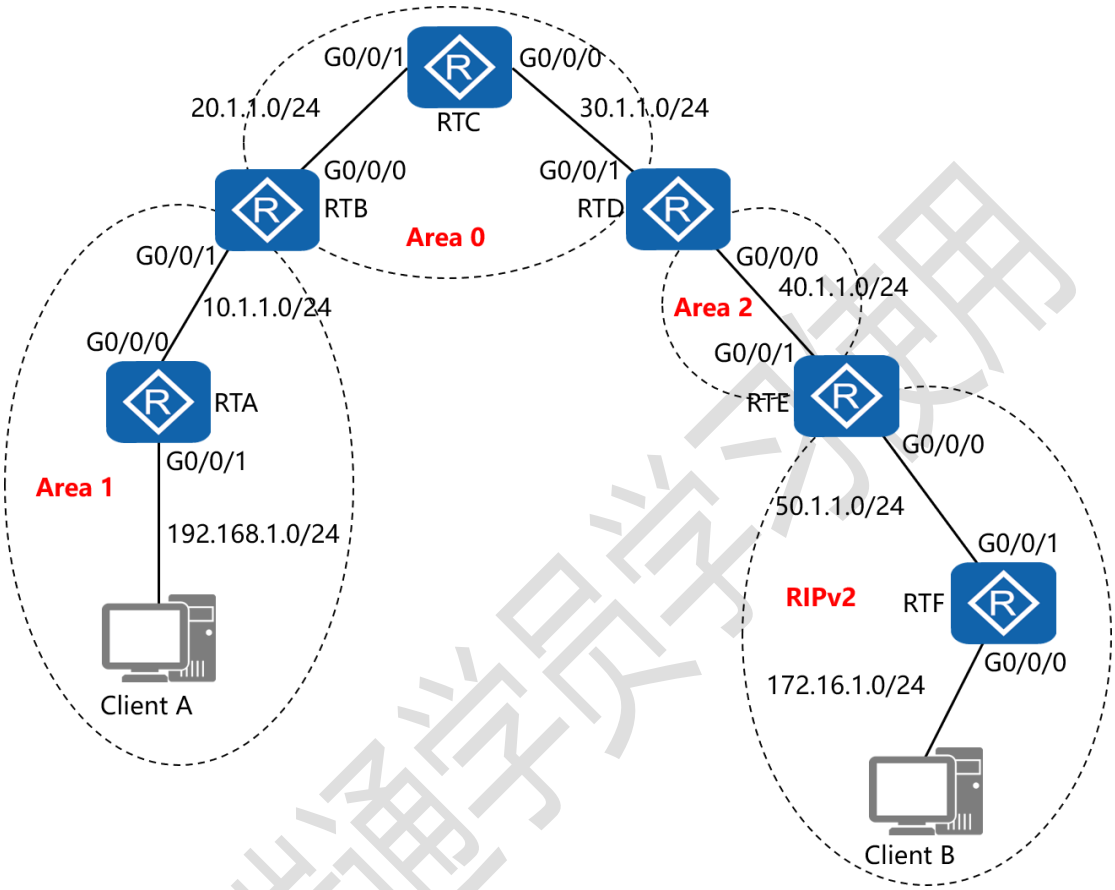
《HCIP – Datacom Core 实验手册》目录

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

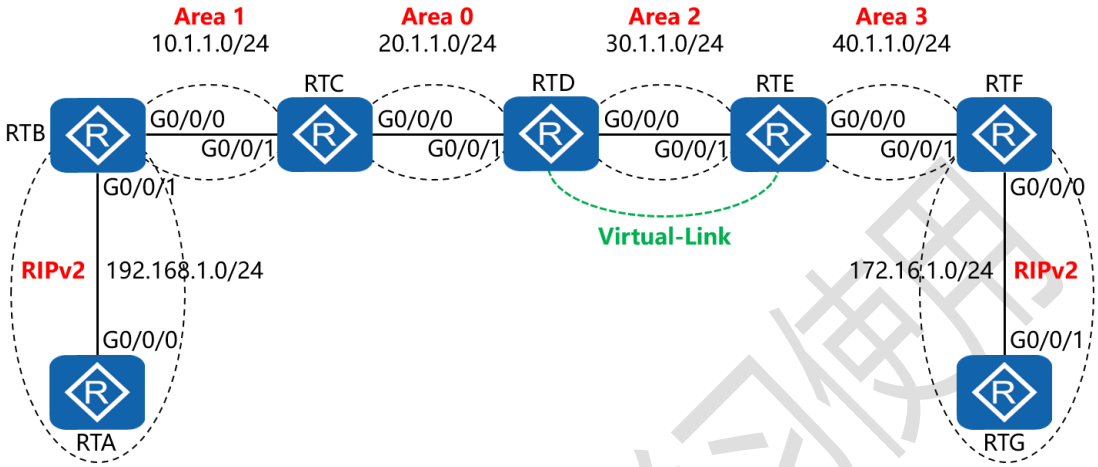
network 50.0.0.0

network 172.16.0.0

undo summary

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

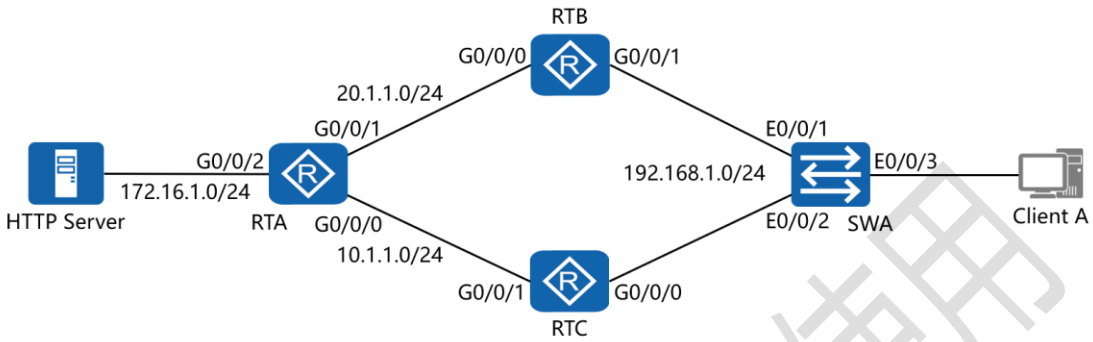
import-route ospf 1

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
```

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

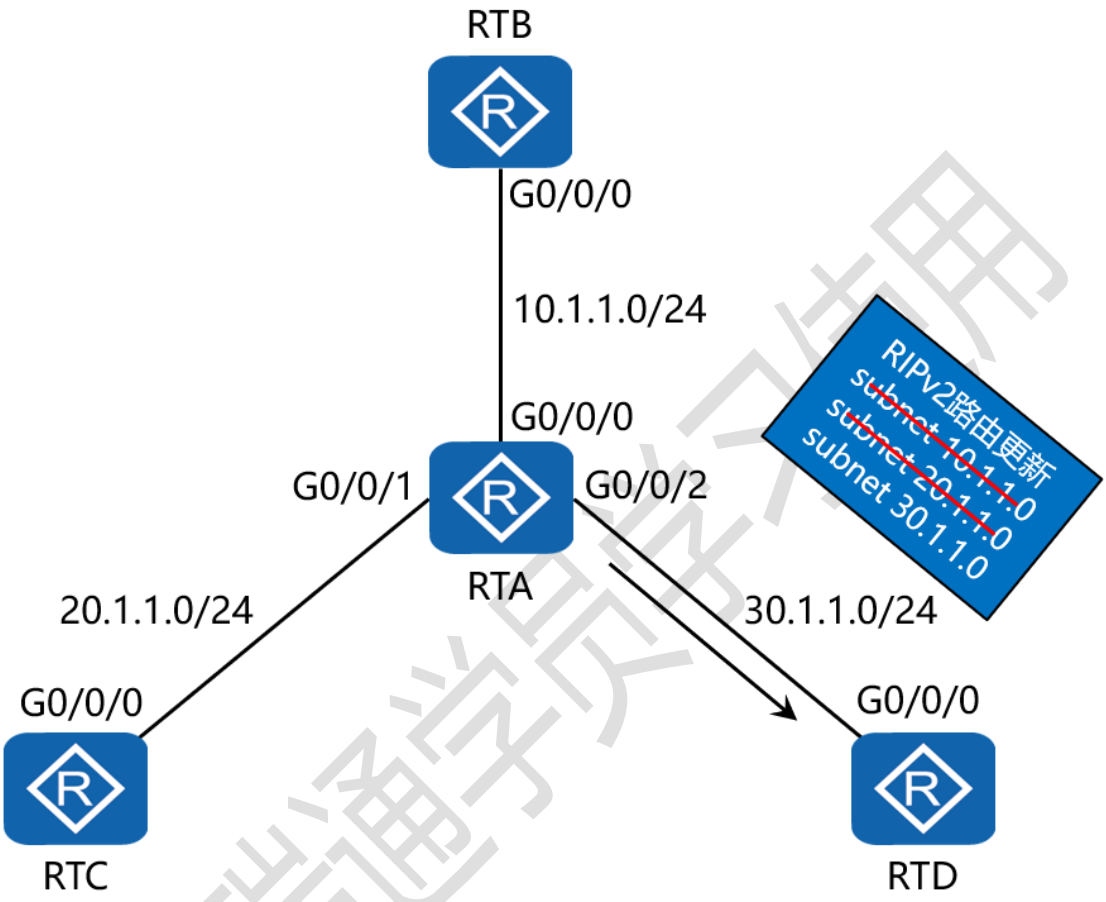
network 192.168.1.0

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

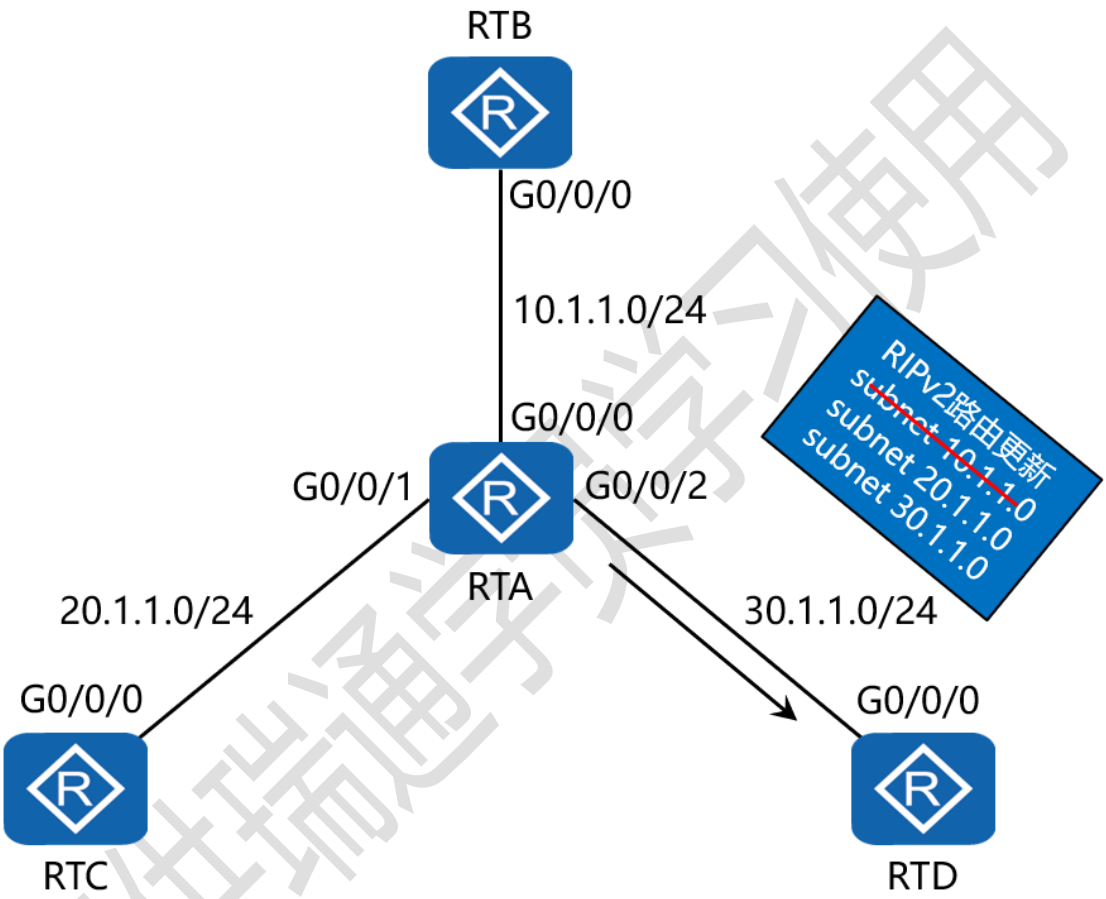
version 2

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

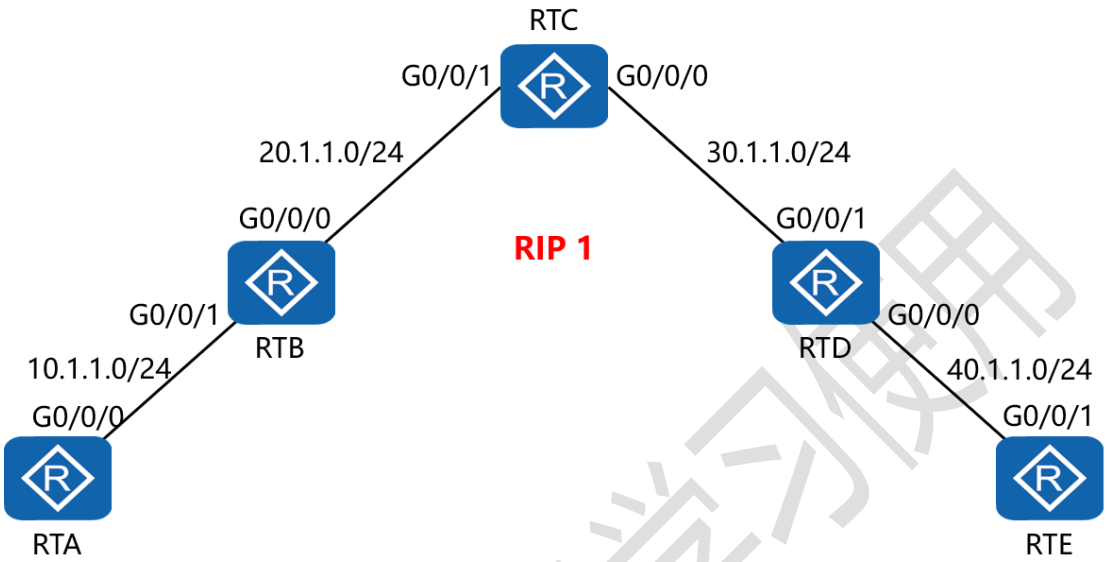
filter-policy 2001 import #使用过滤策略调用 ACL 2001，并应用在入方向上

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

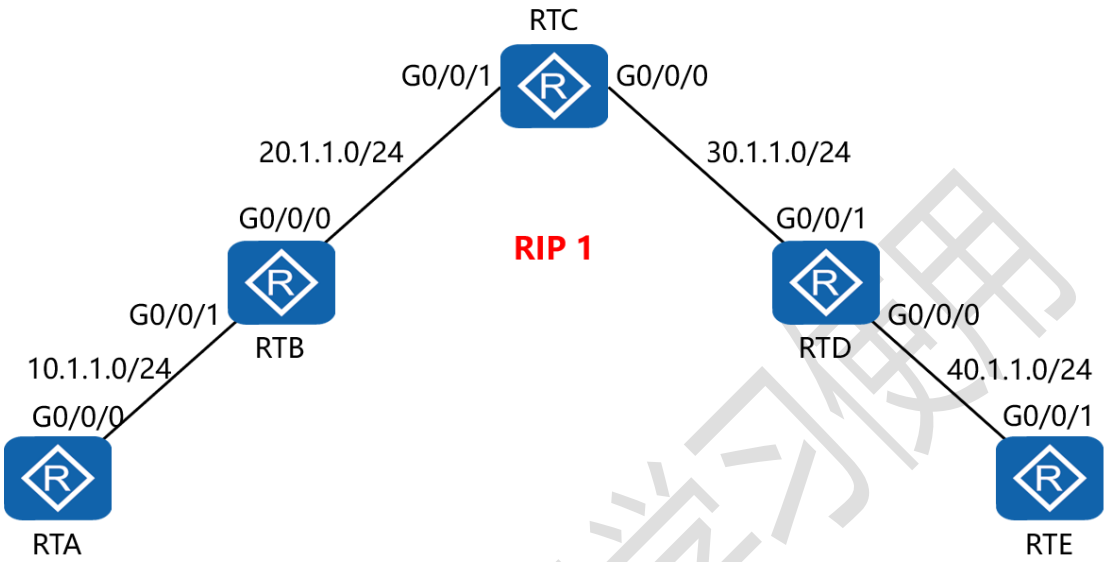
version 2

network 40.0.0.0

undo summary

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

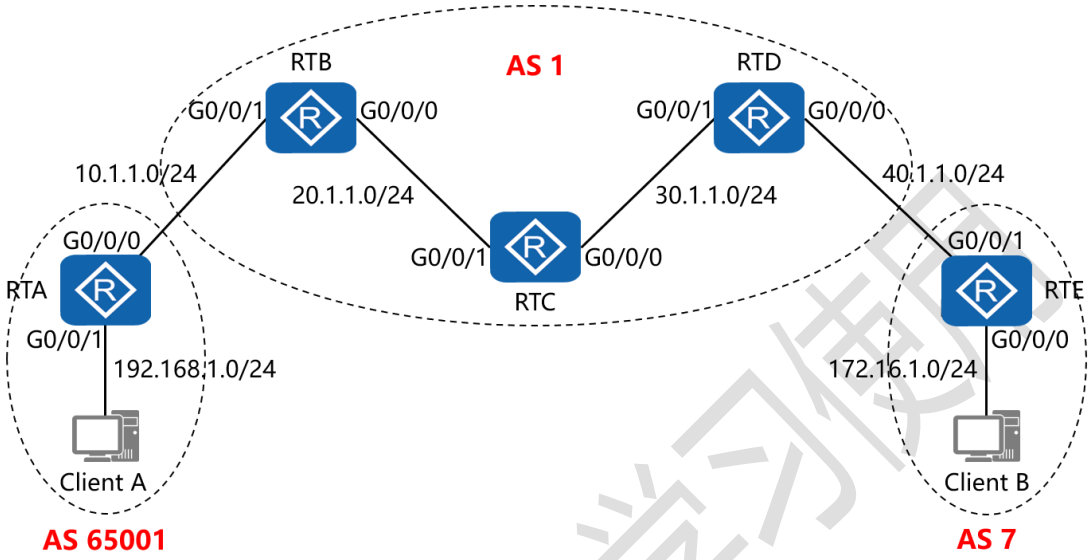
```
interface G0/0/1
ip address 30.1.1.2 24
rip 1
version 2
network 30.0.0.0
network 40.0.0.0
undo summary
```

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 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：

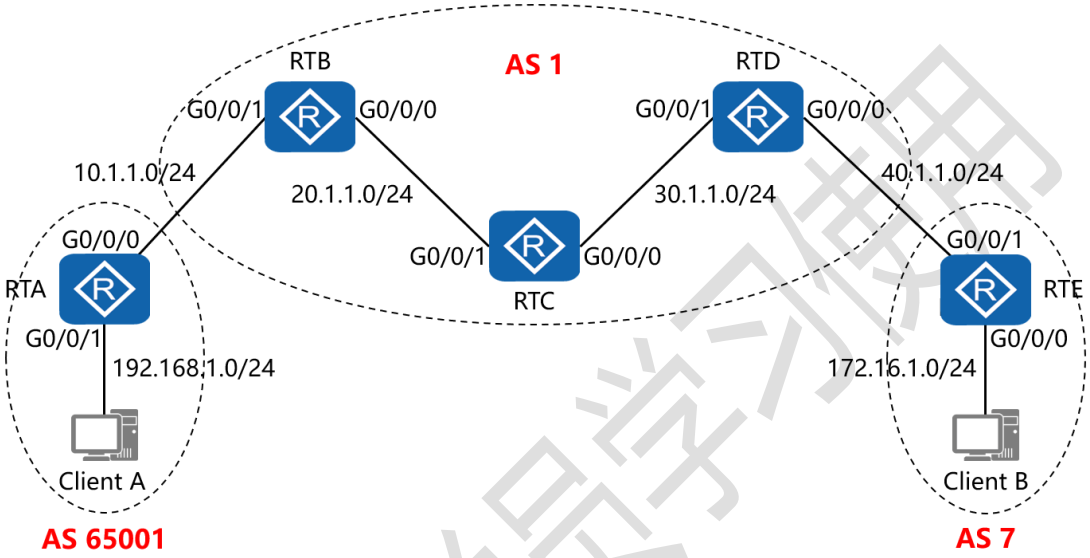
分别在 RTA 与 RTE 上查看路由表：

```
[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

        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
       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
    192.168.1.0/24  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]
```

九、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：

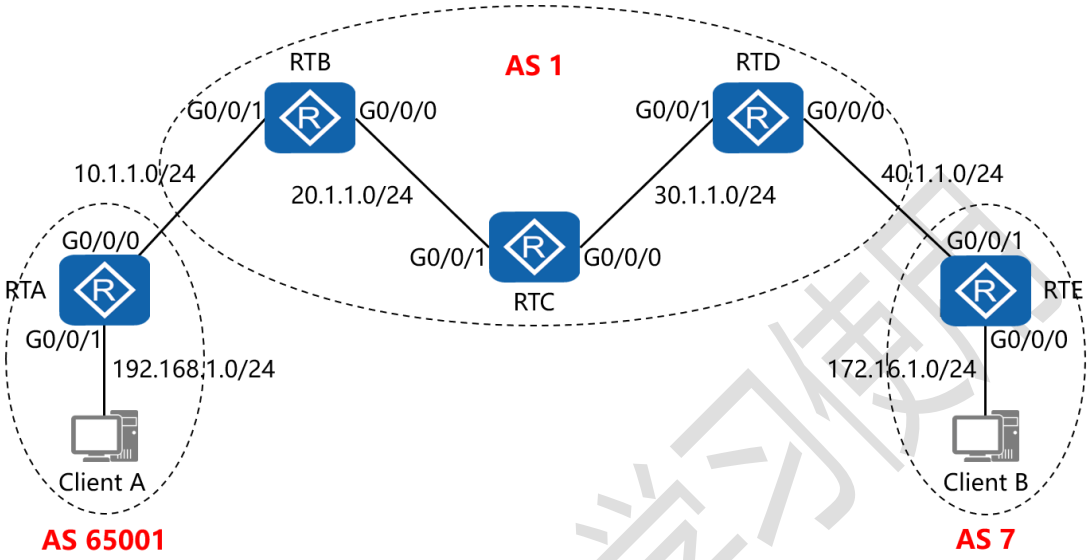
```
[RTE]dis bgp routing-table

 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       1i
 *>   20.1.1.0/24        4.4.4.4         1                     0       1i
 *>   30.1.1.0/24        4.4.4.4         0                     0       1i
 *>   40.1.1.0/24        4.4.4.4         0                     0       1i
 *>   172.16.1.0/24      0.0.0.0         0                     0       i
 *>   192.168.1.0        4.4.4.4                               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                               0       1i
 *>   20.1.1.0/24        4.4.4.4         1                     0       1i
 *>   30.1.1.0/24        4.4.4.4         0                     0       1i
 *>   40.1.1.0/24        4.4.4.4         0                     0       1i
 *>   172.16.1.0/24      0.0.0.0         0                     0       i
 *>   192.168.1.0        4.4.4.4                               0       1i
[RTE]
```

十、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：

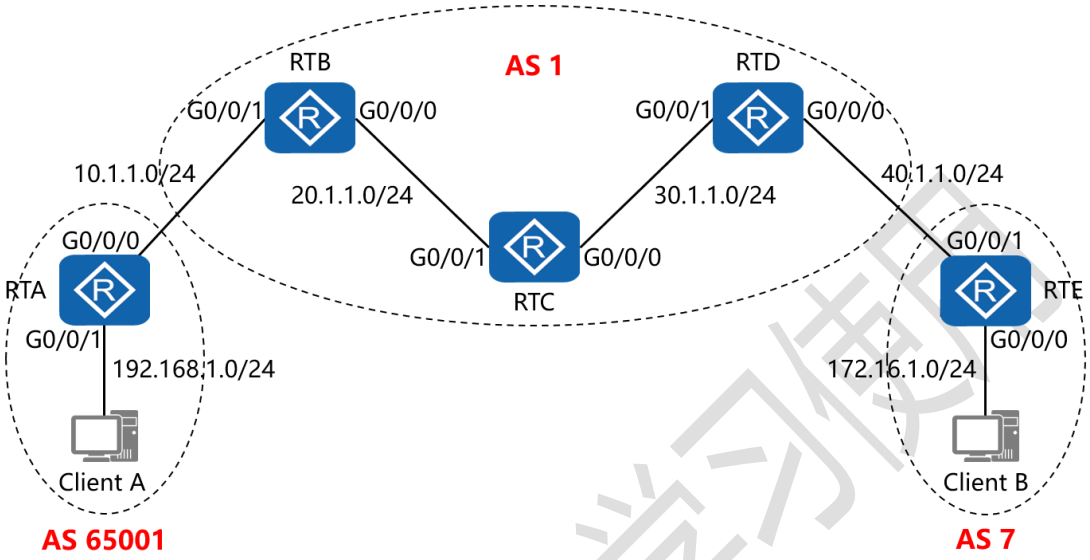
```
[RTE]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        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
       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
    192.168.1.0/24  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

        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
       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]
```

十一、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       1i
 *>   20.1.1.0/24        4.4.4.4         1                     0       1i
 *>   30.1.1.0/24        4.4.4.4         0                     0       1i
 *>   40.1.1.0/24        4.4.4.4         0                     0       1i
 *>   172.16.1.0/24      0.0.0.0         0                     0       i
 *>   192.168.0.0/16     4.4.4.4                               0       1i
[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：

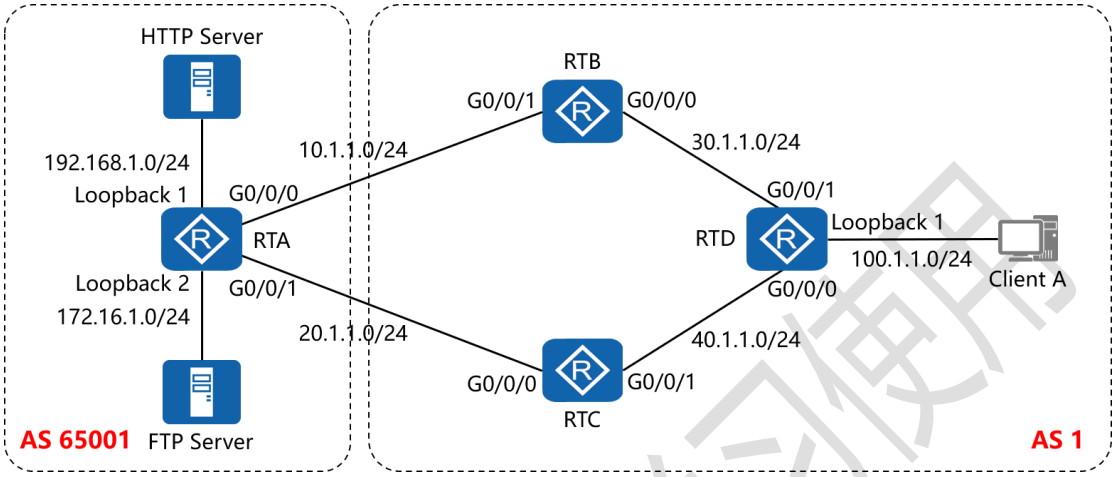
```
[RTE]dis bgp routing-table

 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       1i
 *>   20.1.1.0/24        4.4.4.4         1                     0       1i
 *>   30.1.1.0/24        4.4.4.4         0                     0       1i
 *>   40.1.1.0/24        4.4.4.4         0                     0       1i
 *>   172.16.1.0/24      0.0.0.0         0                     0       i
 *>   192.168.0.0/16     4.4.4.4                               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]
```

十二、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      i
 *>    40.1.1.0/24        0.0.0.0         0                        0      i
 *>    100.1.1.0/24       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：

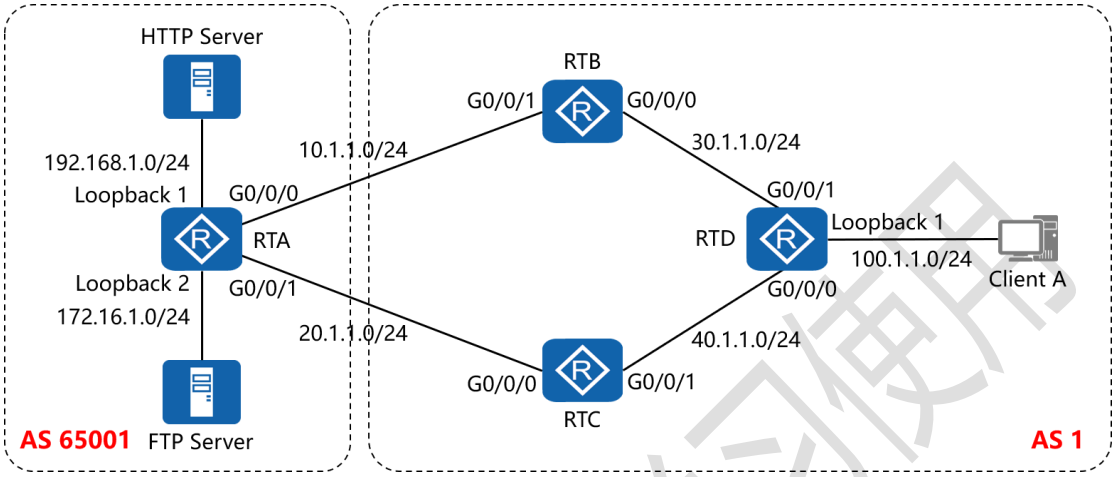
```
[RTD]tracert -a 100.1.1.1 192.168.1.1

