnet permit node 10 #创建路由策略, 并定  
义为允许策略, 序列号为 10

```

if-match acl 2001 #匹配 ACL 2001
apply local-preference 200 #若能成功匹配, 则配置其本地优先级为 200
route-policy atnet permit node 20 #创建路由策略, 并定义为允许策略, 序列号为 20
if-match acl 2002 #匹配 ACL 2002
apply local-preference 100 #若能成功匹配, 则配置其本地优先级为 100
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 255.255.255.0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
    
```

```
peer 3.3.3.3 next-hop-local  
peer 4.4.4.4 next-hop-local  
peer 4.4.4.4 route-policy atnet export # 在指向对等体  
4.4.4.4 的外出方向上，调用名为 atnet 的路由策略
```

```
rip 1  
version 2  
network 2.0.0.0  
network 30.0.0.0  
undo summary  
ip route-static 1.1.1.1 32 10.1.1.1
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 20.1.1.2 24  
interface G0/0/1  
ip address 40.1.1.1 24  
interface LoopBack0  
ip address 3.3.3.3 32  
acl number 2001  
rule 5 permit source 192.168.1.0 0.0.0.255
```

```
acl number 2002
rule 5 permit source 172.16.1.0 0.0.0.255
route-policy atnet permit node 10
if-match acl 2001
apply local-preference 100
route-policy atnet permit node 20
if-match acl 2002
apply local-preference 200
bgp 1
router-id 3.3.3.3
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
```

```
peer 2.2.2.2 next-hop-local
peer 4.4.4.4 next-hop-local
peer 4.4.4.4 route-policy atnet export
rip 1
version 2
network 3.0.0.0
network 40.0.0.0
undo summary
ip route-static 1.1.1.1 32 20.1.1.1
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.2 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
interface LoopBack1
ip address 100.1.1.1 24
bgp 1
```

```
router-id 4.4.4.4
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
network 40.0.0.0
undo summary
```

测试:

在 RTD 上查看其 BGP 表:

```
[RTD]dis bgp routing-table

BGP Local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
  Network          NextHop          MED          LocPrf        PrefVal Path/Ogn
*> 30.1.1.0/24      0.0.0.0          0             0             0       i
*> 40.1.1.0/24      0.0.0.0          0             0             0       i
*> 100.1.1.0/24     0.0.0.0          0             0             0       i
*>i 172.16.1.0/24   3.3.3.3          0             200           0       65001i
* i                2.2.2.2          0             100           0       65001i
*>i 192.168.1.0    2.2.2.2          0             200           0       65001i
* i                3.3.3.3          0             100           0       65001i
[RTD]
```

在 RTD 上从 100.1.1.1 去 ping 192.168.1.1, 观察其转发路径:

```
[RTD]tracert -a 100.1.1.1 192.168.1.1

traceroute to 192.168.1.1(192.168.1.1),
max hops: 30 ,packet length: 40,press CTRL_C to break

 1 30.1.1.1 50 ms 50 ms 40 ms

 2 10.1.1.1 70 ms 60 ms 80 ms
[RTD]
```

在 RTD 上从 100.1.1.1 去 ping 172.16.1.1, 观察其转发路径:

```
[RTD]tracert -a 100.1.1.1 172.16.1.1

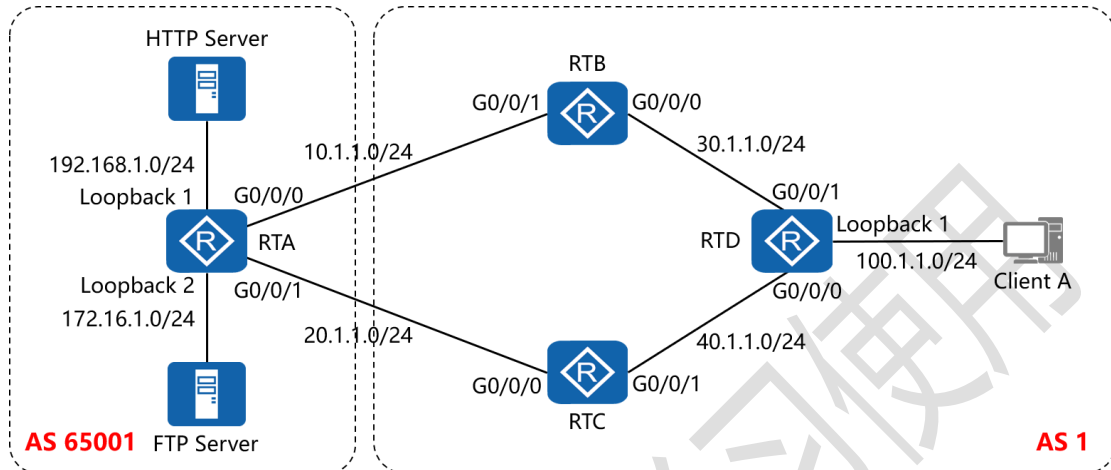
traceroute to 172.16.1.1(172.16.1.1), max hops: 30 ,packet length: 40,press CT
RL_C to break

 1 40.1.1.1 80 ms 50 ms 40 ms

 2 20.1.1.1 70 ms 60 ms 40 ms
[RTD]
```

## 二十、配置 BGP 多出口鉴别实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 BGP 多出口鉴别的配置，令 Client A 访问 HTTP Server 经过 RTB，Client A 访问 FTP Server 经过 RTC

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0  #进入相应接口
    
```



```

ip address 1.1.1.1 32      #配置 IP 地址及子网掩码
interface LoopBack1      #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
interface LoopBack2      #进入相应接口
ip address 172.16.1.1 24  #配置 IP 地址及子网掩码
acl number 2001          #创建基本 ACL 2001
rule 5 permit source 192.168.1.0 0.0.0.255  #匹配源网
段，并定义为允许转发
acl number 2002          #创建基本 ACL 2002
rule 5 permit source 172.16.1.0 0.0.0.255  #匹配源网段，
并定义为允许转发
route-policy atnet permit node 10          #创建路由策略，并定
义为允许策略，序列号为 10
if-match acl 2001          #匹配 ACL 2001
apply cost 200            #若能成功匹配，则配置其 MED 值为 200
route-policy atnet permit node 20          #创建路由策略，并定
义为允许策略，序列号为 20
if-match acl 2002          #匹配 ACL 2002
apply cost 100           #若能成功匹配，则配置其 MED 值为 100
route-policy huawei permit node 10          #创建路由策略，
并定义为允许策略，序列号为 10
if-match acl 2001          #匹配 ACL 2001

```

```

apply cost 100    #若能成功匹配, 则配置其 MED 值为 100
route-policy huawei permit node 20    #创建路由策略,
并定义为允许策略, 序列号为 20
if-match acl 2002    #匹配 ACL 2002
apply cost 200    #若能成功匹配, 则配置其 MED 值为 200
bgp 65001    #开启 BGP 路由功能, 并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID, 以及
远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
EBGP 关系, 并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
与对等体之间用哪个接口来承载更新
peer 2.2.2.2 route-policy huawei export    #在指向对等体
2.2.2.2 的外出方向上, 调用名为 huawei 的路由策略
peer 3.3.3.3 as-number 1    #指定对等体的路由器 ID, 以及
远程自治系统号码
peer 3.3.3.3 ebgp-max-hop 2    #指定自身与对等体为
EBGP 关系, 并指出到对等体所跨越的跳数
peer 3.3.3.3 connect-interface LoopBack0    #指定自身
与对等体之间用哪个接口来承载更新
peer 3.3.3.3 route-policy atnet export    #在指向对等体

```

### 3.3.3.3 的外出方向上，调用名为 atnet 的路由策略

```
network 192.168.1.0 24    #通告自己的网段及子网掩码
network 172.16.1.0 24    #通告自己的网段及子网掩码
undo summary automatic   #关闭自动汇总
ip route-static 2.2.2.2 32 10.1.1.2    #配置静态路由 (对等
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)
ip route-static 3.3.3.3 32 20.1.1.2    #配置静态路由 (对等
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)
```

RTB:

```
system-view
sysname RTB
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface LoopBack0
ip address 2.2.2.2 32
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
```

```
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 10.1.1.0 255.255.255.0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
peer 3.3.3.3 next-hop-local
peer 4.4.4.4 next-hop-local
rip 1
version 2
network 2.0.0.0
network 30.0.0.0
undo summary
ip route-static 1.1.1.1 32 10.1.1.1
```

RTC:

system-view

sysname RTC

```
interface G0/0/0
ip address 20.1.1.2 24
interface G0/0/1
ip address 40.1.1.1 24
interface LoopBack0
ip address 3.3.3.3 32
bgp 1
router-id 3.3.3.3
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 4.4.4.4 as-number 1
peer 4.4.4.4 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
peer 2.2.2.2 next-hop-local
peer 4.4.4.4 next-hop-local
```

```
rip 1
version 2
network 3.0.0.0
network 40.0.0.0
undo summary
ip route-static 1.1.1.1 32 20.1.1.1
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.2 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
interface LoopBack1
ip address 100.1.1.1 24
bgp 1
router-id 4.4.4.4
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
```

```
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
network 30.1.1.0 255.255.255.0
network 40.1.1.0 255.255.255.0
network 100.1.1.0 255.255.255.0
undo summary automatic
rip 1
version 2
network 4.0.0.0
network 30.0.0.0
network 40.0.0.0
undo summary
```

测试:

在 RTD 上查看其 BGP 表:

```
[RTD]dis bgp routing-table

BGP Local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
  Network                NextHop          MED           LocPrf        PrefVal Path/Ogn
*> 30.1.1.0/24           0.0.0.0          0              0             0       i
*> 40.1.1.0/24           0.0.0.0          0              0             0       i
*> 100.1.1.0/24          0.0.0.0          0              0             0       i
*>i 172.16.1.0/24        3.3.3.3          0              200           0       65001i
* i 2.2.2.2              2.2.2.2          0              100           0       65001i
*>i 192.168.1.0          2.2.2.2          0              200           0       65001i
* i 3.3.3.3              3.3.3.3          0              100           0       65001i
[RTD]
```

在 RTD 上从 100.1.1.1 去 ping 192.168.1.1, 观察其转发路径:

```
[RTD]tracert -a 100.1.1.1 192.168.1.1

traceroute to 192.168.1.1(192.168.1.1),
max hops: 30 ,packet length: 40,press CTRL_C to break

 1 30.1.1.1 50 ms 50 ms 40 ms

 2 10.1.1.1 70 ms 60 ms 80 ms
[RTD]
```

在 RTD 上从 100.1.1.1 去 ping 172.16.1.1, 观察其转发路径:

```
[RTD]tracert -a 100.1.1.1 172.16.1.1

traceroute to 172.16.1.1(172.16.1.1), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 40.1.1.1 80 ms 50 ms 40 ms

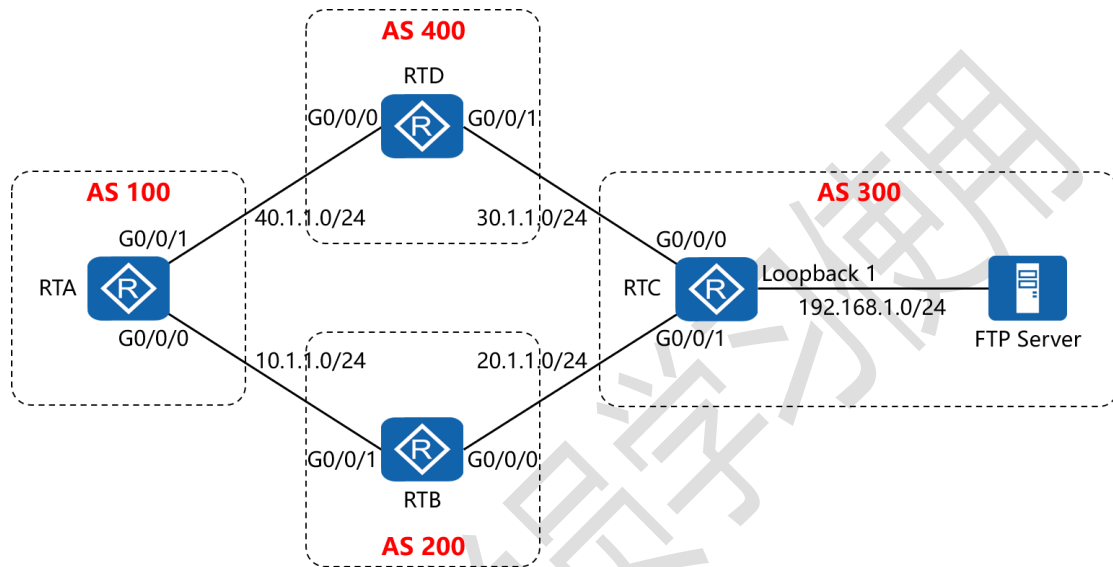
 2 20.1.1.1 70 ms 60 ms 40 ms
[RTD]
```



## 二十一、配置 BGP 优先级值实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

通过 BGP 优先级值的配置，令 RTA 访问 FTP Server 经过 RTD 到达，其余路径根据协议自主选择

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```

ip address 40.1.1.2 24      #配置 IP 地址及子网掩码
interface LoopBack0      #进入相应接口
ip address 1.1.1.1 32     #配置 IP 地址及子网掩码
acl number 2001          #创建基本 ACL 2001
rule 5 permit source 192.168.1.0 0.0.0.255      #匹配源网
段，并定义为允许转发
route-policy atnet permit node 10      #创建路由策略，并定
义为允许策略，序列号为 10
if-match acl 2001        #匹配 ACL 2001
apply preferred-value 100      #若能成功匹配，则配置其优先
级值为 100
route-policy atnet permit node 20      #创建路由策略，并定
义为允许策略，序列号为 20
bgp 100      #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1      #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 200      #指定对等体的路由器 ID，
以及远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2      #指定自身与对等体为
EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0      #指定自身
与对等体之间用哪个接口来承载更新
peer 4.4.4.4 as-number 400      #指定对等体的路由器 ID，

```

以及远程自治系统号码

peer 4.4.4.4 ebgp-max-hop 2 # 指定自身与对等体为  
EBGP 关系，并指出到对等体所跨越的跳数

peer 4.4.4.4 connect-interface LoopBack0 # 指定自身  
与对等体之间用哪个接口来承载更新

peer 4.4.4.4 route-policy atnet import # 在指向对等体  
4.4.4.4 的进入方向上，调用名为 atnet 的路由策略

network 10.1.1.0 24 #通告自己的网段及子网掩码

undo summary automatic #关闭自动汇总

ip route-static 2.2.2.2 32 10.1.1.2 #配置静态路由 (对等  
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

ip route-static 4.4.4.4 32 40.1.1.1 #配置静态路由 (对等  
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 20.1.1.1 24

interface G0/0/1

ip address 10.1.1.2 24

interface LoopBack0

```
ip address 2.2.2.2 32
bgp 200
router-id 2.2.2.2
peer 1.1.1.1 as-number 100
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 3.3.3.3 as-number 300
peer 3.3.3.3 ebgp-max-hop 2
peer 3.3.3.3 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
undo summary automatic
ip route-static 1.1.1.1 32 10.1.1.1
ip route-static 3.3.3.3 32 20.1.1.2
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface LoopBack0
```

```
ip address 3.3.3.3 32
interface LoopBack1
ip address 192.168.1.1 24
bgp 300
router-id 3.3.3.3
peer 2.2.2.2 as-number 200
peer 2.2.2.2 ebgp-max-hop 2
peer 2.2.2.2 connect-interface LoopBack0
peer 4.4.4.4 as-number 400
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 30.1.1.0 255.255.255.0
network 192.168.1.0 255.255.255.0
undo summary automatic
ip route-static 2.2.2.2 32 20.1.1.1
ip route-static 4.4.4.4 32 30.1.1.2
```

RTD:

```
system-view
sysname RTD
interface G0/0/0
ip address 40.1.1.1 24
```

```
interface G0/0/1
ip address 30.1.1.2 24

interface LoopBack0
ip address 4.4.4.4 32

bgp 400
router-id 4.4.4.4
peer 3.3.3.3 as-number 300
peer 3.3.3.3 ebgp-max-hop 2
peer 3.3.3.3 connect-interface LoopBack0
peer 1.1.1.1 as-number 100
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
network 40.1.1.0 255.255.255.0
undo summary automatic
ip route-static 3.3.3.3 32 30.1.1.1
ip route-static 1.1.1.1 32 40.1.1.2
```

测试：

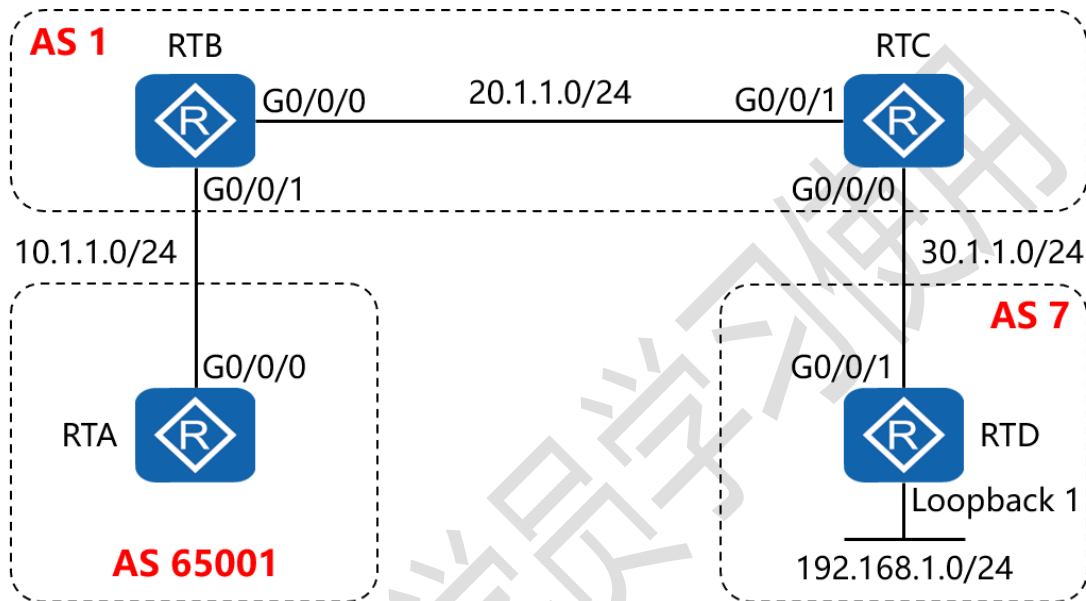
在 RTA 上查看 BGP 表项，确定其访问网络 192.168.1.0 的下一跳为 4.4.4.4，且经过 4.4.4.4 的优先级值为 100

```
[RTA]dis bgp routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
  Network          NextHop         MED         LocPrf     PrefVal Path/Ogn
*> 10.1.1.0/24     0.0.0.0         0           0          0       i
*> 20.1.1.0/24     2.2.2.2         0           0          0       200i
*> 30.1.1.0/24     2.2.2.2         0           0          0       200 300i
*                  4.4.4.4         0           0          0       400 300i
*> 40.1.1.0/24     4.4.4.4         0           0          0       400i
*> 192.168.1.0    4.4.4.4         0           100        0       400 300i
*                  2.2.2.2         0           0          0       200 300i
[RTA]
```

## 二十二、配置 BGP filter-policy 实验 组网

### 一、实验拓扑：



### 二、实验目的：

4 台路由器按图中所示配置 BGP 协议，令其可以彼此通讯，之后在 RTB 上配置 filter-policy，防止 RTB 将网络 192.168.1.0/24 通告至 RTA

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口



```

ip address 10.1.1.1 24      #配置 IP 地址及子网掩码
interface LoopBack0      #进入相应接口
ip address 1.1.1.1 32     #配置 IP 地址及子网掩码
bgp 65001                #开启 BGP 路由功能，并配置其 AS 号
router-id 1.1.1.1        #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1  #指定对等体的路由器 ID，以及
                           远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2 #指定自身与对等体为
                           EBGP 关系，并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0 #指定自身
                           与对等体之间用哪个接口来承载更新
undo summary automatic   #关闭自动汇总
ip route-static 2.2.2.2 32 10.1.1.2 #配置静态路由（对等
                           体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址）

```

RTB:

```

system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24

```

```

interface LoopBack0
ip address 2.2.2.2 32
acl number 2001 #创建基本 ACL 2001
rule 5 deny source 192.168.1.0 0.0.0.255 #匹配源网段,
并定义为拒绝转发
rule 10 permit source 0.0.0.0 255.255.255.255 #匹配源
网段, 并定义为允许所有
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 1.1.1.1 filter-policy 2001 export #在指向 1.1.1.1 的
对等体关系上配置过滤策略, 调用 ACL 2001, 并指定为外出方
向
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
network 10.1.1.0 255.255.255.0
network 20.1.1.0 255.255.255.0
undo summary automatic
ip route-static 1.1.1.1 32 10.1.1.1
rip 1

```

```
version 2
network 20.0.0.0
network 2.0.0.0
undo summary
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface LoopBack0
ip address 3.3.3.3 32
bgp 1
router-id 3.3.3.3
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
peer 4.4.4.4 as-number 7
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
```

```
network 30.1.1.0 255.255.255.0
undo summary automatic
ip route-static 4.4.4.4 32 30.1.1.2
rip 1
version 2
network 20.0.0.0
network 3.0.0.0
undo summary
```

RTD:

```
system-view
sysname RTD
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
interface LoopBack1
ip address 192.168.1.1 24
bgp 7
router-id 4.4.4.4
peer 3.3.3.3 as-number 1
peer 3.3.3.3 ebgp-max-hop 2
```

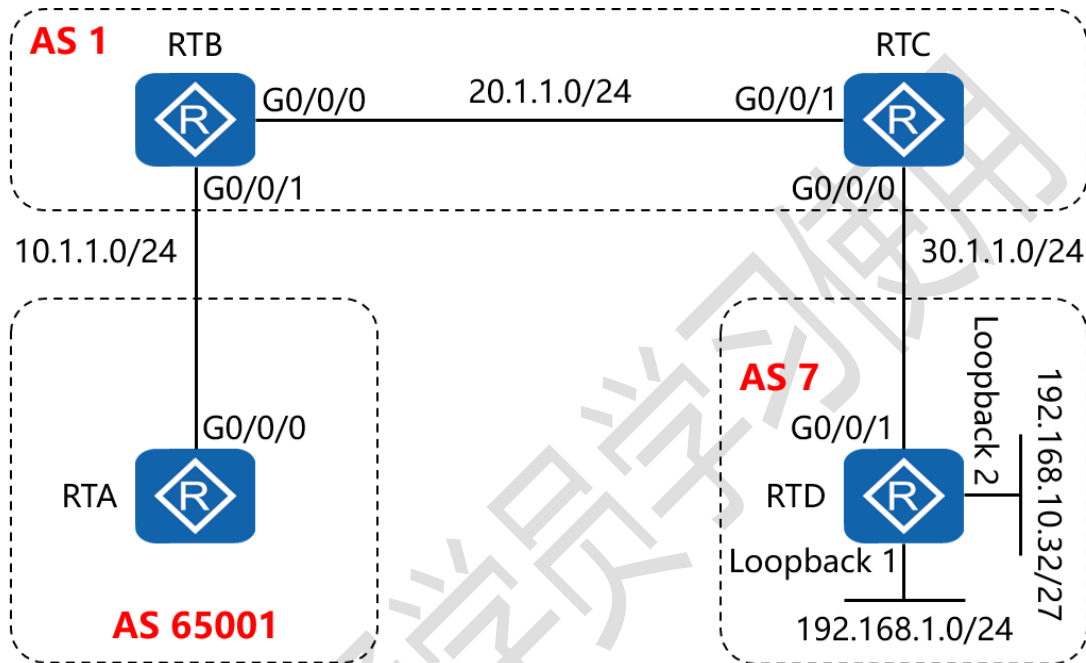
```
peer 3.3.3.3 connect-interface LoopBack0  
network 192.168.1.0 255.255.255.0  
undo summary automatic  
ip route-static 3.3.3.3 32 30.1.1.1
```

仅供瑞通学员学习使用

## 二十三、配置 BGP ip ip-prefix 实验

### 组网

#### 一、实验拓扑：



#### 二、实验目的：

4 台路由器按图中所示配置 BGP 协议，令其可以彼此通讯，之后在 RTB 上配置 ip ip-prefix，防止 RTB 将网络 192.168.1.0/24 通告至 RTA，但允许 RTA 学习网络 192.168.10.32/27 的路由条目

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

```

interface G0/0/0    #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface LoopBack0    #进入相应接口
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
bgp 65001    #开启 BGP 路由功能, 并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 2.2.2.2 as-number 1    #指定对等体的路由器 ID, 以及
#远程自治系统号码
peer 2.2.2.2 ebgp-max-hop 2    #指定自身与对等体为
#EBGP 关系, 并指出到对等体所跨越的跳数
peer 2.2.2.2 connect-interface LoopBack0    #指定自身
#与对等体之间用哪个接口来承载更新
undo summary automatic    #关闭自动汇总
ip route-static 2.2.2.2 32 10.1.1.2    #配置静态路由 (对等
#体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

```

RTB:

```

system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1

```

```

ip address 10.1.1.2 24
interface LoopBack0
ip address 2.2.2.2 32
ip ip-prefix 1 deny 192.0.0.0 8 less-equal 24    #定义前缀列表, 拒绝以 192 开头, 且掩码长度在 8 位至 24 位的网络
ip ip-prefix 1 permit 192.0.0.0 8 greater-equal 25    # 定义前缀列表, 允许以 192 开头, 且掩码长度在 25 位及以上的网络
ip ip-prefix 1 permit 20.0.0.0 8 le 24    #定义前缀列表, 允许以 20 开头, 且掩码长度在 8 位至 24 位的网络
ip ip-prefix 1 permit 30.0.0.0 8 le 24    #定义前缀列表, 允许以 30 开头, 且掩码长度在 8 位至 24 位的网络
bgp 1
router-id 2.2.2.2
peer 1.1.1.1 as-number 65001
peer 1.1.1.1 ebgp-max-hop 2
peer 1.1.1.1 connect-interface LoopBack0
peer 1.1.1.1 ip-prefix 1 export    #在指向 1.1.1.1 的对等体关系上配置前缀列表 1, 并指定为外出方向
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0
network 10.1.1.0 255.255.255.0

```



```
network 20.1.1.0 255.255.255.0
undo summary automatic
ip route-static 1.1.1.1 32 10.1.1.1
rip 1
version 2
network 20.0.0.0
network 2.0.0.0
undo summary
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface LoopBack0
ip address 3.3.3.3 32
bgp 1
router-id 3.3.3.3
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
```

```
peer 4.4.4.4 as-number 7
peer 4.4.4.4 ebgp-max-hop 2
peer 4.4.4.4 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
network 30.1.1.0 255.255.255.0
undo summary automatic
ip route-static 4.4.4.4 32 30.1.1.2
rip 1
version 2
network 20.0.0.0
network 3.0.0.0
undo summary
```

RTD:

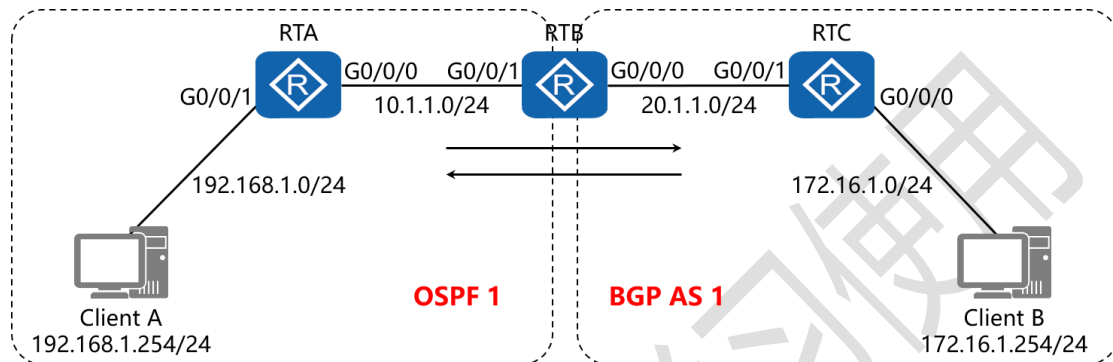
```
system-view
sysname RTD
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 4.4.4.4 32
interface LoopBack1
ip address 192.168.1.1 24
```

```
interface LoopBack2
ip address 192.168.10.33 27
bgp 7
router-id 4.4.4.4
peer 3.3.3.3 as-number 1
peer 3.3.3.3 ebgp-max-hop 2
peer 3.3.3.3 connect-interface LoopBack0
network 192.168.1.0 255.255.255.0
network 192.168.10.32 255.255.255.224
undo summary automatic
ip route-static 3.3.3.3 32 30.1.1.1
```

## 二十四、配置 BGP 双向重发布实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

RTA 与 RTB 运行 OSPF 路由选择协议，RTB 与 RTC 运行 BGP 路由选择协议，在 RTB 上配置双向重发布，最终令 Client A 与 Client B 能够正常通讯

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

```
interface Loopback0    #创建环回接口 0
ip address 1.1.1.1 32   #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
#由器 ID
area 0                #创建 OSPF 区域 0
network 10.1.1.0 0.0.0.255    #通告其直连网段
network 192.168.1.0 0.0.0.255    #通告其直连网段
```

RTB:

```
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.1 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
import-route direct cost 1    #以 COST 值 1 的形式将直连
#路由注入进 OSPF 路由协议
import-route bgp permit-ibgp cost 1    #以 COST 值 1 的
#形式将 BGP 路由注入进 OSPF 路由协议, 同时允许将 IBGP 路
```

由也注入进 OSPF 路由协议中

area 0

network 10.1.1.0 0.0.0.255

bgp 1 #开启 BGP 路由功能，并配置其 AS 号

router-id 2.2.2.2 #配置设备的 BGP 路由器 ID

peer 3.3.3.3 as-number 1 #指定对等体的路由器 ID，以及  
远程自治系统号码

peer 3.3.3.3 connect-interface LoopBack0 #指定自身  
与对等体之间用哪个接口来承载更新

network 20.1.1.0 24 #通告其直连的网段

undo summary automatic #关闭自动汇总

import-route ospf 1 med 1 #将 OSPF 1 的路由条目以  
MED 值 1 的方式注入进 BGP 路由协议

ip route-static 3.3.3.3 32 20.1.1.2 #配置静态路由 (对等  
体路由器 ID+对等体路由器 ID 的子网掩码+下一跳接口地址)

RTC:

system-view

sysname RTC

interface G0/0/0

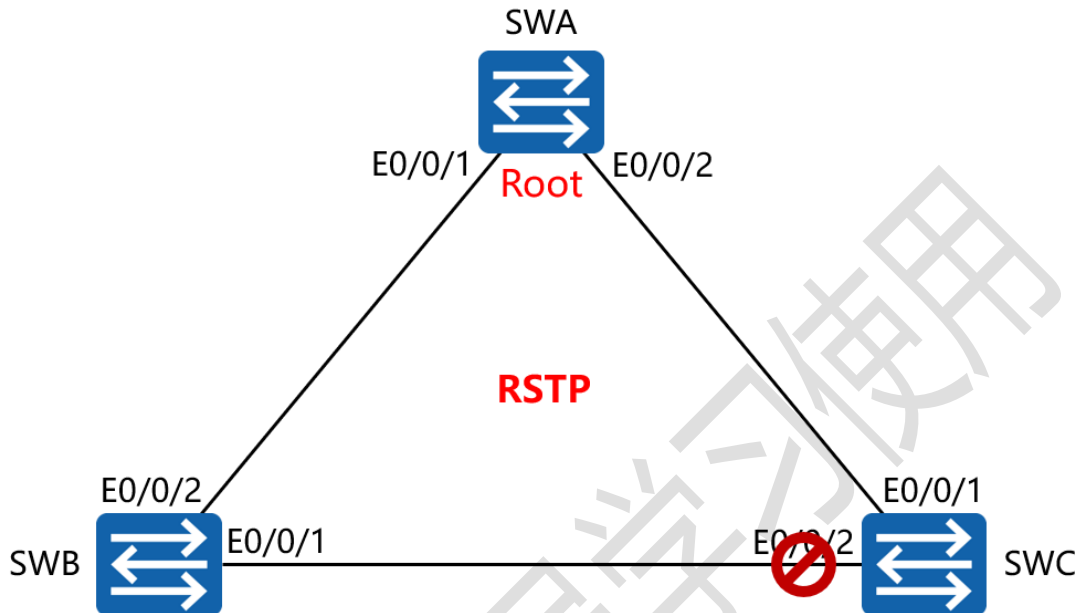
ip address 172.16.1.1 24

interface G0/0/1

```
ip address 20.1.1.2 24
interface LoopBack0
ip address 3.3.3.3 32
bgp 1
router-id 3.3.3.3
peer 2.2.2.2 as-number 1
peer 2.2.2.2 connect-interface LoopBack0
network 20.1.1.0 255.255.255.0
network 172.16.1.0 255.255.255.0
undo summary automatic
ip route-static 2.2.2.2 32 20.1.1.1
```

## 二十五、配置 RSTP 实验组网

### 一、实验拓扑：



### 二、实验目的：

将 3 台交换机的生成树模式配置为 RSTP，同时将 SWA 配置成为根网桥；通过生成树的选举，令 SWC 的 E0/0/2 端口被阻塞掉；在其它主链路失效时，通过 RSTP 的帮助，令 SWC 的 E0/0/2 端口能够尽快恢复

### 三、实验步骤：

SWA:

```

system-view      #进入系统视图模式
sysname SWA     #给设备命名
stp mode rstp   #将 STP 的工作模式配置为 RSTP
stp priority 8192 #将 SWA 的 STP 优先级配置为 8192
    
```



```
interface E0/0/1    #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
```

VLAN 的信息

```
interface E0/0/2    #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
```

VLAN 的信息

SWB:

```
system-view
sysname SWB
stp mode rstp
stp priority 24576
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
```

SWC:

system-view

sysname SWC

stp mode rstp

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type trunk

port trunk allow-pass vlan all

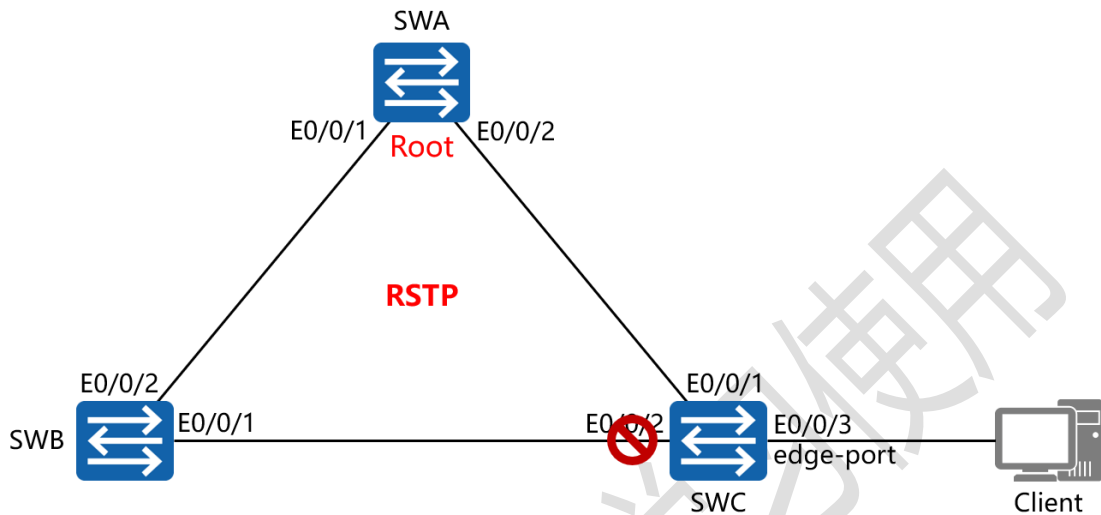
测试:

在 SWC 上查看生成树的端口角色与状态

```
[SWC]display stp brief
MSTID  Port                Role  STP State  Protection
0      Ethernet0/0/1         ROOT  FORWARDING NONE
0      Ethernet0/0/2         ALTE  DISCARDING NONE
[SWC]
```

## 二十六、配置 STP 边缘端口实验组网

### 一、实验拓扑：



### 二、实验目的：

将 SWA 配置为根网桥，将 SWC 的端口 E0/0/3 配置为边缘端口，令该端口在与终端主机相连时，立即进入转发状态

### 三、实验步骤：

SWA:

```

system-view          #进入系统视图模式
sysname SWA         #给设备命名
stp mode rstp       #将 STP 的工作模式配置为 RSTP
stp priority 8192   #将 SWA 的 STP 优先级配置为 8192
interface E0/0/1    #进入相应的端口
port link-type trunk #将端口配置为中继模式
port trunk allow-pass vlan all #允许该中继端口传递所有
    
```

## VLAN 的信息

```
interface E0/0/2    #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
```

## VLAN 的信息

SWB:

```
system-view
sysname SWB
stp mode rstp
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
```

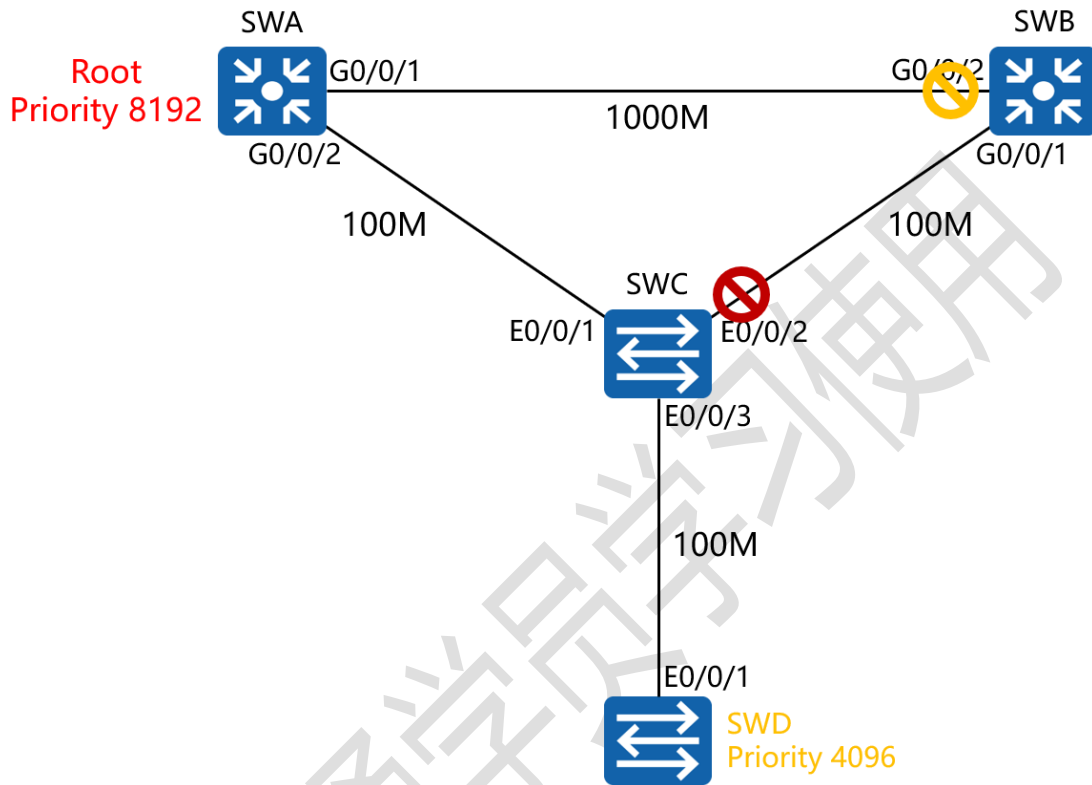
SWC:

```
system-view
sysname SWC
stp mode rstp
interface E0/0/1
```

```
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/3
stp edged-port enable    #在端口下开启边缘端口功能
```

## 二十七、配置 STP 根保护实验组网

### 一、实验拓扑：



### 二、实验目的：

将 SWA 配置为根网桥，SWD 通过端口 E0/0/1 与 SWC 的 E0/0/3 相连，由于 SWD 的网桥优先级相较于 SWA 更低(4096)，因此 SWD 会抢占 SWA 的根网桥状态；为防止上述事件发生，需要在 SWC 上开启根防护，以阻止 SWD 成为新的根网桥

### 三、实验步骤：

SWA:

system-view **#进入系统视图模式**

```

sysname SWA      #给设备命名
stp mode rstp    #将 STP 的工作模式配置为 RSTP
interface G0/0/1  #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
VLAN 的信息
interface G0/0/2  #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
VLAN 的信息
stp priority 8192    #将 SWA 的 STP 优先级配置为 8192

```

SWB:

```

system-view
sysname SWB
stp mode rstp
interface G0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface G0/0/2
port link-type trunk
port trunk allow-pass vlan all

```

SWC:

system-view

sysname SWC

stp mode rstp

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/3

stp root-protection #在端口下开启根防护功能

SWD:

system-view

sysname SWD

stp mode rstp

stp priority 4096

interface E0/0/1

port link-type trunk

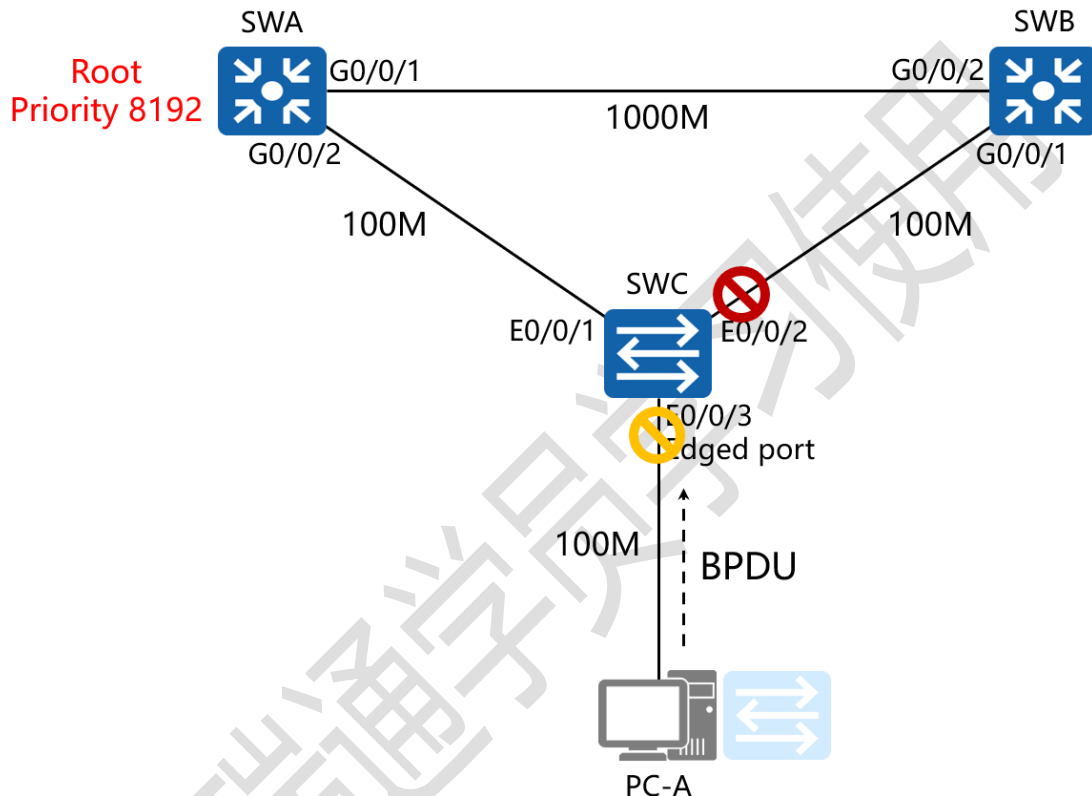
port trunk allow-pass vlan all



## 二十八、配置 STP BPDU 保护实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

将 SWA 配置为根网桥，SWC 的 E0/0/3 端口连接终端主机 PC-A，在 SWC 上配置 BPDU 保护，以防止该端口错误的连接其它网络设备（如：交换机等）后接收到 BPDU，导致其产生临时环路，从而增加整体网络的计算工作量，并可能引起网络震荡

#### 三、实验步骤：

SWA:

```

system-view      #进入系统视图模式
sysname SWA     #给设备命名
stp mode rstp   #将 STP 的工作模式配置为 RSTP
stp priority 4096  #将 SWA 的 STP 优先级配置为 4096
interface G0/0/1  #进入相应的端口
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all  #允许该中继端口传递所有
VLAN 的信息
interface G0/0/2  #进入相应的端口
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all  #允许该中继端口传递所有
VLAN 的信息

```

SWB:

```

system-view
sysname SWB
stp mode rstp
interface G0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface G0/0/2
port link-type trunk

```

---

```
port trunk allow-pass vlan all
```

```
SWC:
```

```
system-view
```

```
sysname SWC
```

```
stp mode rstp
```

```
stp bpdu-protection #开启 BPDU 保护机制
```

```
interface E0/0/1
```

```
port link-type trunk
```

```
port trunk allow-pass vlan all
```

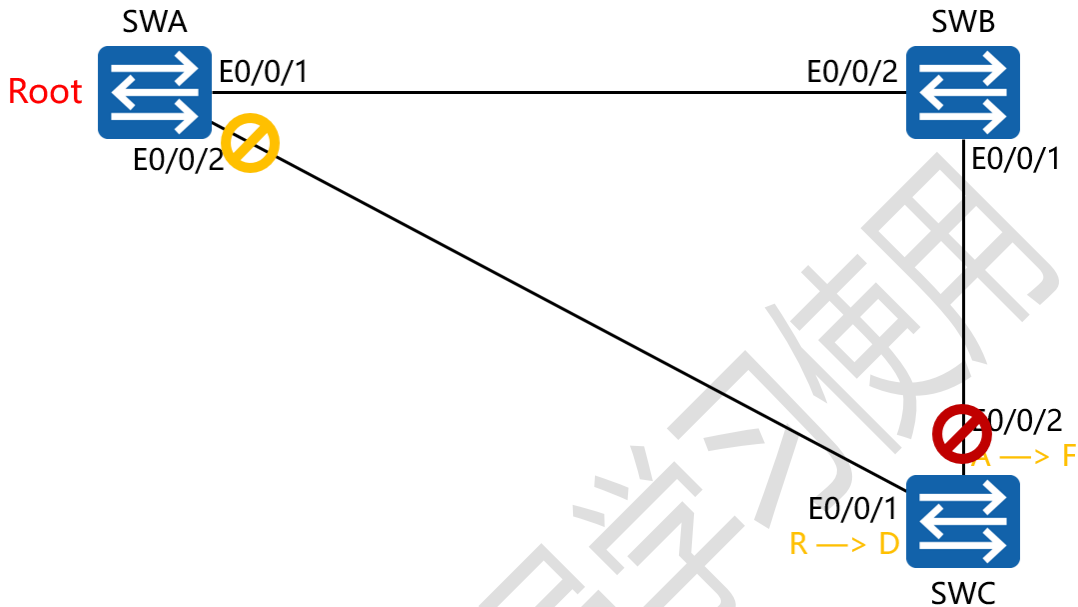
```
interface E0/0/2
```

```
port link-type trunk
```

```
port trunk allow-pass vlan all
```

## 二十九、配置 STP 环路保护实验组网

### 一、实验拓扑：



### 二、实验目的：

将 SWA 配置为根网桥，当 SWA 的端口 E0/0/2 由于链路拥塞或单向链路故障，导致 SWC 不能收到 SWA 发送的 BPDU 报文，因此 SWC 将重新选择根端口；最初的根端口将变更为指定端口，而阻塞端口则将进入转发状态，这将导致环路发生，因此需要在 SWC 的端口 E0/0/1 上开启环路保护机制，以防止上述事件发生

### 三、实验步骤：

SWA:

system-view #进入系统视图模式

```

sysname SWA      #给设备命名
stp mode rstp    #将 STP 的工作模式配置为 RSTP
stp priority 4096 #将 SWA 的 STP 优先级配置为 4096
interface E0/0/1 #进入相应的端口
port link-type trunk #将端口配置为中继模式
port trunk allow-pass vlan all #允许该中继端口传递所有
VLAN 的信息
interface E0/0/2 #进入相应的端口
port link-type trunk #将端口配置为中继模式
port trunk allow-pass vlan all #允许该中继端口传递所有
VLAN 的信息

```

SWB:

```

system-view
sysname SWB
stp mode rstp
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all

```

SWC:

```
system-view
```

```
sysname SWC
```

```
stp mode rstp
```

```
interface E0/0/1
```

```
port link-type trunk
```

```
port trunk allow-pass vlan all
```

```
stp loop-protection #在端口下开启环路保护机制
```

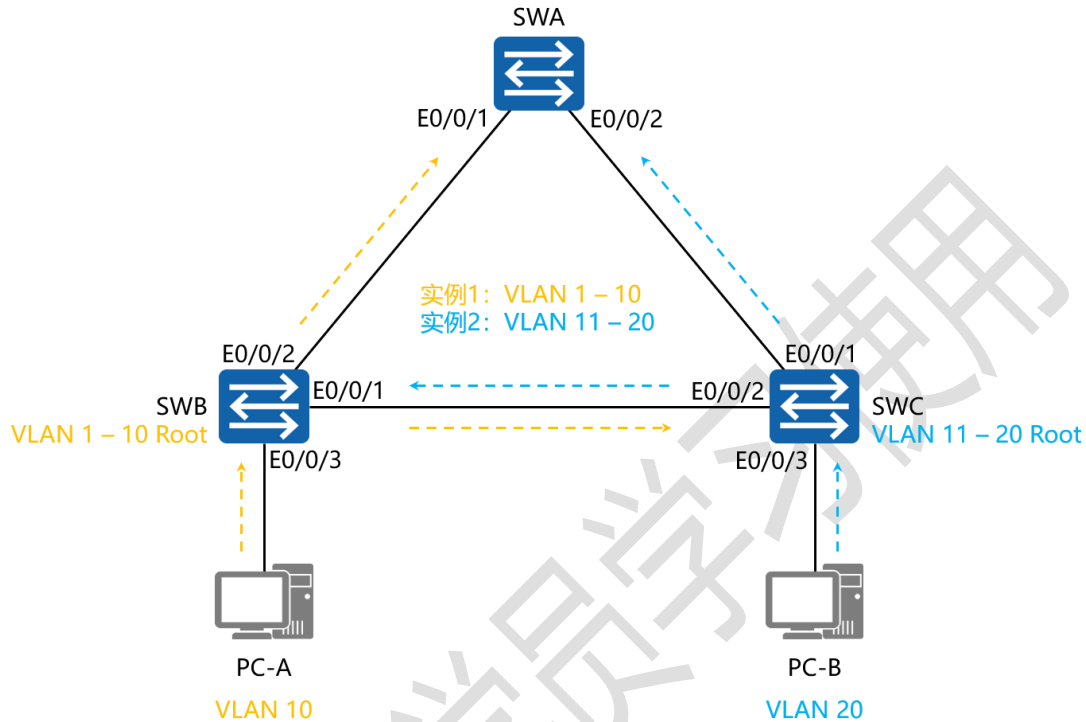
```
interface E0/0/2
```

```
port link-type trunk
```

```
port trunk allow-pass vlan all
```

## 三十、配置 MSTP 实验组网

### 一、实验拓扑：



### 二、实验目的：

通过 MSTP 的配置，令 SWB 成为 VLAN 1 – 10 的主根网桥，成为 VLAN 11 – 20 的备根网桥；同时令 SWC 成为 VLAN 11 – 20 的主根网桥，成为 VLAN 1 – 10 的备根网桥

### 三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

vlan batch 2 to 20 #创建 VLAN 2 到 20

```

stp mode mstp      #将 STP 的工作模式配置为 MSTP
stp region-configuration  #进入 STP 范围配置模式
region-name easthome  #配置该范围的名字
revision-level 0      #配置该范围的版本
instance 1 vlan 1 to 10  #将 VLAN 1 到 10 映射到实例 1
instance 2 vlan 11 to 20  #将 VLAN 11 到 20 映射到实例 2
active region-configuration  #将范围配置开启
interface E0/0/1      #进入相应的端口
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all  #允许该中继端口传递所有 VLAN 的信息
interface E0/0/2      #进入相应的端口
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all  #允许该中继端口传递所有 VLAN 的信息