 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]
```

十三、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      i
 *>    40.1.1.0/24        0.0.0.0         0                      0      i
 *>    100.1.1.0/24       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：

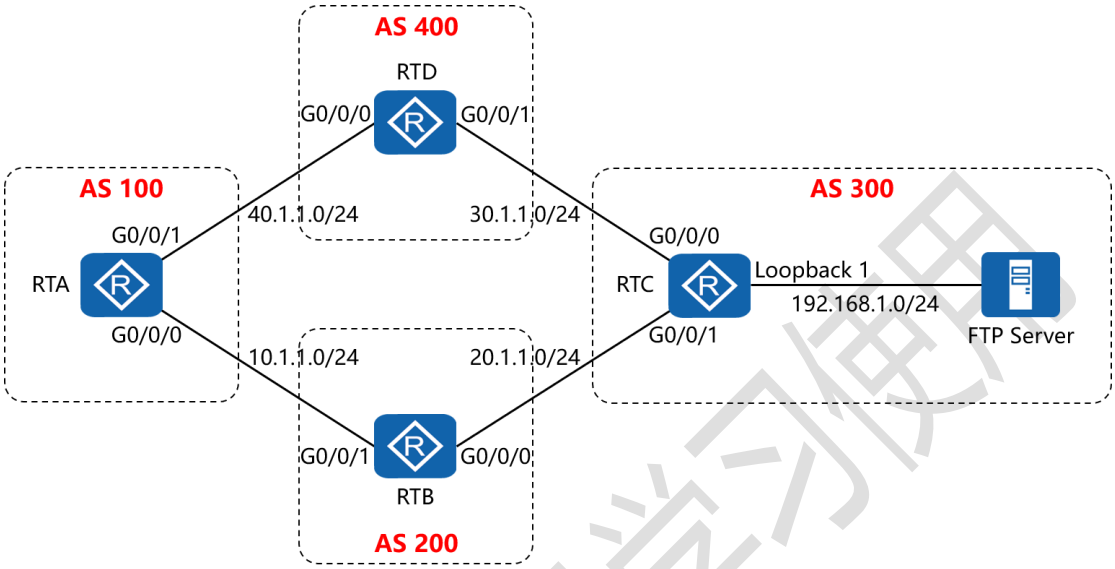
```
[RTD]tracert -a 100.1.1.1 192.168.1.1

 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]
```

十四、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
```

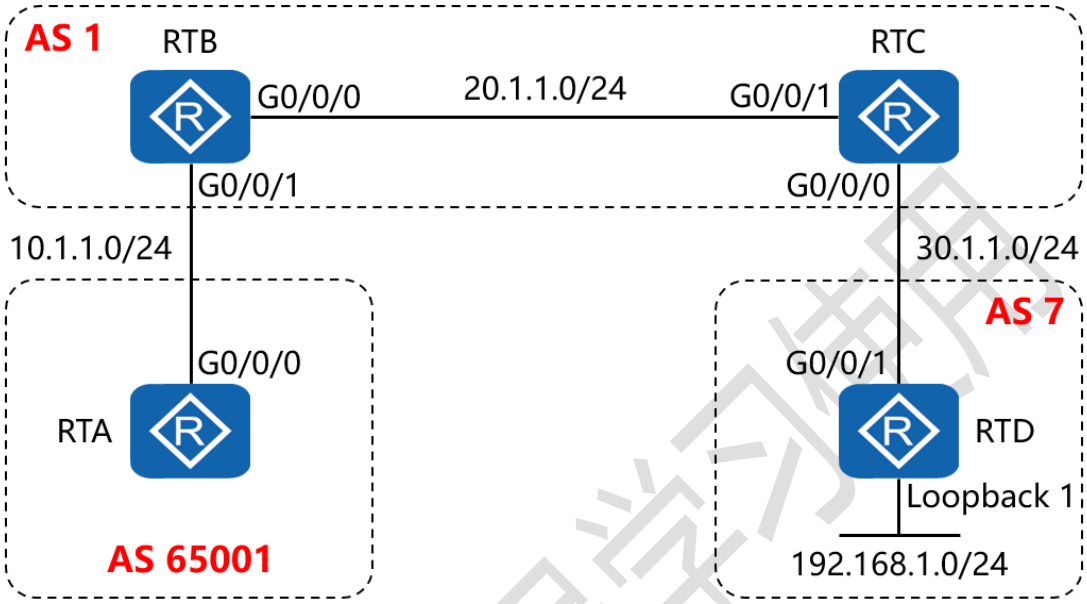
测试：

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       i
 *>   20.1.1.0/24        2.2.2.2         0                    0       200i
 *>   30.1.1.0/24        2.2.2.2                              0       200 300i
 *                       4.4.4.4                              0       400 300i
 *>   40.1.1.0/24        4.4.4.4         0                    0       400i
 *>   192.168.1.0        4.4.4.4                              100     400 300i
 *                       2.2.2.2                              0       200 300i
[RTA]
```

十五、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
```

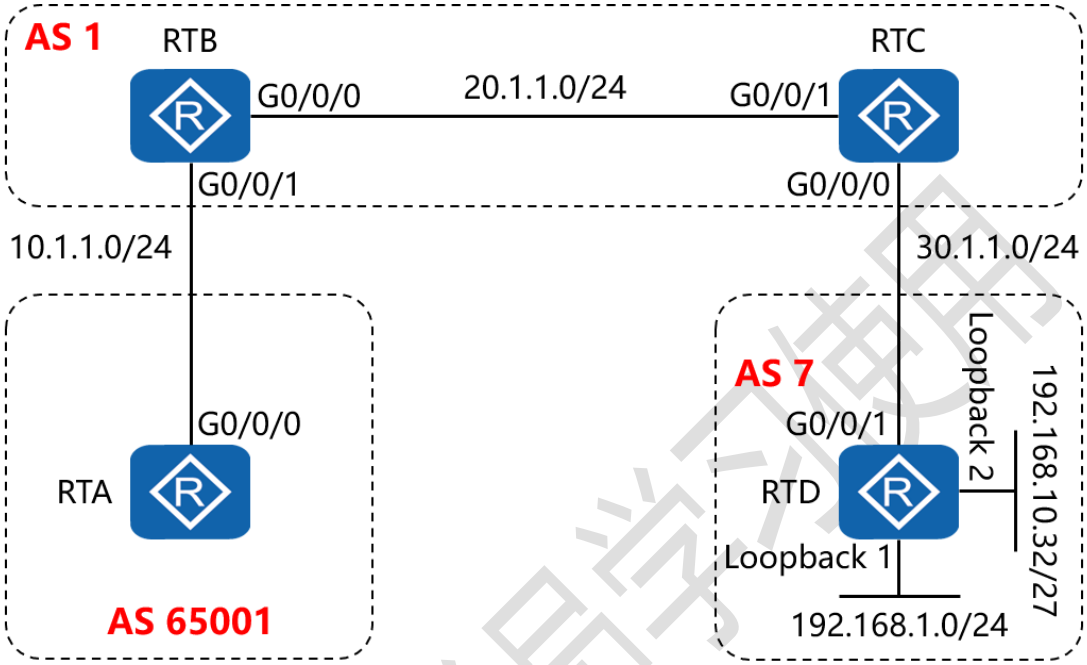
RTD:

```
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
```

十六、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

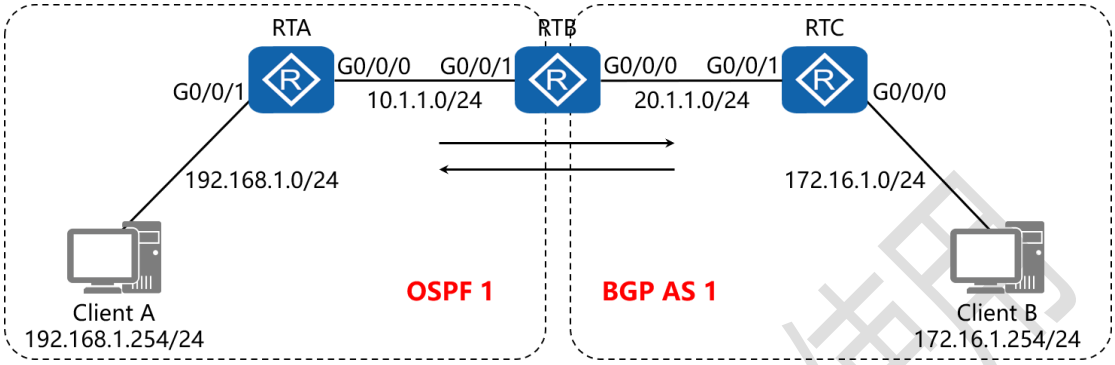
ip address 192.168.1.1 24

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
```

十七、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

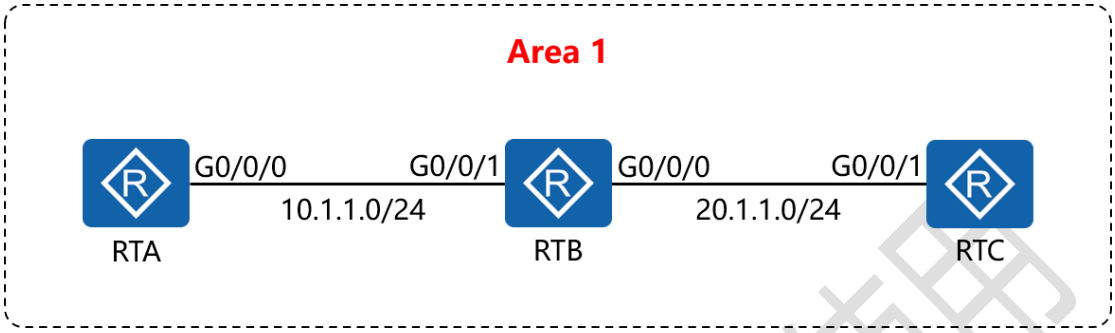
ip address 20.1.1.2 24

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
```

十八、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:

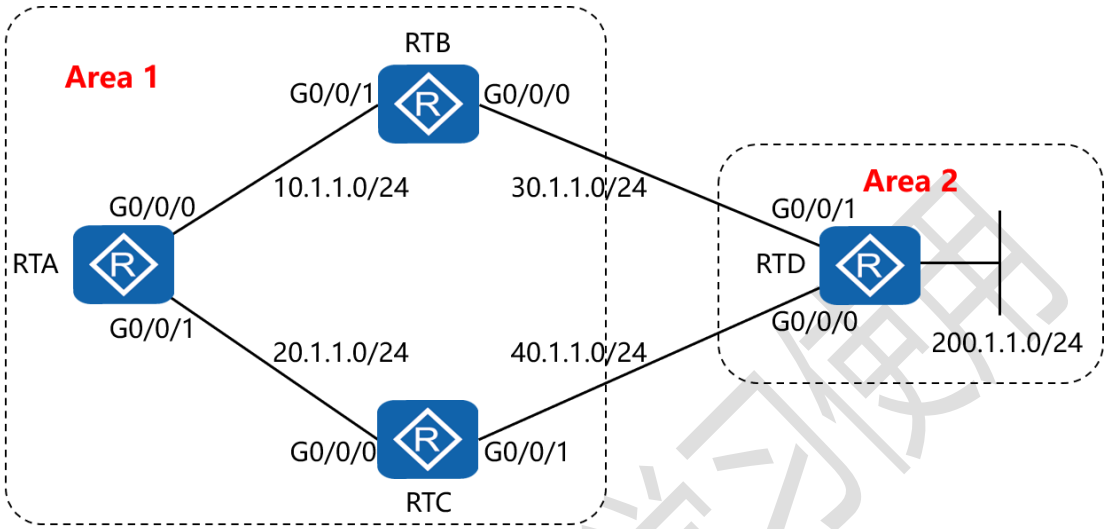
```
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
isis enable 1
interface G0/0/1
ip address 10.1.1.2 24
isis enable 1
isis 1
is-level level-1
network-entity 01.0020.0200.2002.00
```

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
```

十九、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：

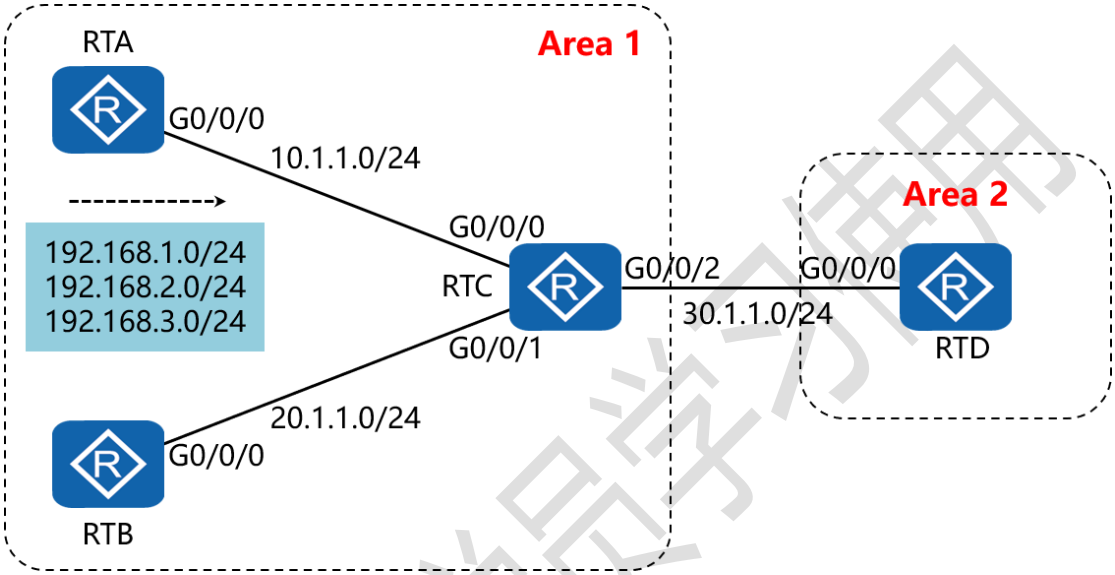
```
[RTA]ping 200.1.1.1
  PING 200.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 200.1.1.1: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

二十、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*

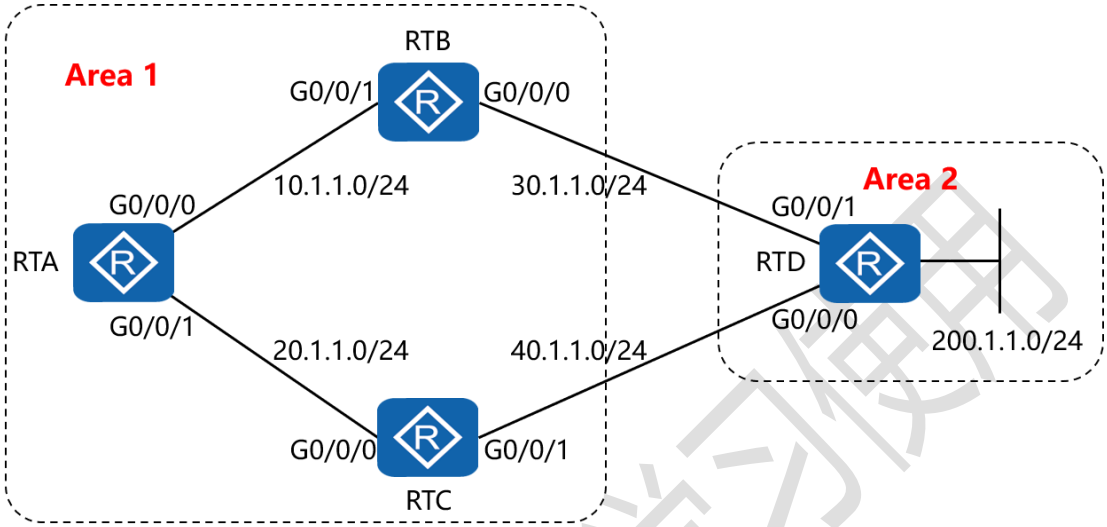
测试：

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]
```

二十一、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/-/-/-
                                         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/-/-/-
     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

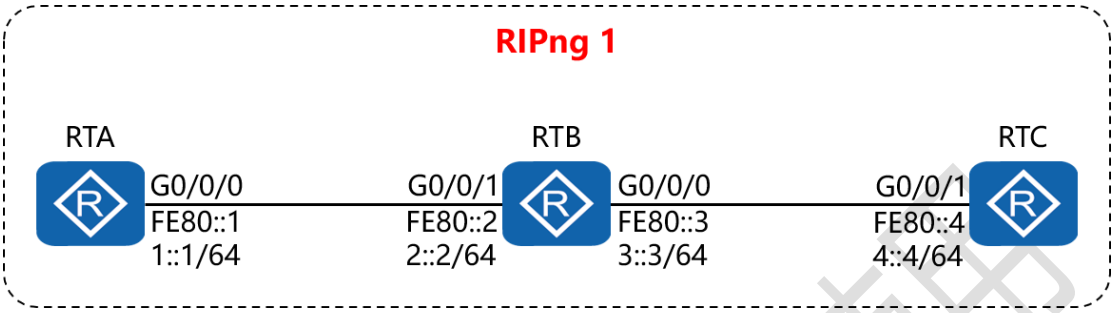
import-route isis level-2 into level-1

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/-/-/-
                                         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
                                         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]
```

二十二、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

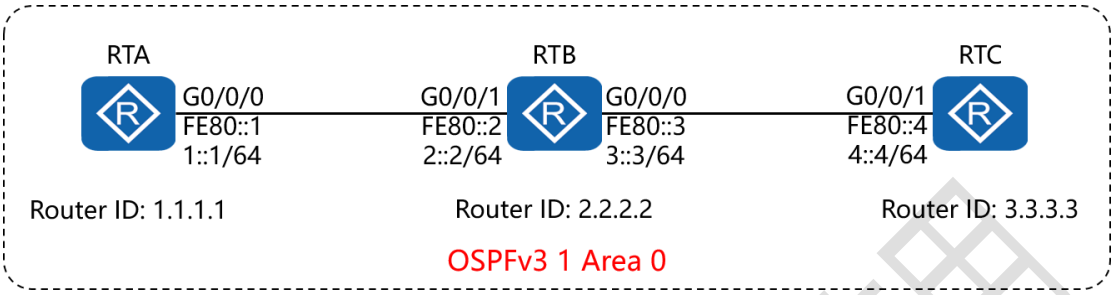
sysname RTC

ipv6

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

二十三、配置 OSPFv3 实验组网

一、实验拓扑：



二、实验目的：

通过 OSPFv3 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

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

ipv6　　#开启设备的 IPv6 功能

ospfv3　　#开启并进入 OSPFv3 进程

router-id 1.1.1.1　　#配置 OSPF 路由器 ID

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

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

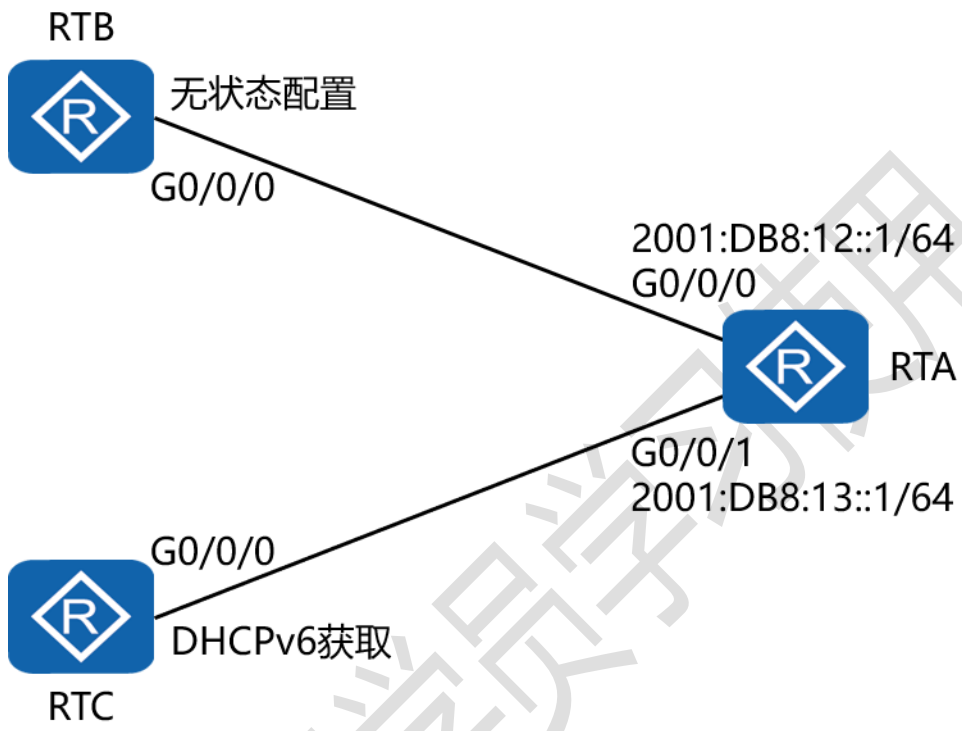
```
ospfv3 1 area 0.0.0.0
```

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
```

二十四、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

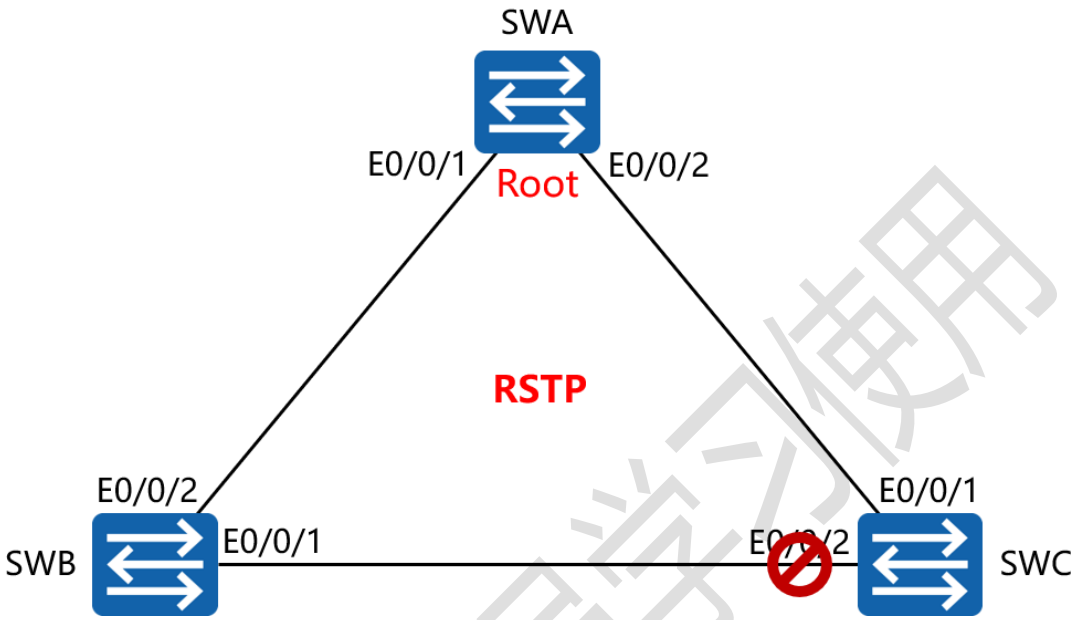
```
[RTB]display interface g0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, GigabitEthernet0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, 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]
```

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

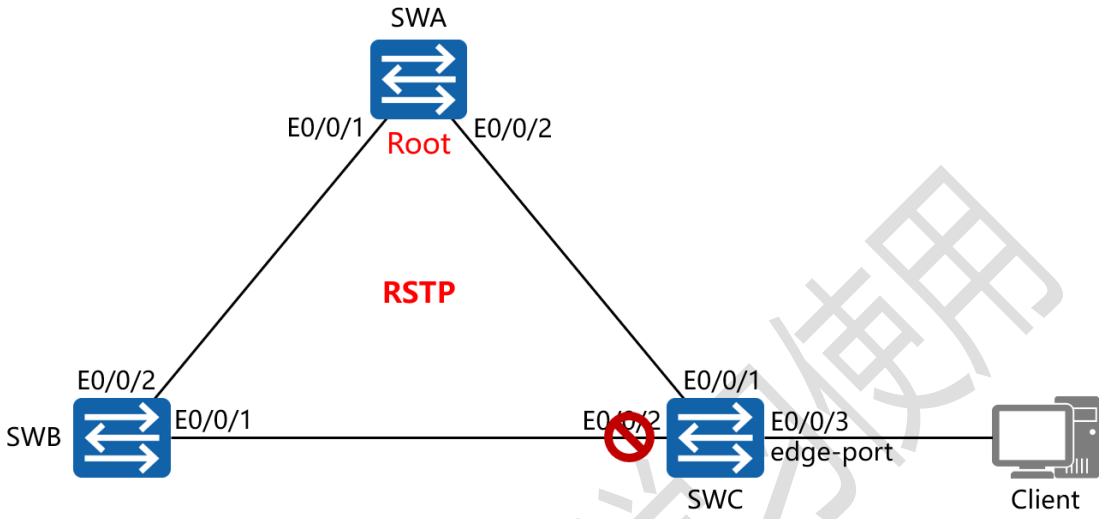
测试：

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

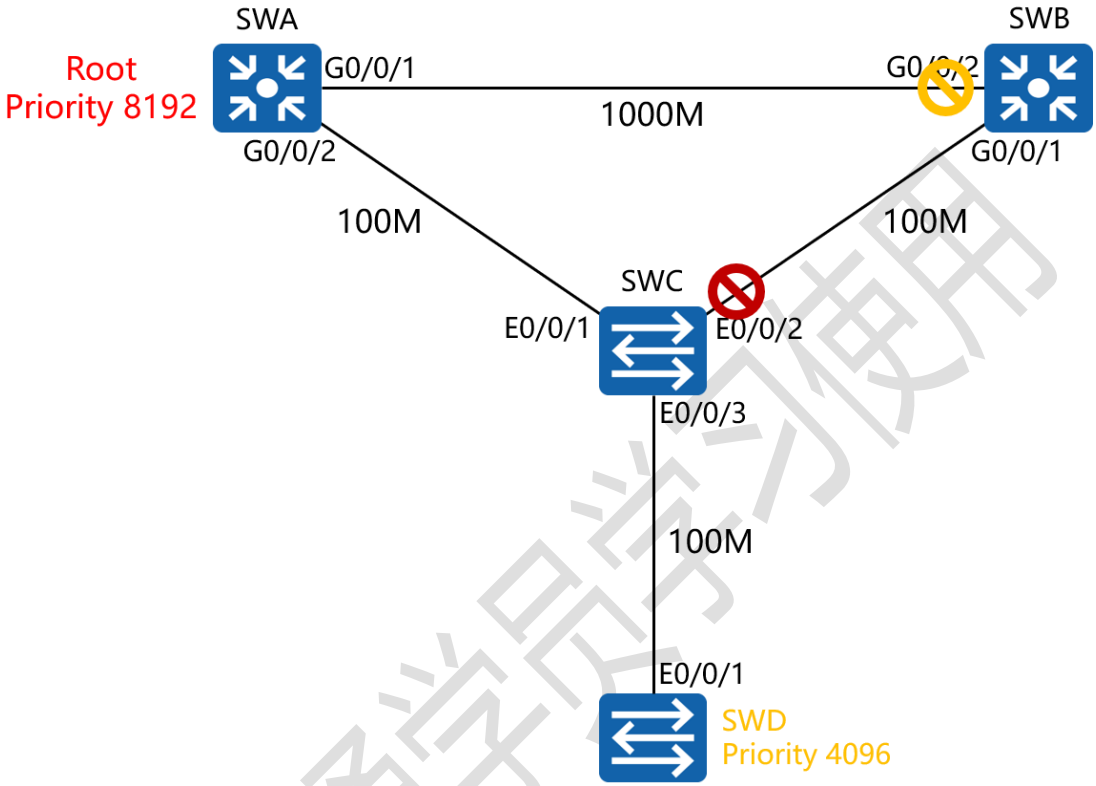
stp mode rstp

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

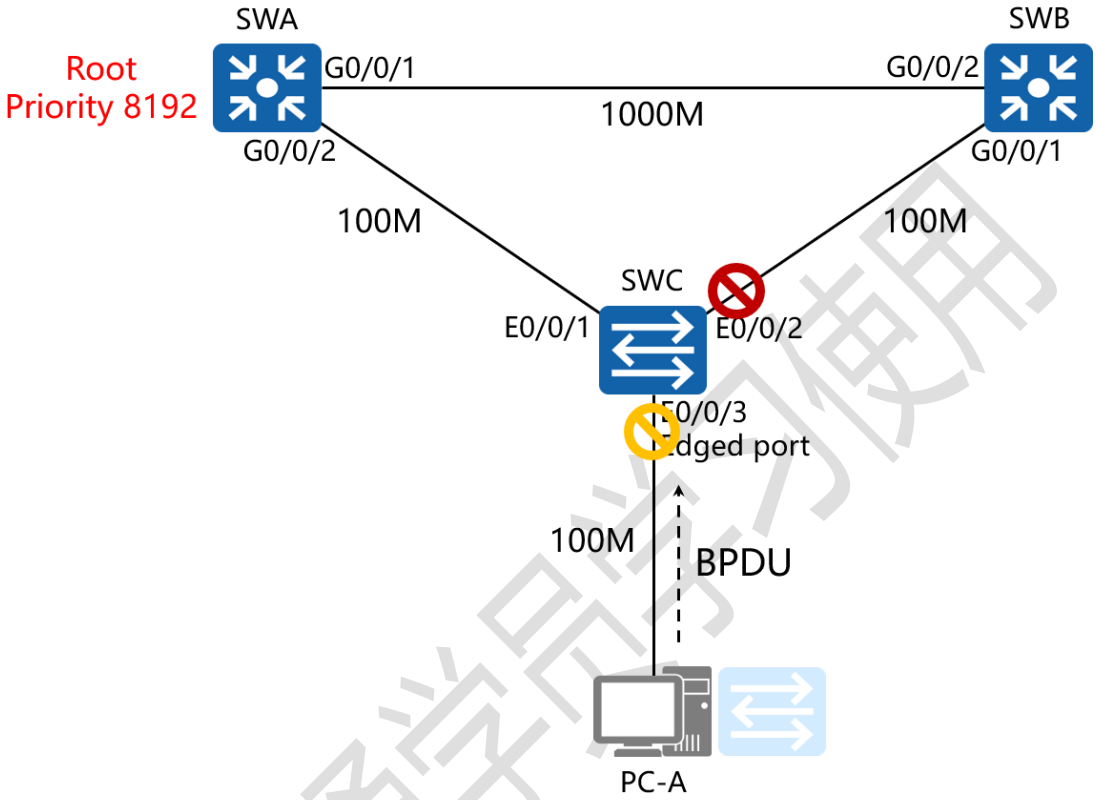
interface E0/0/1

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

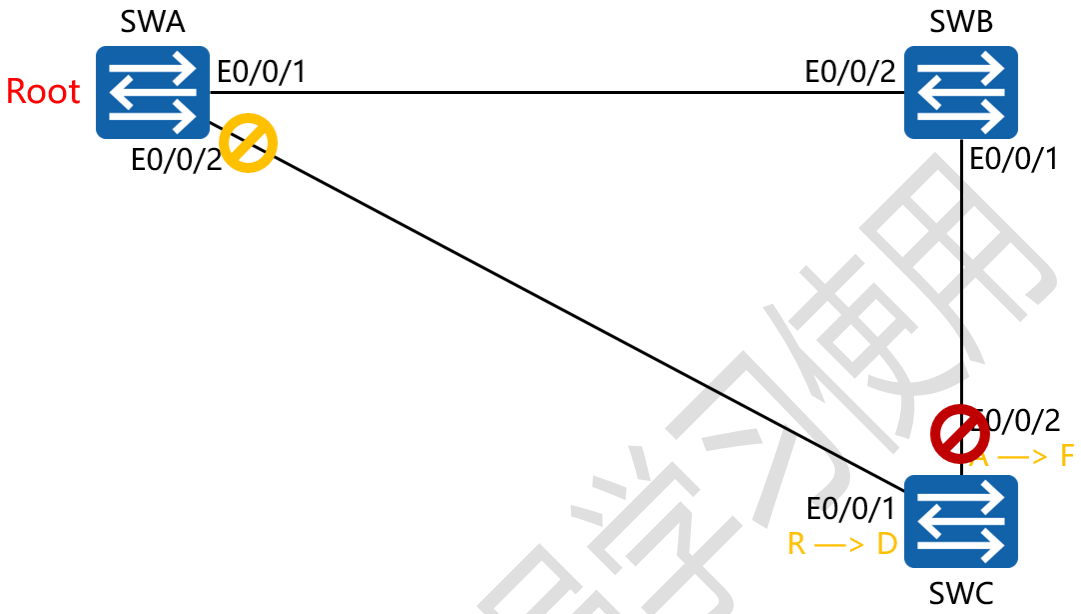
interface E0/0/2

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

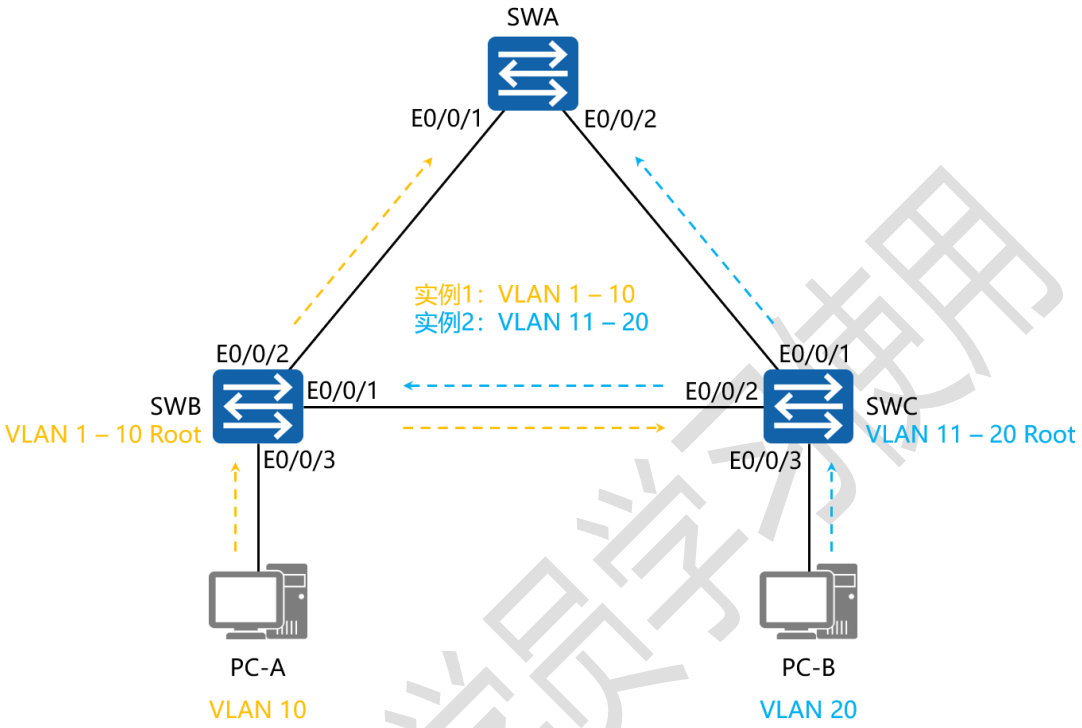
interface E0/0/2

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

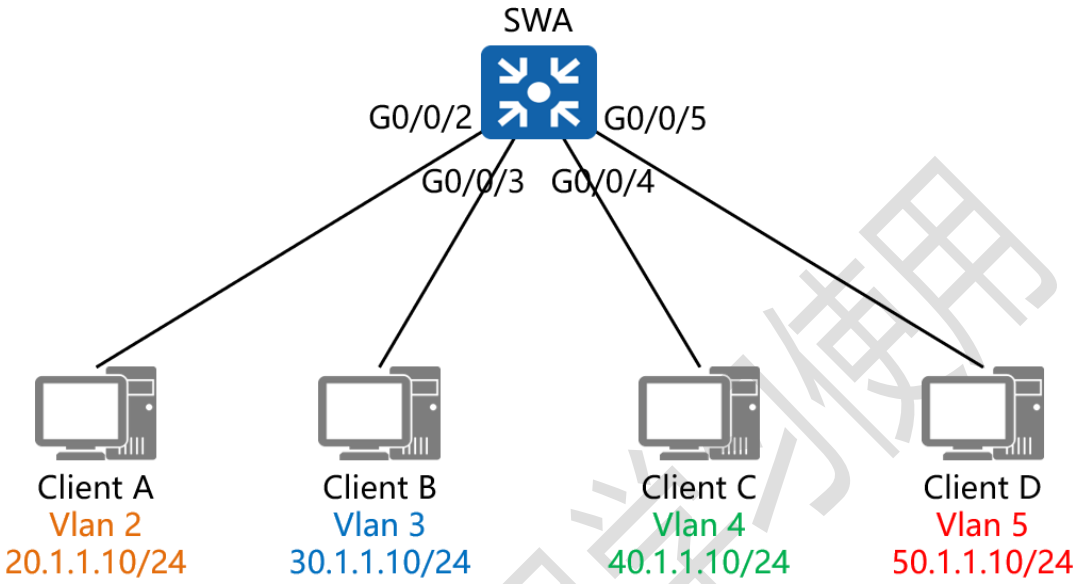
```
[SWB]display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet0/0/1               DESI  FORWARDING      NONE
   0    Ethernet0/0/2               DESI  FORWARDING      NONE
   0    Ethernet0/0/3               DESI  FORWARDING      NONE
   1    Ethernet0/0/1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