```

SWB:

```

system-view
sysname SWB
vlan batch 2 to 20
stp mode mstp

```



```

stp region-configuration
region-name easthome
revision-level 0
instance 1 vlan 1 to 10
instance 2 vlan 11 to 20
active region-configuration
stp instance 1 root primary      #设置该网桥为实例 1 的主
根网桥
stp instance 2 root secondary  #设置该网桥为实例 2 的
备根网桥
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/3
stp edged-port enable          #将该接口配置为边缘模式
port link-type access          #将端口的链路类型配置为接入模
式
port default vlan 10          #将该端口加入进 VLAN 10

```

```
SWC:
system-view
sysname SWC
vlan 2 to 20
stp mode mstp
stp region-configuration
region-name easthome
revision-level 0
instance 1 vlan 1 to 10
instance 2 vlan 11 to 20
active region-configuration
stp instance 1 root secondary
stp instance 2 root primary
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/3
stp edged-port enable
port link-type access
```

port default vlan 20

测试:

在 SWB 上查看生成树中端口的角色与状态

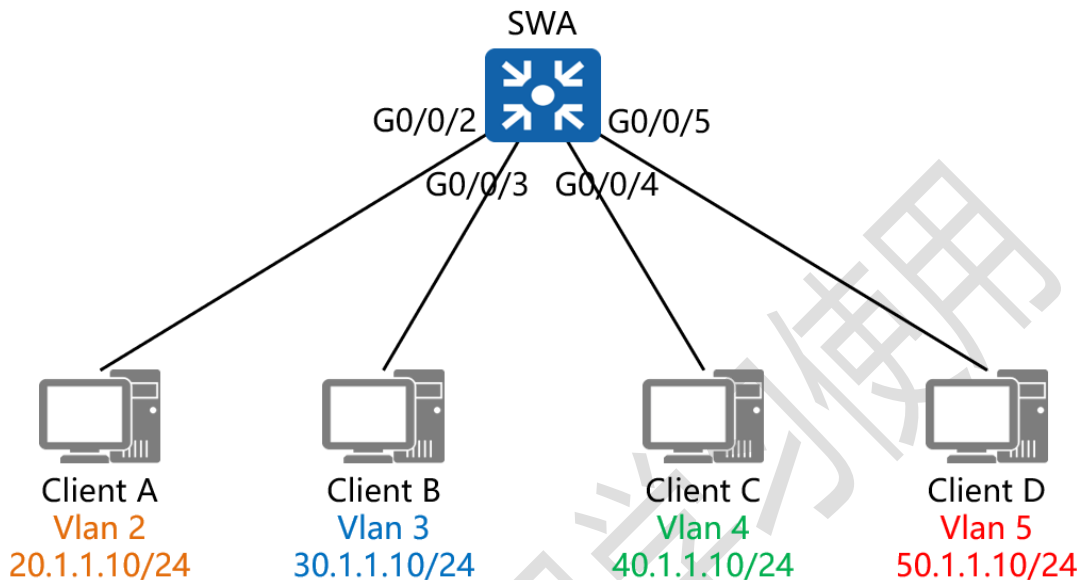
```
[SWB]display stp brief
MSTID  Port                Role  STP State  Protection
0      Ethernet0/0/1        DESI  FORWARDING NONE
0      Ethernet0/0/2        DESI  FORWARDING NONE
0      Ethernet0/0/3        DESI  FORWARDING NONE
1      Ethernet0/0/1        DESI  FORWARDING NONE
1      Ethernet0/0/2        DESI  FORWARDING NONE
1      Ethernet0/0/3        DESI  FORWARDING NONE
2      Ethernet0/0/1        ROOT  FORWARDING NONE
2      Ethernet0/0/2        DESI  LEARNING  NONE
[SWB]
```

在 SWC 上查看生成树中端口的角色与状态

```
[SWC]display stp brief
MSTID  Port                Role  STP State  Protection
0      Ethernet0/0/1        DESI  FORWARDING NONE
0      Ethernet0/0/2        ROOT  FORWARDING NONE
0      Ethernet0/0/3        DESI  FORWARDING NONE
1      Ethernet0/0/1        DESI  FORWARDING NONE
1      Ethernet0/0/2        ROOT  FORWARDING NONE
2      Ethernet0/0/1        DESI  FORWARDING NONE
2      Ethernet0/0/2        DESI  FORWARDING NONE
2      Ethernet0/0/3        DESI  FORWARDING NONE
[SWC]
```

## 三十一、配置三层交换实验组网

### 一、实验拓扑：



### 二、实验目的：

通过三层交换的配置，令不同 VLAN 间的主机能够相互通信

### 三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

vlan 2 #创建 VLAN 2

vlan 3 #创建 VLAN 3

vlan 4 #创建 VLAN 4

vlan 5 #创建 VLAN 5

interface vlan 2 #进入 VLAN 2 接口

```

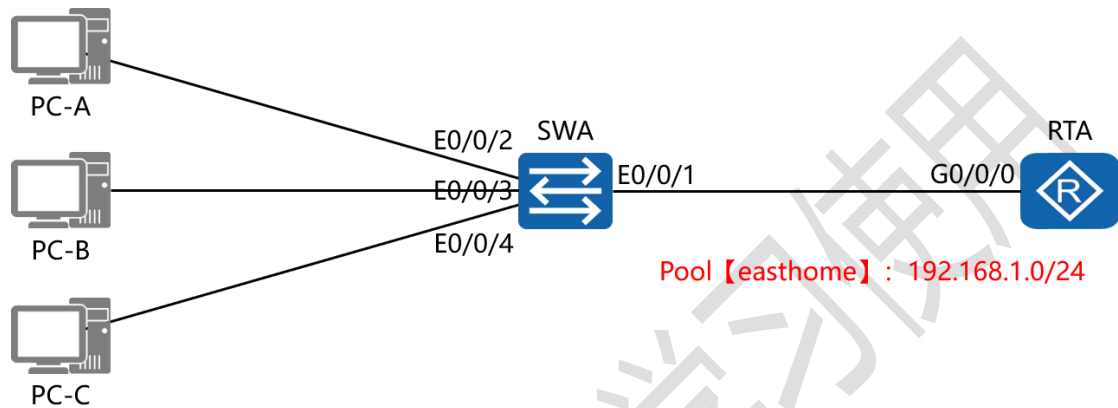
ip address 20.1.1.1 24      #配置 IP 地址及子网掩码
interface vlan 3          #进入 VLAN 3 接口
ip address 30.1.1.1 24    #配置 IP 地址及子网掩码
interface vlan 4          #进入 VLAN 4 接口
ip address 40.1.1.1 24    #配置 IP 地址及子网掩码
interface vlan 5          #进入 VLAN 5 接口
ip address 50.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/2          #进入相应端口
port link-type access     #将端口配置为接入模式
port default vlan 2      #将端口加入进 VLAN 2
interface G0/0/3          #进入相应端口
port link-type access     #将端口配置为接入模式
port default vlan 3      #将端口加入进 VLAN 3
interface G0/0/4          #进入相应端口
port link-type access     #将端口配置为接入模式
port default vlan 4      #将端口加入进 VLAN 4
interface G0/0/5          #进入相应端口
port link-type access     #将端口配置为接入模式
port default vlan 5      #将端口加入进 VLAN 5

```

## 三十二、配置 DHCP 接口地址池实验

### 组网

#### 一、实验拓扑：



#### 二、实验目的：

通过配置 DHCP 接口地址池，令 PC-A、PC-B、PC-C 可以获得与 RTA 的 G0/0/0 接口 IP 地址同网段的 IP 地址

#### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
dhcp enable         #开启 DHCP 功能
interface G0/0/0    #进入相应接口
ip address 192.168.1.1 24 #配置 IP 地址及子网掩码
dhcp select interface #配置 DHCP 的工作模式为接口模
    
```

式

dhcp server excluded-ip-address 192.168.1.2 #配置在

分配地址时排除的地址

dhcp server dns-list 202.106.49.151 #配置分配的 DNS

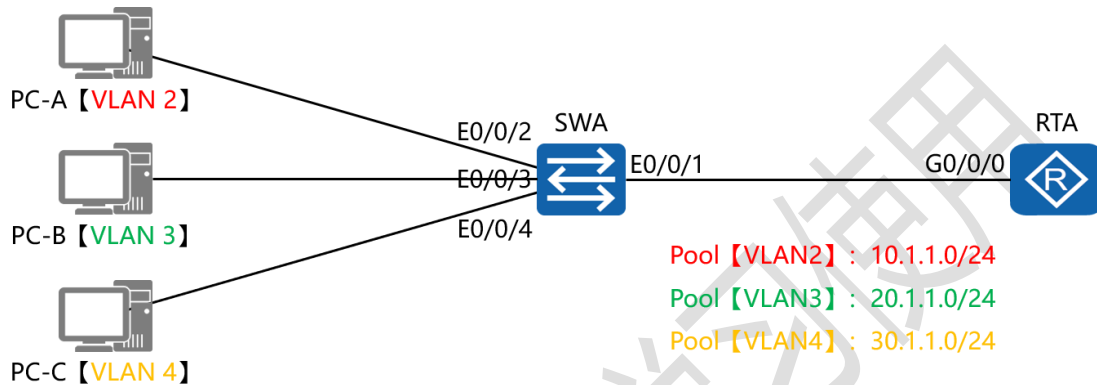
地址

dhcp server lease day 8 #配置 DHCP 的地址租期

## 三十三、配置 DHCP 全局地址池实验

### 组网

#### 一、实验拓扑：



#### 二、实验目的：

通过配置 DHCP 全局地址池，令 PC-A、PC-B、PC-C 分别从 3 个不同的地址池获取不同网段的 IP 地址，并能够实现互访

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

dhcp enable #开启 DHCP 功能

ip pool VLAN2 #创建地址池并命名

network 10.1.1.0 mask 24 #配置地址池内可分配的地址段及掩码

gateway-list 10.1.1.1 #配置分配的网关地址



```

dns-list 202.106.49.151    #配置分配的 DNS 地址
lease day 8                #配置 DHCP 的地址租期
ip pool VLAN3              #创建地址池并命名
network 20.1.1.0 mask 24   #配置地址池内可分配的地址段
                             及掩码
gateway-list 20.1.1.1     #配置分配的网关地址
dns-list 202.106.49.151   #配置分配的 DNS 地址
lease day 8                #配置 DHCP 的地址租期
ip pool VLAN4              #创建地址池并命名
network 30.1.1.0 mask 24   #配置地址池内可分配的地址段
                             及掩码
gateway-list 30.1.1.1     #配置分配的网关地址
dns-list 202.106.49.151   #配置分配的 DNS 地址
lease day 8                #配置 DHCP 的地址租期
interface G0/0/0.1        #进入第 1 个子接口
dot1q termination vid 2    #配置其 VLAN 的封装方式为
802.1Q, 并且令该子接口为 VLAN 2 的主机提供路由转发服务
ip address 10.1.1.1 24     #配置接口的 IP 地址及子网掩码
arp broadcast enable       #在子接口下开启 ARP 广播功能
dhcp select global        #配置 DHCP 的工作模式为全局模式
interface G0/0/0.2        #进入第 2 个子接口
dot1q termination vid 3    #配置其 VLAN 的封装方式为

```

802.1Q, 并且令该子接口为 VLAN 3 的主机提供路由转发服务

ip address 20.1.1.1 24 #配置接口的 IP 地址及子网掩码

arp broadcast enable #在子接口下开启 ARP 广播功能

dhcp select global #配置 DHCP 的工作模式为全局模式

interface G0/0/0.3 #进入第 2 个子接口

dot1q termination vid 4 #配置其 VLAN 的封装方式为

802.1Q, 并且令该子接口为 VLAN 3 的主机提供路由转发服务

ip address 30.1.1.1 24 #配置接口的 IP 地址及子网掩码

arp broadcast enable #在子接口下开启 ARP 广播功能

dhcp select global #配置 DHCP 的工作模式为全局模式

SWA:

system-view

sysname SWA

vlan 2

vlan 3

vlan 4

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

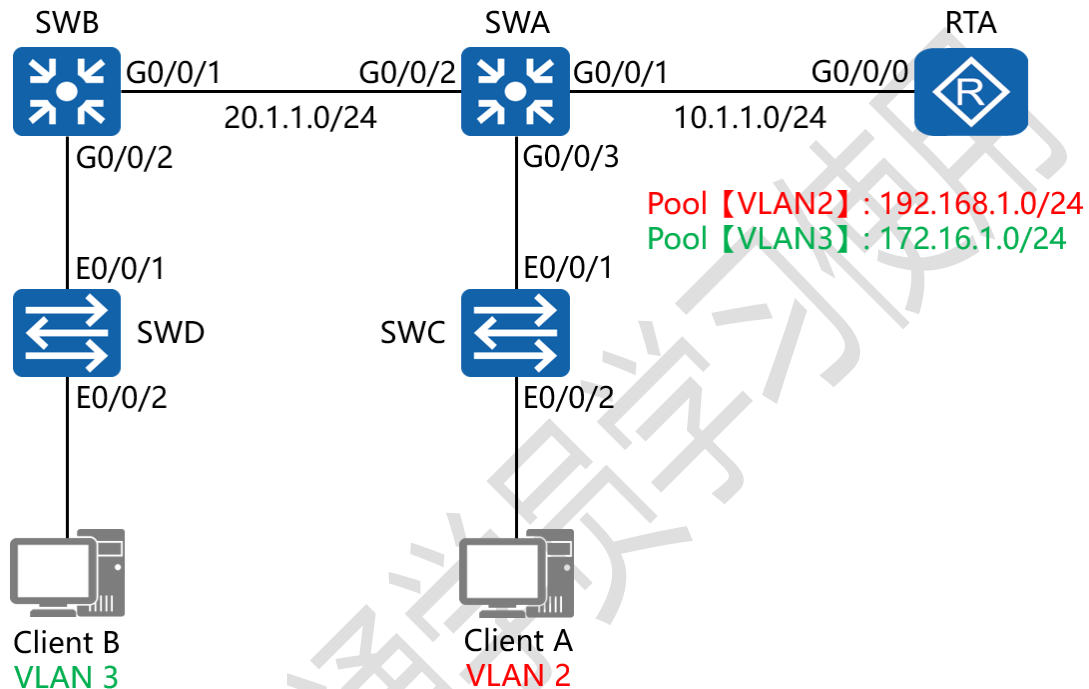
port link-type access

```
port default vlan 2
interface E0/0/3
port link-type access
port default vlan 3
interface E0/0/4
port link-type access
port default vlan 4
```

## 三十四、配置 DHCP 中继代理实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

将 RTA 配置为 DHCP 服务器，在 SWA 与 SWB 上配置并启用 DHCP 中继代理，令 RTA 给 VLAN 2 中的 Client A 分配 192.168.1.0/24 网段的地址，给 VLAN 3 中的 Client B 分配 172.16.1.0/24 网段的地址

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

```

sysname RTA      #给设备命名
dhcp enable      #开启 DHCP 功能
ip pool VLAN2    #创建地址池并命名
network 192.168.1.0 mask 24    #配置地址池内可分配的地址段及掩码
gateway-list 192.168.1.1      #配置分配的网关地址
dns-list 202.106.49.151      #配置分配的 DNS 地址
lease day 8      #配置 DHCP 的地址租期
ip pool VLAN3    #创建地址池并命名
network 172.16.1.0 mask 24    #配置地址池内可分配的地址段及掩码
gateway-list 172.16.1.1      #配置分配的网关地址
dns-list 202.106.0.20      #配置分配的 DNS 地址
lease day 8      #配置 DHCP 的地址租期
interface G0/0/0      #进入相应接口
ip address 10.1.1.1 24      #配置接口的 IP 地址及子网掩码
dhcp select global      #配置 DHCP 的工作模式为全局模式
rip
version 2
network 10.0.0.0
undo summary

```

```
SWA:
system-view
sysname SWA
dhcp enable
vlan 2
vlan 10
vlan 20
interface vlan 2      #进入 vlan 2 接口
ip address 192.168.1.1 24
dhcp select relay      #开启 DHCP 中继代理功能
dhcp relay server-ip 10.1.1.1  #指定 DHCP 服务器 IP 地址
interface vlan 10
ip address 10.1.1.2 24
interface vlan 20
ip address 20.1.1.1 24
interface G0/0/1
port link-type access
port default vlan 10
interface G0/0/2
port link-type access
```

```
port default vlan 20
interface G0/0/3
port link-type trunk
port trunk allow-pass vlan all
rip
version 2
network 10.0.0.0
network 20.0.0.0
network 192.168.1.0
undo summary
```

SWB:

```
system-view
sysname SWB
dhcp enable
vlan 3
vlan 20
interface vlan 3
ip address 172.16.1.1 24
dhcp select relay
dhcp relay server-ip 10.1.1.1
interface vlan 20
```

```
ip address 20.1.1.2 24
interface G0/0/1
port link-type access
port default vlan 20
interface G0/0/2
port link-type trunk
port trunk allow-pass vlan all
rip
version 2
network 20.0.0.0
network 172.16.0.0
undo summary
```

```
SWC:
system-view
sysname SWC
vlan 2
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type access
```



---

port default vlan 2

SWD:

system-view

sysname SWD

vlan 3

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

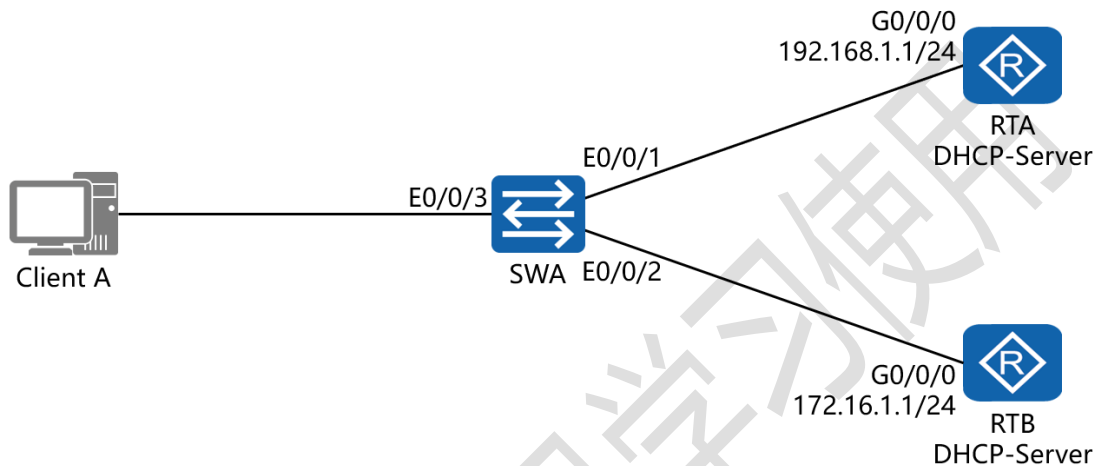
port link-type access

port default vlan 3

## 三十五、配置 DHCP Snooping 实验

### 组网

#### 一、实验拓扑：



#### 二、实验目的：

将 RTA 与 RTB 均配置为基于接口的 DHCP 服务器，在 SWA 上配置并启用 DHCP Snooping 功能，令其信任端口 E0/0/1 所连接的 RTA，并让 Client A 成功获取 192.168.1.0/24 网段的地址；在 RTA 或与 RTA 相连的链路失效后，不让 Client A 从 RTB 获取 IP 地址（即：不信任 RTB）；同时启用 IPSG 功能，防止攻击者仿冒合法的源 IP 地址进行攻击

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

```
dhcp enable          #开启 DHCP 功能
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
dhcp select interface  #配置 DHCP 的工作模式为接口模式
dhcp server dns-list 202.106.49.151 #配置分配的 DNS 地址
dhcp server lease day 8    #配置 DHCP 的地址租期
```

RTB:

```
system-view
sysname RTB
dhcp enable
interface G0/0/0
ip address 172.16.1.1 24
dhcp select interface
dhcp server dns-list 202.106.0.20
dhcp server lease day 8
```

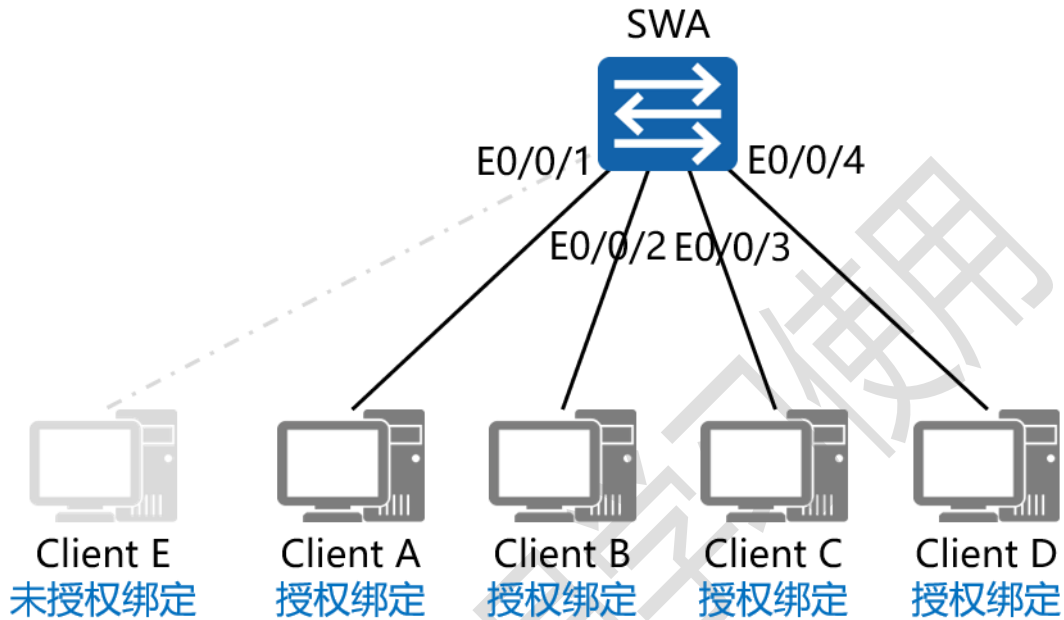
SWA:

```
system-view
sysname SWA
```

```
dhcp enable
dhcp snooping enable      #开启 DHCP Snooping 功能
interface E0/0/1
dhcp snooping enable      #在端口下开启 DHCP Snooping
功能
dhcp snooping trusted     #将当前端口配置为信任模式（默
认模式为非信任模式）
interface E0/0/2
dhcp snooping enable      #在端口下开启 DHCP Snooping
功能
ip source check user-bind enable  #启用 IPSG 功能，防
止攻击者仿冒合法源 IP 地址进行攻击
```

## 三十六、配置端口安全实验组网

### 一、实验拓扑：



### 二、实验目的：

将 SWA 的端口 E0/0/1 – E0/0/4 配置端口安全，并手工绑定其所连接的主机终端的 MAC 地址，之后将端口 E0/0/1 与未授权绑定终端 Client E 相连，检测其是否可以与其它终端通讯

### 三、实验步骤：

SWA:

```
system-view      #进入系统视图模式
sysname SWA     #给设备命名
interface E0/0/1 #进入相应端口
port-security enable #开启端口安全功能
```

port-security max-mac-num 1 #配置该端口最多可学习  
1 个 MAC 地址

port-security mac-address sticky #开启手工配置 MAC  
地址模式

port-security mac-address sticky 5489-9824-323A vlan 1  
#手工输入该端口绑定的 MAC 地址与其所属的 VLAN ID

port-security protect-action shutdown #配置当该端口  
连接了其它未授权设备时执行的动作为 shutdown

interface E0/0/2 #进入相应端口

port-security enable #开启端口安全功能

port-security max-mac-num 1 #配置该端口最多可学习  
1 个 MAC 地址

port-security mac-address sticky #开启手工配置 MAC  
地址模式

port-security mac-address sticky 5489-984C-74A5 vlan 1  
#手工输入该端口绑定的 MAC 地址与其所属的 VLAN ID

port-security protect-action shutdown #配置当该端口  
连接了其它未授权设备时执行的动作为 shutdown

interface E0/0/3 #进入相应端口

port-security enable #开启端口安全功能

port-security max-mac-num 1 #配置该端口最多可学习  
1 个 MAC 地址

port-security mac-address sticky #开启手工配置 MAC  
地址模式

port-security mac-address sticky 5489-9813-4A9B vlan 1  
#手工输入该端口绑定的 MAC 地址与其所属的 VLAN ID

port-security protect-action shutdown #配置当该端口  
连接了其它未授权设备时执行的动作为 shutdown

interface E0/0/4 #进入相应端口

port-security enable #开启端口安全功能

port-security max-mac-num 1 #配置该端口最多可学习  
1 个 MAC 地址

port-security mac-address sticky #开启手工配置 MAC  
地址模式

port-security mac-address sticky 5489-98D8-2CCB vlan 1  
#手工输入该端口绑定的 MAC 地址与其所属的 VLAN ID

port-security protect-action shutdown #配置当该端口  
连接了其它未授权设备时执行的动作为 shutdown

注：

当配置了端口安全的端口连接过非授权主机后，该端口将会被 shutdown，无法正常通讯，此时，即便再将该端口重新连接回原先的授权主机，该端口依旧无法正常通讯；需通知管理人员，在该端口下手动执行命令【restart】，方可令该端口重新恢复至

转发状态

```
[Huawei]interface E0/0/1
```

```
[Huawei-Ethernet0/0/1]restart
```

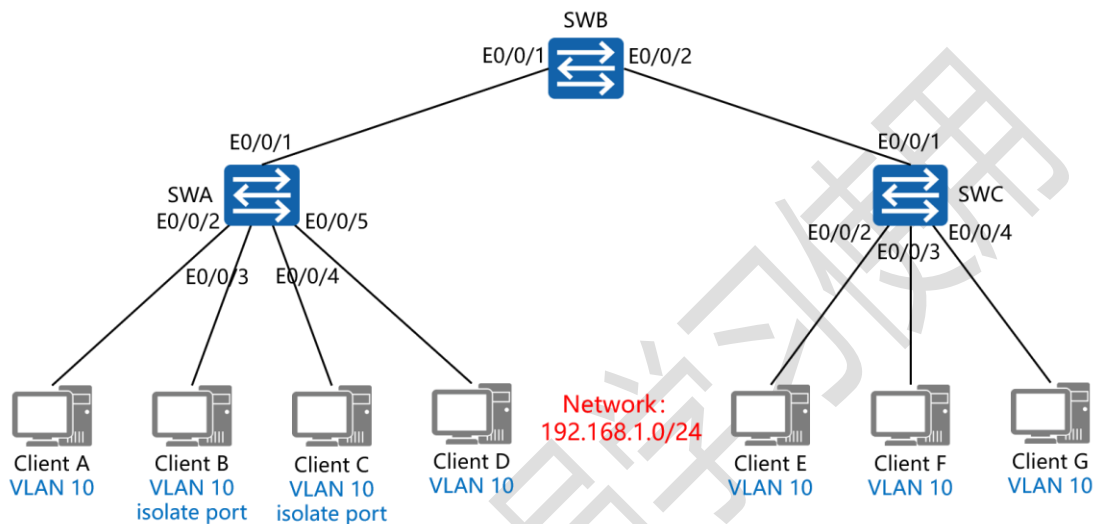
仅供瑞通学员学习使用



## 三十七、配置二层隔离三层互通的端口

### 隔离实验组网

#### 一、实验拓扑：



#### 二、实验目的：

将 SWA 的隔离端口模式配置为二层隔离三层互通模式，再将 E0/0/3 与 E0/0/4 端口配置为隔离端口，测试 Client A 与 Client B 是否能通讯，以及 Client B 与 Client C 是否能通讯；之后在 SWA 上为 VLAN 10 配置管理 IP 地址；再次测试 Client A 与 Client B 是否能通讯，以及 Client B 与 Client C 是否能通讯

#### 三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

```

vlan 10      #创建 VLAN 10

port-isolate mode l2    #配置设备的隔离端口模式为二层隔离三层互通

interface E0/0/1      #进入相应端口

port link-type trunk    #将端口类型配置为中继模式

port trunk allow-pass vlan all    #配置允许中继链路传递所有 VLAN 标记的数据帧

interface E0/0/2      #进入相应端口

port link-type access    #将端口类型配置为接入模式

port default vlan 10    #将端口加入 VLAN 10

interface E0/0/3      #进入相应端口

port link-type access    #将端口类型配置为接入模式

port default vlan 10    #将端口加入 VLAN 10

port-isolate enable group 1    #开启隔离端口功能

interface E0/0/4      #进入相应端口

port link-type access    #将端口类型配置为接入模式

port default vlan 10    #将端口加入 VLAN 10

port-isolate enable group 1    #开启隔离端口功能

interface E0/0/5      #进入相应端口

port link-type access    #将端口类型配置为接入模式

port default vlan 10    #将端口加入 VLAN 10

```

SWB:

system-view

sysname SWB

vlan 10

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type trunk

port trunk allow-pass vlan all

SWC:

system-view

sysname SWC

vlan 10

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type access

port default vlan 10

interface E0/0/3

port link-type access

port default vlan 10

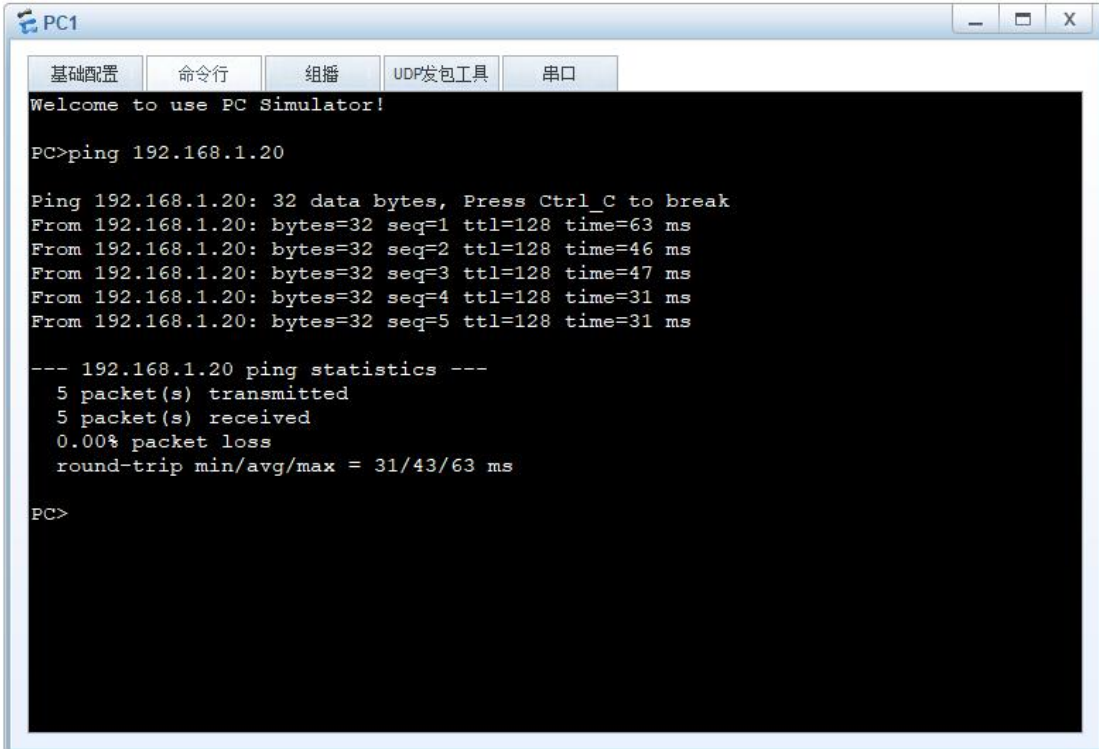
interface E0/0/4

port link-type access

port default vlan 10

测试:

Client A 与 Client B 可正常通讯



The screenshot shows a window titled 'PC1' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The main area is a black terminal window with white text. The text shows a 'Welcome to use PC Simulator!' message, followed by a 'ping 192.168.1.20' command. The output shows five successful ping attempts with varying response times (63ms, 46ms, 47ms, 31ms, 31ms). Below the individual pings, there is a summary: '--- 192.168.1.20 ping statistics ---', '5 packet(s) transmitted', '5 packet(s) received', '0.00% packet loss', and 'round-trip min/avg/max = 31/43/63 ms'. The prompt 'PC>' is visible at the bottom.

```
PC1
基础配置  命令行  组播  UDP发包工具  串口
Welcome to use PC Simulator!
PC>ping 192.168.1.20

Ping 192.168.1.20: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: bytes=32 seq=1 ttl=128 time=63 ms
From 192.168.1.20: bytes=32 seq=2 ttl=128 time=46 ms
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/63 ms

PC>
```

## Client B 与 Client C 无法正常通讯

The screenshot shows a terminal window titled 'PC2' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The terminal output is as follows:

```

Welcome to use PC Simulator!

PC>ping 192.168.1.30

Ping 192.168.1.30: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: Destination host unreachable
From 192.168.1.20: Destination host unreachable
From 192.168.1.20: Destination host unreachable
From 192.168.1.20: Destination host unreachable
From 192.168.1.20: Destination host unreachable

--- 192.168.1.30 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
    
```

之后在 SWA 上为 VLAN 10 配置管理 IP 地址，并将该地址配置为所有 Client 的网关

SWA:

interface vlan 10

ip add 192.168.1.1 24

arp-proxy inner-sub-vlan-proxy enable #开启同 VLAN

内 ARP 代理功能

再次测试：

Client A 与 Client B 依旧可以正常通讯

```

PC1
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/63 ms

PC>ping 192.168.1.20

Ping 192.168.1.20: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=32 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=47 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/40/47 ms

PC>
    
```

Client B 与 Client C 此时亦可正常通讯

```

PC2
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.30: bytes=32 seq=3 ttl=127 time=63 ms
From 192.168.1.30: bytes=32 seq=4 ttl=127 time=47 ms
From 192.168.1.30: bytes=32 seq=5 ttl=127 time=47 ms

--- 192.168.1.30 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 32/50/63 ms

PC>ping 192.168.1.30

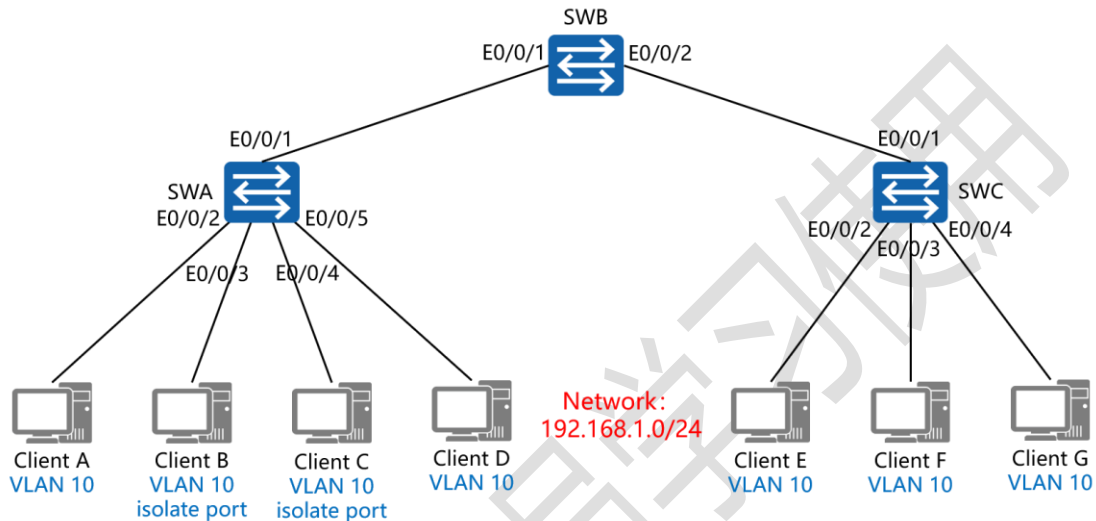
Ping 192.168.1.30: 32 data bytes, Press Ctrl_C to break
From 192.168.1.30: bytes=32 seq=1 ttl=127 time=47 ms
From 192.168.1.30: bytes=32 seq=2 ttl=127 time=31 ms
From 192.168.1.30: bytes=32 seq=3 ttl=127 time=47 ms
From 192.168.1.30: bytes=32 seq=4 ttl=127 time=47 ms
From 192.168.1.30: bytes=32 seq=5 ttl=127 time=47 ms

--- 192.168.1.30 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/47 ms

PC>
    
```

# 三十八、配置二层三层均隔离的端口隔离实验组网

## 一、实验拓扑：



## 二、实验目的：

将 SWA 的隔离端口模式配置为二层三层均隔离模式，再将 E0/0/3 与 E0/0/4 端口配置为隔离端口，测试 Client A 与 Client B 是否能通讯，以及 Client B 与 Client C 是否能通讯；之后在 SWA 上为 VLAN 10 配置管理 IP 地址；再次测试 Client A 与 Client B 是否能通讯，以及 Client B 与 Client C 是否能通讯

## 三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

```

vlan 10      #创建 VLAN 10

port-isolate mode all      #配置设备的隔离端口模式为二层
三层均隔离

interface E0/0/1      #进入相应端口

port link-type trunk      #将端口类型配置为中继模式

port trunk allow-pass vlan all      #配置允许中继链路传递所有 VLAN 标记的数据帧

interface E0/0/2      #进入相应端口

port link-type access      #将端口类型配置为接入模式

port default vlan 10      #将端口加入 VLAN 10

interface E0/0/3      #进入相应端口

port link-type access      #将端口类型配置为接入模式

port default vlan 10      #将端口加入 VLAN 10

port-isolate enable group 1      #开启隔离端口功能

interface E0/0/4      #进入相应端口

port link-type access      #将端口类型配置为接入模式

port default vlan 10      #将端口加入 VLAN 10

port-isolate enable group 1      #开启隔离端口功能

interface E0/0/5      #进入相应端口

port link-type access      #将端口类型配置为接入模式

port default vlan 10      #将端口加入 VLAN 10

```



SWB:

system-view

sysname SWB

vlan 10

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type trunk

port trunk allow-pass vlan all

SWC:

system-view

sysname SWC

vlan 10

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

port link-type access

port default vlan 10

interface E0/0/3

port link-type access

port default vlan 10

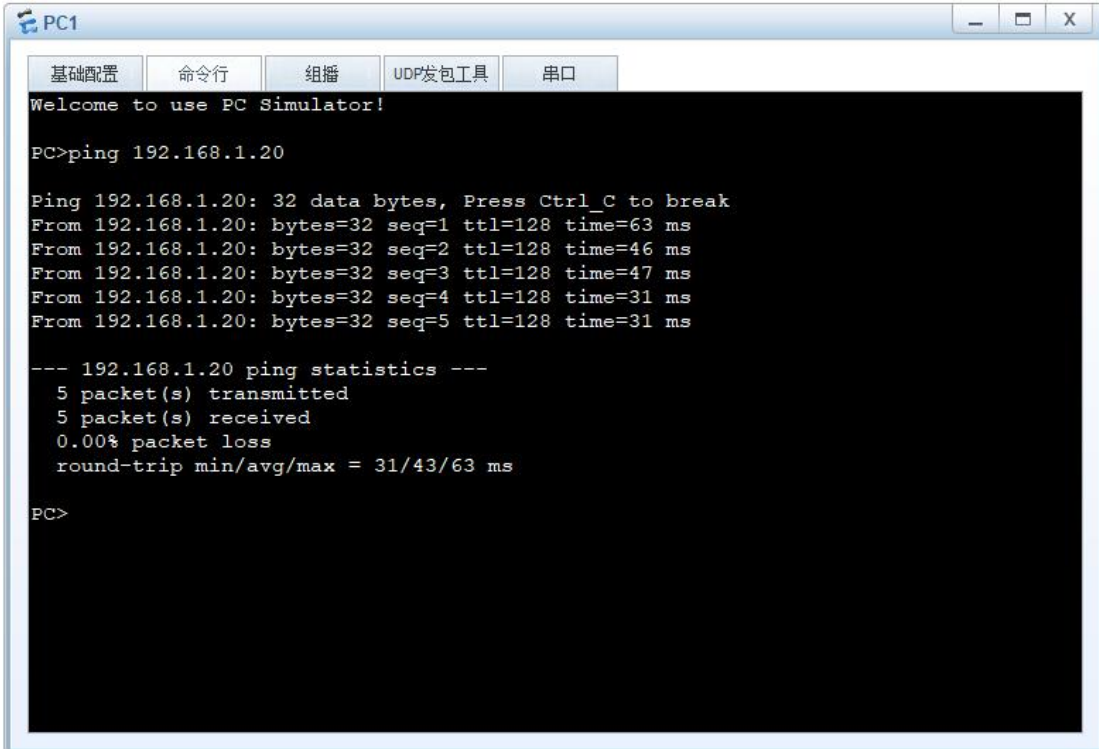
interface E0/0/4

port link-type access

port default vlan 10

测试:

Client A 与 Client B 可正常通讯



```

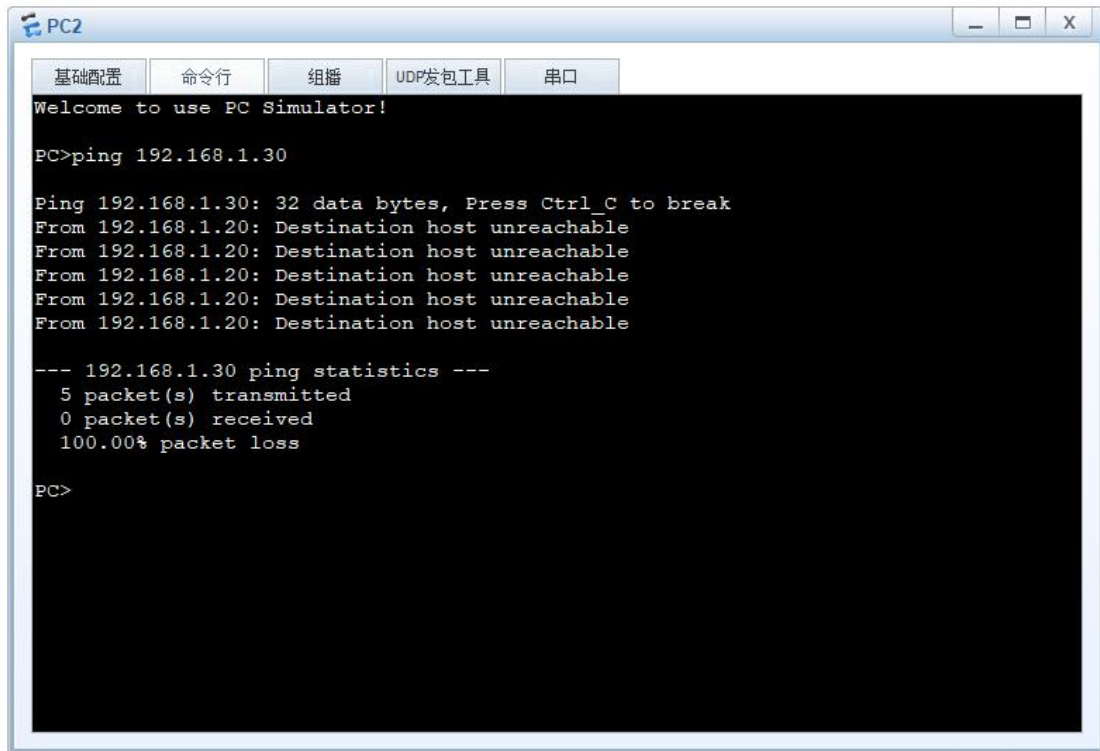
PC1
基础配置  命令行  组播  UDP发包工具  串口
Welcome to use PC Simulator!
PC>ping 192.168.1.20

Ping 192.168.1.20: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: bytes=32 seq=1 ttl=128 time=63 ms
From 192.168.1.20: bytes=32 seq=2 ttl=128 time=46 ms
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/63 ms

PC>
    
```

## Client B 与 Client C 无法正常通讯



之后在 SWA 上为 VLAN 10 配置管理 IP 地址，并将该地址配置为所有 Client 的网关

SWA:

```
interface vlan 10
```

```
ip add 192.168.1.1 24
```

```
arp-proxy inner-sub-vlan-proxy enable #开启同 VLAN
```

内 ARP 代理功能

再次测试：

Client A 与 Client B 依旧可以正常通讯

```

PC1
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/63 ms

PC>ping 192.168.1.20

Ping 192.168.1.20: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=32 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=47 ms

--- 192.168.1.20 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/40/47 ms

PC>
    
```

Client B 与 Client C 此时依旧无法正常通讯

```

PC2
基础配置 命令行 组播 UDP发包工具 串口
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.1.30 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>ping 192.168.1.30

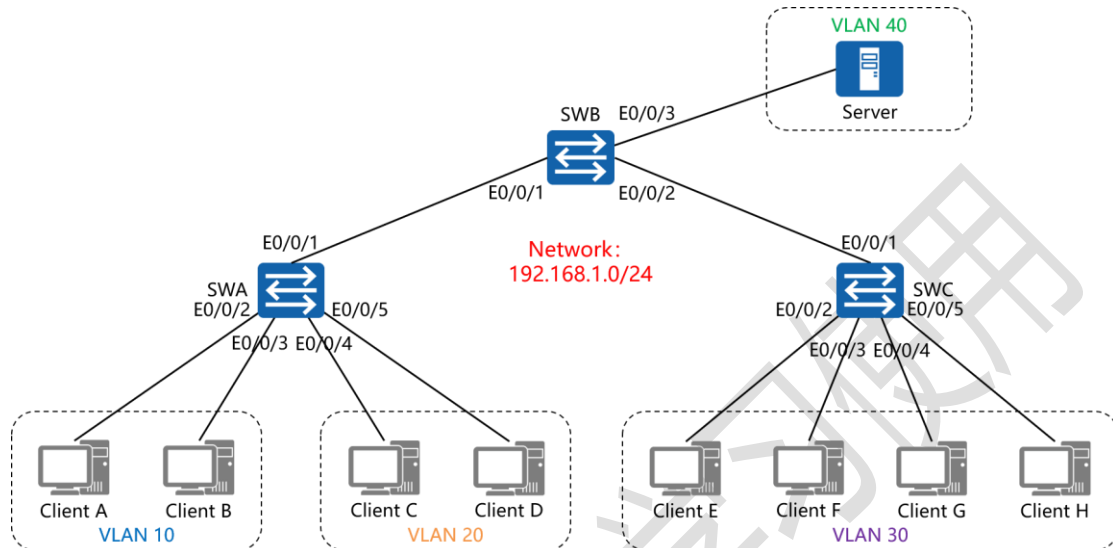
Ping 192.168.1.30: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.1.30 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
    
```

## 三十九、配置 MUX VLAN 实验组网

### 一、实验拓扑：



### 二、实验目的：

将 VLAN 40 配置为 Principal VLAN, VLAN 10 与 VLAN 20 配置为 Group VLAN, VLAN 30 配置为 Separate VLAN, 令 VLAN 10 内终端可相互访问, VLAN 20 内终端可相互访问, VLAN 30 内终端彼此之间不可相互访问, 同时与 VLAN 10 和 VLAN 20 内的终端也不可相互访问, 但所有终端均可与 VLAN 40 内的 Server 相互访问

### 三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

```

vlan 10      #创建 VLAN 10
vlan 20      #创建 VLAN 20
vlan 30      #创建 VLAN 30
vlan 40      #创建 VLAN 40

mux-vlan     #将 VLAN 40 配置为主 VLAN

subordinate group 10 20      #关联互通型 VLAN 10 和 20
subordinate separate 30     #关联隔离型 VLAN 40

interface E0/0/1      #进入相应端口
port link-type trunk  #将端口类型配置为中继模式
port trunk allow-pass vlan all #配置允许中继链路传递所有 VLAN 标记的数据帧

interface E0/0/2      #进入相应端口
port link-type access #将端口类型配置为接入模式
port default vlan 10  #将端口加入 VLAN 10
port mux-vlan enable  #在端口下开启 MUX VLAN 功能

interface E0/0/3      #进入相应端口
port link-type access #将端口类型配置为接入模式
port default vlan 10  #将端口加入 VLAN 10
port mux-vlan enable  #在端口下开启 MUX VLAN 功能

interface E0/0/4      #进入相应端口
port link-type access #将端口类型配置为接入模式
port default vlan 20  #将端口加入 VLAN 20

```

```
port mux-vlan enable      #在端口下开启 MUX VLAN 功能
interface E0/0/5          #进入相应端口
port link-type access     #将端口类型配置为接入模式
port default vlan 20      #将端口加入 VLAN 20
port mux-vlan enable      #在端口下开启 MUX VLAN 功能
```

SWB:

```
system-view
sysname SWB
vlan 10
vlan 20
vlan 30
vlan 40
mux-vlan
subordinate group 10 20
subordinate separate 30
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
```

```
interface E0/0/3
port link-type access
port default vlan 40
port mux-vlan enable
```

SWC:

```
system-view
sysname SWC
vlan 10
vlan 20
vlan 30
vlan 40
mux-vlan
subordinate group 10 20
subordinate separate 30
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type access
port default vlan 30
port mux-vlan enable
```



```
interface E0/0/3
port link-type access
port default vlan 30
port mux-vlan enable
interface E0/0/4
port link-type access
port default vlan 30
port mux-vlan enable
interface E0/0/5
port link-type access
port default vlan 30
port mux-vlan enable
```

测试:

VLAN 10 内的 Client A 与 Client B 可相互访问

```

PC9
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=32 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=63 ms

--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 32/50/63 ms

PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time=46 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time=16 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=62 ms

--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 16/46/63 ms

PC>
    
```

VLAN 20 内的 Client C 与 Client D 可相互访问

```

PC11
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.4: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.4: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.4: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.4 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/43/47 ms

PC>ping 192.168.1.4

Ping 192.168.1.4: 32 data bytes, Press Ctrl_C to break
From 192.168.1.4: bytes=32 seq=1 ttl=128 time=31 ms
From 192.168.1.4: bytes=32 seq=2 ttl=128 time=47 ms
From 192.168.1.4: bytes=32 seq=3 ttl=128 time=62 ms
From 192.168.1.4: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.4: bytes=32 seq=5 ttl=128 time=46 ms

--- 192.168.1.4 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/46/62 ms

PC>|
    
```

## VLAN 10 内的 Client A 与 VLAN 20 内的 Client C 无法互访

```

PC9
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
--- 192.168.1.3 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
PC>ping 192.168.1.3
Ping 192.168.1.3: 32 data bytes, Press Ctrl_C to break
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
--- 192.168.1.3 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
PC>
    
```

## VLAN 30 内的所有 Client 均不可相互访问

```

PC13
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
--- 192.168.1.6 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
PC>ping 192.168.1.6
Ping 192.168.1.6: 32 data bytes, Press Ctrl_C to break
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
--- 192.168.1.6 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
PC>
    
```

## VLAN 10 内的 Client A 与 VLAN 30 内的 Client E 不可互访

```

PC9
基础配置  命令行  组播  UDP发包工具  串口
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable

--- 192.168.1.5 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss

PC>ping 192.168.1.5

Ping 192.168.1.5: 32 data bytes, Press Ctrl_C to break
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable

--- 192.168.1.5 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss

PC>
    
```

## VLAN 20 内的 Client C 与 VLAN 30 内的 Client E 不可互访

```

PC11
基础配置  命令行  组播  UDP发包工具  串口
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable

--- 192.168.1.5 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss

PC>ping 192.168.1.5

Ping 192.168.1.5: 32 data bytes, Press Ctrl_C to break
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable
From 192.168.1.3: Destination host unreachable

--- 192.168.1.5 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss

PC>
    
```

## VLAN 10 内的 Client A 与 VLAN 40 内的 Server 可相互访问

```

PC9
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=78 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=109 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/84/110 ms

PC>ping 192.168.1.254

Ping 192.168.1.254: 32 data bytes, Press Ctrl_C to break
From 192.168.1.254: bytes=32 seq=1 ttl=128 time=94 ms
From 192.168.1.254: bytes=32 seq=2 ttl=128 time=109 ms
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=125 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=109 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=78 ms

--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 78/103/125 ms

PC>
    
```

## VLAN 20 内的 Client C 与 VLAN 40 内的 Server 可相互访问

```

PC11
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=78 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=110 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=79 ms

--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 63/81/110 ms

PC>ping 192.168.1.254

Ping 192.168.1.254: 32 data bytes, Press Ctrl_C to break
From 192.168.1.254: bytes=32 seq=1 ttl=128 time=79 ms
From 192.168.1.254: bytes=32 seq=2 ttl=128 time=63 ms
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=79 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=63 ms

--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 63/69/79 ms

PC>
    
```

## VLAN 30 内的 Client E 与 VLAN 40 内的 Server 可相互访问

```

PC13
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=78 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=110 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=78 ms