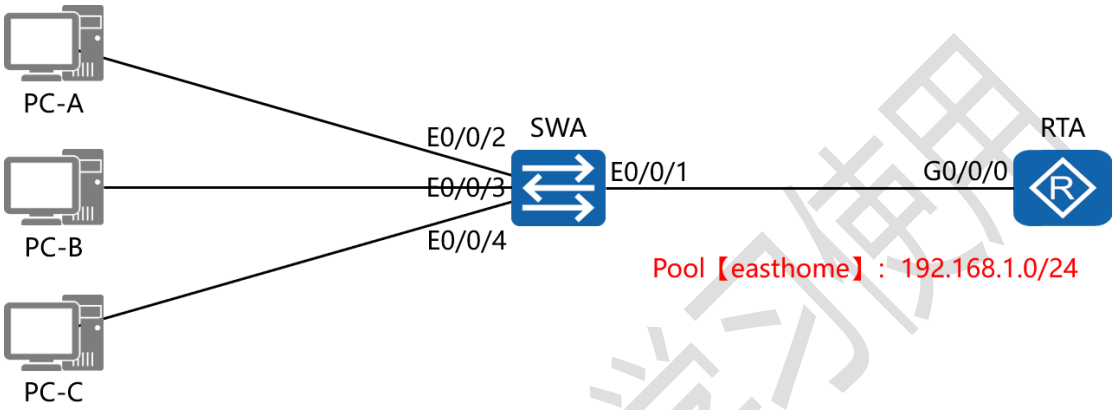
vlan 5　　#创建 VLAN 5

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

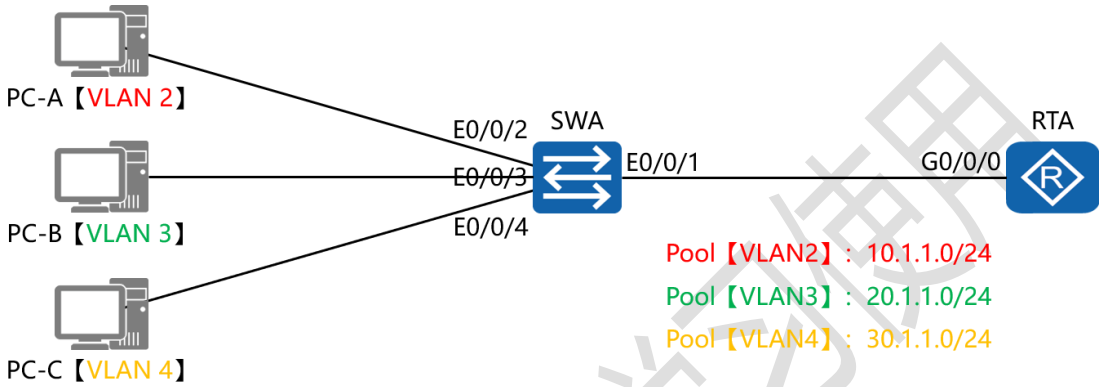
dhcp server excluded-ip-address 192.168.1.2 #配置在分配地址时排除的地址

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

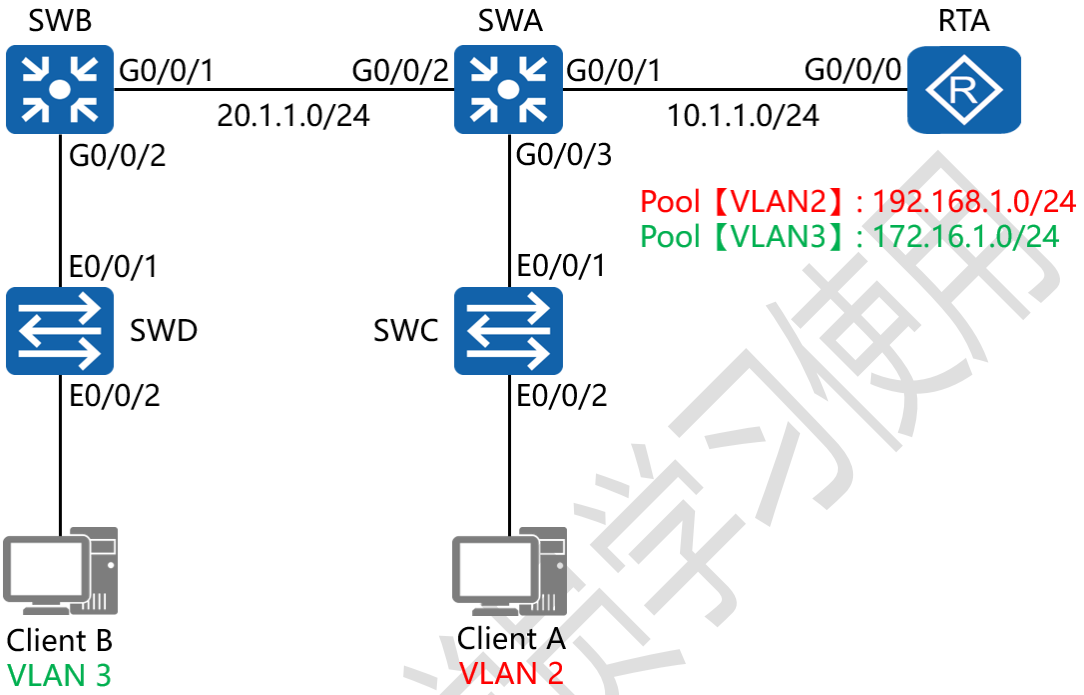
interface E0/0/2

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

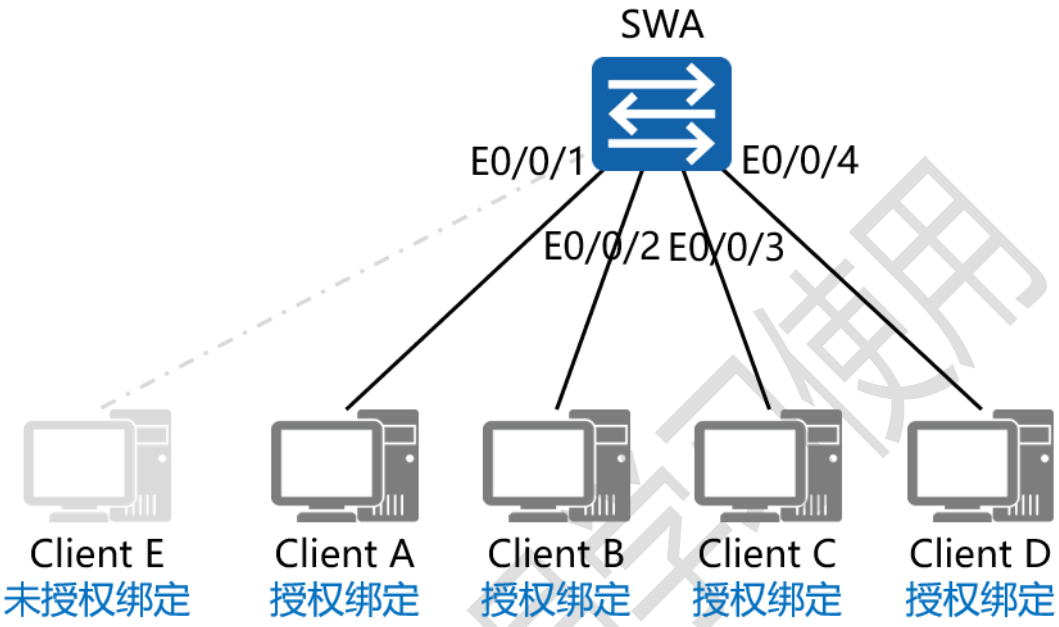
interface E0/0/2

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

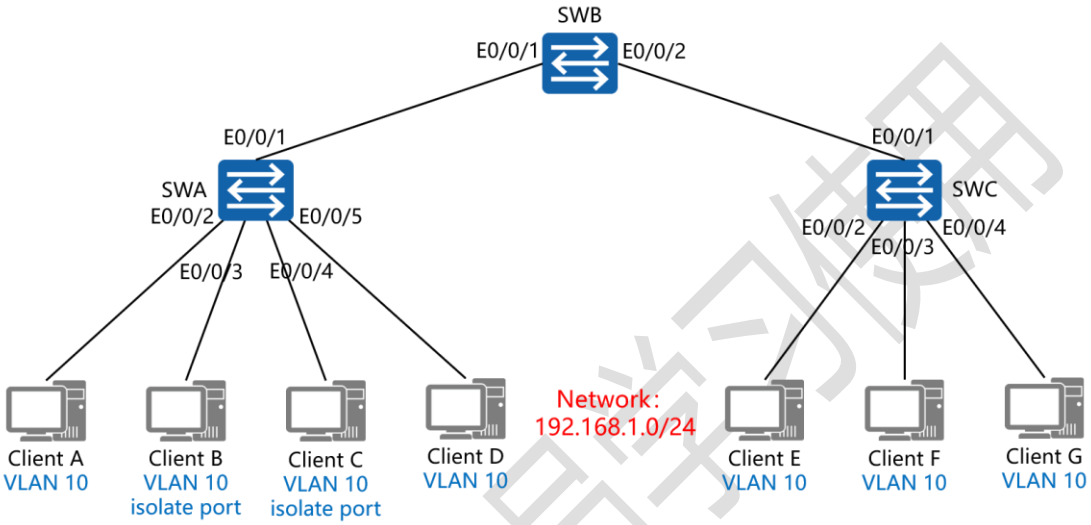
转发状态

[Huawei]interface E0/0/1

[Huawei-Ethernet0/0/1]restart

三十六、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

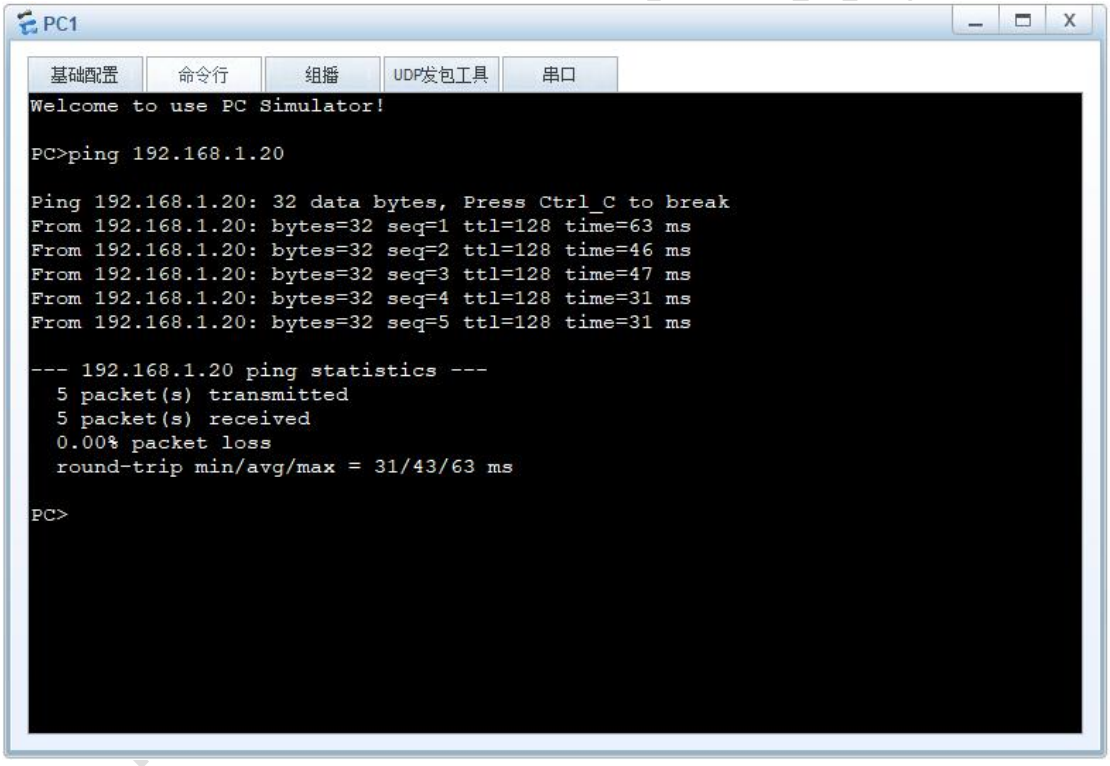
interface E0/0/4

port link-type access

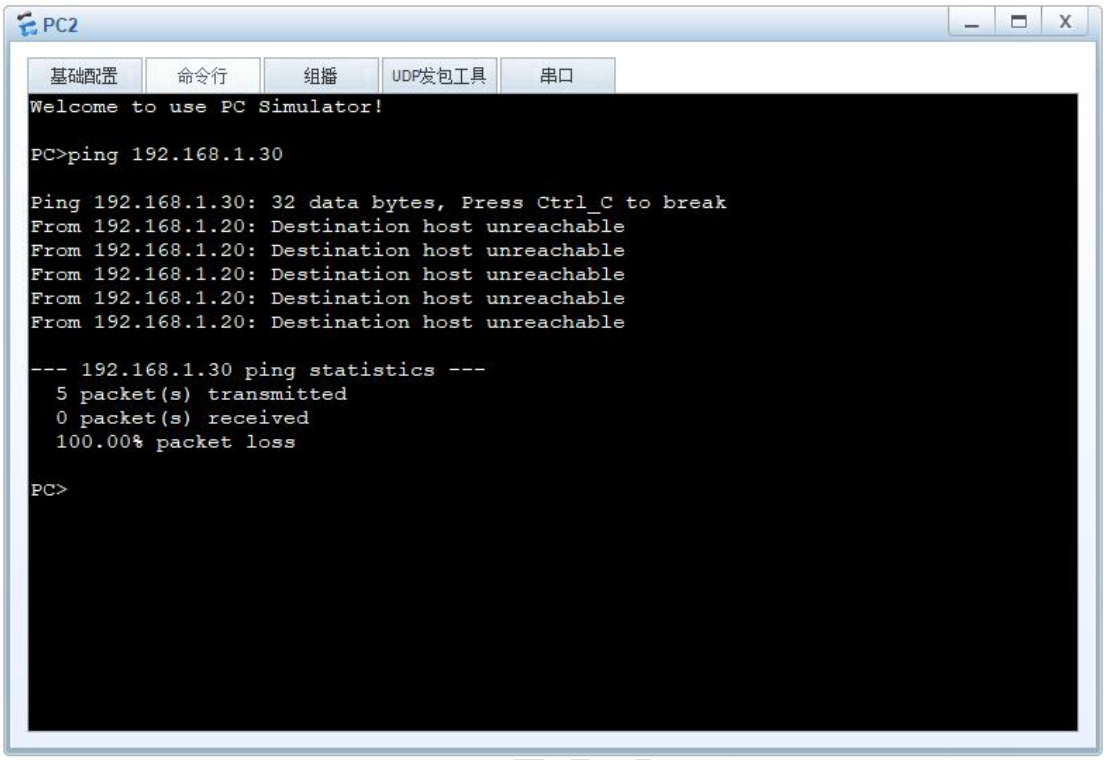
port default vlan 10

测试：

Client A 与 Client B 可正常通讯



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:

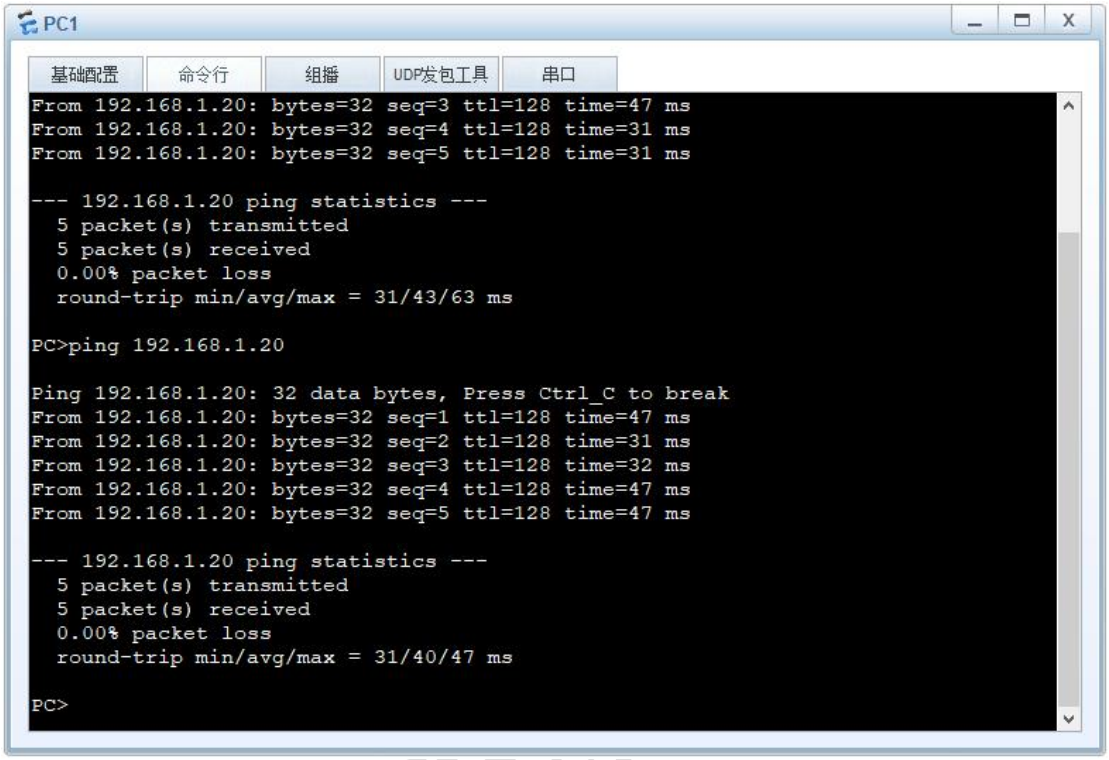
interface vlan 10

ip add 192.168.1.1 24

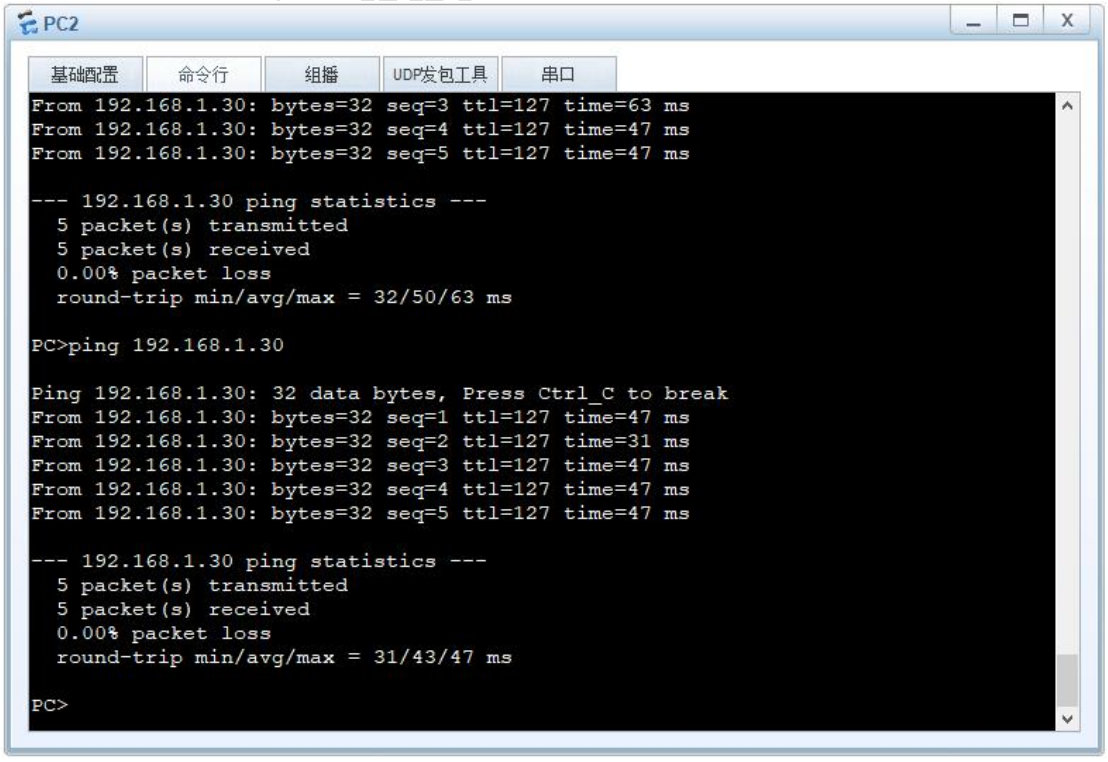
arp-proxy inner-sub-vlan-proxy enable　　#开启同 VLAN 内 ARP 代理功能