--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 78/84/110 ms

PC>ping 192.168.1.254

Ping 192.168.1.254: 32 data bytes, Press Ctrl_C to break
From 192.168.1.254: bytes=32 seq=1 ttl=128 time=79 ms
From 192.168.1.254: bytes=32 seq=2 ttl=128 time=93 ms
From 192.168.1.254: bytes=32 seq=3 ttl=128 time=125 ms
From 192.168.1.254: bytes=32 seq=4 ttl=128 time=94 ms
From 192.168.1.254: bytes=32 seq=5 ttl=128 time=110 ms

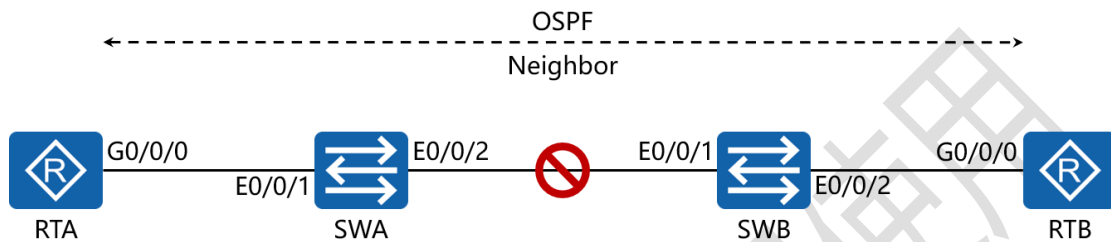
--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 79/100/125 ms

PC>
    
```

## 四十、配置 BFD 与 OSPF 联动实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

RTA 与 RTB 运行 OSPF 路由协议，之后在 RTA 与 RTD 上开启 BFD 功能，令 OSPF 与 BFD 联动，采用 BFD 控制数据方式，实现当 RTA 或 RTB 与二层交换机之间以及二层交换机之间的链路出现故障【如链路 down】时，BFD 能够快速感知并通告 OSPF 协议

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

bfd #全局开启 BFD 功能

interface G0/0/0 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

```

interface Loopback0    #创建环回接口 0
ip address 1.1.1.1 32   #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
                           #器 ID
bfd all-interfaces enable    #为所有运行 OSPF 路由协议的
                             #接口开启 BFD 功能
area 0    #创建 OSPF 区域 0
network 192.168.1.0 0.0.0.255    #通告其直连网段

```

RTB:

```

system-view
sysname RTB
bfd
interface G0/0/0
ip address 192.168.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
bfd all-interfaces enable
area 0
network 192.168.1.0 0.0.0.255

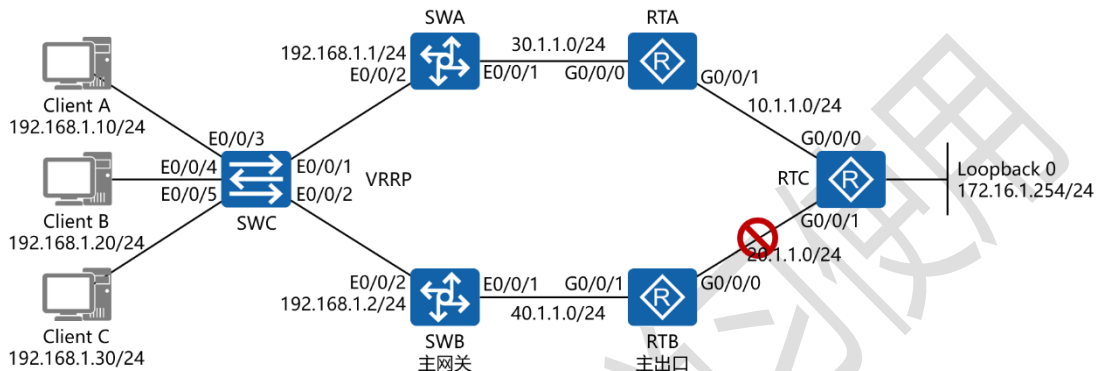
```



# 四十一、配置 BFD 与 VRRP 联动实验

## 组网

### 一、实验拓扑：



### 二、实验目的：

全网使用 RIPv2 路由协议联通, SWA 与 SWB 为 VRRP 备份组, SWB 为 Master; 在 SWB 与 RTC 上启用 BFD, 当 RTB 与 RTC 的互联链路出现故障时, SWB 的 BFD 功能能够快速感知并切换为备用网关状态, 令 SWA 成为主用网关

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 30.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
rip 1    #进入 RIP 进程 1
version 2    #配置使用版本 2
network 10.0.0.0    #通告其直连网段
network 30.0.0.0    #通告其直连网段
undo summary    #关闭自动汇总
```

RTB:

```
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 40.1.1.1 24
rip 1
version 2
network 20.0.0.0
network 40.0.0.0
undo summary
```

RTC:

```
system-view
```

```

sysname RTC

bfd      #全局开启 BFD 功能

interface G0/0/0
ip address 10.1.1.2 24

interface G0/0/1
ip address 20.1.1.2 24

interface Loopback0
ip address 172.16.1.254 24

rip 1
version 2
network 10.0.0.0
network 20.0.0.0
network 172.16.0.0
undo summary
bfd 1 bind peer-ip 40.1.1.2 source-ip 20.1.1.2 auto
#开启 BFD 自动会话功能，并指定目标地址与源地址
commit   #确认开启此功能
    
```

SWA:

```

system-view

sysname SWA

vlan 100   #创建 VLAN 100
    
```

```

vlan 200    #创建 VLAN 200

interface vlan 100    #进入 VLAN 100 接口
ip address 30.1.1.2 24    #配置 IP 地址及子网掩码

interface vlan 200    #进入 VLAN 300 接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码

vrrp vrid 47 virtual-ip 192.168.1.254    #开启 VRRP 功能, 设置组号为 47, 并指定虚拟 IP 地址为 192.168.1.254

interface E0/0/1    #进入相应端口
port link-type access    #将端口配置为接入模式
port default vlan 100    #将端口加入进 VLAN 100

interface E0/0/2    #进入相应端口
port link-type access    #将端口配置为接入模式
port default vlan 200    #将端口加入进 VLAN 200

rip 1
version 2
network 30.0.0.0
network 192.168.1.0
undo summary

```

SWB:

system-view

sysname SWB

```
bfd
vlan 100
vlan 200
interface vlan 100
ip address 40.1.1.2 24
interface vlan 200
ip address 192.168.1.2 24
vrrp vrid 47 virtual-ip 192.168.1.254
vrrp vrid 47 priority 200      #配置优先级为 200
vrrp vrid 47 track bfd-session session-name 1 reduced
110
#在 VRRP 下跟踪 BFD 会话 1，若被跟踪链路发生故障，则
VRRP 优先级降低 110
interface E0/0/1
port link-type access
port default vlan 100
interface E0/0/2
port link-type access
port default vlan 200
rip 1
version 2
network 40.0.0.0
```

```
network 192.168.1.0
```

```
undo summary
```

```
bfd 1 bind peer-ip 20.1.1.2 source-ip 40.1.1.2 auto
```

```
commit
```

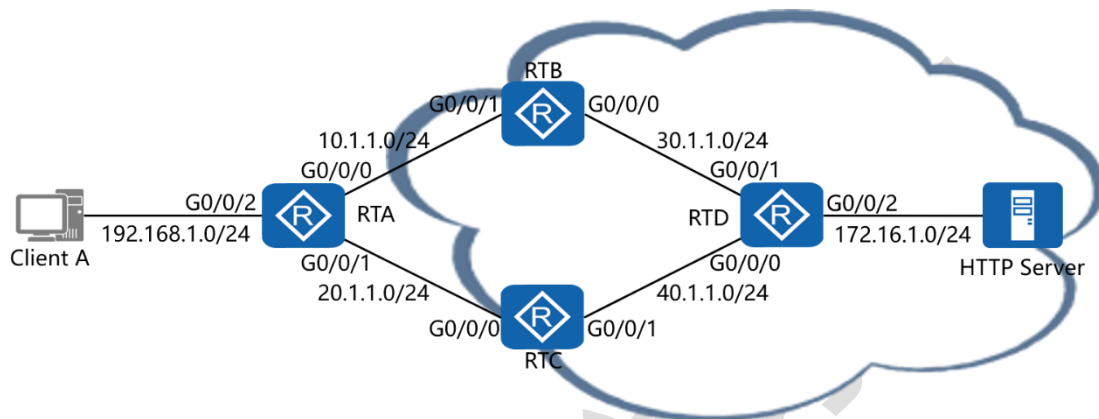
```
SWC:
```

```
system-view
```

```
sysname SWC
```

## 四十二、配置 BFD 与静态路由联动实验组网

### 一、实验拓扑：



### 二、实验目的：

RTA 模拟某园区网的双出口点，分别连通 RTB (ISP1) 与 RTC (ISP2)，正常情况下默认路由通往 RTB (ISP1)，RTC (ISP2) 处在备用状态；在 RTA 与 RTD 上开启 BFD 功能，当 RTB(ISP1) 通往 RTD 的网络出现故障的时候，能够快速切换至 RTC (ISP2) 方向

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

bfd #全局开启 BFD 功能

interface G0/0/0 #进入相应接口

```

ip address 10.1.1.1 24      #配置 IP 地址及子网掩码
interface G0/0/1          #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/2          #进入相应接口
ip address 192.168.1.1 24 #配置 IP 地址及子网掩码
bfd 1 bind peer-ip 30.1.1.2 source-ip 10.1.1.1 auto
#开启 BFD 自动会话功能，并指定目标地址与源地址
commit                    #确认开启此功能
ip route-static 30.1.1.0 255.255.255.0 10.1.1.2      #配置默
认路由到达 30.1.1.0 网段
ip route-static 40.1.1.0 255.255.255.0 20.1.1.2      #配置默
认路由到达 40.1.1.0 网段
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 track bfd-session 1
#配置缺省路由，并联动 BFD 跟踪会话 1，若被跟踪链路发生
故障，则将该链路置为非激活状态，并在路由表中删除此条路
由
ip route-static 0.0.0.0 0.0.0.0 20.1.1.2 preference 80
#配置缺省路由，设置其路由优先级值为 80，令其成为备份路
由

```

RTB:

system-view



```
sysname RTB
interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
ip route-static 20.1.1.0 255.255.255.0 10.1.1.1
ip route-static 40.1.1.0 255.255.255.0 30.1.1.2
ip route-static 172.16.1.0 255.255.255.0 30.1.1.2
ip route-static 192.168.1.0 255.255.255.0 10.1.1.1
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 20.1.1.2 24
interface G0/0/1
ip address 40.1.1.1 24
ip route-static 10.1.1.0 255.255.255.0 20.1.1.1
ip route-static 30.1.1.0 255.255.255.0 40.1.1.2
ip route-static 172.16.1.0 255.255.255.0 40.1.1.2
ip route-static 192.168.1.0 255.255.255.0 20.1.1.1
```

```
RTD:
system-view
sysname RTD
bfd
interface G0/0/0
ip address 40.1.1.2 24
interface G0/0/1
ip address 30.1.1.2 24
interface G0/0/2
ip address 172.16.1.1 24
bfd 1 bind peer-ip 10.1.1.1 source-ip 30.1.1.2 auto
commit
ip route-static 0.0.0.0 0.0.0.0 30.1.1.1 track bfd-session 1
ip route-static 0.0.0.0 0.0.0.0 40.1.1.1 preference 80
ip route-static 10.1.1.0 255.255.255.0 30.1.1.1
ip route-static 20.1.1.0 255.255.255.0 40.1.1.1
```

测试:

在 RTB 与 RTD 之间的链路没有失效时, 查看 RTA 的路由表项:

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 17          Routes : 16

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
0/0/0               0.0.0.0/0 Static  60    0              RD   10.1.1.2          GigabitEthernet
0/0/0               10.1.1.0/24 Direct  0     0              D    10.1.1.1          GigabitEthernet
0/0/0               10.1.1.1/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/0               10.1.1.255/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/0               20.1.1.0/24 Direct  0     0              D    20.1.1.1          GigabitEthernet
0/0/1               20.1.1.1/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/1               20.1.1.255/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/1               30.1.1.0/24 Static  60    0              RD   10.1.1.2          GigabitEthernet
0/0/0               40.1.1.0/24 Static  60    0              RD   20.1.1.2          GigabitEthernet
0/0/1               127.0.0.0/8 Direct  0     0              D    127.0.0.1         InLoopBack0
0/0/1               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
0/0/1               192.168.1.0/24 Direct  0     0              D    192.168.1.1       GigabitEthernet
0/0/2               192.168.1.1/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/2               192.168.1.255/32 Direct  0     0              D    127.0.0.1         GigabitEthernet
0/0/2               255.255.255.255/32 Direct  0     0              D    127.0.0.1         InLoopBack0

[RTA]
```



在 RTB 与 RTD 之间的链路失效后，再次查看 RTA 的路由表项：

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 18          Routes : 16

Destination/Mask    Proto    Pre  Cost           Flags NextHop           Interface
-----
0/0/1 0.0.0.0/0          Static  80    0              RD   20.1.1.2             GigabitEthernet
0/0/1
0/0/0 10.1.1.0/24        Direct  0     0              D    10.1.1.1             GigabitEthernet
0/0/0
0/0/0 10.1.1.1/32        Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/0
0/0/0 10.1.1.255/32       Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/0
0/0/1 20.1.1.0/24        Direct  0     0              D    20.1.1.1             GigabitEthernet
0/0/1
0/0/1 20.1.1.1/32        Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/1
0/0/1 20.1.1.255/32       Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/1
0/0/0 30.1.1.0/24        Static  60    0              RD   10.1.1.2             GigabitEthernet
0/0/0
0/0/1 40.1.1.0/24        Static  60    0              RD   20.1.1.2             GigabitEthernet
0/0/1
0/0/1 127.0.0.0/8         Direct  0     0              D    127.0.0.1            InLoopBack0
0/0/1 127.0.0.1/32        Direct  0     0              D    127.0.0.1            InLoopBack0
127.255.255.255/32  Direct  0     0              D    127.0.0.1            InLoopBack0
0/0/2 192.168.1.0/24     Direct  0     0              D    192.168.1.1          GigabitEthernet
0/0/2
0/0/2 192.168.1.1/32     Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/2
0/0/2 192.168.1.255/32   Direct  0     0              D    127.0.0.1            GigabitEthernet
0/0/2
255.255.255.255/32  Direct  0     0              D    127.0.0.1            InLoopBack0

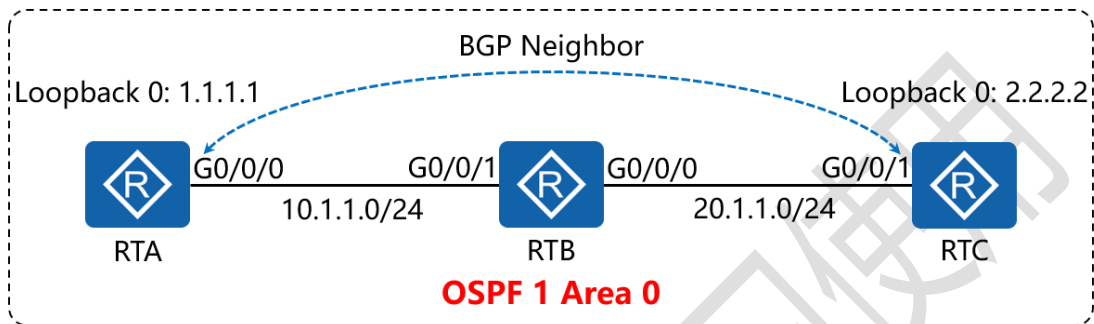
[RTA]
```

通过路由表项的输出结果可以明显看到，当 RTB 与 RTD 之间的链路失效后，在 BFD 的帮助下，RTA 的缺省路由立即执行了自动切换至备份路径（RTC）的操作

## 四十三、配置 BFD 与 BGP 联动实验组

### 网

#### 一、实验拓扑：



#### 二、实验目的：

RTA、RTB 与 RTC 首先运行 OSPF 路由协议，之后在 RTA 与 RTC 上配置 BGP，令其互为对等体关系，再在 RTA 与 RTC 上开启 BFD 功能，采用 BFD 控制数据方式实现当 RTA 或 RTC 与中间网络设备以及中间网络通道内部链路出现故障时，BFD 能够快速感知并通告 BGP 协议

#### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

bfd #全局开启 BFD 功能

interface G0/0/0 #进入相应接口

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

```

interface Loopback0    #创建环回接口 0
ip address 1.1.1.1 32   #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路
由器 ID
area 0                #创建 OSPF 区域 0
network 10.1.1.0 0.0.0.255    #通告其直连网段
network 1.1.1.1 0.0.0.0    #通告其环回接口地址
bgp 65001             #开启 BGP 路由功能, 并配置其 AS 号
router-id 1.1.1.1    #配置设备的 BGP 路由器 ID
peer 3.3.3.3 as-number 65001    #指定对等体的路由器 ID,
以及远程自治系统号码
peer 3.3.3.3 connect-interface LoopBack0    #指定自身
与对等体之间用哪个接口来承载更新
network 10.1.1.0 24    #通告自己的网段及子网掩码
undo summary automatic    #关闭自动汇总
peer 3.3.3.3 bfd enable    #在 BGP 协议中与对等体开启
BFD 功能

```

RTB:

system-view

sysname RTB

interface G0/0/0

```
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
network 2.2.2.2 0.0.0.0
```

RTC:

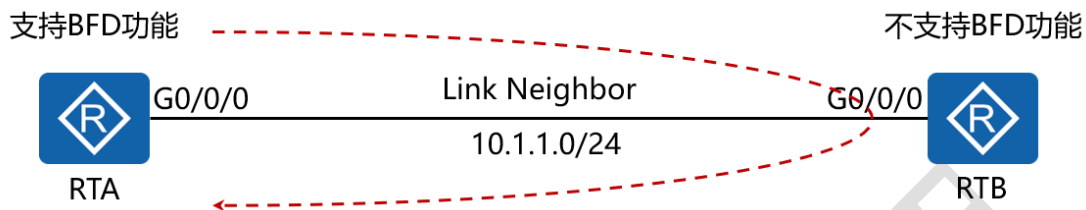
```
system-view
sysname RTC
bfd
interface G0/0/0
ip address 20.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
area 0
network 20.1.1.0 0.0.0.255
```

```
network 3.3.3.3 0.0.0.0  
bgp 65001  
router-id 3.3.3.3  
peer 1.1.1.1 as-number 65001  
peer 1.1.1.1 connect-interface LoopBack0  
network 20.1.1.0 24  
undo summary automatic  
peer 1.1.1.1 bfd enable
```



## 四十四、配置 BFD 单臂回声实验组网

### 一、实验拓扑：



### 二、实验目的：

RTA 与 RTB 直连，RTA 支持 BFD 功能，而 RTB 不支持 BFD 功能，在 RTA 上配置 BFD 单臂回声，从而实现转发链路的连通性检测功能

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
bfd                  #全局开启 BFD 功能
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24 #配置 IP 地址及子网掩码
bfd 1 bind peer-ip 10.1.1.2 interface g0/0/0 source-ip
10.1.1.1 one-arm-echo #配置 BFD 单臂回声功能，指定对
端地址与本地外出接口
discriminator local 100 #配置本地标识符
    
```

---

commit #确认开启此功能

RTB:

system-view

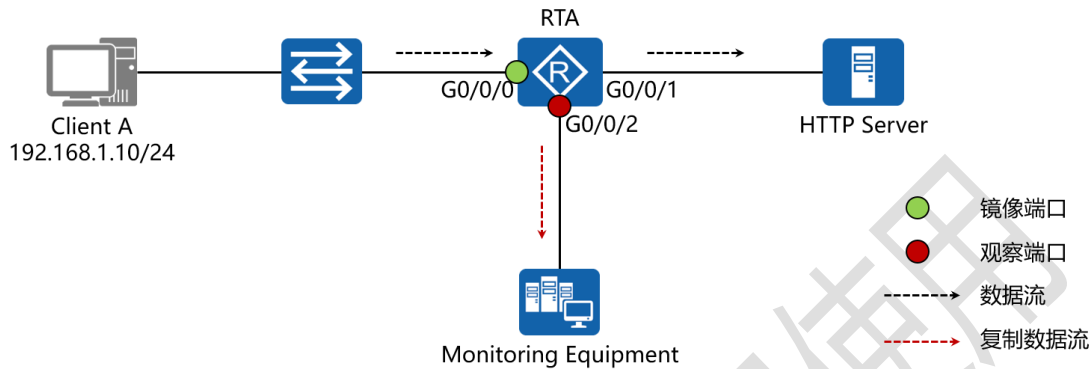
sysname RTB

interface G0/0/0

ip address 10.1.1.2 24

## 四十五、配置端口镜像实验组网

### 一、实验拓扑：



### 二、实验目的：

在 RTA 上配置端口镜像，将 Client A (192.168.1.10/24) 访问 HTTP Server 的所有流量全部镜像至 G0/0/2 接口所连接的监控设备上

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

observe-port interface G0/0/2 #将 G0/0/2 接口配置为观察端口

acl 2001 #创建基本访问控制列表

rule permit source 192.168.1.10 0 #匹配源地址  
192.168.1.10

traffic classifier *clienta* operator or #创建传输类别并指  
定其运行【或】运算

if-match acl 2001 #指定其匹配 ACL 2001

traffic behavior *clienta* #创建传输行为

mirror to observe-port #将传输类别匹配上的地址的流量  
镜像至观察端口

traffic policy *atnet* #创建传输策略

classifier *clienta* behavior *clienta* #应用传输类别与传  
输行为

interface G0/0/0 #进入相应的接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

traffic-policy *atnet* inbound #将传输策略应用在镜像端  
口的入方向上

interface G0/0/1 #进入相应的接口

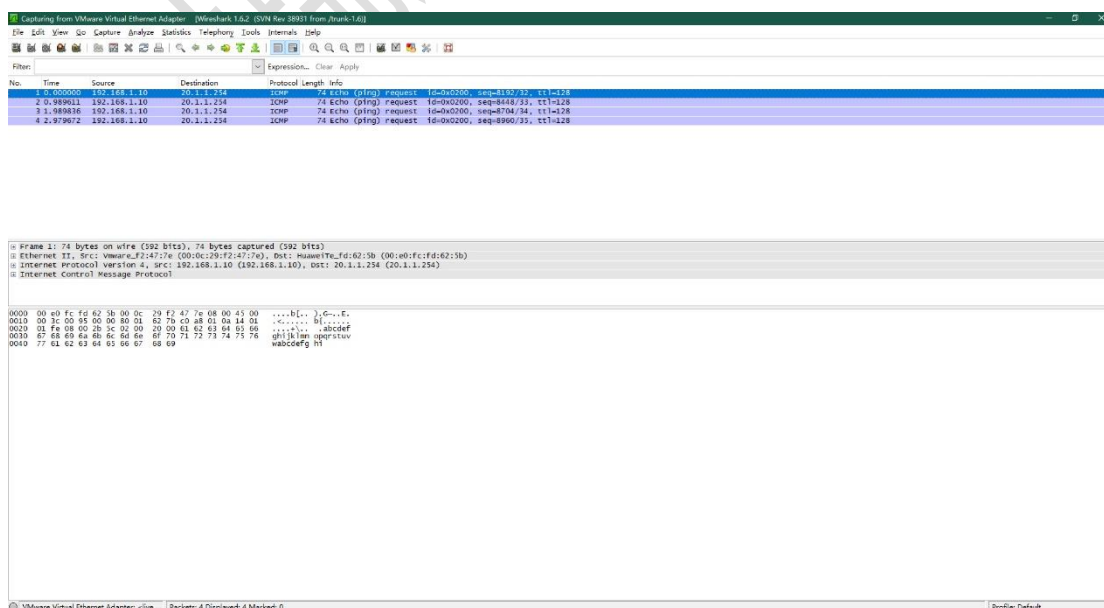
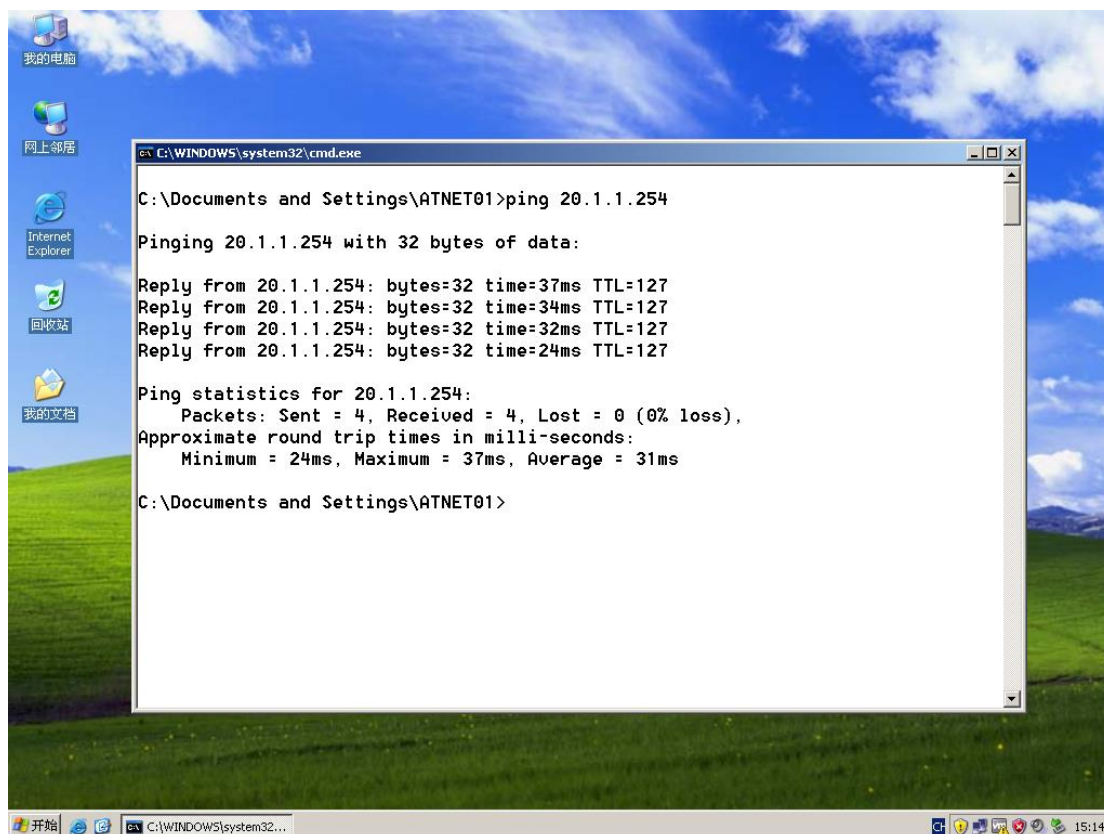
ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/2 #进入相应的接口

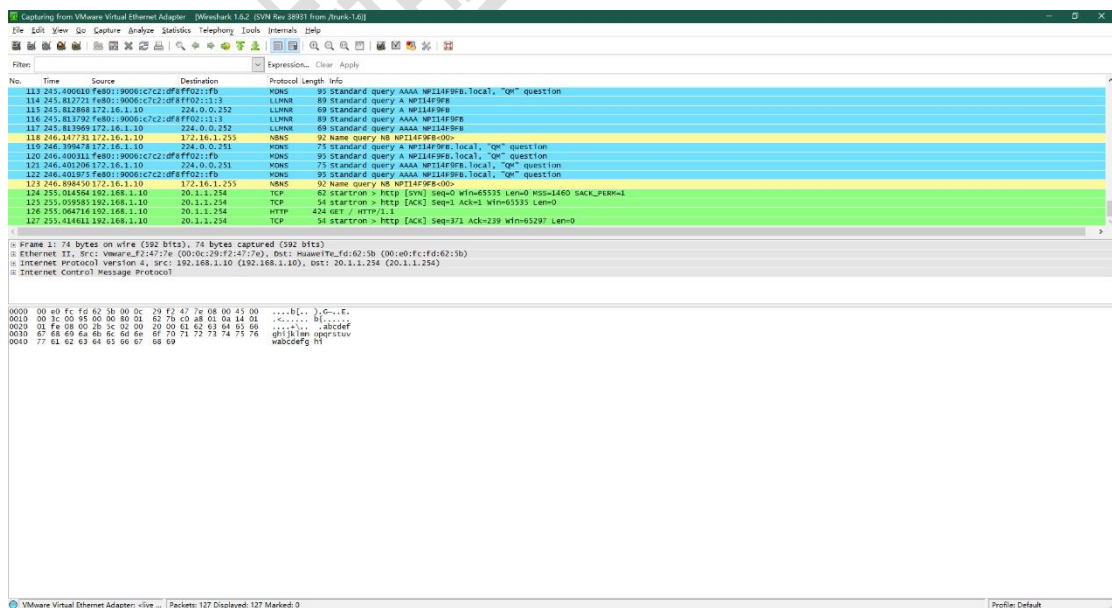
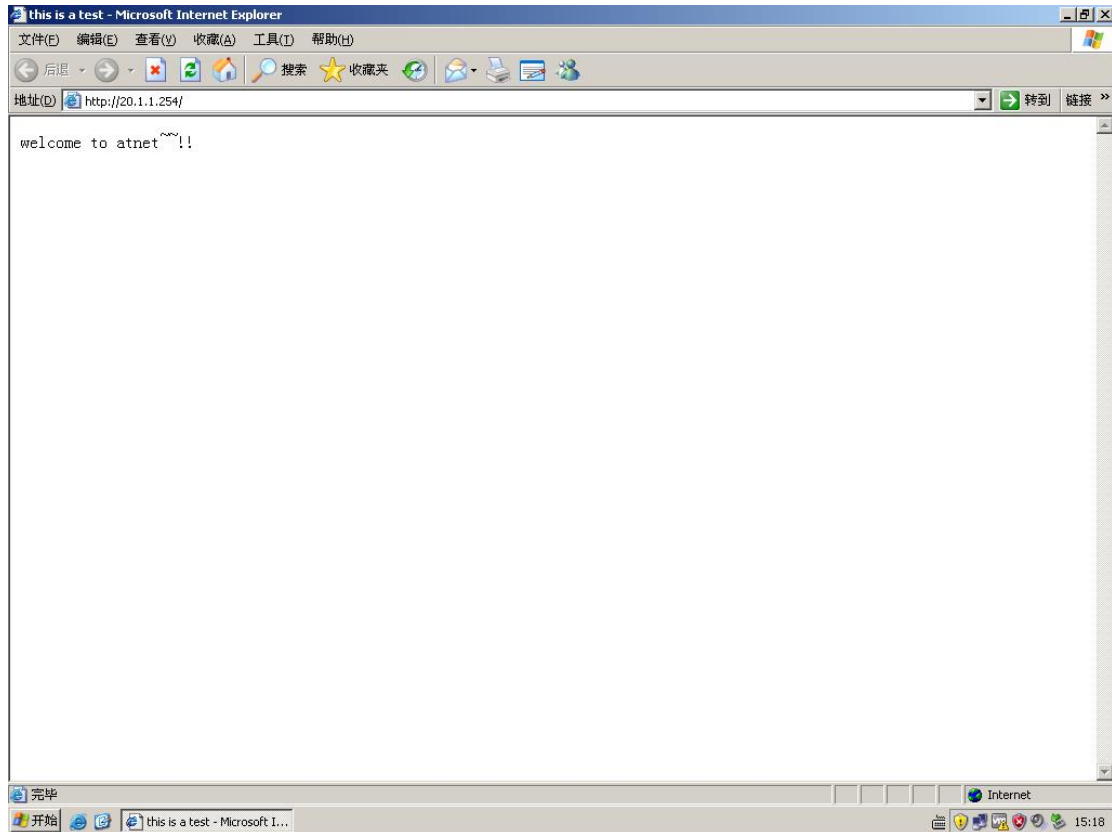
ip address 172.16.1.1 24 #配置 IP 地址及子网掩码

测试:

从 Client A 去 ping HTTP Server (20.1.1.254/24), 同时在监控设备上使用 Wireshark 观察结果:

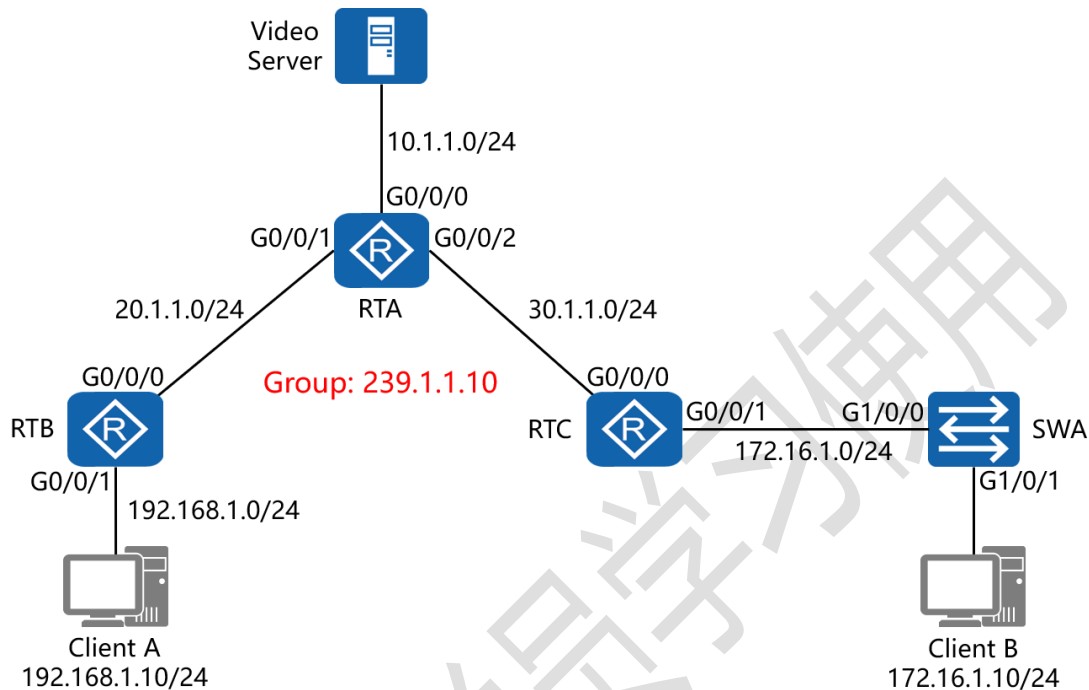


从 Client A 去访问 HTTP Server (20.1.1.254/24) 的网页，  
同时在监控设备上使用 Wireshark 观察结果：



## 四十六、配置组播综合实验组网

### 一、实验拓扑：



### 二、实验目的：

全网运行 OSPF 路由选择协议，在所有路由器上开启组播路由功能并配置使用 PIM-SM，使 RTA 成为候选 BSR 与候选 RP；令 Video Server 向组播组 239.1.1.10 发送组播数据；Client A 直接与 RTB 的 G0/0/1 接口相连，当 Client A 接收组播数据时，在 RTB 上观察组播组的动态加入与离开过程；RTC 与 SWA（使用 CE6800）相连，在 SWA 上开启 IGMP Snooping 与 IGMP Snooping proxy 功能，令 Client B 也能够正常接收来自 Video Server 的组播数据

### 三、实验步骤：

RTA:

```

system-view      #进入系统视图模式
sysname RTA     #给设备命名
multicast routing-enable    #开启组播路由功能
interface G0/0/0    #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
pim sm           #配置接口运行 PIM 的稀疏模式
interface G0/0/1    #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
pim sm           #配置接口运行 PIM 的稀疏模式
interface G0/0/2    #进入相应接口
ip address 30.1.1.1 24    #配置 IP 地址及子网掩码
pim sm           #配置接口运行 PIM 的稀疏模式
interface Loopback0    #创建环回接口 0
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
pim             #进入 PIM 的配置模式
c-bsr G0/0/0     #指定接口 G0/0/0 为候选 BSR
c-rp G0/0/0     #指定接口 G0/0/0 为候选 RP
c-bsr priority 200    #配置候选 BSR 的优先级为 200
c-rp priority 100    #配置候选 RP 的优先级为 100
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1，并指定其路
    
```



## 由器 ID

```

area 0      #创建 OSPF 区域 0

network 10.1.1.0 0.0.0.255  #通告其直连网段
network 20.1.1.0 0.0.0.255  #通告其直连网段
network 30.1.1.0 0.0.0.255  #通告其直连网段
    
```

RTB:

```

system-view
sysname RTB
multicast routing-enable
interface G0/0/0
ip address 20.1.1.2 24
pim sm
interface G0/0/1
ip address 192.168.1.1 24
igmp enable      #开启 IGMP 功能
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 20.1.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
    
```

RTC:

```
system-view
```

```
sysname RTC
```

```
multicast routing-enable
```

```
interface G0/0/0
```

```
ip address 30.1.1.2 24
```

```
pim sm
```

```
interface G0/0/1
```

```
ip address 172.16.1.1 24
```

```
igmp enable
```

```
interface Loopback0
```

```
ip address 3.3.3.3 32
```

```
ospf 1 router-id 3.3.3.3
```

```
area 0
```

```
network 30.1.1.0 0.0.0.255
```

```
network 172.16.1.0 0.0.0.255
```

SWA:

```
system-view immediately #进入系统视图模式并配置为让  
命令立即生效
```

```
sysname SWA
```

```
multicast routing-enable
```

igmp snooping enable #全局下启用 IGMP Snooping 功能

vlan 1 #进入 VLAN 1 的配置模式

igmp snooping enable #在 VLAN 下启用 IGMP Snooping 功能

igmp snooping proxy #在 VLAN 下启用 IGMP Snooping 代理功能

interface G1/0/0

undo shutdown #CE6800 交换机的端口默认

shutdown, 需手动启用

interface G1/0/1

undo shutdown

测试：

在 Client A 没有加入组播组接收组播数据时，在 RTB 上查看 IGMP 的组信息：

```
[RTB]display igmp group interface g0/0/1
[RTB]
```

通过查看发现没有任何的组成员加入

当 Client A 加入组播组 239.1.1.10 并收看 Video Server 发布的视频时，再次查看 RTB 的 IGMP 组信息：

```
[RTB]display igmp group interface g0/0/1
Interface group report information of VPN-Instance: public net
GigabitEthernet0/0/1(192.168.1.1):
  Total 1 IGMP Group reported
  Group Address      Last Reporter      Uptime             Expires
  239.1.1.10         192.168.1.10      00:00:04           00:02:06
[RTB]
```

发现组播组中立即出现组成员：192.168.1.10

在 SWA 上查看 VLAN 1 下的 IGMP Snooping 路由端口：

```
[SWA]display igmp snooping router-port vlan 1
Port Name                UpTime             Expires            Flags
-----
VLAN 1, 1 router-port(s)
GE1/0/0                   00h17m13s         00h02m46s        DYNAMIC
[SWA]
```

在 Client B 没有加入组播组接收组播数据时，在 SWA 上查看 IGMP Snooping 的端口信息：

```
[SWA]display igmp snooping port-info
-----
Flag: S:Static      D:Dynamic      M:Ssm-mapping
      A:Active      P:Protocol     T:Trill
              (Source, Group)  Port
Flag
-----
VLAN 1, 1 Entry(s)
              (*, 239.1.1.10)
-A-
-----
[SWA]
```

当 Client B 加入组播组 239.1.1.10 并收看 Video Server 发布的视频时，再次查看 SWA 的 IGMP Snooping 端口信息：

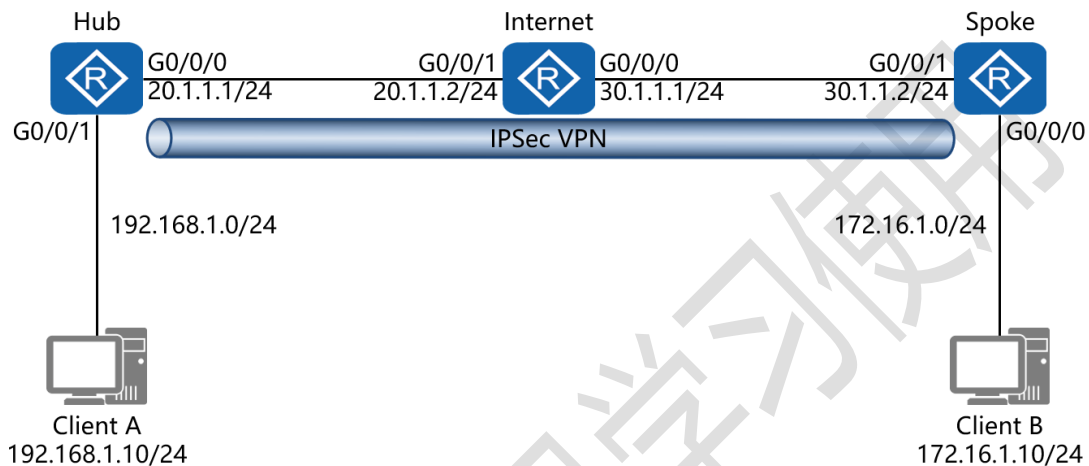
```
[SWA]display igmp snooping port-info
-----
Flag: S:Static      D:Dynamic      M:Ssm-mapping
      A:Active      P:Protocol     T:Trill
              (Source, Group)  Port
Flag
-----
VLAN 1, 1 Entry(s)
              (*, 239.1.1.10)
PA-
                                GE1/0/1
-D-
                                1 port(s) include
-----
[SWA]
```

发现组播组中立即出现成员端口：GE1/0/1

## 四十七、配置 IKE 方式的 IPsec VPN

### 实验组网

#### 一、实验拓扑：



#### 二、实验目的：

Hub 路由器为公司总部边界路由，Spoke 路由器为公司分部边界路由，Internet 路由器为互联网公有路由；在 Hub 与 Spoke 路由器上配置 IPsec VPN，令 Client A 与 Client B 可相互通讯

#### 三、实验步骤：

Hub:

system-view #进入系统视图模式

sysname Hub #给设备命名

interface G0/0/0 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```

ip address 192.168.1.1 24      #配置 IP 地址及子网掩码
acl number 3001      #创建高级 ACL
rule 5 permit ip source 192.168.1.0 0.0.0.255 destination
172.16.1.0 0.0.0.255      #定义感兴趣流，允许本地网段
192.168.1.0/24 访问远端网段 172.16.1.0/24
ipsec proposal huawei      #创建并进入 IPsec 提议视图
esp authentication-algorithm sha1      #配置 ESP 协议使用的
认证算法为 sha1
ike peer spoke v1      #使用 IKE 版本 1 并指定对端名称
pre-shared-key cipher P@ssw0rd      #使用预共享密钥并
创建加密密钥
remote-address 30.1.1.2      #指定远端公网地址
ipsec policy easthome 1 isakmp      #创建 IPsec 策略集
security acl 3001      #调用高级 ACL 定义的感兴趣流
ike-peer spoke      #调用先前创建的 IKE 对等体
proposal huawei      #调用先前创建的 IPsec 提议视图
interface G0/0/0      #进入相应接口
ipsec policy easthome      #在外出接口上调用该策略集
ip route-static 0.0.0.0 0 20.1.1.2      #配置缺省路由

```

Internet:

```
interface G0/0/0
```

---

ip address 30.1.1.1 24

interface G0/0/1

ip address 20.1.1.2 24

Spoke:

system-view

sysname Spoke

interface G0/0/0

ip address 172.16.1.1 24

interface G0/0/1

ip address 30.1.1.2 24

acl number 3001

rule 5 permit ip source 172.16.1.0 0.0.0.255 destination

192.168.1.0 0.0.0.255

ipsec proposal *huawei*

esp authentication-algorithm sha1

ike peer *hub* v1

pre-shared-key cipher *P@ssword*

remote-address 20.1.1.1

ipsec policy *easthome* 1 isakmp

security acl 3001

ike-peer *hub*



proposal *huawei*

interface G0/0/1

ipsec policy *easthome*

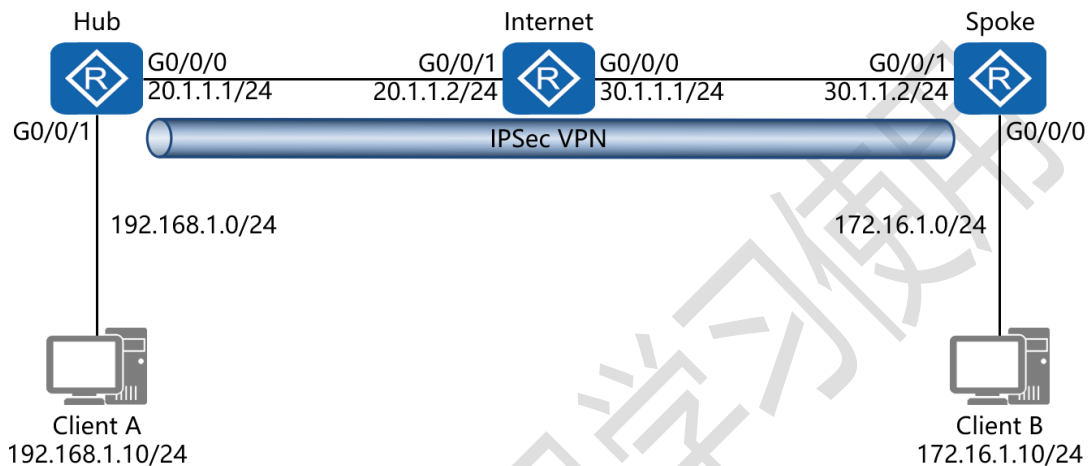
ip route-static 0.0.0.0 0 30.1.1.1

仅供瑞通学员学习使用

## 四十八、配置手动方式的 IPsec VPN

### 实验组网

#### 一、实验拓扑：



#### 二、实验目的：

Hub 路由器为公司总部边界路由，Spoke 路由器为公司分部边界路由，Internet 路由器为互联网公有路由；在 Hub 与 Spoke 路由器上配置 IPsec VPN，令 Client A 与 Client B 可相互通讯

#### 三、实验步骤：

Hub:

system-view #进入系统视图模式

sysname Hub #给设备命名

interface G0/0/0 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```

ip address 192.168.1.1 24      #配置 IP 地址及子网掩码
acl number 3001      #创建高级 ACL
rule 5 permit ip source 192.168.1.0 0.0.0.255 destination
172.16.1.0 0.0.0.255      #定义感兴趣流，允许本地网段
192.168.1.0/24 访问远端网段 172.16.1.0/24
ipsec proposal huawei      #创建并进入 IPsec 提议视图
esp authentication-algorithm sha1      #配置 ESP 协议使用的
认证算法为 sha1
ipsec policy easthome 1 manual      #创建 IPsec 策略集并指
定为手工模式
security acl 3001      #调用高级 ACL 定义的感兴趣流
proposal huawei      #调用先前创建的 IPsec 提议视图
tunnel local 20.1.1.1      #指定隧道本端地址
tunnel remote 30.1.1.2      #指定隧道远端地址
sa spi inbound esp 54321      #配置安全联盟入方向的安全参
数索引 (SPI); 本端入方向安全联盟的 SPI 值必须与对端出方
向的安全联盟的 SPI 值相同
sa string-key inbound esp cipher P@ssw0rd      #配置安全
联盟入方向的认证密钥
sa spi outbound esp 12345      #配置安全联盟出方向的安全
参数索引 (SPI); 本端出方向安全联盟的 SPI 值必须与对端
入方向的安全联盟的 SPI 值相同

```

sa string-key outbound esp cipher *P@ssw0rd* #配置安

全联盟出方向的认证密钥

interface G0/0/0 #进入相应接口

ipsec policy *easthome* #在外出接口上调用该策略集

ip route-static 0.0.0.0 0.0.0.0 20.1.1.2 #配置缺省路由

Internet:

interface G0/0/0

ip address 30.1.1.1 24

interface G0/0/1

ip address 20.1.1.2 24

Spoke:

system-view

sysname Spoke

interface G0/0/0

ip address 172.16.1.1 24

interface G0/0/1

ip address 30.1.1.2 24

acl number 3001

rule 5 permit ip source 172.16.1.0 0.0.0.255 destination

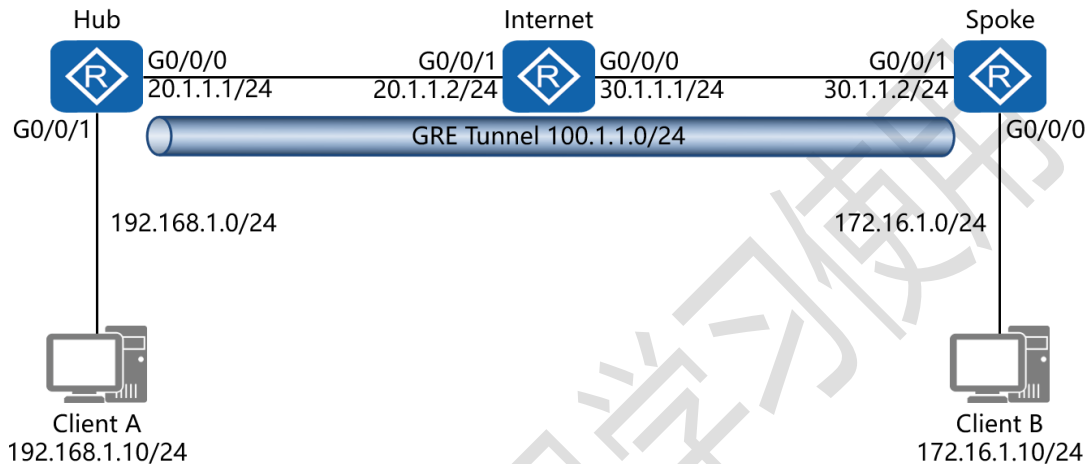
192.168.1.0 0.0.0.255

```
ipsec proposal huawei  
esp authentication-algorithm sha1  
ipsec policy easthome 1 manual  
security acl 3001  
proposal huawei  
tunnel local 30.1.1.2  
tunnel remote 20.1.1.1  
sa spi inbound esp 12345  
sa string-key inbound esp cipher P@ssw0rd  
sa spi outbound esp 54321  
sa string-key outbound esp cipher P@ssw0rd  
interface G0/0/1  
ipsec policy easthome  
ip route-static 0.0.0.0 0.0.0.0 30.1.1.1
```

# 四十九、配置 GRE VPN 实验组网

## (一)

### 一、实验拓扑：



### 二、实验目的：

Hub 路由器为公司总部边界路由，Spoke 路由器为公司分部边界路由，Internet 路由器为互联网公有路由；在 Hub 与 Spoke 路由器上配置 GRE Tunnel，令 Client A 与 Client B 可相互通讯

### 三、实验步骤：

Hub:

system-view #进入系统视图模式

sysname Hub #给设备命名

interface G0/0/0 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

```

ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface tunnel0/0/0      #创建并进入隧道接口
ip address 100.1.1.1 24    #配置隧道内 IP 地址及子网掩码
tunnel-protocol gre       #指定隧道协议为 GRE
source 20.1.1.1           #指定隧道的源 IP 地址
destination 30.1.1.2      #指定隧道的目的 IP 地址
ip route-static 0.0.0.0 0 20.1.1.2    #配置缺省路由
ip route-static 172.16.1.0 24 tunnel0/0/0    #配置静态路由，指定到达对端内部网段的外出接口为隧道接口

```

Internet:

```

interface G0/0/0
ip address 30.1.1.1 24
interface G0/0/1
ip address 20.1.1.2 24

```

Spoke:

```

system-view
sysname Spoke
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1

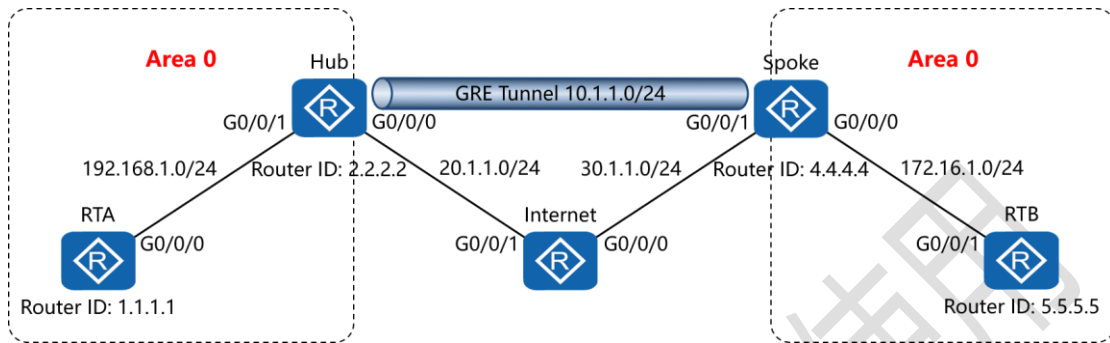
```

```
ip address 30.1.1.2 24
interface tunnel0/0/0
ip address 100.1.1.2 24
tunnel-protocol gre
source 30.1.1.2
destination 20.1.1.1
ip route-static 0.0.0.0 0 30.1.1.1
ip route-static 192.168.1.0 24 tunnel0/0/0
```



## 五十、配置 GRE VPN 实验组网（二）

### 一、实验拓扑：



### 二、实验目的：

RTA 与 Hub 路由器为公司总部网络，Spoke 与 RTB 为公司分部网络，公司总部与分部均运行 OSPF 路由选择协议，在 Hub 和 Spoke 路由器上运行 GRE Tunnel，令总部与分部的 OSPF 路由协议可以相互学习彼此的路由条目，进而实现相互通讯

### 三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24 #配置 IP 地址及子网掩码
interface Loopback0 #创建并进入环回接口
ip address 1.1.1.1 32 #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1 #进入 OSPF 进程 1，并指定其路
    
```