再次测试：

Client A 与 Client B 依旧可以正常通讯

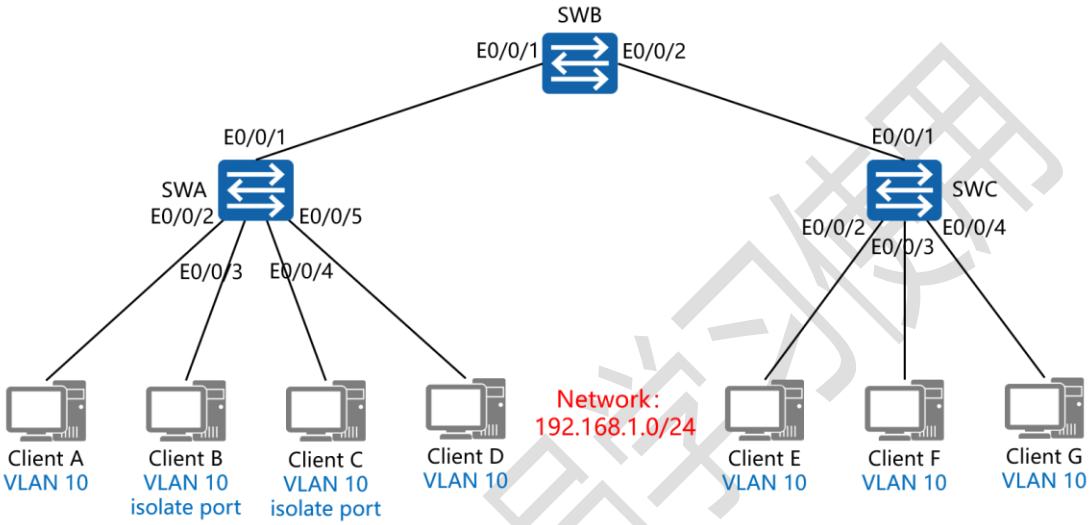


Client B 与 Client C 此时亦可正常通讯



三十七、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

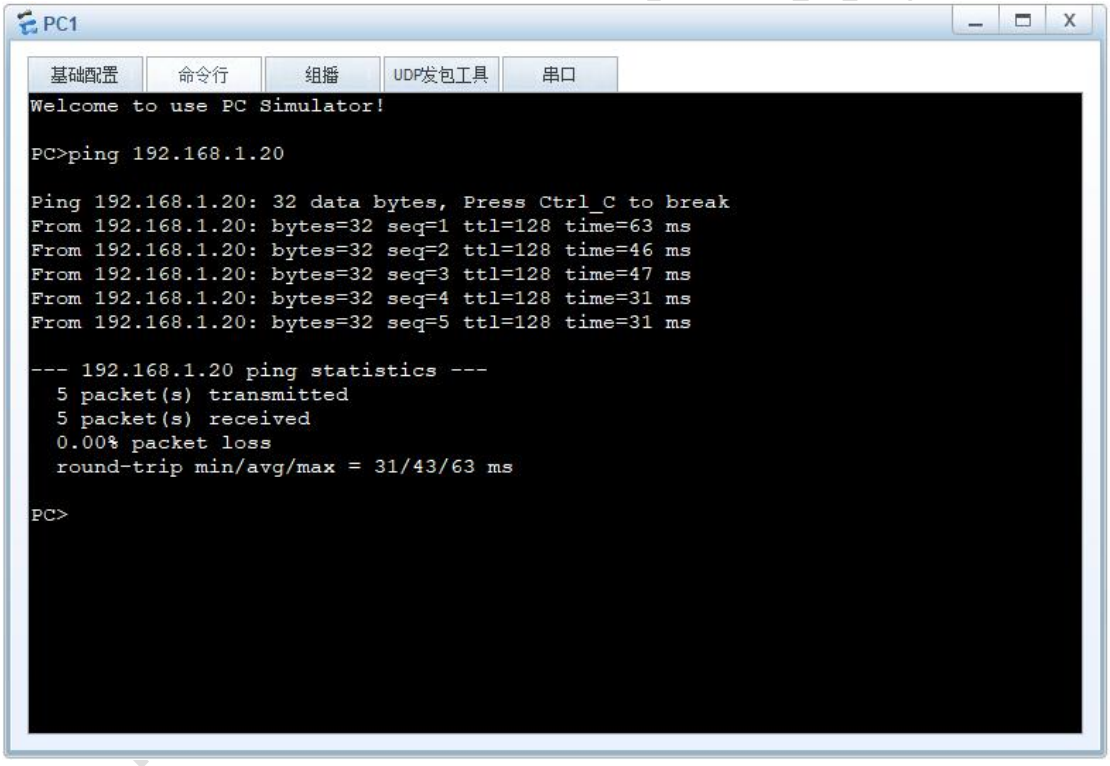
interface E0/0/4

port link-type access

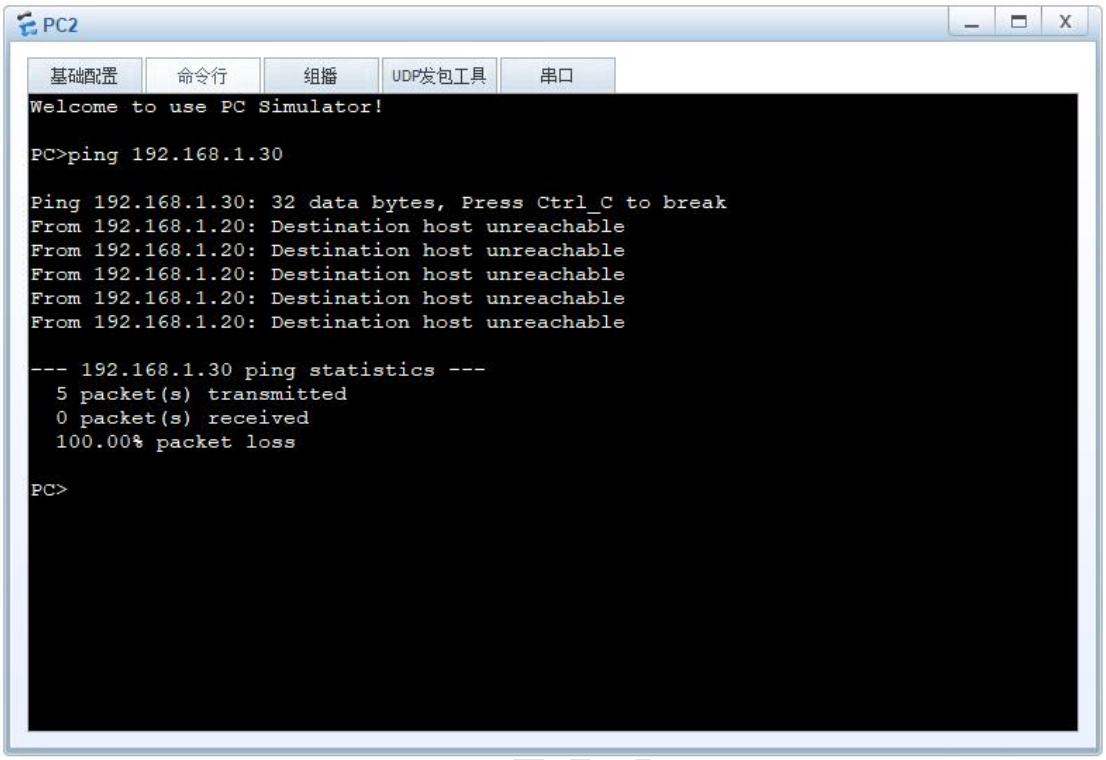
port default vlan 10

测试：

Client A 与 Client B 可正常通讯



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:

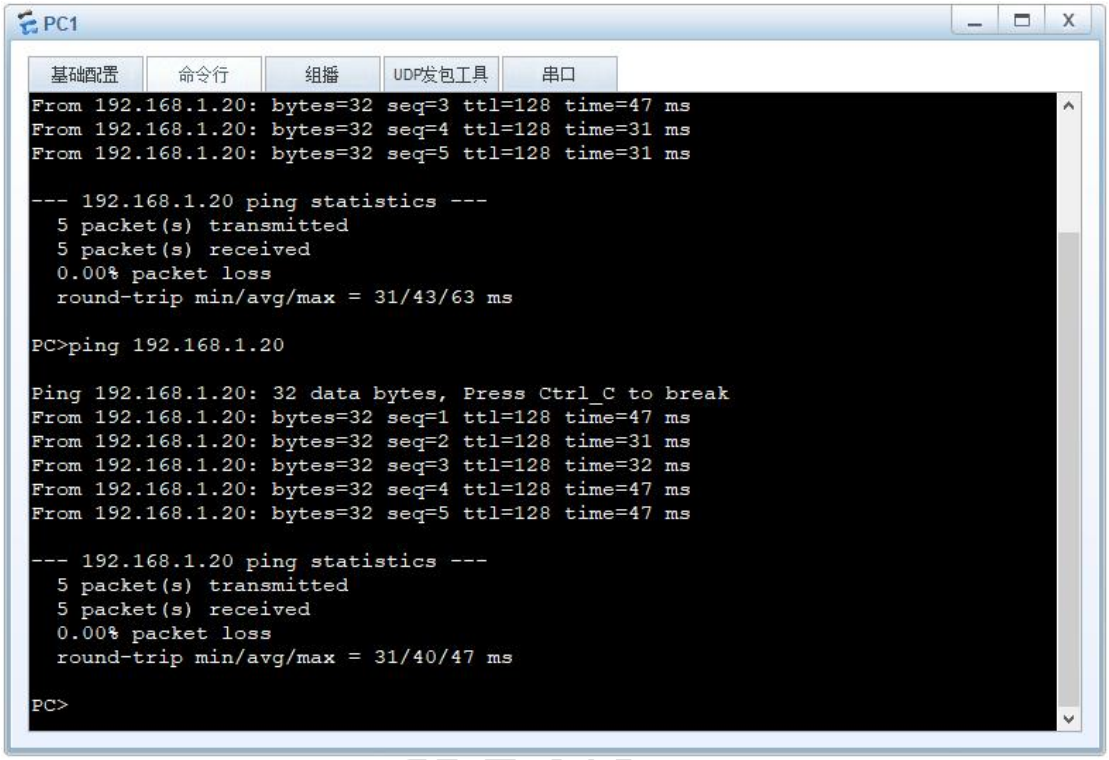
interface vlan 10

ip add 192.168.1.1 24

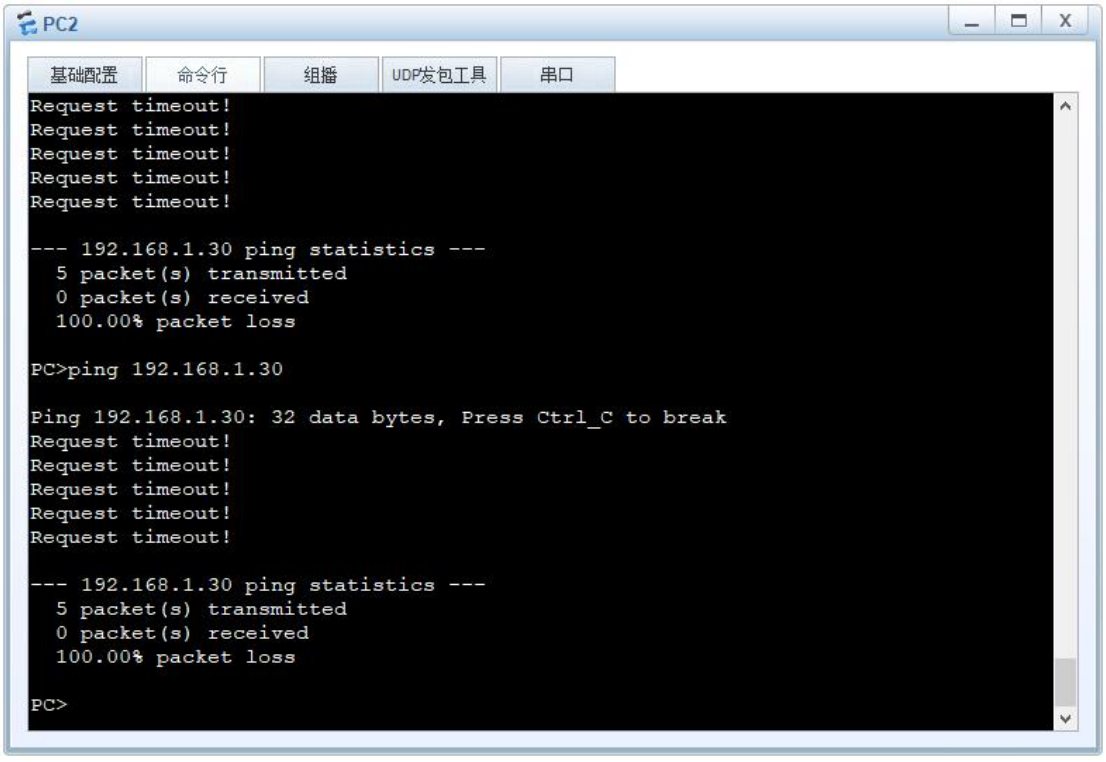
arp-proxy inner-sub-vlan-proxy enable　　#开启同 VLAN 内 ARP 代理功能

再次测试：

Client A 与 Client B 依旧可以正常通讯

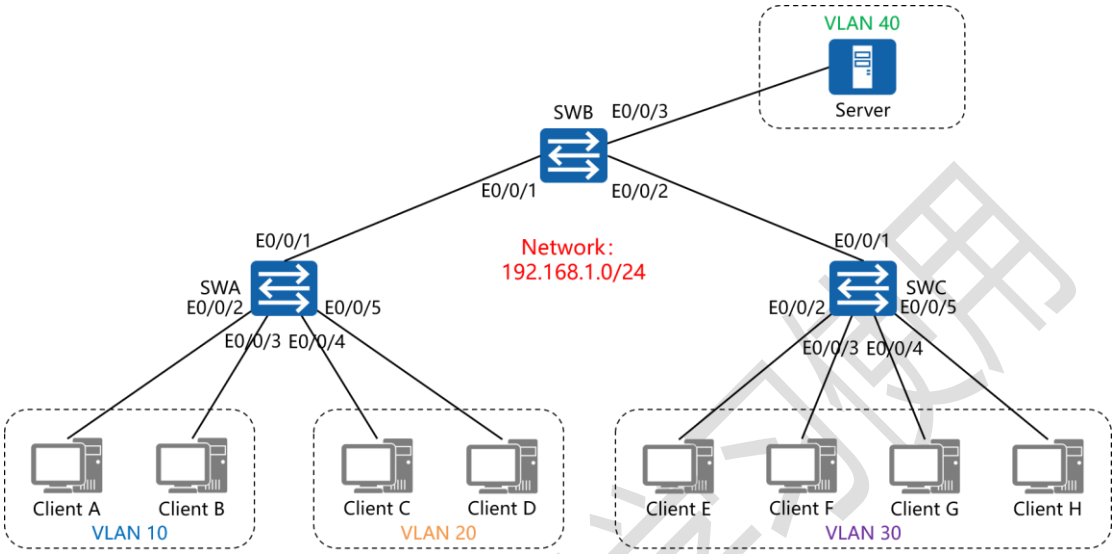


Client B 与 Client C 此时依旧无法正常通讯



三十八、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

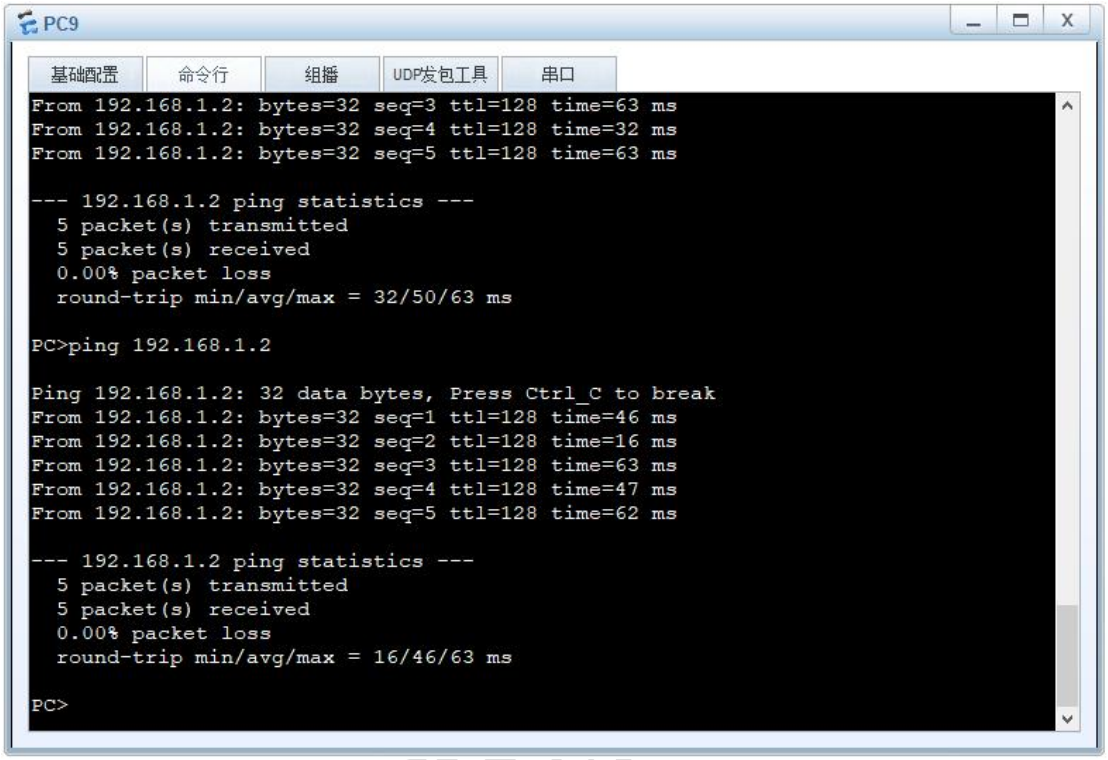
port trunk allow-pass vlan all

```
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
```

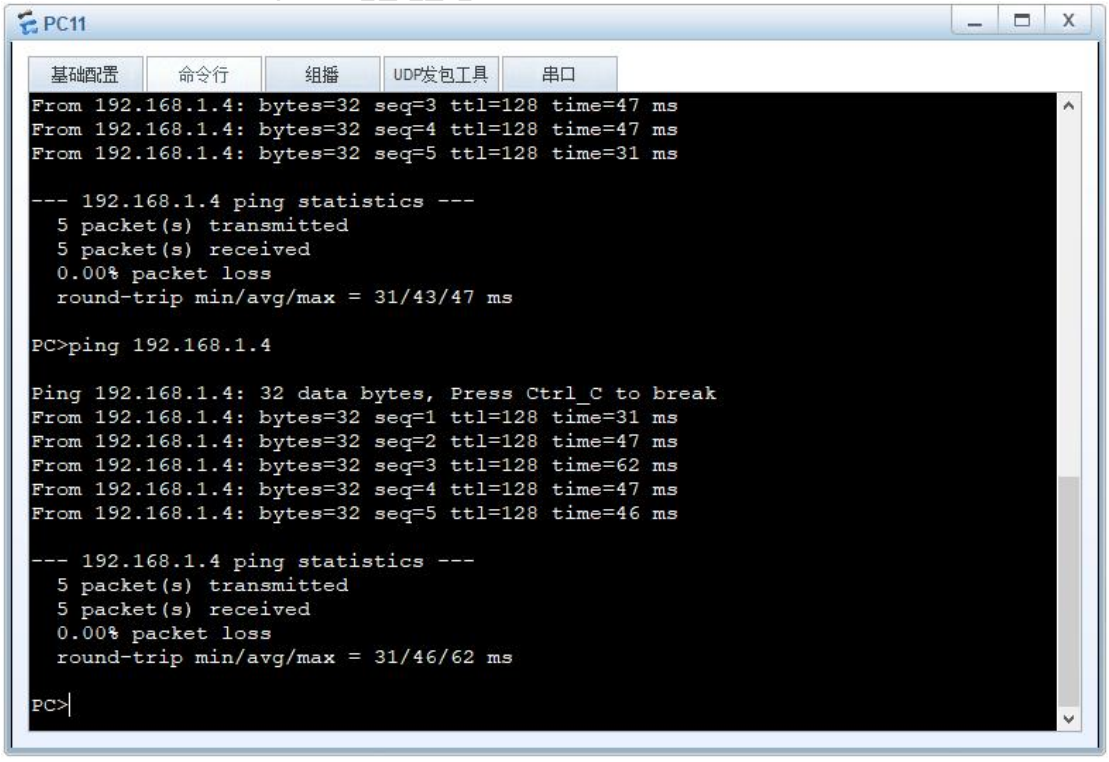
```
interface E0/0/3
port link-type access
port default vlan 30
port mux-vlan enable
interface E0/0/4
port link-type access
port default vlan 30
port mux-vlan enable
interface E0/0/5
port link-type access
port default vlan 30
port mux-vlan enable
```

测试：

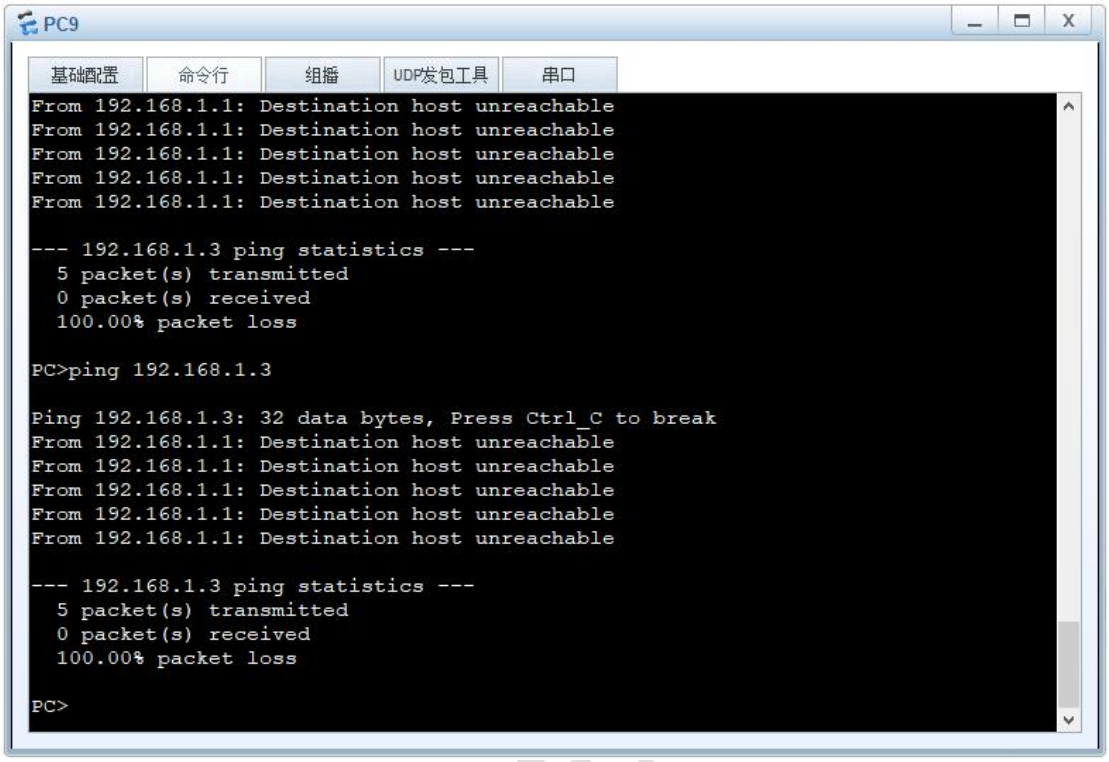
VLAN 10 内的 Client A 与 Client B 可相互访问



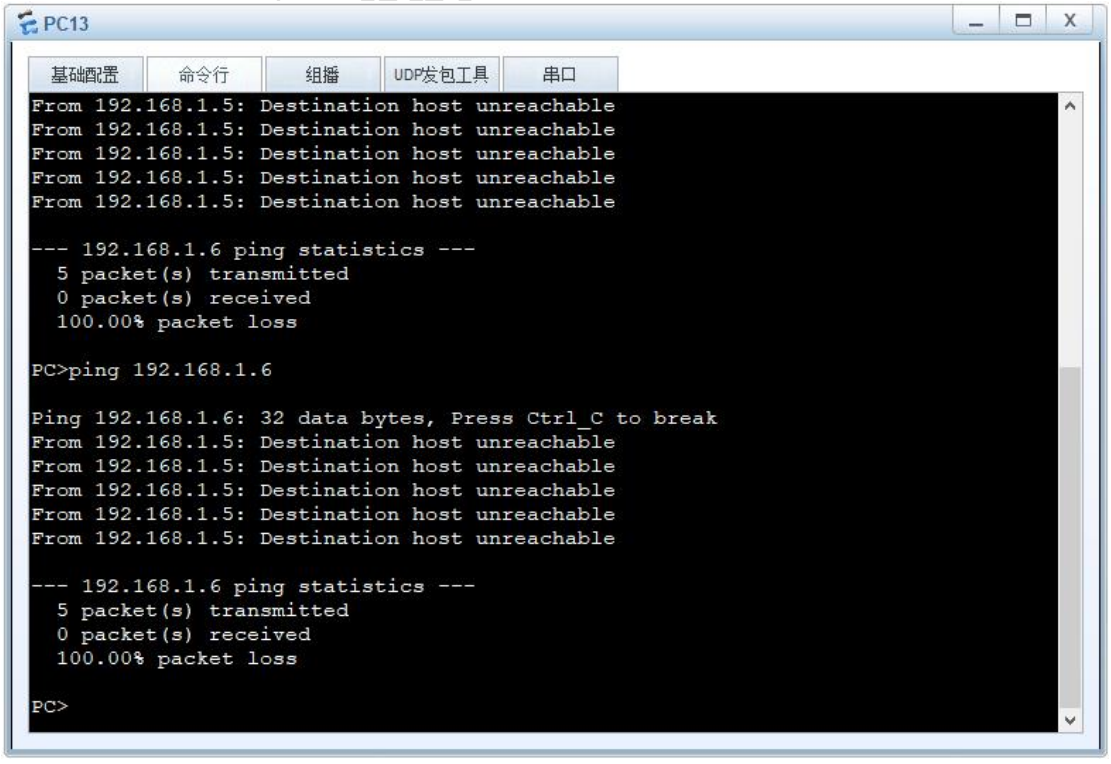
VLAN 20 内的 Client C 与 Client D 可相互访问



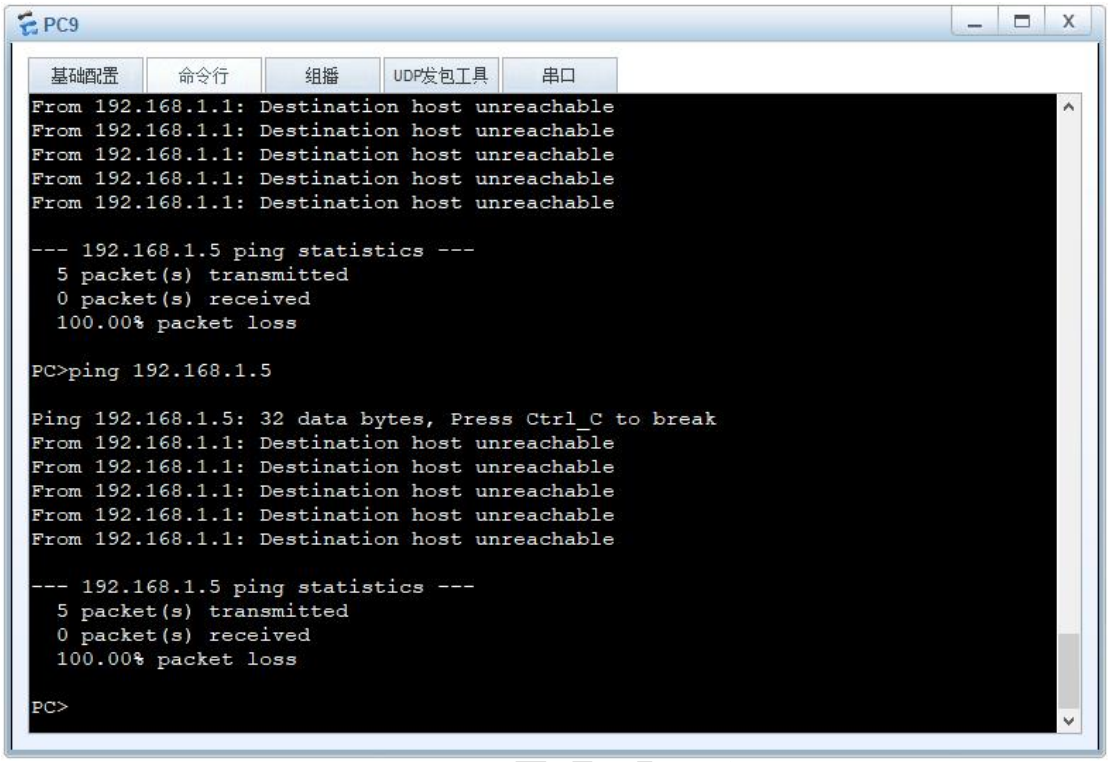
VLAN 10 内的 Client A 与 VLAN 20 内的 Client C 无法互访