## 由器 ID

area 0 #创建 OSPF 区域 0

network 192.168.1.0 0.0.0.255 #通告其直连网段

Hub:

system-view

sysname Hub

interface G0/0/0

ip address 20.1.1.1 24

interface G0/0/1

ip address 192.168.1.2 24

interface Loopback0

ip address 2.2.2.2 32

interface tunnel0/0/0 #创建并进入隧道接口

ip address 10.1.1.1 24 #配置隧道内 IP 地址及子网掩码

tunnel-protocol gre #指定隧道协议为 GRE

source 20.1.1.1 #指定隧道的源 IP 地址

destination 30.1.1.2 #指定隧道的目的 IP 地址

keepalive period 3 #开启 GRE 隧道接口的 Keepalive 检测功能，并指定检测报文的发送周期为 3s

ospf 1 router-id 2.2.2.2

area 0

```
network 192.168.1.0 0.0.0.255  
network 10.1.1.0 0.0.0.255  
ip route-static 0.0.0.0 0 20.1.1.2 #配置缺省路由
```

Internet:

```
interface G0/0/0  
ip address 30.1.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24
```

Spoke:

```
system-view  
sysname Spoke  
interface G0/0/0  
ip address 172.16.1.1 24  
interface G0/0/1  
ip address 30.1.1.2 24  
interface Loopback0  
ip address 4.4.4.4 32  
interface tunnel0/0/0  
ip address 10.1.1.2 24  
tunnel-protocol gre
```

```
source 30.1.1.2  
destination 20.1.1.1  
ospf 1 router-id 4.4.4.4  
area 0  
network 172.16.1.0 0.0.0.255  
network 10.1.1.0 0.0.0.255  
ip route-static 0.0.0.0 0 30.1.1.1
```

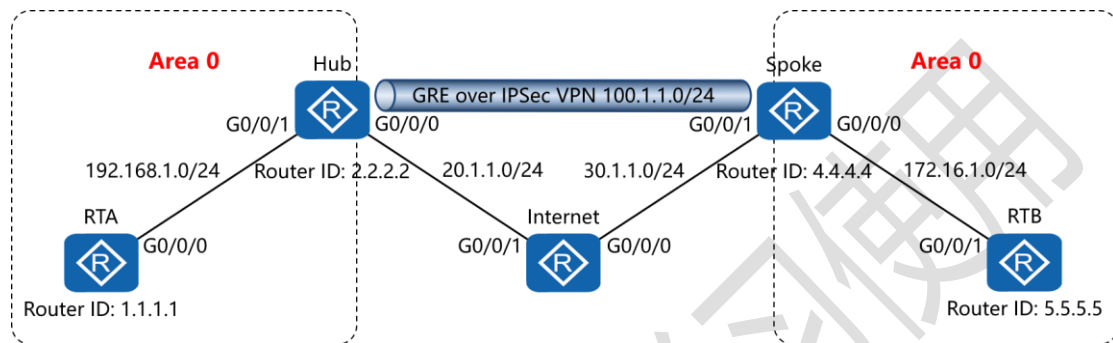
RTB:

```
system-view  
sysname RTB  
interface G0/0/1  
ip address 172.16.1.2 24  
interface Loopback0  
ip address 5.5.5.5 32  
ospf 1 router-id 5.5.5.5  
area 0  
network 172.16.1.0 0.0.0.255
```

# 五十一、配置 GRE over IPsec VPN

## 实验组网

### 一、实验拓扑：



### 二、实验目的：

RTA 与 Hub 路由器为公司总部网络，Spoke 与 RTB 为公司分部网络，公司总部与分部均运行 OSPF 路由选择协议，在 Hub 和 Spoke 路由器上运行 GRE over IPsec VPN，令总部与分部的 OSPF 路由协议可以相互学习彼此的路由条目，进而实现相互通讯

### 三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

```

interface Loopback0    #创建并进入环回接口
ip address 1.1.1.1 32   #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
                        器 ID
area 0                #创建 OSPF 区域 0
network 192.168.1.0 0.0.0.255    #通告其直连网段

Hub:
system-view
sysname Hub
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 192.168.1.2 24
interface Loopback0
ip address 2.2.2.2 32
acl 3001              #创建高级 ACL
rule 5 permit ip source 20.1.1.1 0 destination 30.1.1.2 0
#定义感兴趣流, 允许本端外网地址 20.1.1.1 访问远端外网地址 30.1.1.2
ipsec proposal huawei    #创建并进入 IPSec 提议视图
esp authentication-algorithm md5    #配置 ESP 协议使用

```

的认证算法为 md5

esp encryption-algorithm 3des #配置 ESP 协议使用的加

密算法为 3des

ike peer *spoke* v1 #使用 IKE 版本 1 并指定对端名称

pre-shared-key cipher *P@sswOrd* #使用预共享密钥并

创建加密密钥

remote-address 30.1.1.2 #指定远端外网地址

ipsec policy *easthome* 1 isakmp #创建 IPsec 策略集

security acl 3001 #调用高级 ACL 定义的感兴趣流

ike-peer *spoke* #调用先前创建的 IKE 对等体

proposal *huawei* #调用先前创建的 IPsec 提议视图

interface G0/0/0

ipsec policy *easthome* #在外出接口上调用该策略集

interface tunnel0/0/0 #创建并进入隧道接口

ip address 100.1.1.1 24 #配置隧道内 IP 地址及子网掩码

tunnel-protocol gre #指定隧道协议为 GRE

source 20.1.1.1 #指定隧道的源 IP 地址

destination 30.1.1.2 #指定隧道的目的 IP 地址

ospf 1 router-id 2.2.2.2

area 0

network 192.168.1.0 0.0.0.255

network 100.1.1.0 0.0.0.255

---

ip route-static 0.0.0.0 0 20.1.1.2 #配置缺省路由

Internet:

interface G0/0/0

ip address 30.1.1.1 24

interface G0/0/1

ip address 20.1.1.2 24

Spoke:

system-view

sysname Spoke

interface G0/0/0

ip address 172.16.1.1 24

interface G0/0/1

ip address 30.1.1.2 24

interface Loopback0

ip address 4.4.4.4 32

acl 3001

rule 5 permit ip source 30.1.1.2 0 destination 20.1.1.1 0

ipsec proposal *huawei*

esp authentication-algorithm md5

esp encryption-algorithm 3des



```
ike peer hub v1
pre-shared-key cipher P@ssw0rd
remote-address 20.1.1.1
ipsec policy easthome 1 isakmp
security acl 3001
ike-peer hub
proposal huawei
interface G0/0/1
ipsec policy easthome
interface tunnel0/0/0
ip address 100.1.1.2 24
tunnel-protocol gre
source 30.1.1.2
destination 20.1.1.1
ospf 1 router-id 4.4.4.4
area 0
network 172.16.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
ip route-static 0.0.0.0 0 30.1.1.1
```

RTB:

system-view

sysname RTB

interface G0/0/1

ip address 172.16.1.2 24

interface Loopback0

ip address 5.5.5.5 32

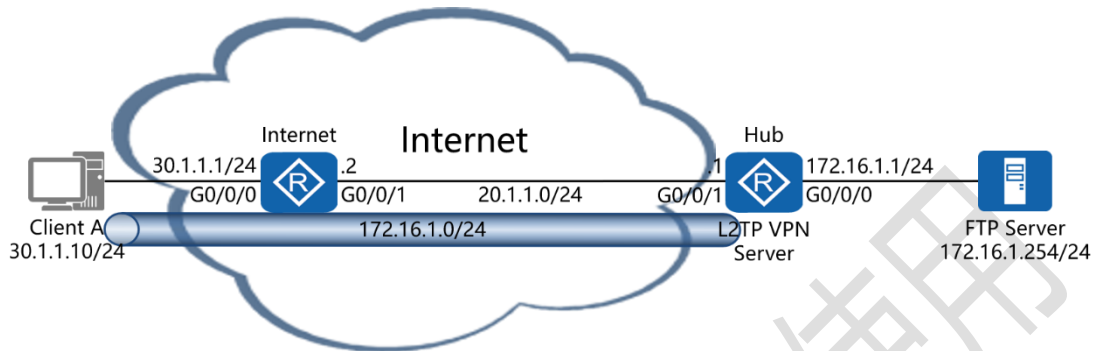
ospf 1 router-id 5.5.5.5

area 0

network 172.16.1.0 0.0.0.255

## 五十二、配置 L2TP VPN 实验组网

### 一、实验拓扑：



### 二、实验目的：

Hub 路由器为公司总部边界路由，在 Hub 路由器上配置 L2TP VPN，令连接在 Internet 路由器上的 Client A 能够通过 secoclient 软件正常拨入，与 Hub 路由器建立 L2TP 隧道

### 三、实验步骤：

Hub:

```

system-view          #进入系统视图模式
sysname Hub         #给设备命名
interface G0/0/0     #进入相应接口
ip address 172.16.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 20.1.1.1 24    #配置 IP 地址及子网掩码
aaa                 #进入 AAA 的配置模式
local-user easthome password cipher P@ssword #创
    
```

## 建用户及登录密钥

local-user *easthome* service-type ppp #配置该用户的服  
务类型为 PPP

ip pool *l2tpvpn* #创建地址池并命名

network 192.168.1.0 mask 24 #配置地址池内可分配的地址段及掩码

gateway-list 192.168.1.1 #配置分配的网关

interface Virtual-Template1 #创建并进入虚拟模板接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

ppp authentication-mode chap #配置认证模式使用

## CHAP

remote address pool *l2tpvpn* #指定远端用户从该地址池中获取 IP 地址

l2tp enable #开启 L2TP 功能

l2tp-group 1 #创建并进入 L2TP 组

mandatory-chap #启用 CHAP 的重协商功能

undo tunnel authentication #关闭隧道认证功能

mandatory-lcp #启用 LCP 的重协商功能

allow l2tp virtual-template 1 #允许 L2TP 绑定虚拟模板接口

tunnel name *easthome* #为隧道命名

ip route-static 0.0.0.0 0 20.1.1.2 #配置缺省路由

Internet:

interface G0/0/0

ip address 30.1.1.1 24

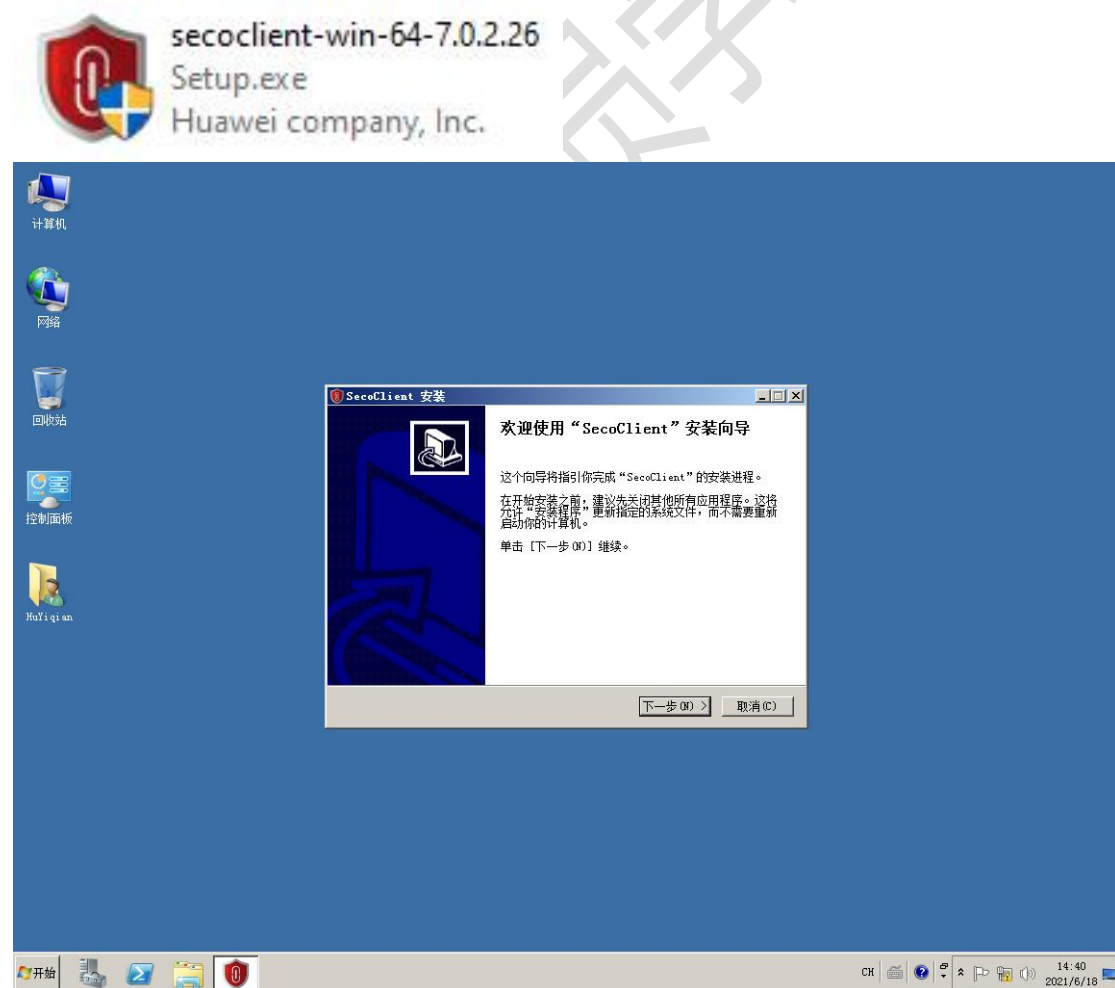
interface G0/0/1

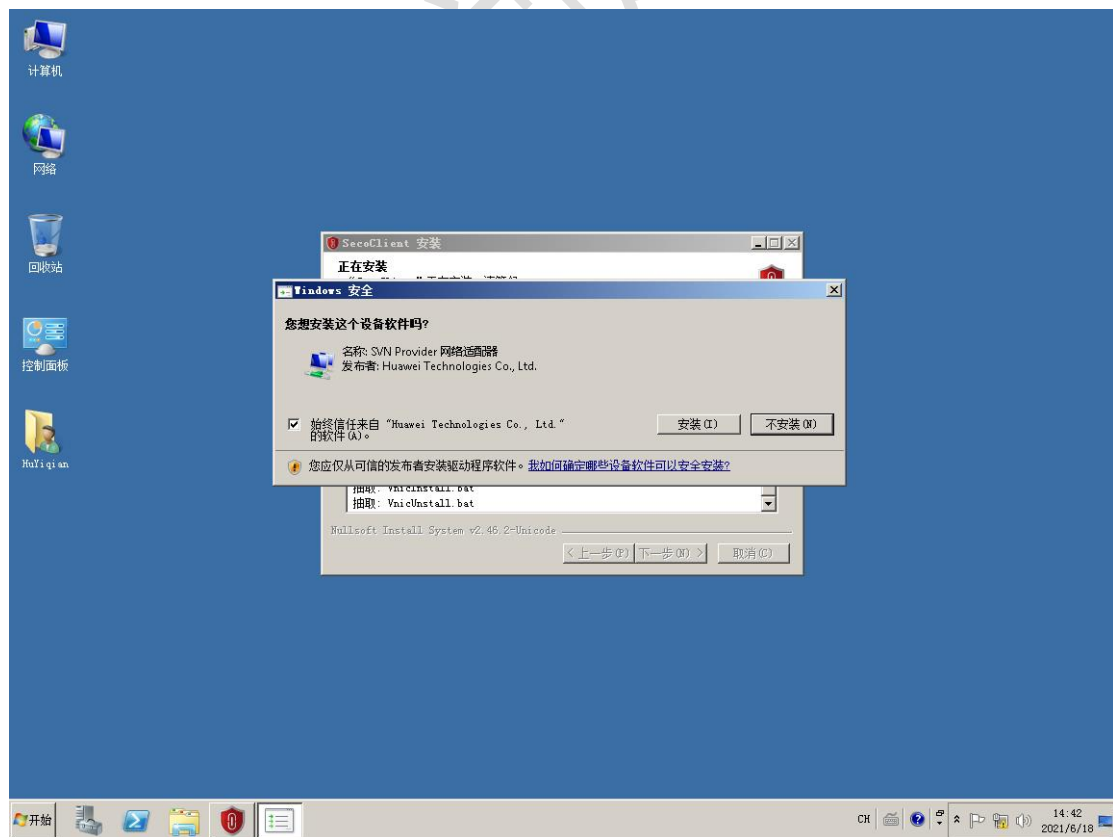
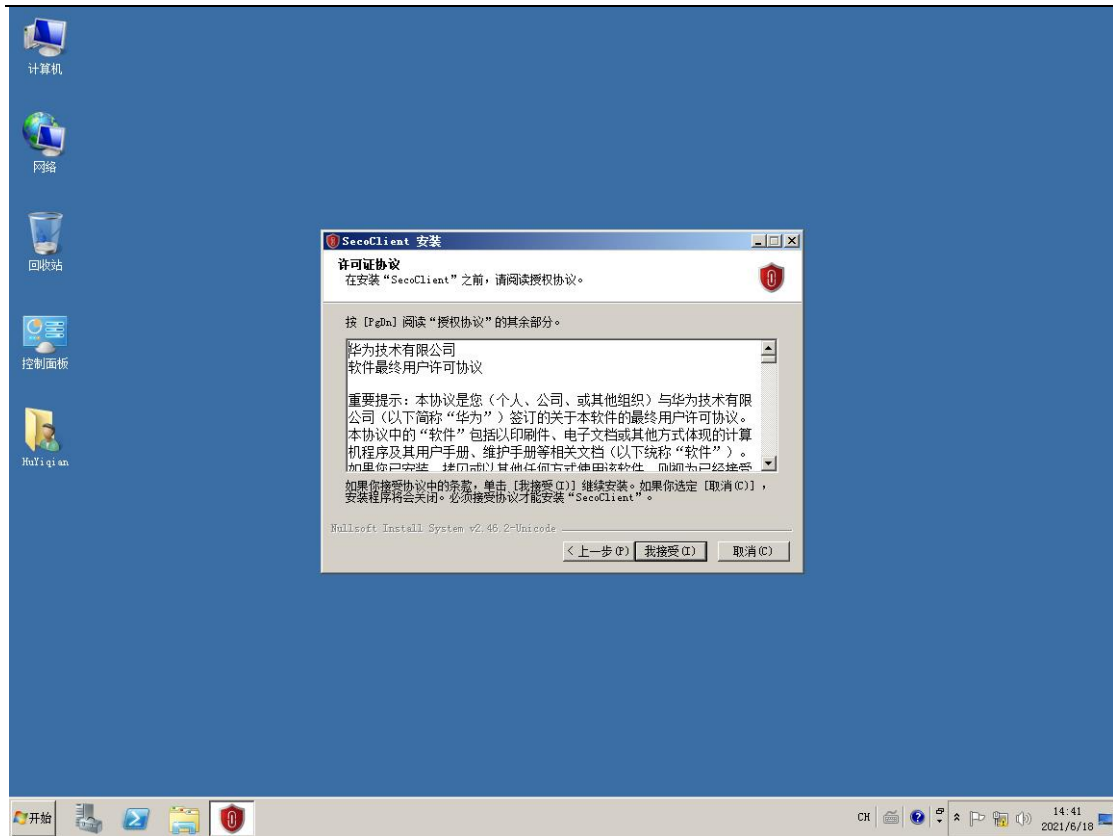
ip address 20.1.1.2 24

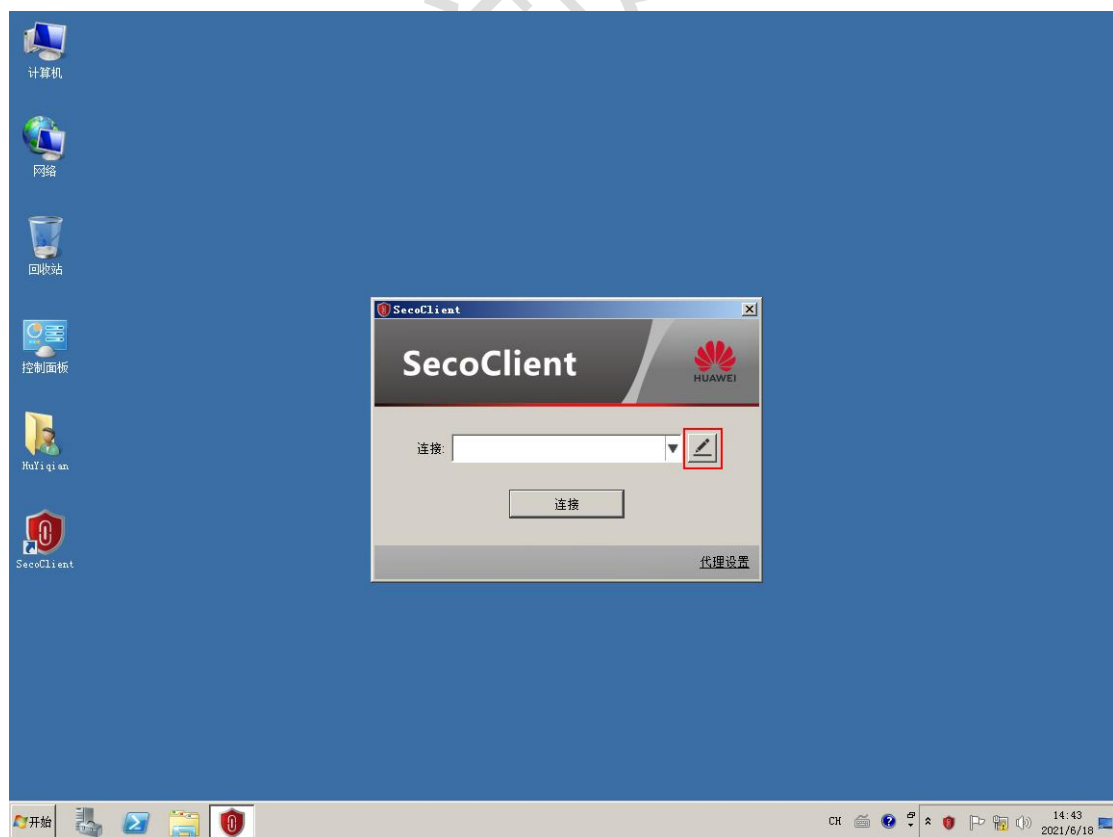
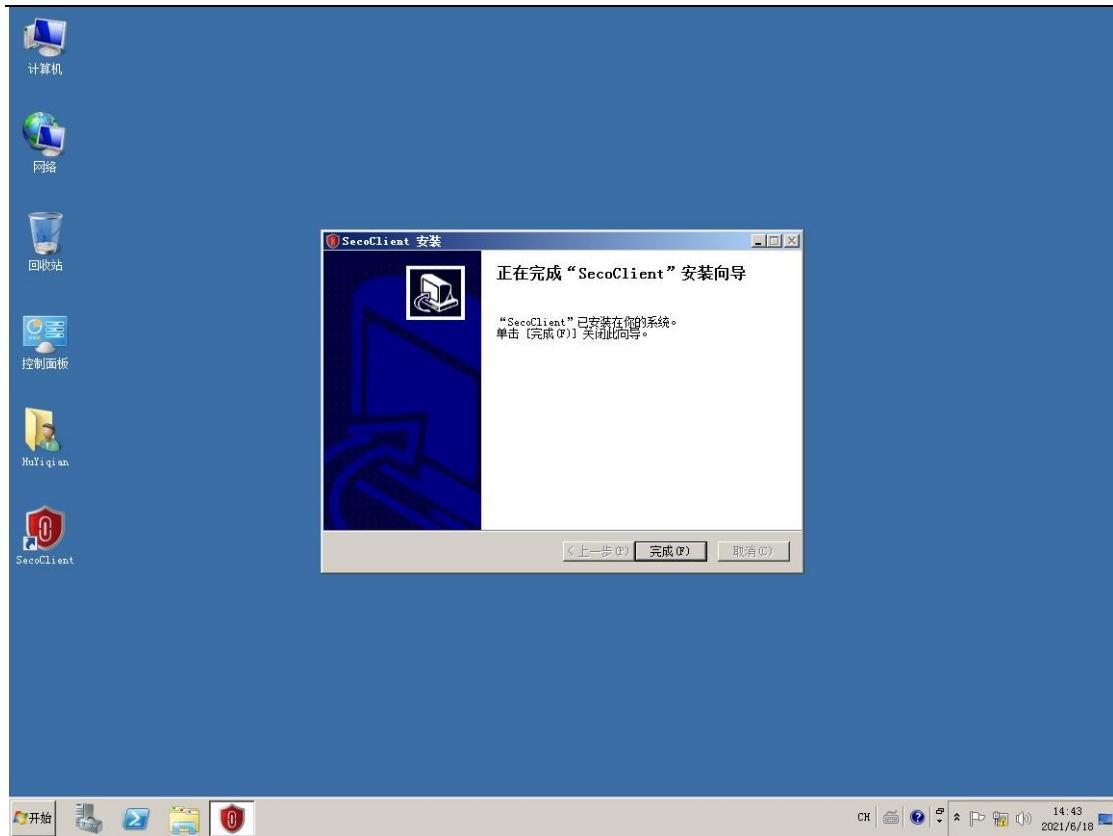
Client A:

在客户端上安装 secoclient 【VPN 客户端软件】

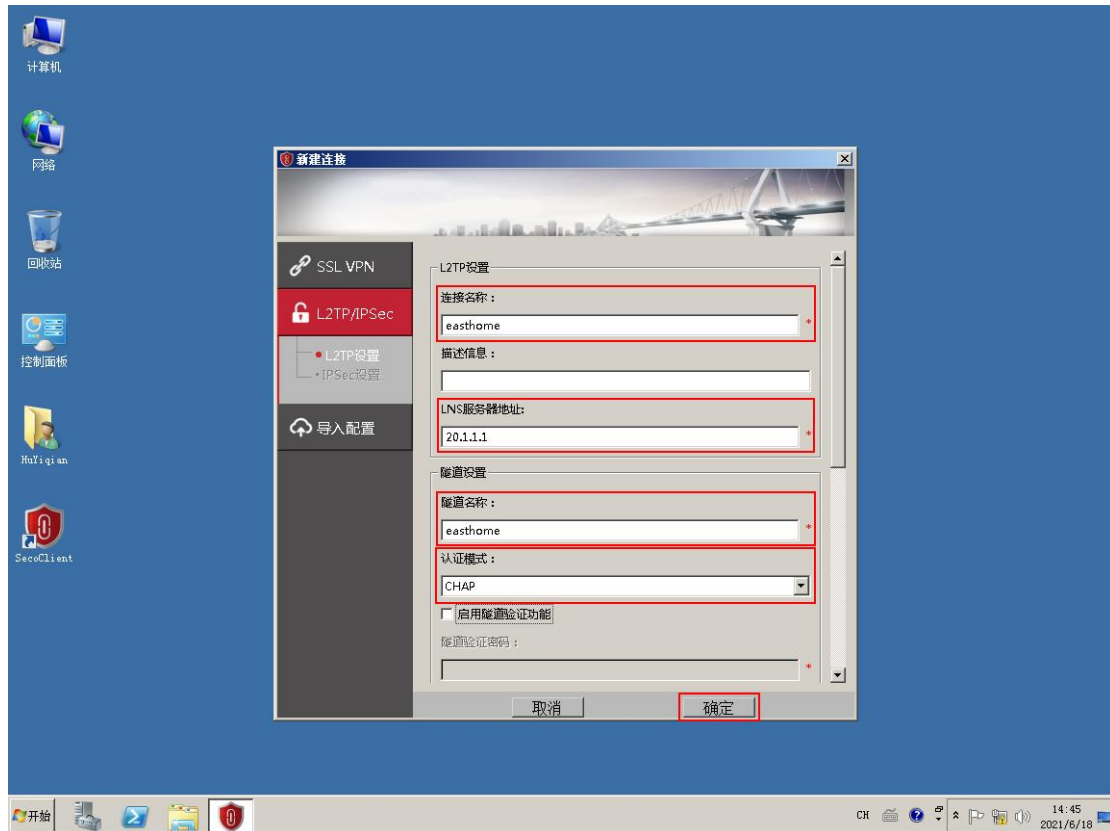
注：客户端使用的操作系统最低版本要求为 Windows Vista





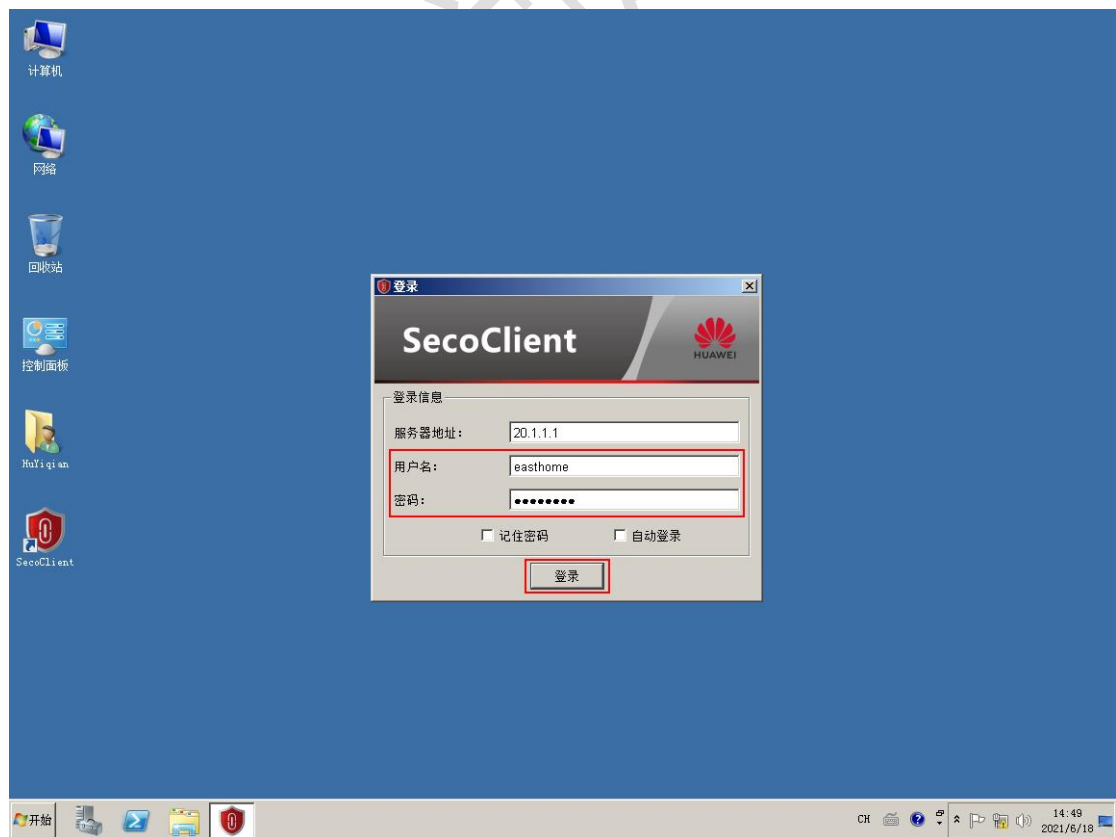
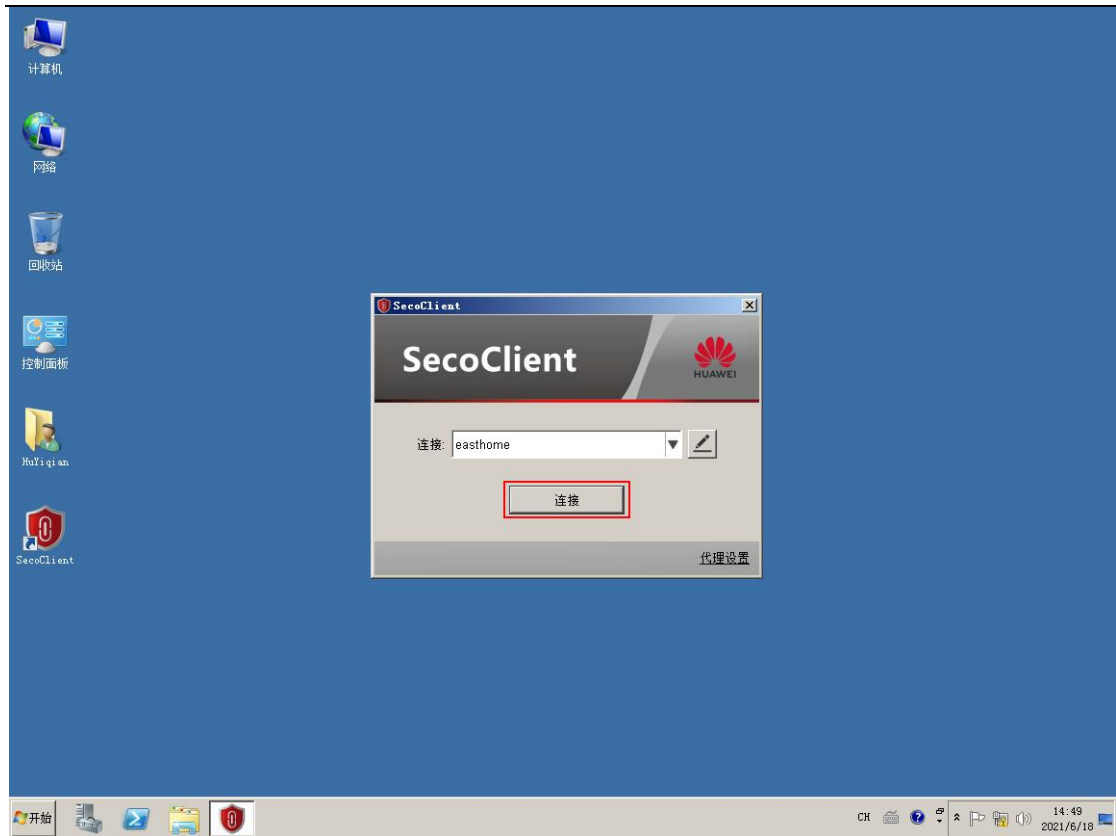


选择左侧的【L2TP/IPSec】，之后填写【连接名称（可随意填写）】、【LNS 服务器地址（Hub 路由器的外网接口地址）】、【隧道名称（填写路由器上配置的隧道名称）】、【认证模式（选择路由器上配置的认证模式）】

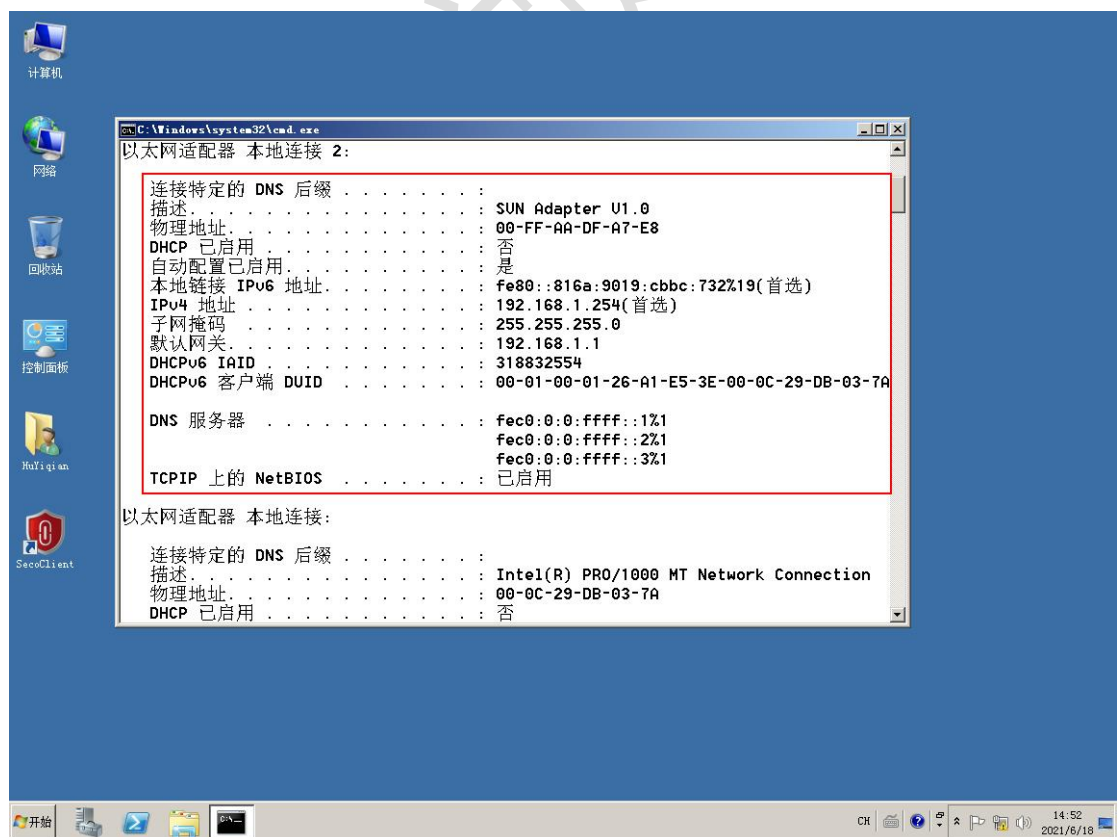
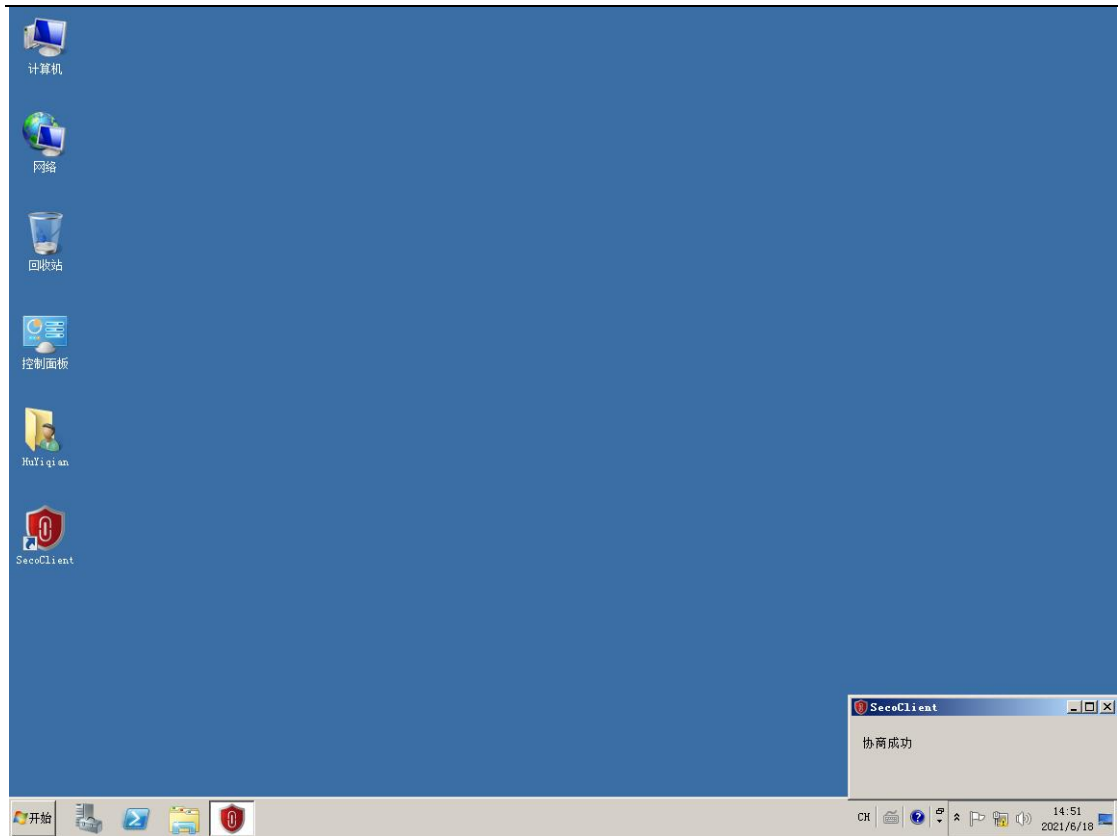


全部填写完毕后点击【确定】





填写完用户名及密码后，点击【登录】



查看客户端获取的 IP 地址、子网掩码、网关等信息

测试：

查看 Hub 路由器上 L2TP 隧道的建立情况：

```
[Hub]display l2tp tunnel

Total tunnel = 1
LocalTID RemoteTID RemoteAddress      Port    Sessions RemoteName
1         131         30.1.1.10      42246  1         easthome
[Hub]
```

查看 Hub 路由器上 L2TP 的会话情况：

```
[Hub]display l2tp session

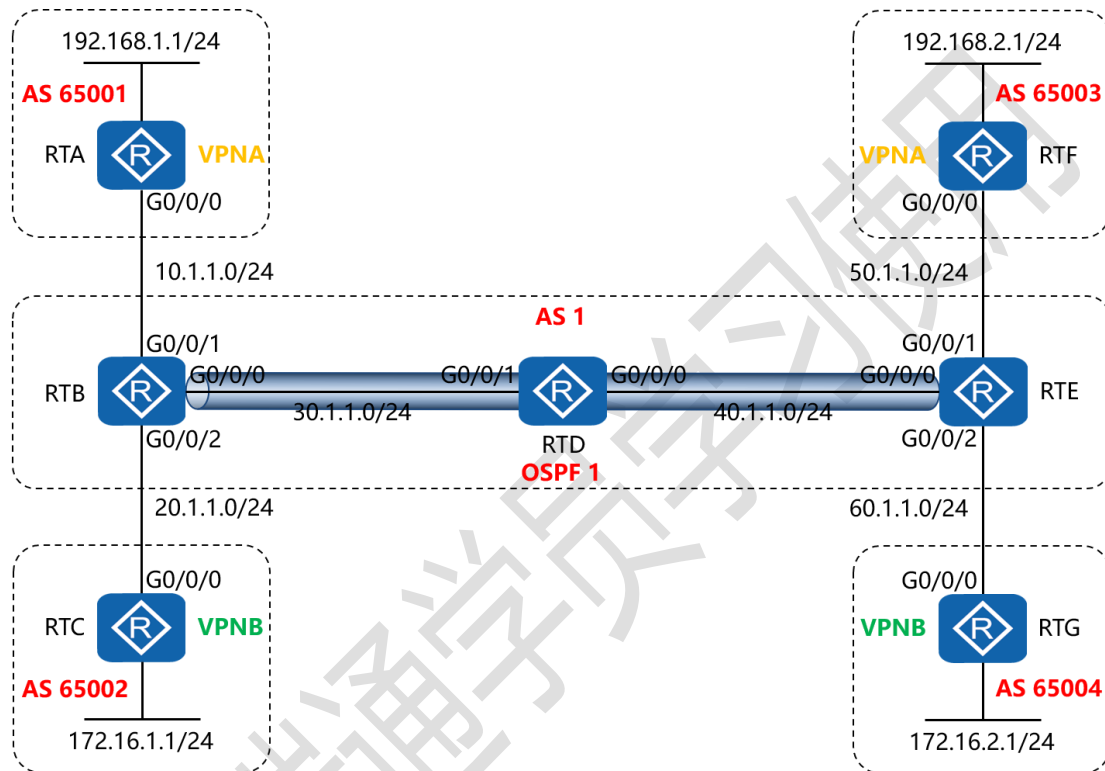
LocalSID  RemoteSID  LocalTID
1         131       1

Total session = 1
[Hub]
```

# 五十三、配置 MBGP MPLS VPN 实验

## 组网

### 一、实验拓扑：



### 二、实验目的：

RTA (AS 65001) 与 RTF (AS 65003) 为同一家公司的两地网络，RTC (AS 65002) 与 RTG (AS 65004) 为另一家公司的两地网络，RTB、RTD、RTE 为运营商网络，内部 IGP 使用 OSPF 连通，外网构建 BGP 网络，令 RTB 与 RTE 之间实现 MPLS VPN，在穿越 BGP 网络环境下实现公司内部的通信

### 三、实验步骤:

RTA:

```

system-view      #进入系统视图模式
sysname RTA     #给设备命名
interface G0/0/0  #进入相应的接口
ip address 10.1.1.1 24  #配置 IP 地址及子网掩码
interface LoopBack0  #进入 Loopback 0 接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
rip 1           #开启 RIP 路由协议进程 1
version 2       #启用 RIP 版本 2
network 10.0.0.0  #通告自己直连的网段
network 192.168.1.0  #通告自己直连的网段
undo summary    #关闭自动汇总
    
```

RTB:

```

system-view
sysname RTB
router id 1.1.1.1  #配置路由器 ID
mpls lsr-id 1.1.1.1  #配置 MPLS 标签交换路由器 ID
mpls  #开启多协议标签交换功能
mpls ldp  #开启 MPLS 标签分发协议
interface G0/0/0
    
```

```

ip address 30.1.1.1 24

mpls      #接口下开启多协议标签交换功能

mpls ldp  #接口下开启 MPLS 标签分发协议

interface G0/0/1

ip binding vpn-instance VPNA      #配置接口与 VPN 实例
绑定

ip address 10.1.1.2 24

mpls

interface G0/0/2

ip binding vpn-instance VPNB      #配置接口与 VPN 实例
绑定

ip address 20.1.1.2 24

mpls

interface LoopBack0

ip address 1.1.1.1 32

ip vpn-instance VPNA      #创建 VPN 实例为 VPNA

route-distinguisher 100:1      #配置路由区分器 100:1

vpn-target 100:1 export-extcommunity      #配置路由标记
发送 100:1

vpn-target 100:1 import-extcommunity      #配置路由标记
接收 100:1

ip vpn-instance VPNB      #创建 VPN 实例为 VPNB

```

```

route-distinguisher 100:2    #配置路由标记发送 100:2
vpn-target 100:2 export-extcommunity    #配置路由标记
发送 100:2
vpn-target 100:2 import-extcommunity    #配置路由标记
接收 100:2
bgp 1
peer 3.3.3.3 as-number 1
peer 3.3.3.3 connect-interface LoopBack0    #指定自身
与对等体之间用 Loopback0 接口来承载更新
ipv4-family vpnv4    #进入 BGP-VPNv4 子地址族
peer 3.3.3.3 enable    #使能对等体交换 BGP-VPNv4 路由
信息
ipv4-family vpn-instance VPNA    #进入 VPN 路由转发实
例 VPNA 地址族
import-route rip 1    #将 RIP 进程 1 的路由注入进 VPNA
实例
ipv4-family vpn-instance VPNB    #进入 VPN 路由转发实
例 VPNB 地址族
import-route rip 2    #将 RIP 进程 2 的路由注入进 VPNB
实例
ospf 1
area 0

```

```

network 1.1.1.1 0.0.0.0
network 30.1.1.0 0.0.0.255
rip 1 vpn-instance VPNA      #开启 VPNA 实例的 RIP 进程
1
version 2
network 10.0.0.0
import-route bgp      #将 BGP 路由注入进 RIP 进程 1
undo summary
rip 2 vpn-instance VPNB    #开启 VPNB 实例的 RIP 进程
2
version 2
network 20.0.0.0
import-route bgp      #将 BGP 路由注入进 RIP 进程 2
undo summary

RTC:
system-view
sysname RTC
interface G0/0/0
ip address 20.1.1.1 24
interface LoopBack0
ip address 172.16.1.1 24

```



```
rip 2  
version 2  
network 20.0.0.0  
network 172.16.0.0  
undo summary
```

RTD:

```
system-view  
sysname RTD  
router id 2.2.2.2  
mpls lsr-id 2.2.2.2  
mpls  
mpls ldp  
interface G0/0/0  
ip address 40.1.1.1 24  
mpls  
mpls ldp  
interface G0/0/1  
ip address 30.1.1.2 24  
mpls  
mpls ldp  
interface LoopBack0
```

```
ip address 2.2.2.2 32
ospf 1
area 0
network 30.1.1.0 0.0.0.255
network 40.1.1.0 0.0.0.255
network 2.2.2.2 0.0.0.0
```

RTE:

```
system-view
sysname RTE
router id 3.3.3.3
mpls lsr-id 3.3.3.3
mpls
mpls ldp
interface G0/0/0
ip address 40.1.1.2 24
mpls
mpls ldp
interface G0/0/1
ip binding vpn-instance VPNA
ip address 50.1.1.2 24
mpls
```

```
interface G0/0/2
ip binding vpn-instance VPNB
ip address 60.1.1.2 24
mpls
interface LoopBack0
ip address 3.3.3.3 32
ip vpn-instance VPNA
route-distinguisher 100:1
vpn-target 100:1 export-extcommunity
vpn-target 100:1 import-extcommunity
ip vpn-instance VPNB
route-distinguisher 100:2
vpn-target 100:2 export-extcommunity
vpn-target 100:2 import-extcommunity
bgp 1
peer 1.1.1.1 as-number 1
peer 1.1.1.1 connect-interface LoopBack0
ipv4-family vpnv4
peer 1.1.1.1 enable
ipv4-family vpn-instance VPNA
import-route rip 1
ipv4-family vpn-instance VPNB
```

```
import-route rip 2
ospf 1
area 0
network 3.3.3.3 0.0.0.0
network 40.1.1.0 0.0.0.255
rip 1 vpn-instance VPNA
version 2
network 50.0.0.0
import-route bgp
undo summary
rip 2 vpn-instance VPNB
version 2
network 60.0.0.0
import-route bgp
undo summary
```

RTF:

```
system-view
sysname RTF
interface G0/0/0
ip address 50.1.1.1 24
interface LoopBack0
```

---

```
ip address 192.168.2.1 24
```

```
rip 1
```

```
version 2
```

```
network 50.0.0.0
```

```
network 192.168.2.0
```

```
undo summary
```

```
RTG:
```

```
system-view
```

```
sysname RTG
```

```
interface G0/0/0
```

```
ip address 60.1.1.1 24
```

```
interface LoopBack0
```

```
ip address 172.16.2.1 24
```

```
rip 2
```

```
version 2
```

```
network 60.0.0.0
```

```
network 172.16.0.0
```

```
undo summary
```

测试:

在 RTA 上用 192.168.1.1 ping 192.168.2.1:

```
[RTA]ping -a 192.168.1.1 192.168.2.1
PING 192.168.2.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=252 time=50 ms
  Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=252 time=50 ms
  Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=252 time=40 ms
  Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=252 time=40 ms
  Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=252 time=50 ms

--- 192.168.2.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 40/46/50 ms

[RTA]
```

在 RTF 上用 192.168.2.1 ping 192.168.1.1:

```
[RTF]ping -a 192.168.2.1 192.168.1.1
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=252 time=40 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=252 time=50 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=252 time=60 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=252 time=50 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=252 time=50 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 40/50/60 ms

[RTF]
```

在 RTC 上用 172.16.1.1 ping 172.16.2.1:

```
[RTC]ping -a 172.16.1.1 172.16.2.1
PING 172.16.2.1: 56 data bytes, press CTRL_C to break
  Reply from 172.16.2.1: bytes=56 Sequence=1 ttl=252 time=40 ms
  Reply from 172.16.2.1: bytes=56 Sequence=2 ttl=252 time=60 ms
  Reply from 172.16.2.1: bytes=56 Sequence=3 ttl=252 time=40 ms
  Reply from 172.16.2.1: bytes=56 Sequence=4 ttl=252 time=40 ms
  Reply from 172.16.2.1: bytes=56 Sequence=5 ttl=252 time=40 ms

--- 172.16.2.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 40/44/60 ms

[RTC]
```

在 RTG 上用 172.16.2.1 ping 172.16.1.1:

```
[RTG]ping -a 172.16.2.1 172.16.1.1
PING 172.16.1.1: 56 data bytes, press CTRL_C to break
  Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=252 time=40 ms
  Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=252 time=50 ms
  Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=252 time=50 ms
  Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=252 time=40 ms
  Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=252 time=40 ms

--- 172.16.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 40/44/50 ms

[RTG]
```