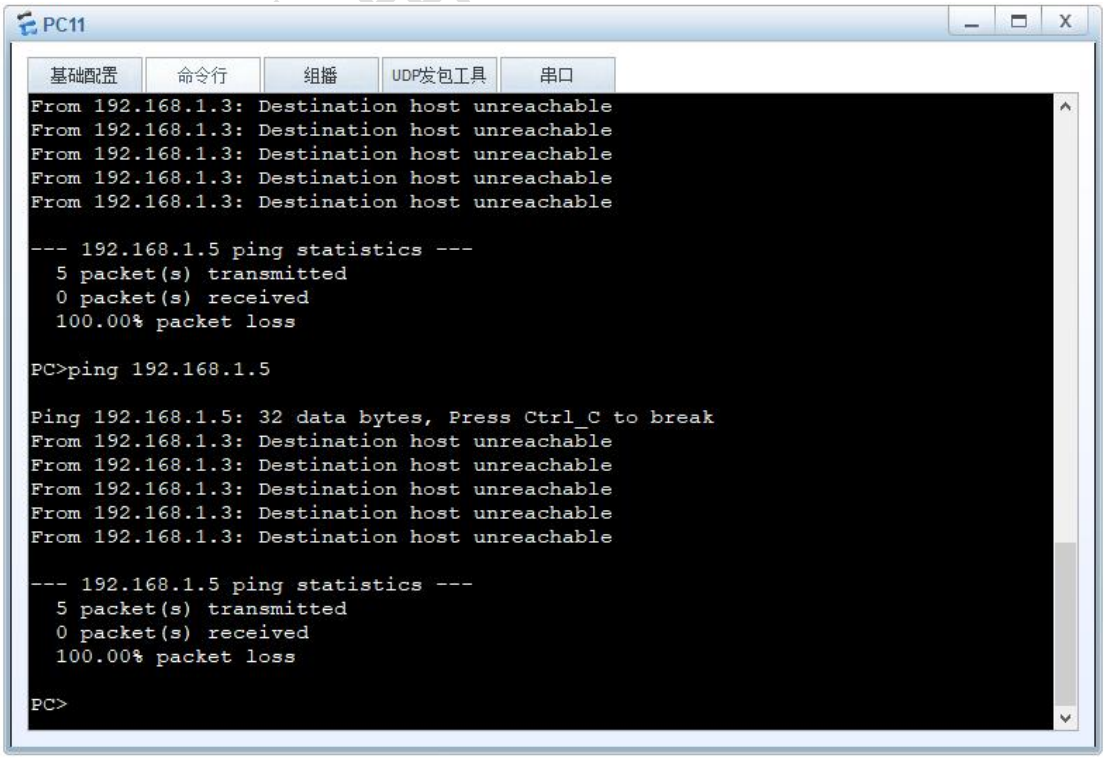
VLAN 30 内的所有 Client 均不可相互访问



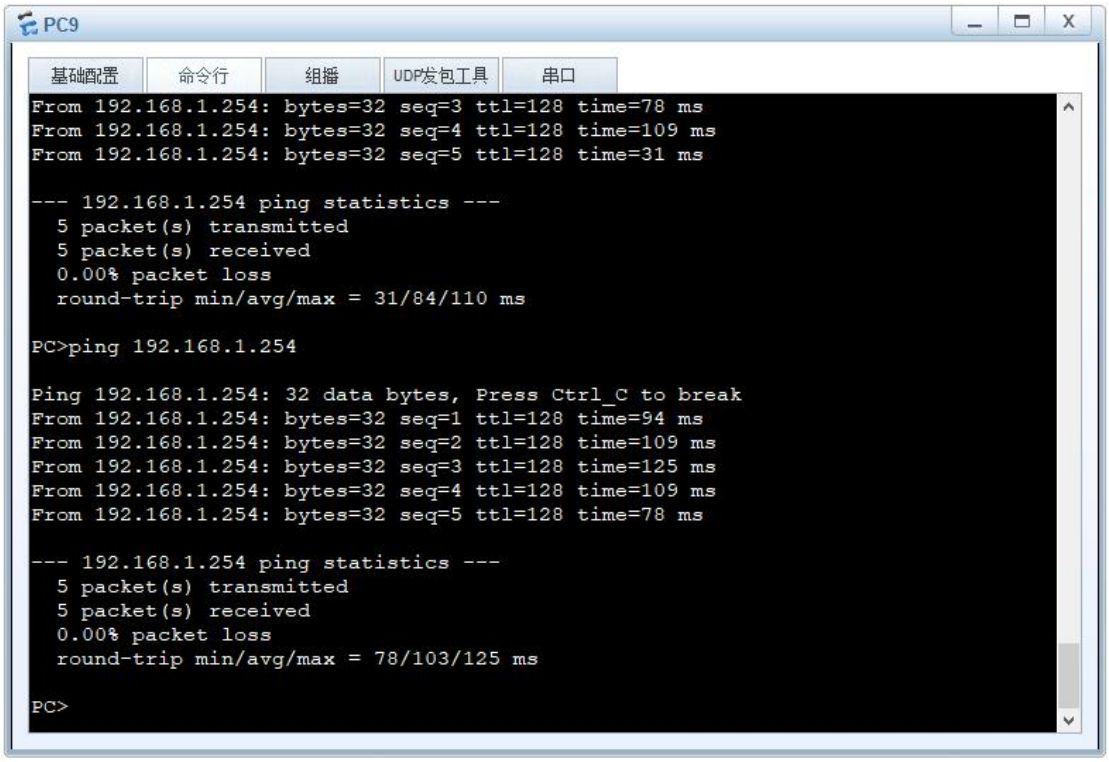
VLAN 10 内的 Client A 与 VLAN 30 内的 Client E 不可互访



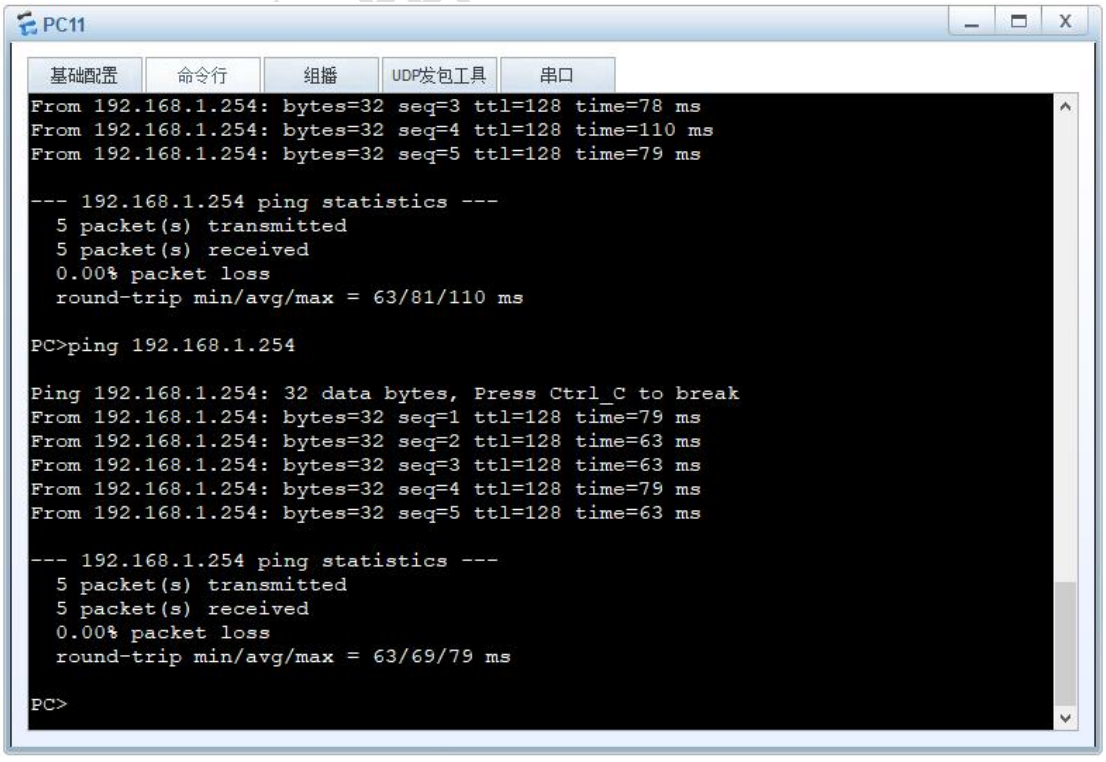
VLAN 20 内的 Client C 与 VLAN 30 内的 Client E 不可互访



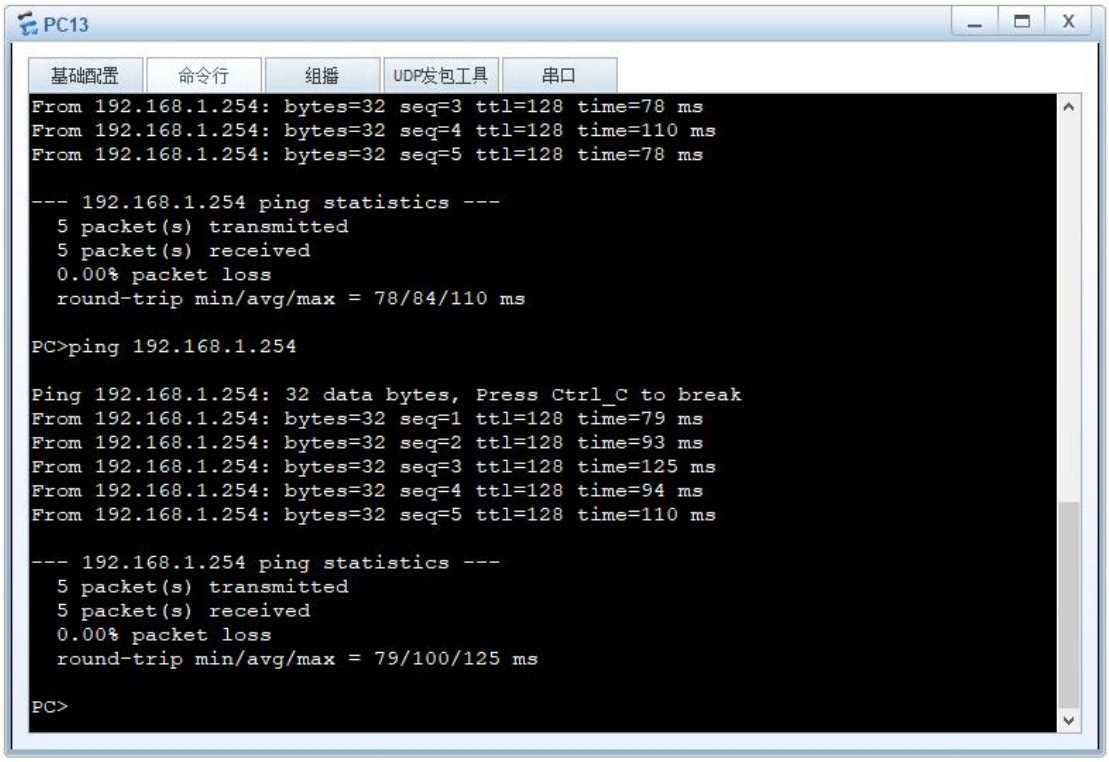
VLAN 10 内的 Client A 与 VLAN 40 内的 Server 可相互访问



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

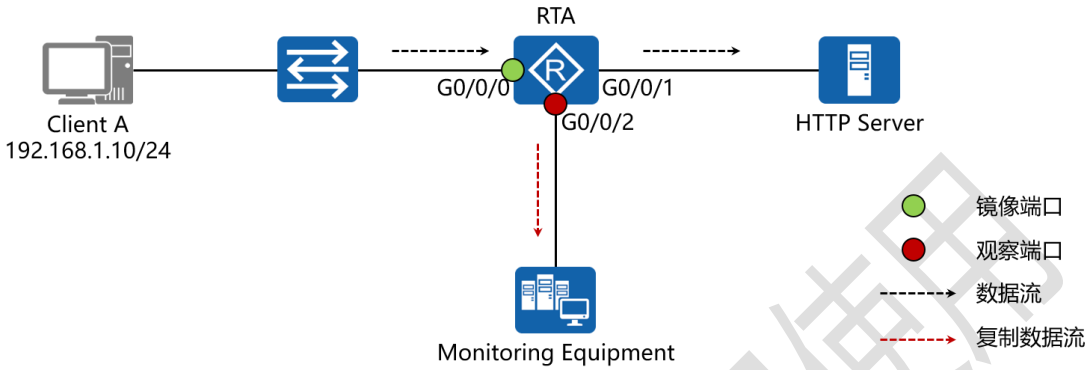


VLAN 30 内的 Client E 与 VLAN 40 内的 Server 可相互访问



三十九、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

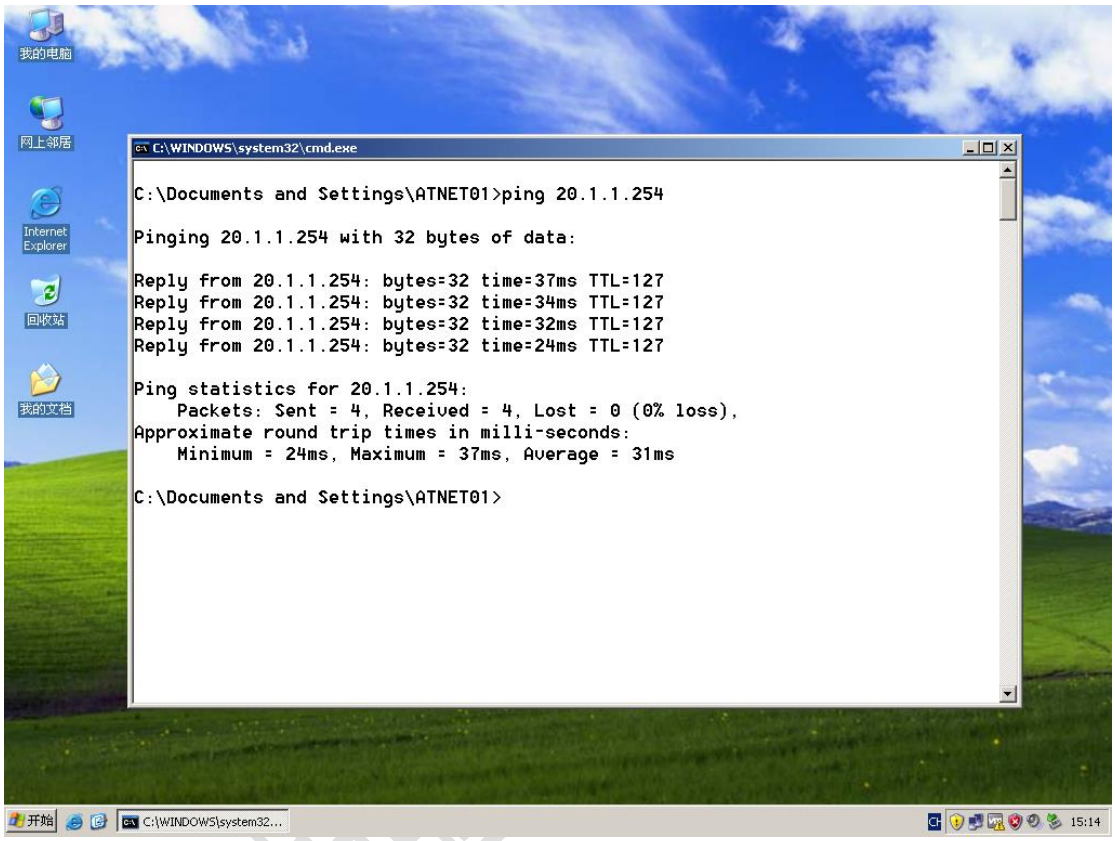
ip address 20.1.1.1 24　　#配置 IP 地址及子网掩码

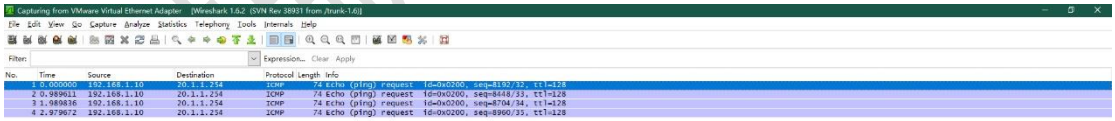
interface G0/0/2　　#进入相应的接口

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

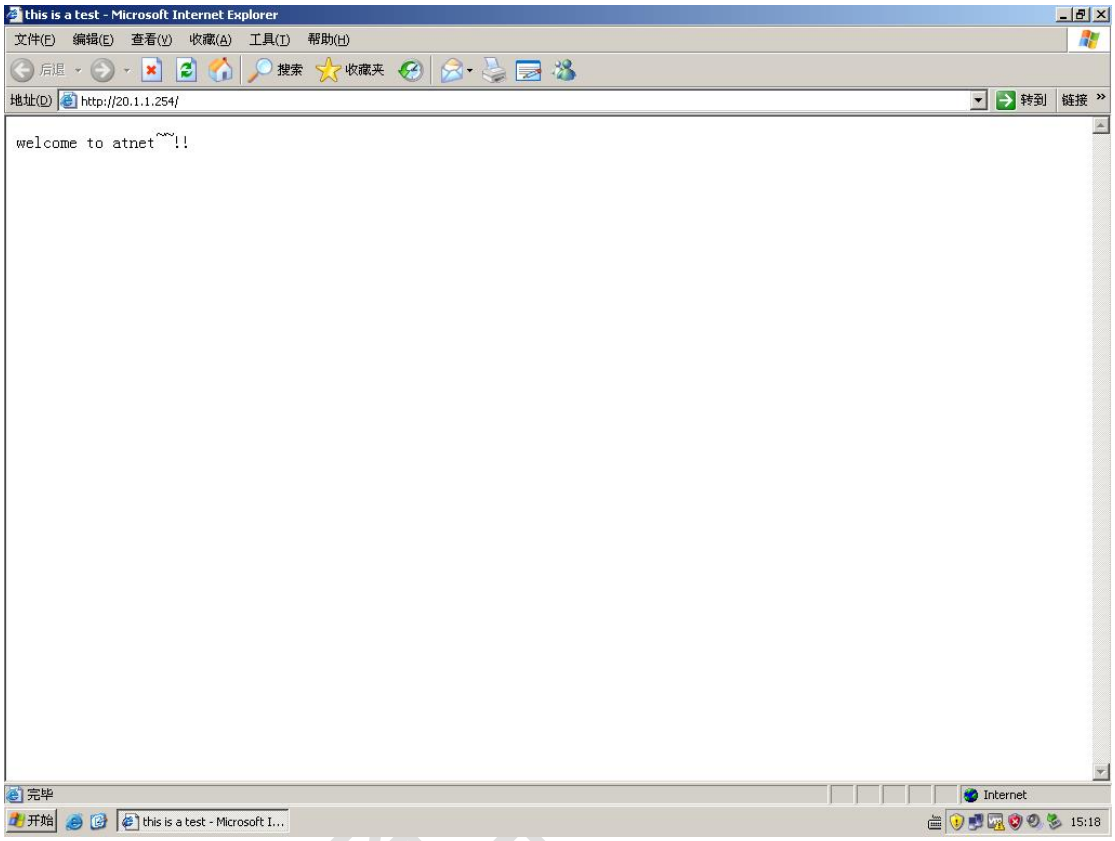
测试：

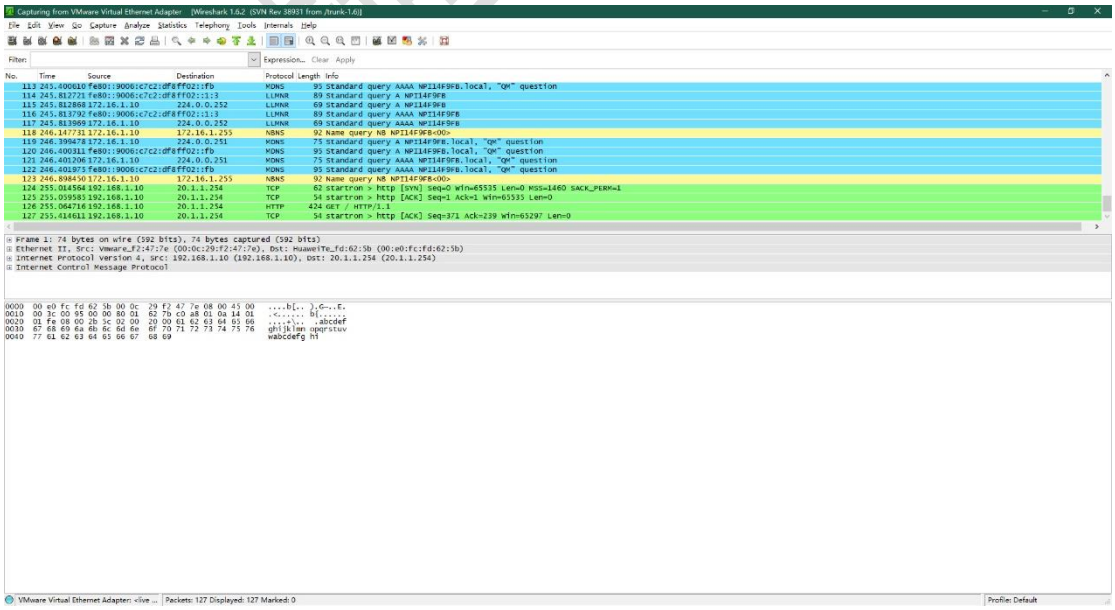
从 Client A 去 ping HTTP Server（20.1.1.254/24），同时在监控设备上使用 Wireshark 观察结果：





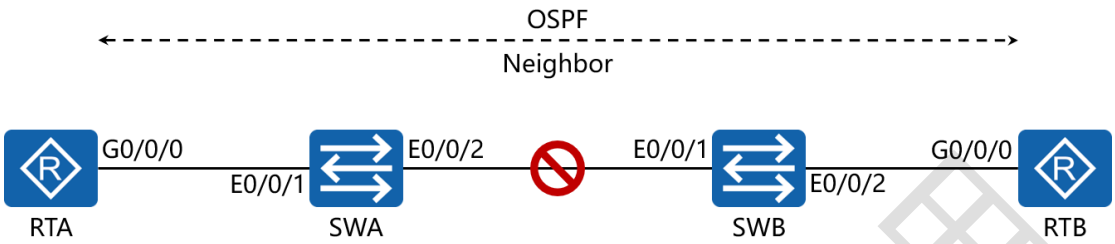
从 Client A 去访问 HTTP Server（20.1.1.254/24）的网页，同时在监控设备上使用 Wireshark 观察结果：





四十、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

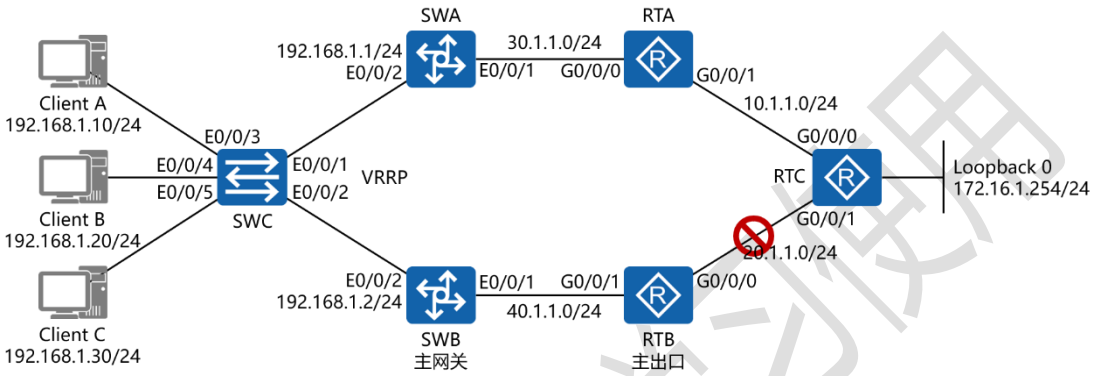
bfd all-interfaces enable

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

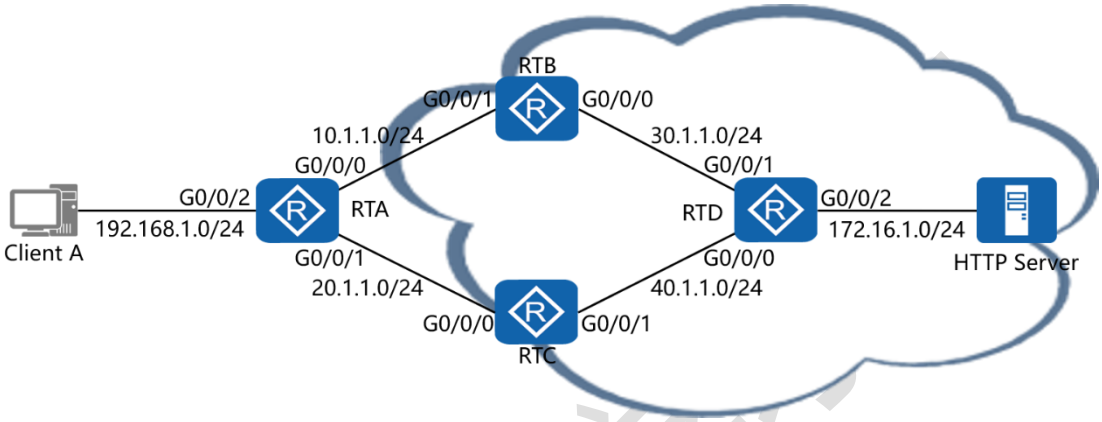
SWC:

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   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
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/2
    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]
```

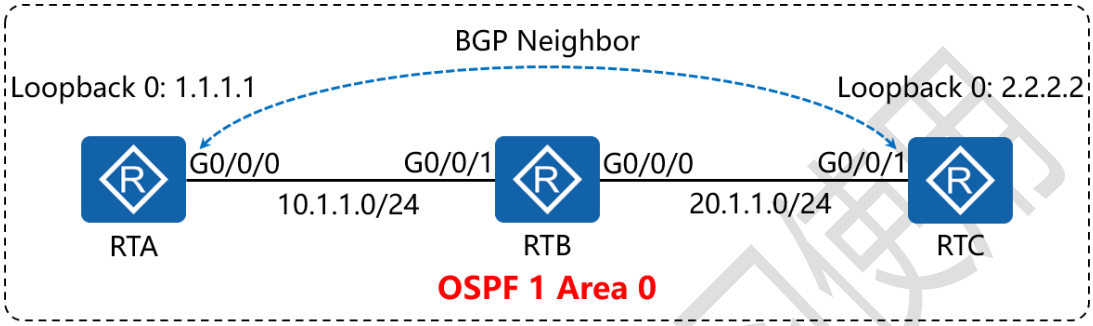
在 RTB 与 RTD 之间的链路失效后，再次查看 RTA 的路由表项：

```
[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

        0.0.0.0/0   Static  80   0           RD  20.1.1.2        GigabitEthernet
0/0/1
       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
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/2
    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]
```

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

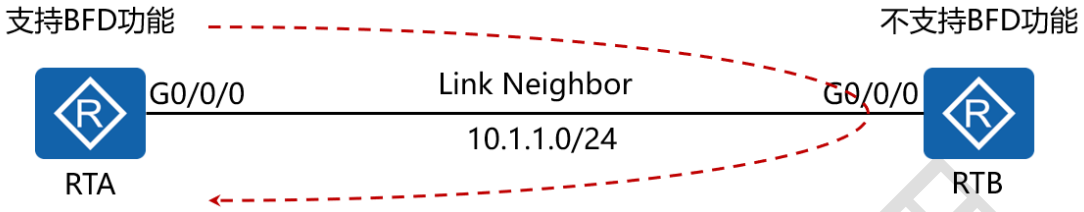
area 0

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

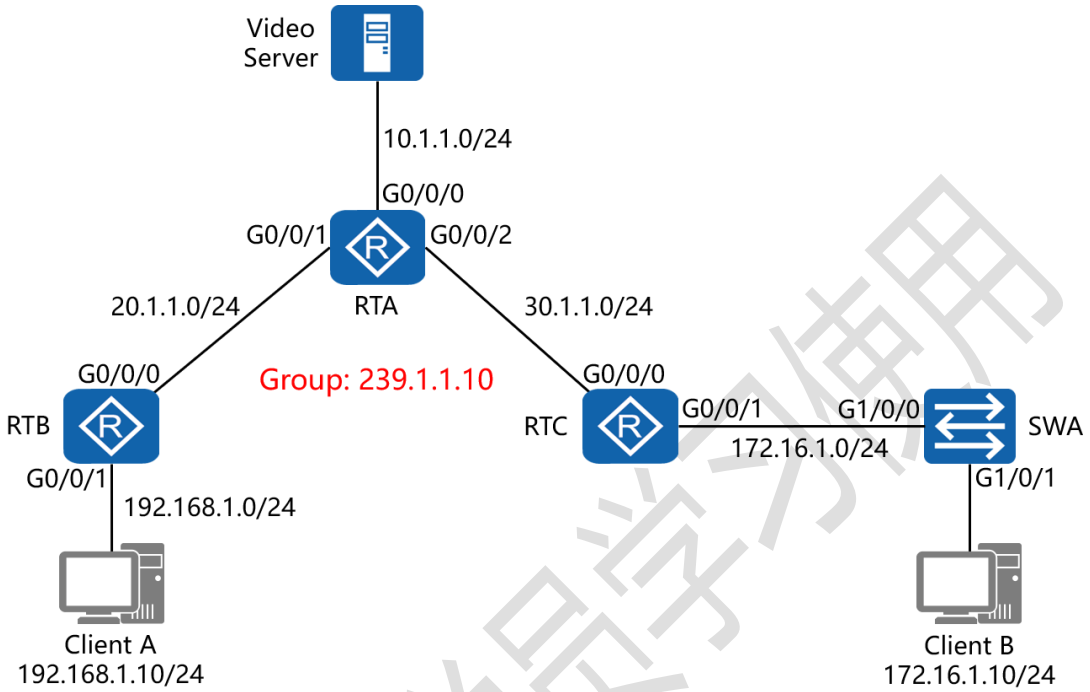
sysname RTB

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]
```

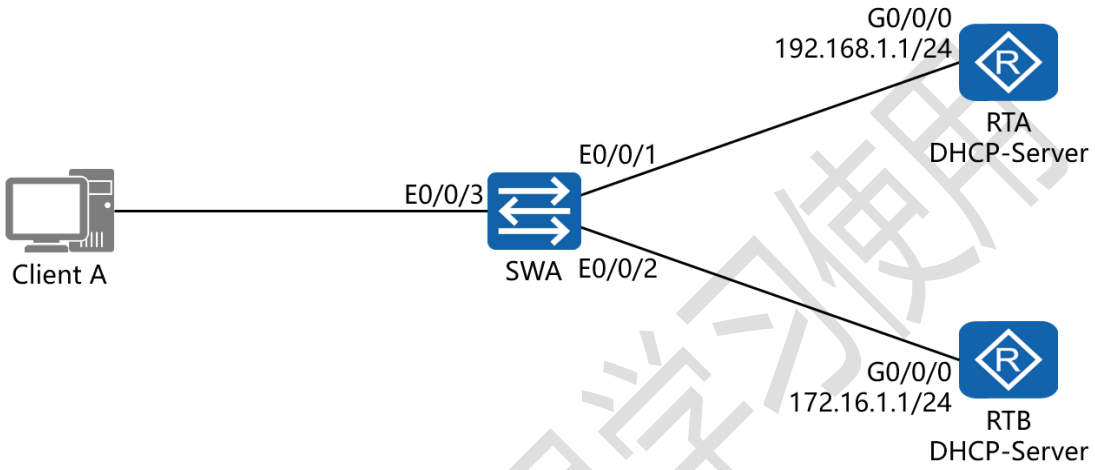
当 Client B 加入组播组 239.1.1.10 并收看 Video Server 发布的视频时，再次查看 SWA 的 IGMP Snooping 端口信息：

```
[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

四十六、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:

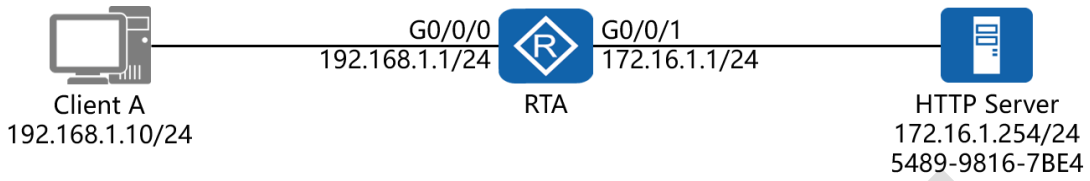
system-view

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
```

四十七、配置简单流分类实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上配置简单流分类，针对 HTTP Server【5489-9816-7BE4】发出的所有流量，将 DSCP 值重标记为 2

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 G0/0/1　　#进入相应接口

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

traffic classifier test　　#创建传输类列表

if-match source-mac 5489-9816-7BE4　　#匹配 HTTP Server 的 MAC 地址

traffic behavior test　　#创建传输行为列表

remark dscp 2　　#重标记 DSCP 值为 2

traffic policy easthome　　#创建传输策略列表

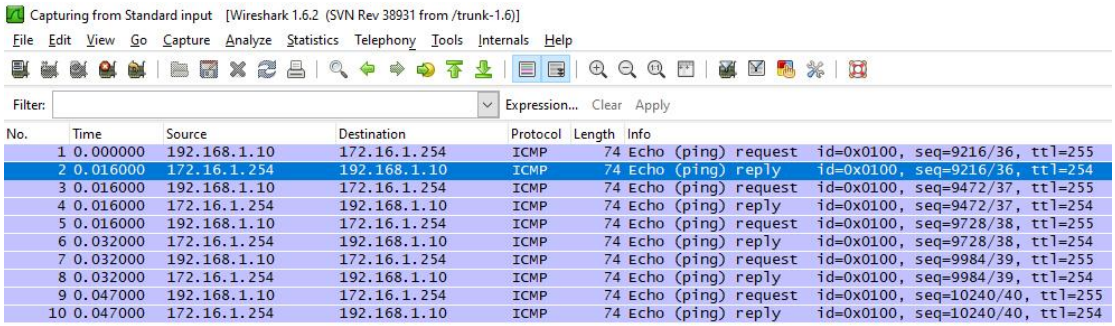
classifier test behavior test　　#同时调用传输类与传输行为列表

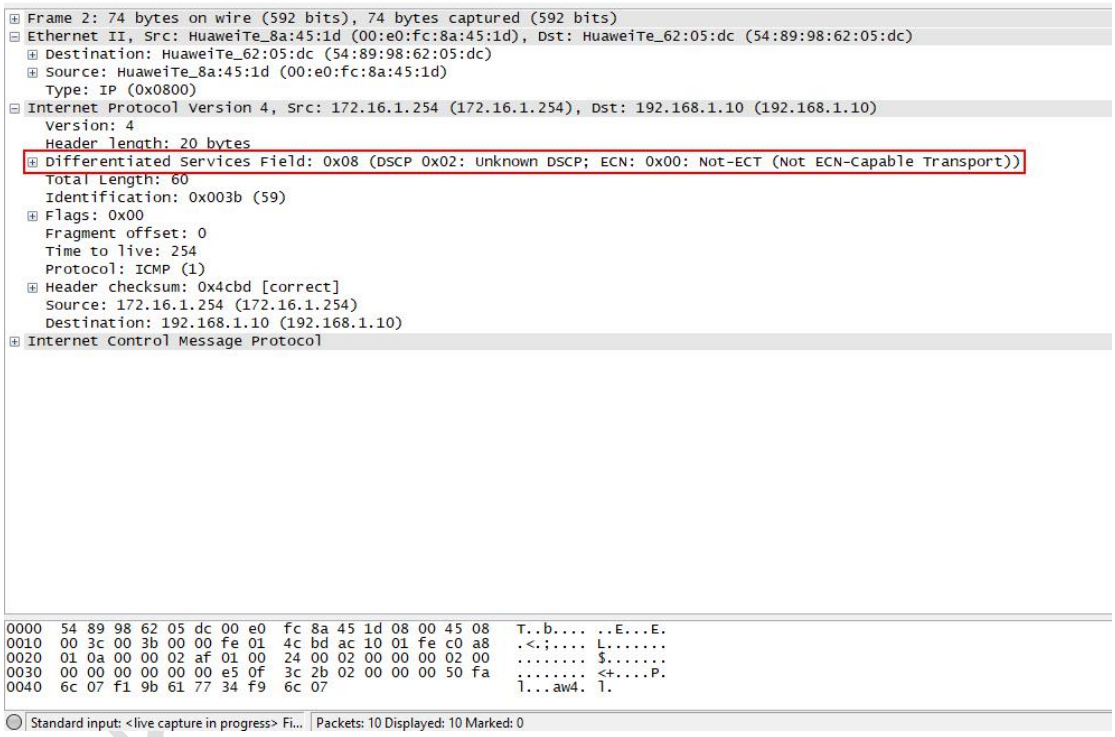
interface G0/0/1　　#进入相应接口

traffic-policy easthome inbound　　#在接口的入方向上调用传输策略

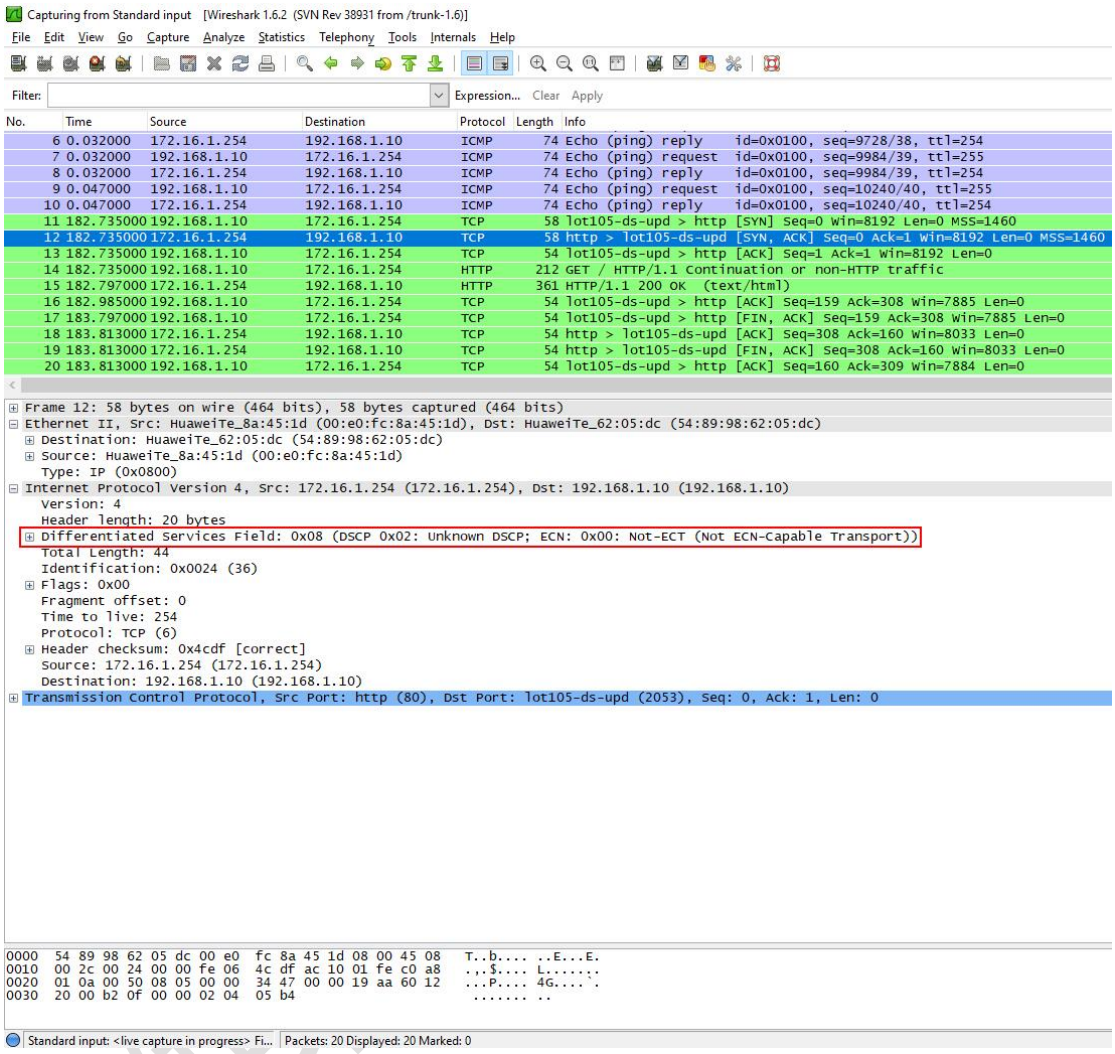
测试：

通过 Client A ping HTTP Server，在 RTA 的 G0/0/0 接口上抓包，观察当前报文的 DSCP 值

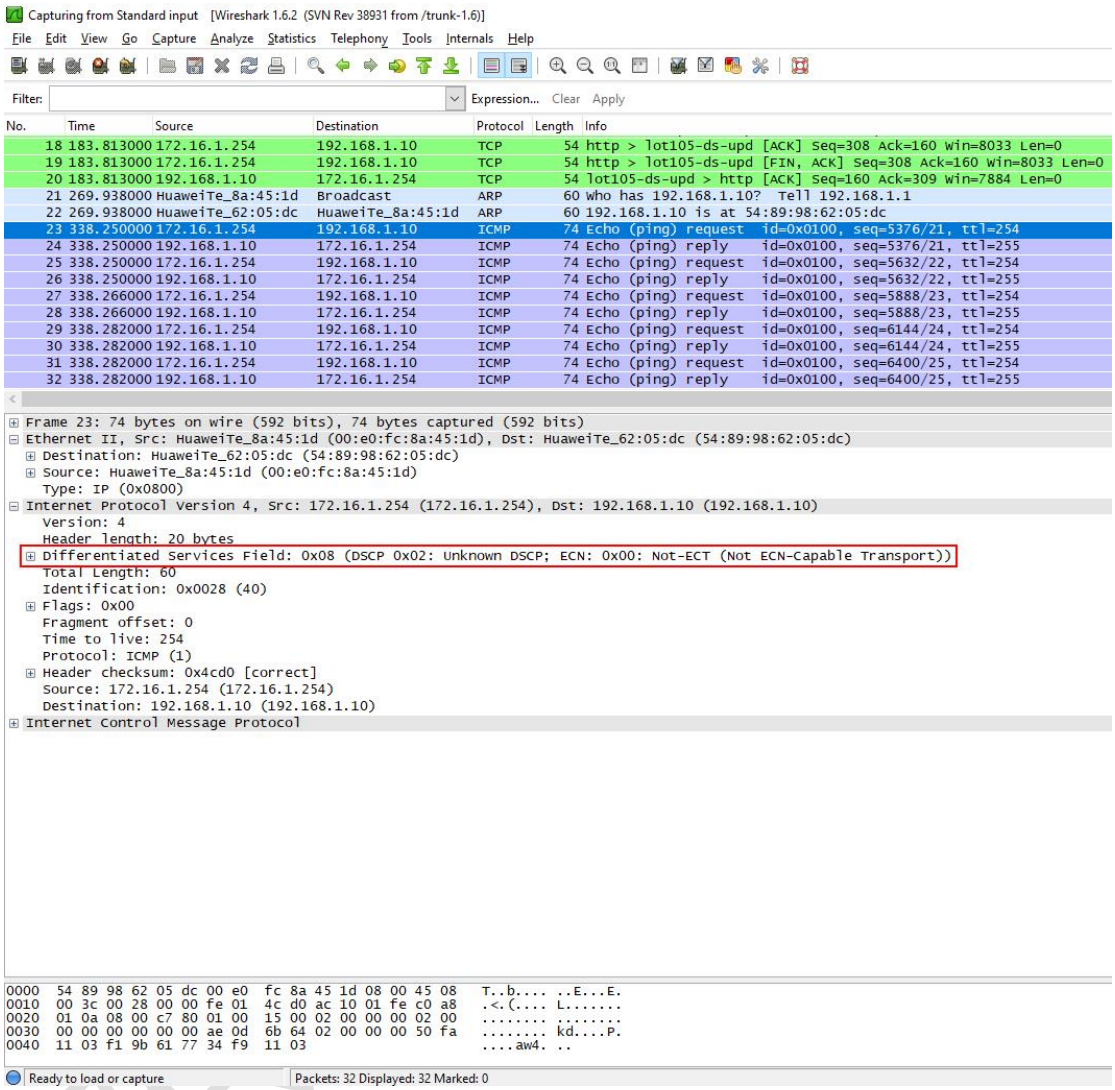




令 Client A 访问 HTTP Server 的网页内容，在 RTA 的 G0/0/0 接口上抓包，观察当前报文的 DSCP 值

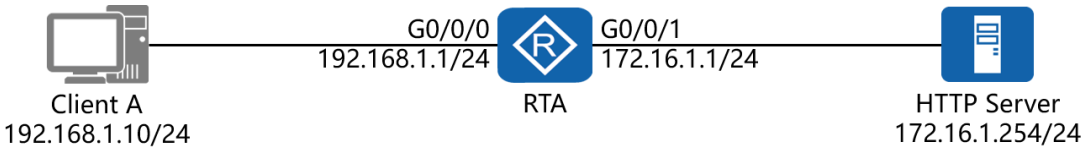


通过 HTTP Server ping Client A，在 RTA 的 G0/0/0 接口上抓包，观察当前报文的 DSCP 值



四十八、配置复杂流分类实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上配置复杂流分类，为 HTTP Server 的流量传输提供优先转发服务

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 G0/0/1　　#进入相应接口

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

acl 3001　　#创建高级 ACL

rule permit tcp source-port eq 80　　#匹配 TCP 服务源端口号码

traffic classifier http　　#创建传输类列表

if-match acl 3001　　#匹配 ACL 3001

traffic behavior http　　#创建传输行为列表

remark dscp 3　　#重标记 DSCP 值为 3

traffic policy easthome　　#创建传输策略列表

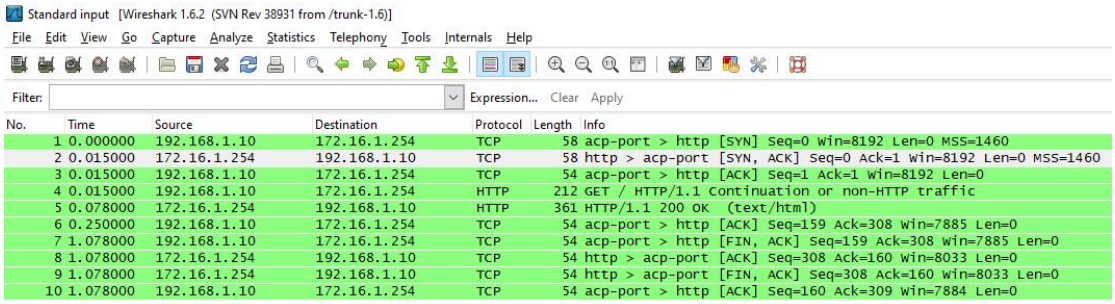
classifier http behavior http　　#同时调用传输类与传输行为列表

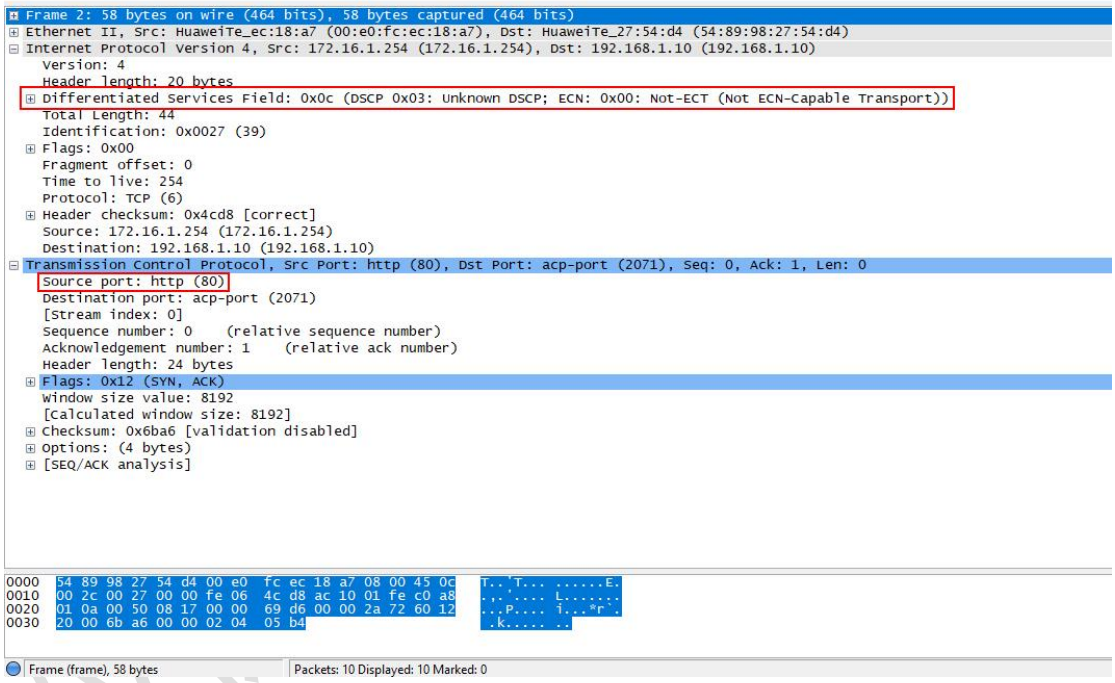
interface G0/0/0　　#进入相应接口

traffic-policy easthome outbound　　#在接口的出方向上调用传输策略

测试：

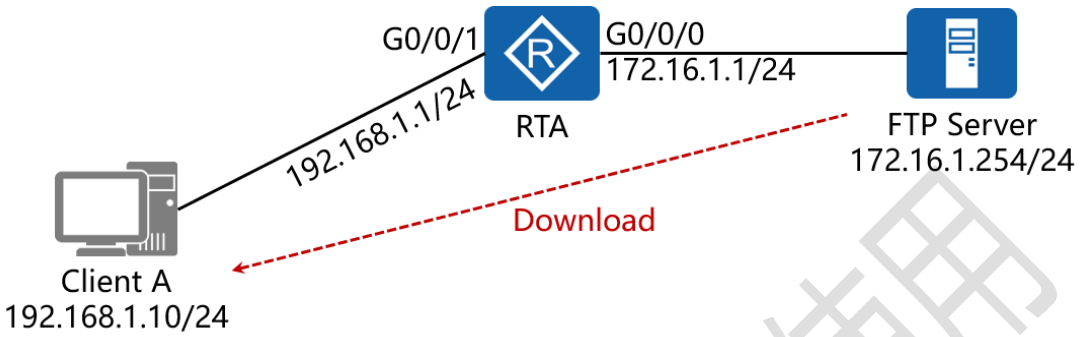
令 Client A 访问 HTTP Server 的网页内容，在 RTA 的 G0/0/0 接口上抓包，观察当前报文的 DSCP 值





四十九、配置流量整形实验组网

一、实验拓扑：



二、实验目的：

按上图所示，配置好所有设备的 IP 地址，保证 Client A 能够与 FTP Server 正常通讯，之后在 RTA 的 G0/0/1 接口的外出方向上配置流量整形限制速率，令 Client A 从 FTP Server 上下载文件，观察其速率的前后变化

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 172.16.1.1 24　　#配置 IP 地址及子网掩码

interface G0/0/1　　#进入相应的接口

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

acl 3001　　#创建高级 ACL

rule permit tcp source 172.16.1.254 0 source-port eq 20 destination 192.168.1.10 0 #在 TCP 协议下，允许来自 172.16.1.254，源端口 20，去往目的地 192.168.1.10 的流量

rule permit tcp source 172.16.1.254 0 source-port eq 21 destination 192.168.1.10 0 #在 TCP 协议下，允许来自 172.16.1.254，源端口 21，去往目的地 192.168.1.10 的流量

rule deny ip source any destination any #拒绝其它所有流量

traffic classifier ftp #创建传输类列表

if-match acl 3001 #匹配 ACL 3001

traffic behavior ftp #创建传输行为列表

gts cir 512 cbs 96256 #配置 GTS，并限定速率为 512Kbps

traffic policy atnet #创建传输策略列表

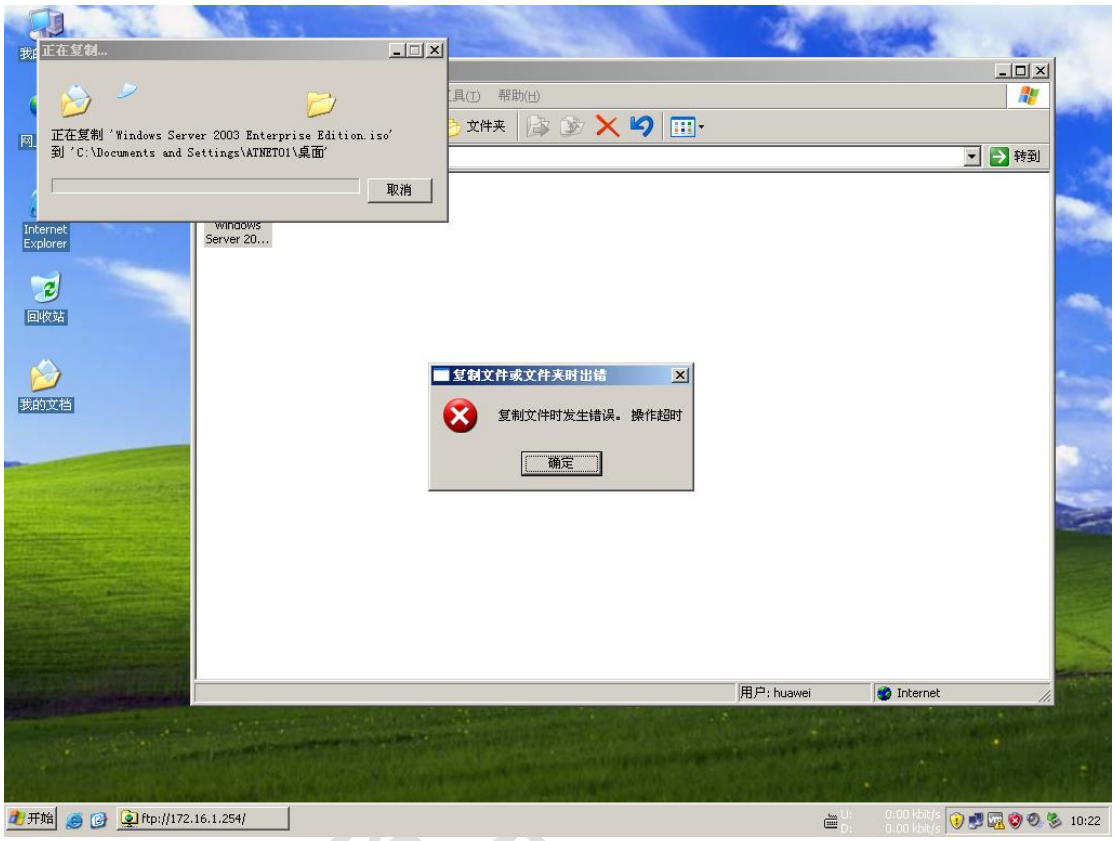
classifier ftp behavior ftp #同时调用传输类与传输行为列表

interface G0/0/1 #进入相应的接口

traffic-policy atnet outbound #在接口的出方向上调用传输策略

测试：

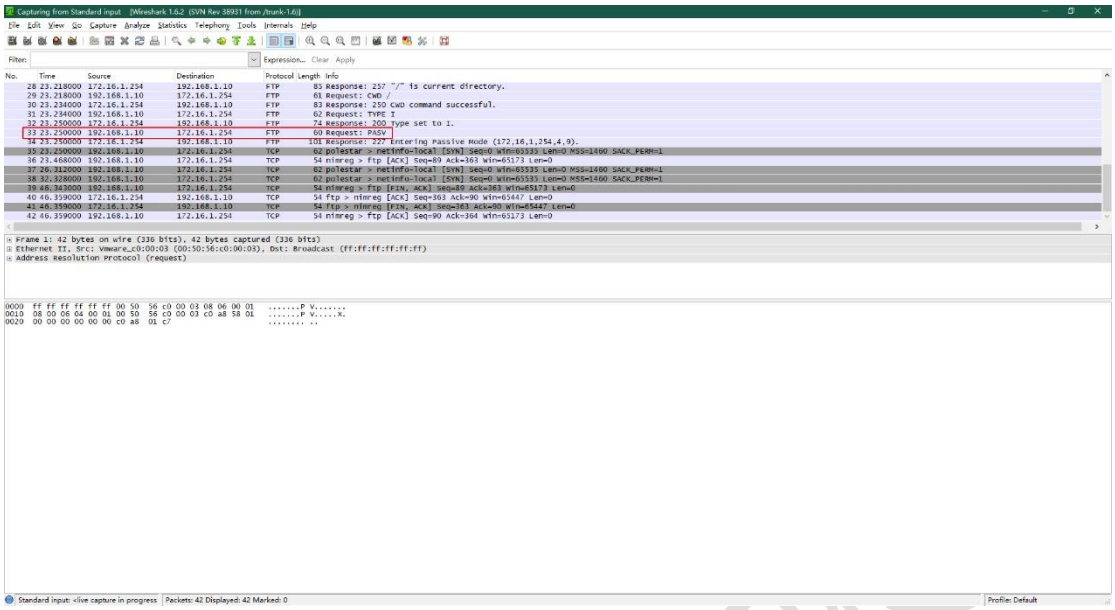
在 Client A 上访问 FTP Server，并开始下载文件



经测试，Client A 无法下载 FTP Server 上的文件

```
[RTA]display acl 3001
Advanced ACL 3001, 3 rules
Acl's step is 5
 rule 5 permit tcp source 172.16.1.254 0 source-port eq ftp-data destination 192
.168.1.10 0
 rule 10 permit tcp source 172.16.1.254 0 source-port eq ftp destination 192.168
.1.10 0 (36 matches)
 rule 15 deny ip (10 matches)

[RTA]
```

在 RTA 上查看 ACL 3001，发现 Client A 与 FTP Server 建立连接的语句被匹配了 36 次，其余所有数据传输均被拒绝，ftp-data 的语句没有被匹配到



通过在 RTA 的 G0/0/1 接口上抓包发现，来自 192.168.1.10，去往 172.16.1.254 的 FTP 的 Request（请求）报文中，其模式为 PASV（PASV 为 FTP 的被动模式）

注：FTP（文件传输协议）分为主动模式与被动模式

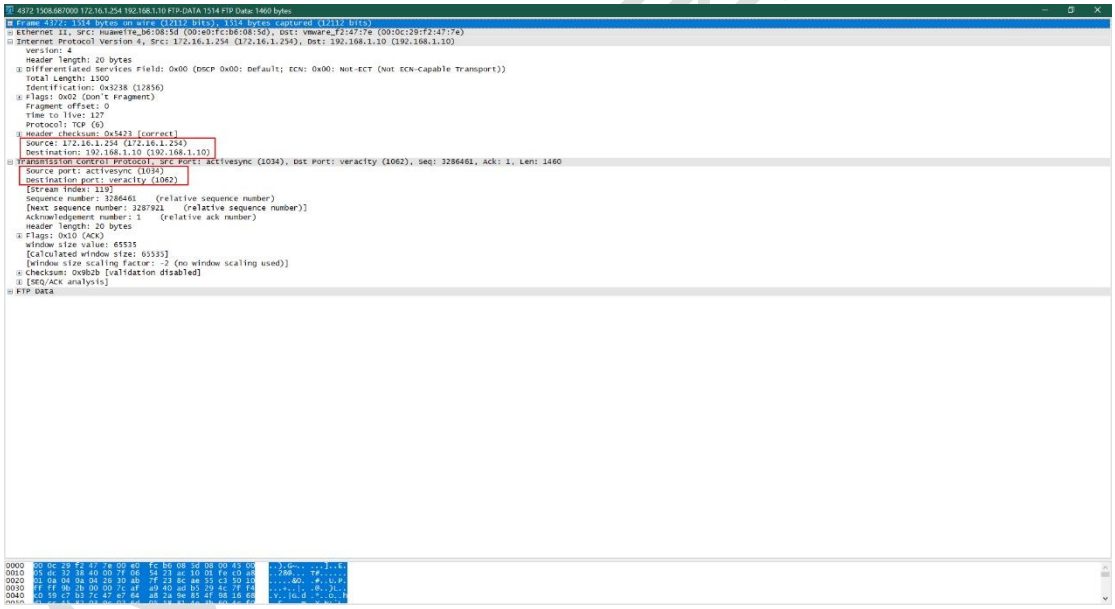
在主动模式下，FTP 客户端从任意的非特殊端口（N > 1023）连接至 FTP 服务器的命令端口（21），之后客户端在 N+1（N+1 >= 1024）端口进行监听，并通过 N+1（N+1 >= 1024）端口发送命令至 FTP 服务器，服务器再通过 20 号端口反向连接客户端本地指定的数据端口

在被动（PASV）模式下，命令连接及数据连接均由客户端发起。当开启一个 FTP 连接时，客户端打开两个任意的非特殊本地端口（N > 1024 及 N+1）。第一个端口连接服务器的 21 号端口，但与主动方式的 FTP 不同，客户端不会提交 PORT 命令并允许

服务器反向连接其数据端口，而是提交 PASV 命令。此时服务器会开启一个任意的非特殊端口（P > 1024），并发送 PORT（P）命令给客户端，之后客户端发起自本地端口（N+1）至服务器的端口（P）的连接用来传输数据

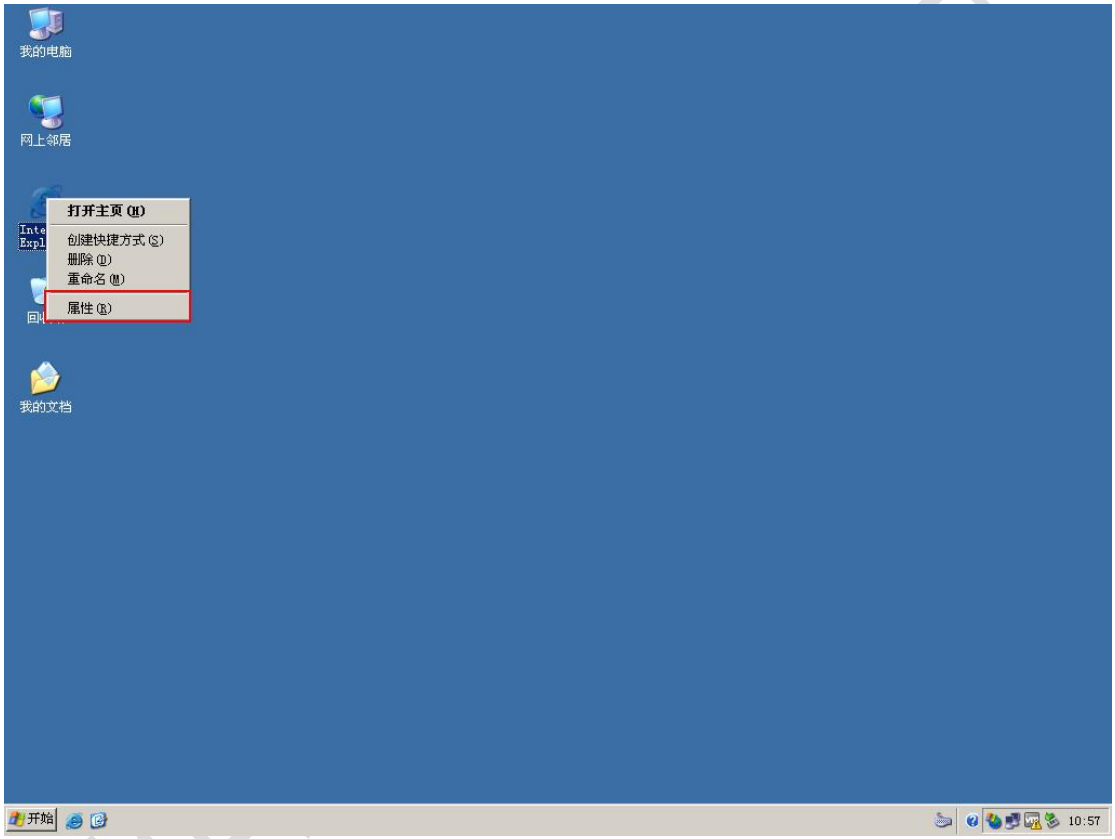
默认情况下，FTP Server 使用被动模式

此时，为验证 FTP Server 的被动模式，先将 RTA 接口 G0/0/1 上的传输策略删除，令传输不被阻止，之后再次抓取接口 G0/0/1 上的数据包

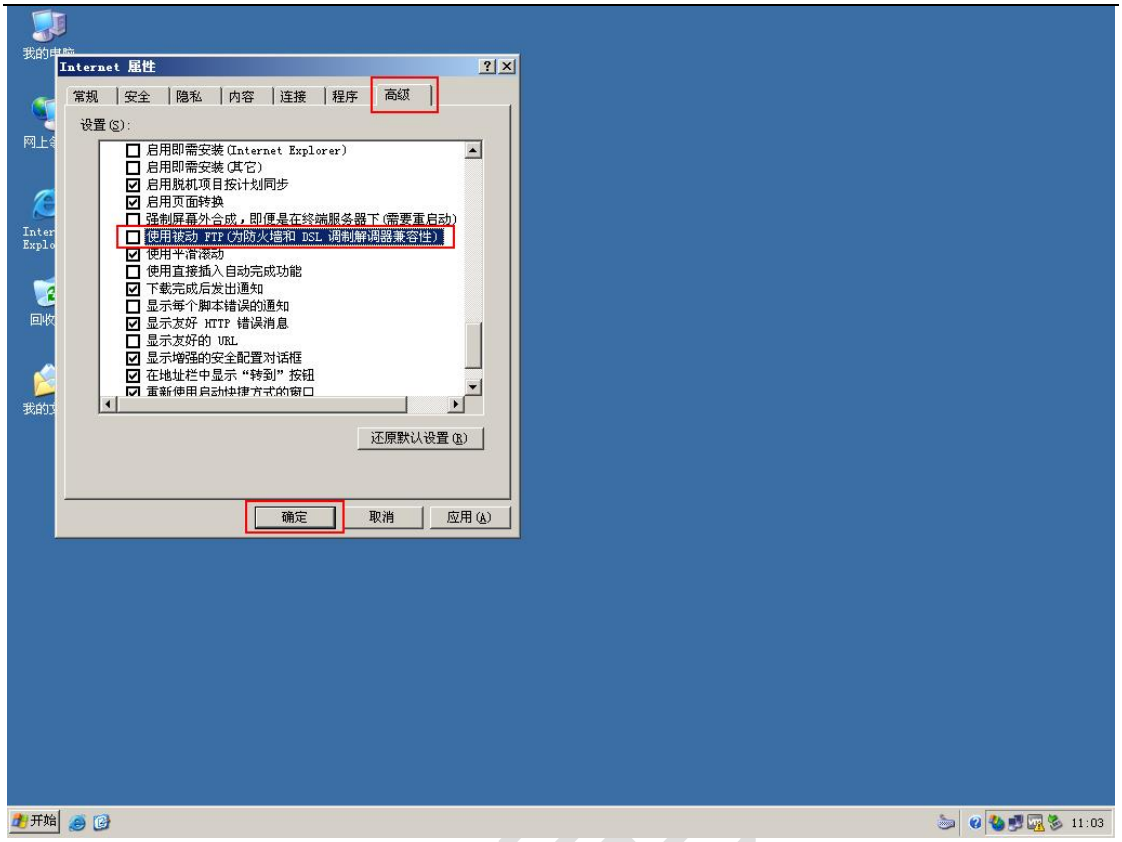


通过抓取接口 G0/0/1 上的数据包发现，FTP Server 使用端口号 1034 作为源端口号码向 Client A 传输数据；因此，RTA 上 ACL 3001 中的 ftp-data 语句不会被匹配，故所有数据流量均被拒绝

若希望 ACL 3001 中的 ftp-data 语句能够被成功匹配，则需要将 FTP Server 的被动模式更改为主动模式，令其通过 20 号端口发送数据，在 Windows Server 上，更改 FTP 为主动模式的方式如下：



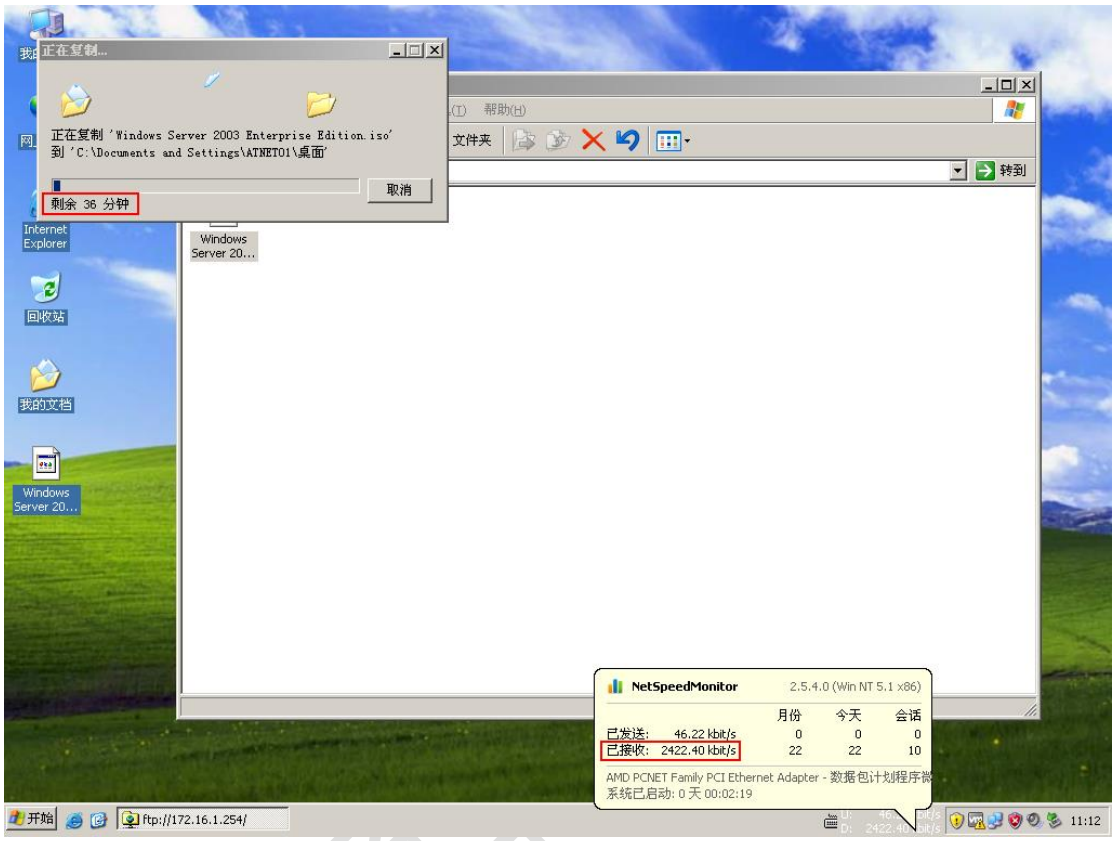
在 IE 浏览器上单击右键，选择“属性”



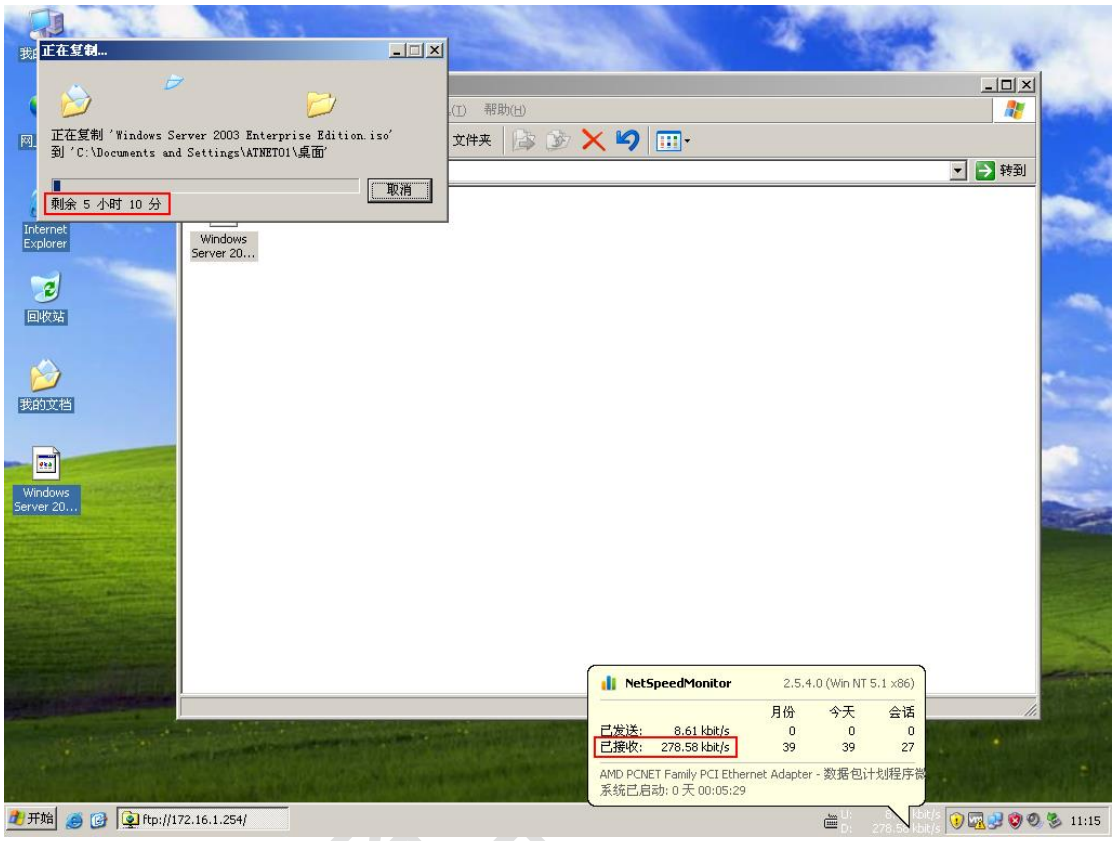
在打开的属性页面中，选择“高级”选项页，取消掉“使用被动 FTP (为防火墙和 DSL 调制解调器兼容性)”选项，并单击确定，之后需重启系统；在 Client A 上，亦需要同样的操作，此处不再截图赘述

FTP Server 与 Client A 上的操作完成后，再次使用 Client A 连接 FTP Server，进行文件的下载

在 RTA 的接口 G0/0/1 没有应用传输策略时，观察其下载速率与所需时间



此时，在 RTA 的接口 G0/0/1 上应用传输策略，再次观察其下载速率与所需时间

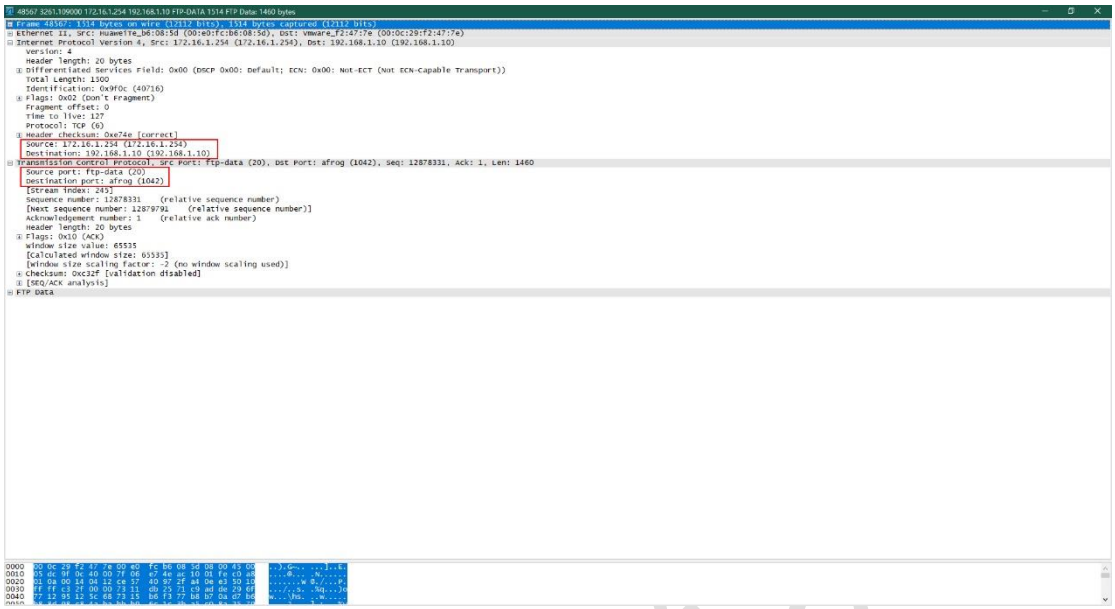


实验结果证明，通过传输策略的干预，下载速率明显下降，同时下载所需时间明显加长，再在 RTA 上观察 ACL 3001 的匹配结果

```
[RTA]display acl 3001
Advanced ACL 3001, 3 rules
Acl's step is 5
 rule 5 permit tcp source 172.16.1.254 0 source-port eq ftp-data destination 192
.168.1.10 0 (5925 matches)
 rule 10 permit tcp source 172.16.1.254 0 source-port eq ftp destination 192.168
.1.10 0 (17 matches)
 rule 15 deny ip

[RTA]
```

结果证明，传输的所有数据均被 ftp-data 的语句匹配，拒绝语句不再被匹配

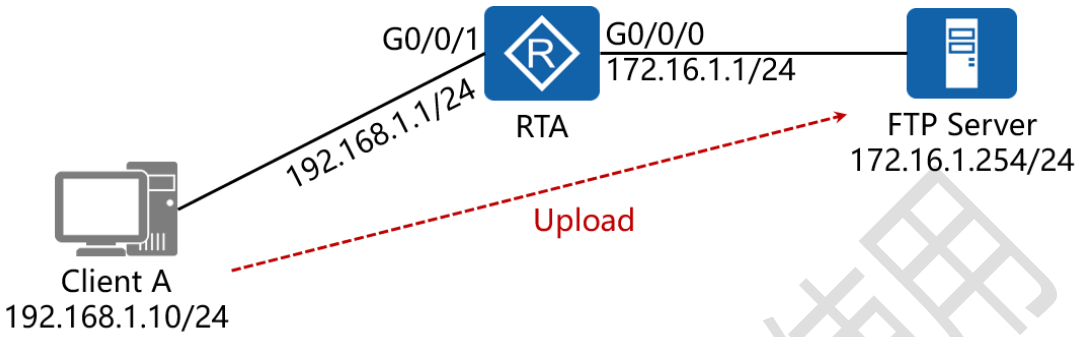
在 RTA 的接口 G0/0/1 上再次抓包并分析



通过获取的数据包发现，此时 FTP Server 向 Client A 传输的数据，使用的源端口号码为 20 号（ftp-data）

五十、配置流量监管实验组网

一、实验拓扑：



二、实验目的：

按上图所示，配置好所有设备的 IP 地址，保证 Client A 能够与 FTP Server 正常通讯，之后在 RTA 的 G0/0/0 接口的外出方向上配置流量监管限制速率，令 Client A 向 FTP Server 上传文件，观察其速率的前后变化

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 172.16.1.1 24　　#配置 IP 地址及子网掩码

interface G0/0/1　　#进入相应的接口

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

acl 3001　　#创建高级 ACL

rule permit tcp source 192.168.1.10 0 destination 172.16.1.254 0 destination-port eq 20 #在 TCP 协议下，允许来自 192.168.1.10，去往 172.16.1.254，目标端口为 20 的流量

rule permit tcp source 192.168.1.10 0 destination 172.16.1.254 0 destination-port eq 21 #在 TCP 协议下，允许来自 192.168.1.10，去往 172.16.1.254，目标端口为 21 的流量

rule deny ip source any destination any #拒绝其它所有流量

traffic classifier ftp #创建传输类列表

if-match acl 3001 #匹配 ACL 3001

traffic behavior ftp #创建传输行为列表

car cir 512 cbs 96256 pbs 160256 green pass yellow pass red discard

#通过流量监管限制其速率，并指定在峰值突发量之内的流量均被允许转发，超过峰值突发量的流量全部丢弃

traffic policy atnet #创建传输策略列表

classifier ftp behavior ftp #同时调用传输类与传输行为列表

interface G0/0/0 #进入相应的接口

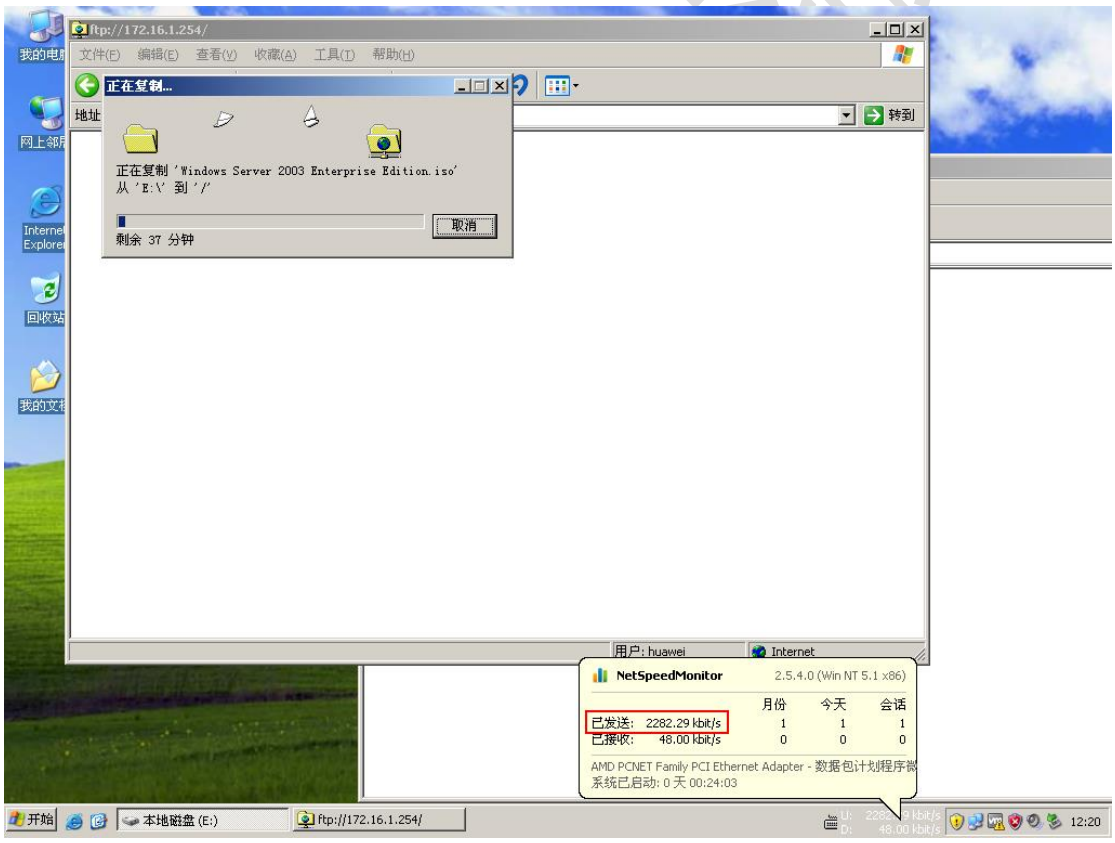
traffic-policy atnet outbound #在接口的出方向上调用传

输策略

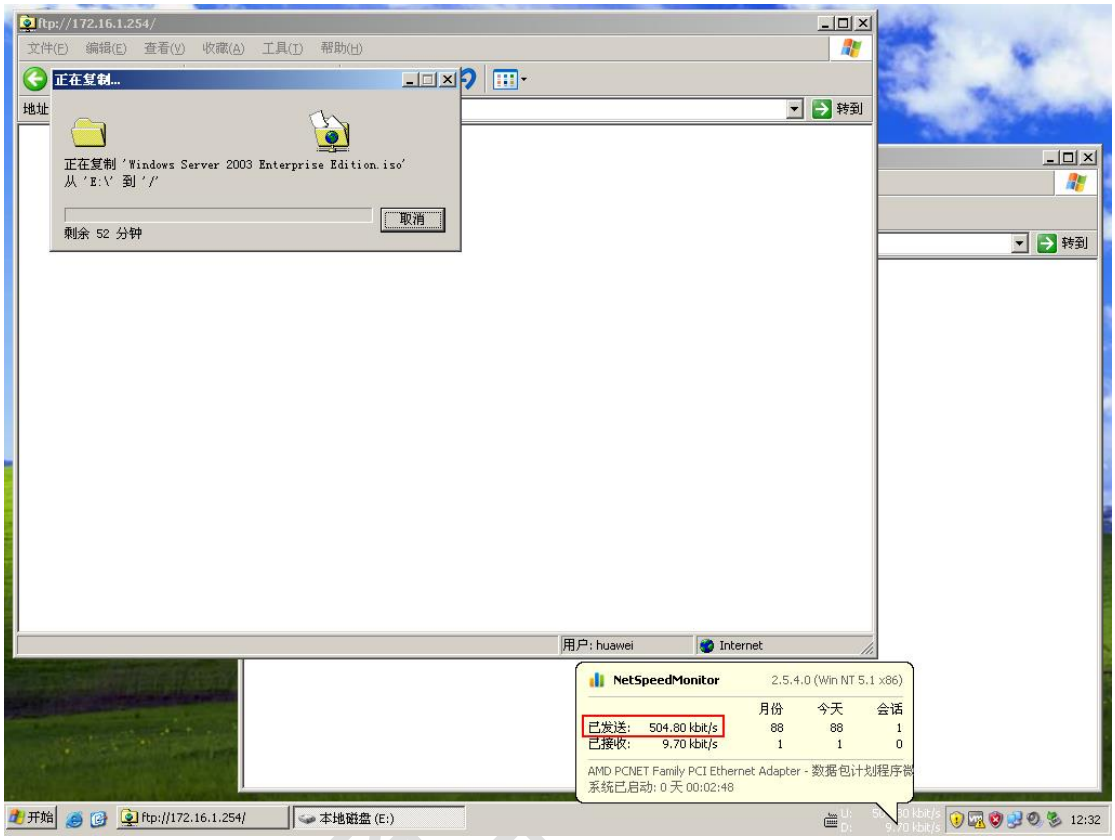
测试：

首先将 FTP Server 与 Client A 的 FTP 模式更改为主动模式（上一篇实验已教授过更改方式，此处不再赘述）

通过 Client A 向 FTP Server 上传文件，在 RTA 的接口 G0/0/0 上没有应用传输策略时，速率如下：

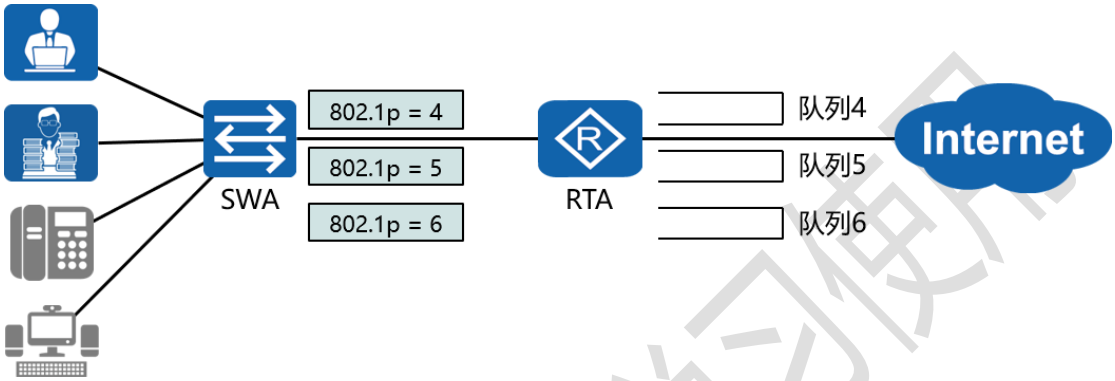


此时，通过在 RTA 的接口 G0/0/0 的外出方向上应用传输策略，通过流量监管限制其速率，再次观察效果：



五十一、配置加权公平队列（WFQ）实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上为 0 至 7（8 个队列）配置加权公平队列（WFQ），并为队列 4 配置权重值 70，为队列 5 配置权重值 80，为队列 6 配置权重值 90

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

qos queue-profile wfq　　#进入 QoS 队列配置模式

schedule wfq 0 to 7　　#将 0 至 7（8 个队列）全部配置为 WFQ

queue 4 weight 70　　#将队列 4 的权重配置为 70

queue 5 weight 80　　#将队列 5 的权重配置为 80

queue 6 weight 90　　#将队列 6 的权重配置为 90

interface G0/0/1　　#进入相应的接口

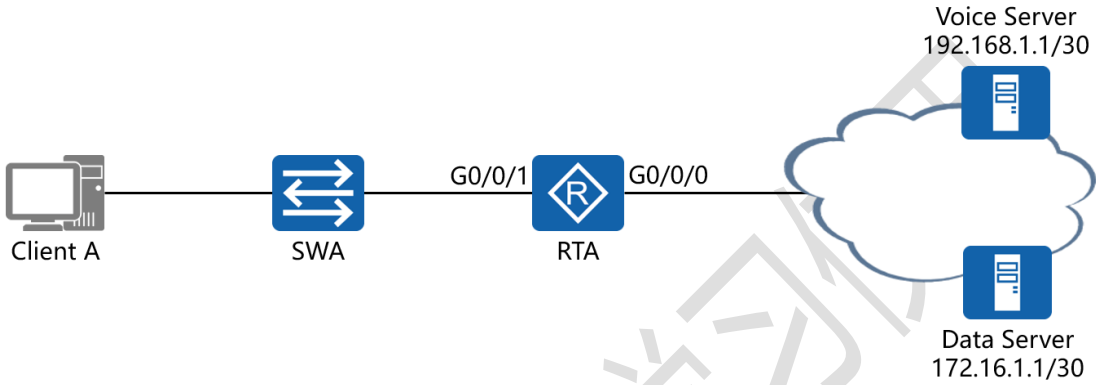
qos queue-profile wfq　　#在外出接口调用

测试：

```
[RTA]display qos queue-profile wfq
Queue-profile: wfq
Queue   Schedule   Weight   Length(Bytes/Packets)  GTS(CIR/CBS)
------------------------------------------------------------------
0       WFQ        10                 -/-              -/-
1       WFQ        10                 -/-              -/-
2       WFQ        10                 -/-              -/-
3       WFQ        10                 -/-              -/-
4       WFQ        70                 -/-              -/-
5       WFQ        80                 -/-              -/-
6       WFQ        90                 -/-              -/-
7       WFQ        10                 -/-              -/-
[RTA]
```

五十二、配置基于类的加权公平队列（CBQ）实验组网

一、实验拓扑：



二、实验目的：

通过在 RTA 上配置基于类的加权公平队列（CBQ），将 Client A 访问 Voice Server（192.168.1.1）的语音业务匹配进 EF 队列，为其分配 50%的带宽；而将 Client A 访问 Data Server（172.16.1.1）的数据业务匹配进 AF11 队列，为其分配 20%的带宽

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

acl 3001　　#创建高级 ACL 3001

rule permit ip source any destination 192.168.1.1 0

#在 IP 协议下，匹配来自任何信源，访问主机 192.168.1.1 的流量

rule deny ip source any destination any　　#拒绝其它所有流量

acl 3002　　#创建高级 ACL 3001

rule permit ip source any destination 172.16.1.1 0　　#在 IP 协议下，匹配来自任何信源，访问主机 172.16.1.1 的流量

rule deny ip source any destination any　　#拒绝其它所有流量

traffic classifier voice　　#创建传输类列表 voice

if-match acl 3001　　#匹配 ACL 3001

traffic classifier data　　#创建传输类列表 data

if-match acl 3002　　#匹配 ACL 3002

traffic behavior voice　　#创建传输行为列表 voice

remark dscp ef　　#将其 DSCP 重标记为 EF

queue ef bandwidth pct 50　　#设置其队列使用 50%的带宽

traffic behavior data　　#创建传输行为列表 data

remark dscp af11　　#将其 DSCP 重标记为 AF11

queue af bandwidth pct 20　　#设置其队列使用 20%的带宽

traffic policy atnet　　#创建传输策略列表

classifier voice behavior voice　　#同时调用传输类 voice 与传输行为列表 voice

classifier data behavior data　　#同时调用传输类 data 与传输行为列表 data

interface G0/0/0　　#进入相应的接口

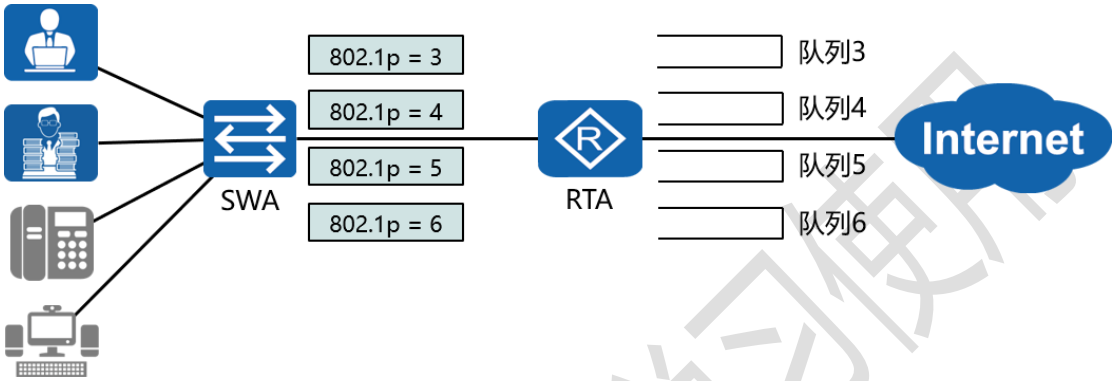
traffic-policy atnet outbound　　#在接口的外出方向上调用传输策略

测试：

```
[RTA]display traffic policy user-defined atnet
  User Defined Traffic Policy Information:
  Policy: atnet
   Classifier: voice
    Operator: OR
     Behavior: voice
      Marking:
        Remark DSCP ef
      Expedited Forwarding:
        Bandwidth 50 (%)
        Queue Length: 64 (Packets) 131072 (Bytes)

   Classifier: data
    Operator: OR
     Behavior: data
      Marking:
        Remark DSCP af11
      Assured Forwarding:
        Bandwidth 20 (%)
        Drop Method: Tail
        Queue Length: 64 (Packets) 131072 (Bytes)

[RTA]
```

五十三、配置优先级队列（PQ）实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上为 3 至 6（4 个队列）配置优先级队列（PQ）

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

qos queue-profile pq　　#进入 QoS 队列配置模式

schedule pq 3 to 6　　#将 3 至 6（4 个队列）配置为 PQ

interface G0/0/1　　#进入相应的接口

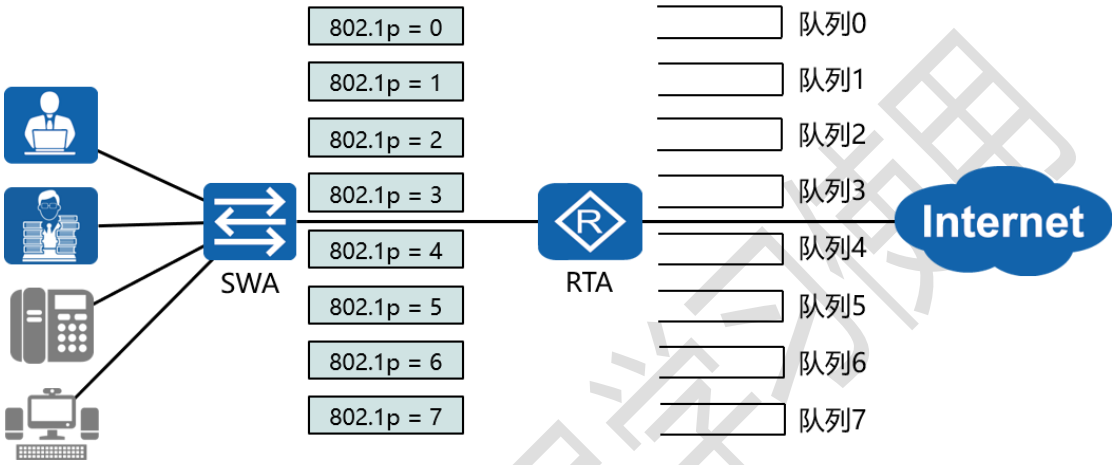
qos queue-profile pq　　#在外出接口调用

测试：

```
[RTA]display qos queue-profile pq
Queue-profile: pq
Queue  Schedule  Weight  Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------
3      PQ        -                 -/-              -/-
4      PQ        -                 -/-              -/-
5      PQ        -                 -/-              -/-
6      PQ        -                 -/-              -/-
[RTA]
```

五十四、配置加权循环队列（WRR）实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上为 0 至 7（8 个队列）配置加权循环队列（WRR），并为队列 7 分配 70 的权重值，为队列 6 分配 60 的权重值，为队列 5 分配 50 的权重值，为队列 4 分配 40 的权重值，为队列 3 分配 30 的权重值，为队列 2 分配 20 的权重值，为队列 1 分配 10 的权重值，为队列 0 分配 5 的权重值，保证在拥塞发生时，各队列按照预先配置的权重值转发相对应的数据包数量

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

```
qos queue-profile wrr        #进入 QoS 队列配置模式
schedule wrr 0 to 7          #将 0 至 7（8 个队列）配置为 WRR
queue 7 weight 70            #将队列 7 的权重值配置为 70
queue 6 weight 60            #将队列 6 的权重值配置为 60
queue 5 weight 50            #将队列 5 的权重值配置为 50
queue 4 weight 40            #将队列 4 的权重值配置为 40
queue 3 weight 30            #将队列 3 的权重值配置为 30
queue 2 weight 20            #将队列 2 的权重值配置为 20
queue 1 weight 10            #将队列 1 的权重值配置为 10
queue 0 weight 5     #将队列 0 的权重值配置为 5
interface G0/0/1     #进入相应的接口
qos queue-profile wrr        #在外出接口调用
```

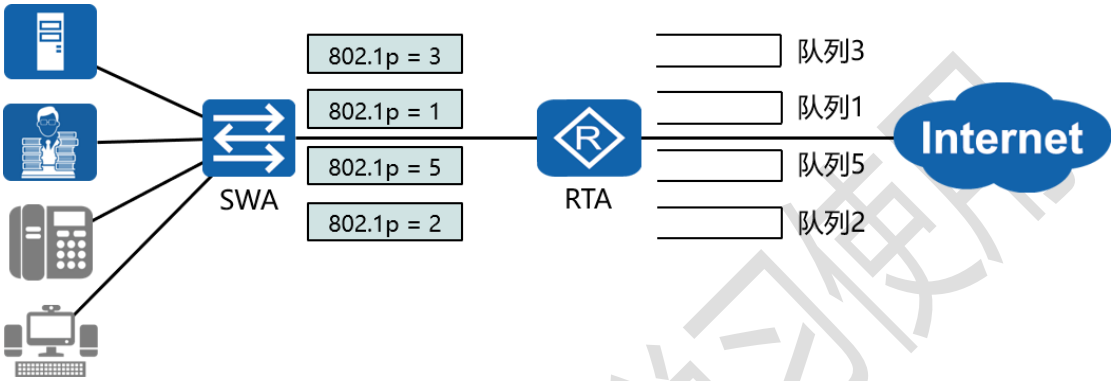
测试：

```
[RTA]display qos queue-profile wrr
Queue-profile: wrr
Queue   Schedule   Weight   Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------------
0       WRR        5                    -/-              -/-
1       WRR        10                   -/-              -/-
2       WRR        20                   -/-              -/-
3       WRR        30                   -/-              -/-
4       WRR        40                   -/-              -/-
5       WRR        50                   -/-              -/-
6       WRR        60                   -/-              -/-
7       WRR        70                   -/-              -/-
[RTA]
```

五十五、配置加权随机早期检测(WRED)

实验组网

一、实验拓扑：



二、实验目的：

在RTA上配置其队列的排队方式为PQ+WFQ，令队列5为PQ，队列1至3为WFQ；通过配置WRED实现加权随机早期检测，令部门经理的流量在其队列满载程度达到 50%时，到达的数据包随机丢弃10%，其队列满载程度达到70%时，全部丢弃；令FTP 的流量在其队列满载程度达到 70%时，到达的数据包随机丢弃10%，其队列满载程度达到90%时，全部丢弃；令Video的流量在其队列满载程度达到 60%时，到达的数据包随机丢弃20%，其队列满载程度达到80%时，全部丢弃

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

drop-profile manager　　#创建丢弃列表 manager

wred dscp　　#配置其根据 DSCP 值使用 WRED

dscp 8 low-limit 50 high-limit 70 discard-percentage 10

#设置 DSCP 值为 8 的队列，其低门限为 50，高门限为 70，丢弃概率为 10%

drop-profile ftp　　#创建丢弃列表 ftp

wred dscp　　#配置其根据 DSCP 值使用 WRED

dscp 16 low-limit 70 high-limit 90 discard-percentage 10

#设置 DSCP 值为 16 的队列，其低门限为 70，高门限为 90，丢弃概率为 10%

drop-profile video　　#创建丢弃列表 video

wred dscp　　#配置其根据 DSCP 值使用 WRED

dscp 24 low-limit 60 high-limit 80 discard-percentage 20

#设置 DSCP 值为 24 的队列，其低门限为 60，高门限为 80，丢弃概率为 20%

qos queue-profile easthome　　#进入 QoS 队列配置模式

schedule pq 5　　#将队列 5 配置为 PQ

schedule wfq 1 to 3　　#将队列 1 至 3 配置为 WFQ

queue 1 drop-profile manager　　#配置队列 1 调用丢弃列表 manager

queue 2 drop-profile ftp　　#配置队列 2 调用丢弃列表 ftp

queue 3 drop-profile video　　#配置队列 3 调用丢弃列表 video

interface G0/0/0　　#进入相应的接口

qos queue-profile easthome　　#将 QoS 队列应用在接口上

测试：

```
[RTA]display qos queue-profile easthome
Queue-profile: easthome
Queue   Schedule   Weight   Length(Bytes/Packets)  GTS(CIR/CBS)
------------------------------------------------------------------------
1       WFQ        10                   -/-              -/-
2       WFQ        10                   -/-              -/-
3       WFQ        10                   -/-              -/-
5       PQ         -                    -/-              -/-
[RTA]
```

```
[RTA]display drop-profile
    Index           Drop-profile name
------------------------------------------------------------------------
    1           manager
    2           ftp
    3           video
------------------------------------------------------------------------
 Total    63      Used    3
[RTA]
```

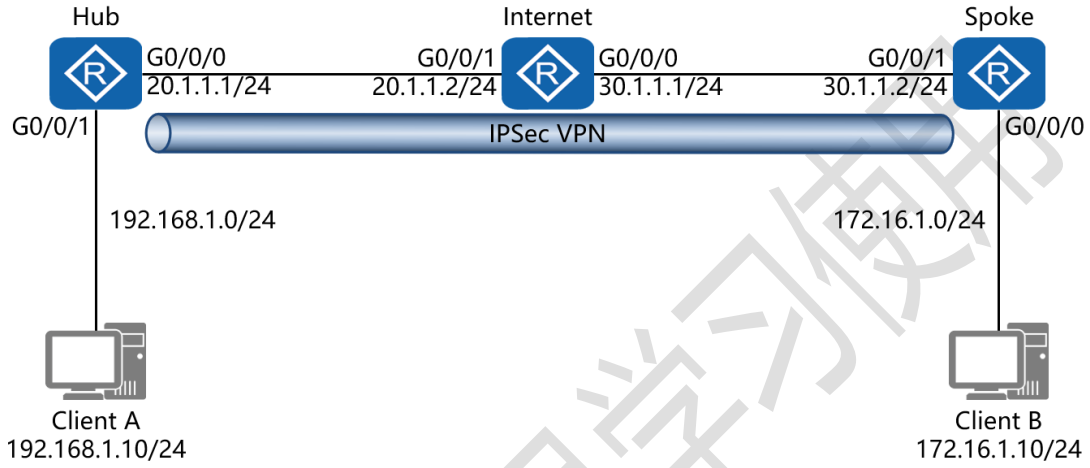
```
[RTA]display drop-profile manager
Drop-profile[1]: manager
DSCP               Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------
0(default)         30          100         10
1                  30          100         10
2                  30          100         10
3                  30          100         10
4                  30          100         10
5                  30          100         10
6                  30          100         10
7                  30          100         10
8(cs1)             50          70          10
9                  30          100         10
10(af11)           30          100         10
11                 30          100         10
12(af12)           30          100         10
13                 30          100         10
14(af13)           30          100         10
15                 30          100         10
16(cs2)            30          100         10
17                 30          100         10
18(af21)           30          100         10
19                 30          100         10
20(af22)           30          100         10
  ---- More ----
```

```
[RTA]display drop-profile ftp
Drop-profile[2]: ftp
DSCP               Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------
0(default)         30          100         10
1                  30          100         10
2                  30          100         10
3                  30          100         10
4                  30          100         10
5                  30          100         10
6                  30          100         10
7                  30          100         10
8(cs1)             30          100         10
9                  30          100         10
10(af11)           30          100         10
11                 30          100         10
12(af12)           30          100         10
13                 30          100         10
14(af13)           30          100         10
15                 30          100         10
16(cs2)            70          90          10
17                 30          100         10
18(af21)           30          100         10
19                 30          100         10
20(af22)           30          100         10
  ---- More ----
```

```
[RTA]display drop-profile video
Drop-profile[3]: video
DSCP               Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------------------
0(default)         30          100         10
1                  30          100         10
2                  30          100         10
3                  30          100         10
4                  30          100         10
5                  30          100         10
6                  30          100         10
7                  30          100         10
8(cs1)             30          100         10
9                  30          100         10
10(af11)           30          100         10
11                 30          100         10
12(af12)           30          100         10
13                 30          100         10
14(af13)           30          100         10
15                 30          100         10
16(cs2)            30          100         10
17                 30          100         10
18(af21)           30          100         10
19                 30          100         10
20(af22)           30          100         10
21                 30          100         10
22(af23)           30          100         10
23                 30          100         10
24(cs3)            60          80          20
  ---- More ----
```

五十六、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*

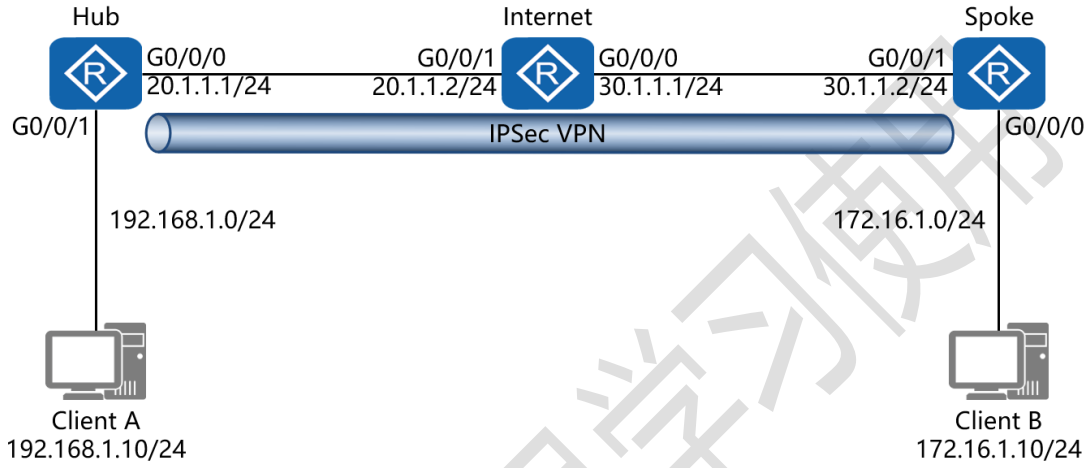
interface G0/0/1

ipsec policy *easthome*

ip route-static 0.0.0.0 0 30.1.1.1

五十七、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

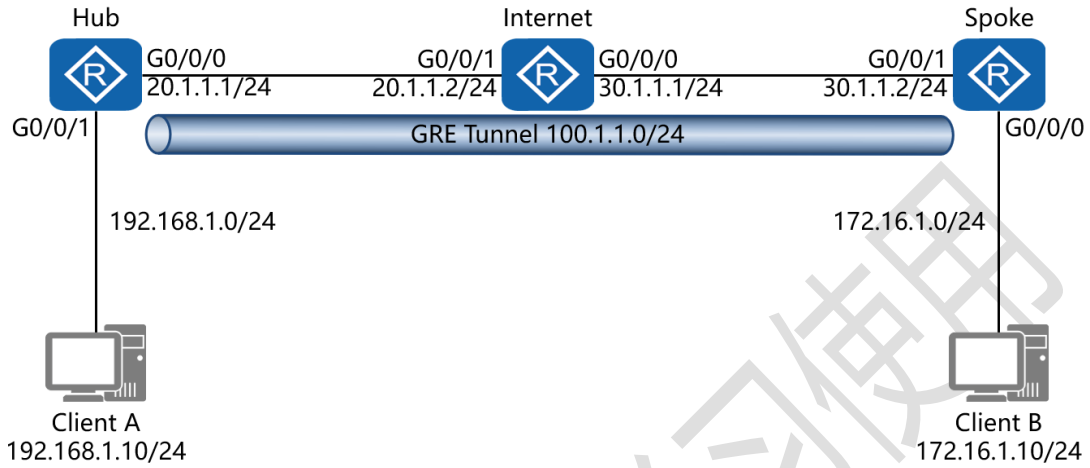
acl number 3001

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
```

五十八、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

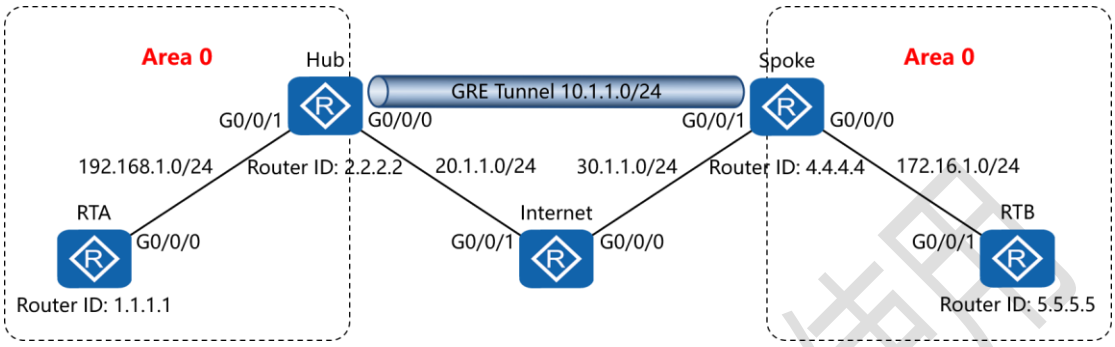
interface G0/0/1

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
```

五十九、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

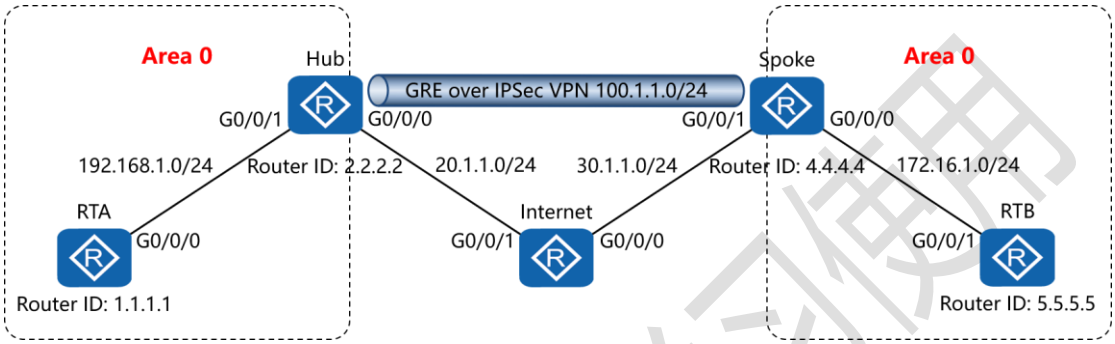
ospf 1 router-id 5.5.5.5

area 0

network 172.16.1.0 0.0.0.255

六十、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@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

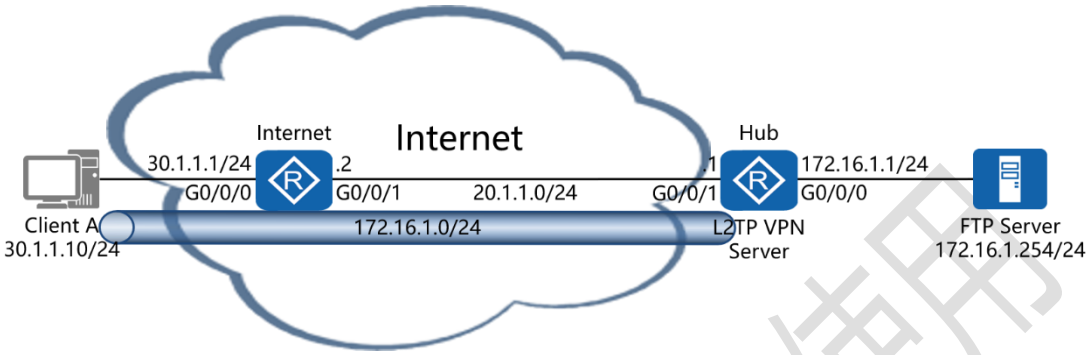
ospf 1 router-id 5.5.5.5

area 0

network 172.16.1.0 0.0.0.255

六十一、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

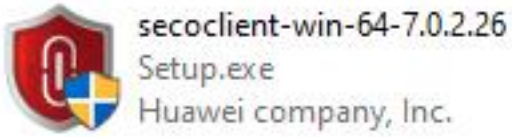
interface G0/0/1

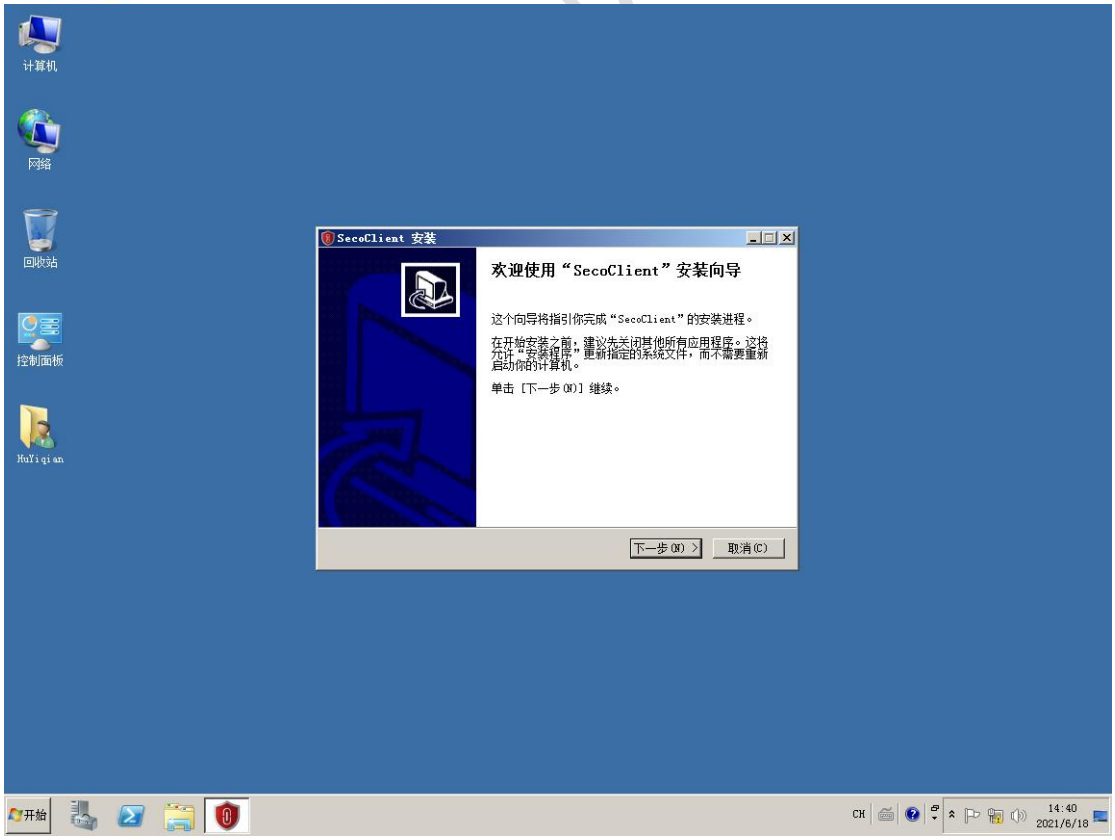
ip address 20.1.1.2 24

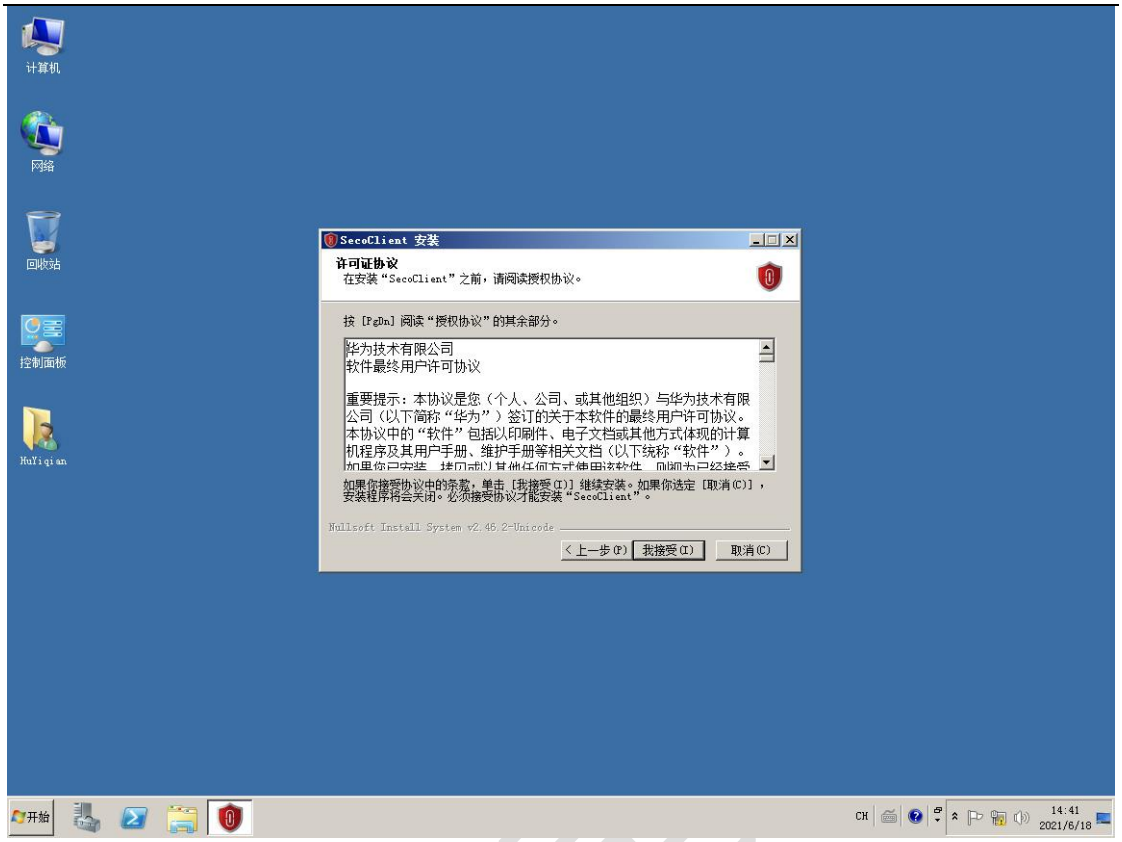
Client A:

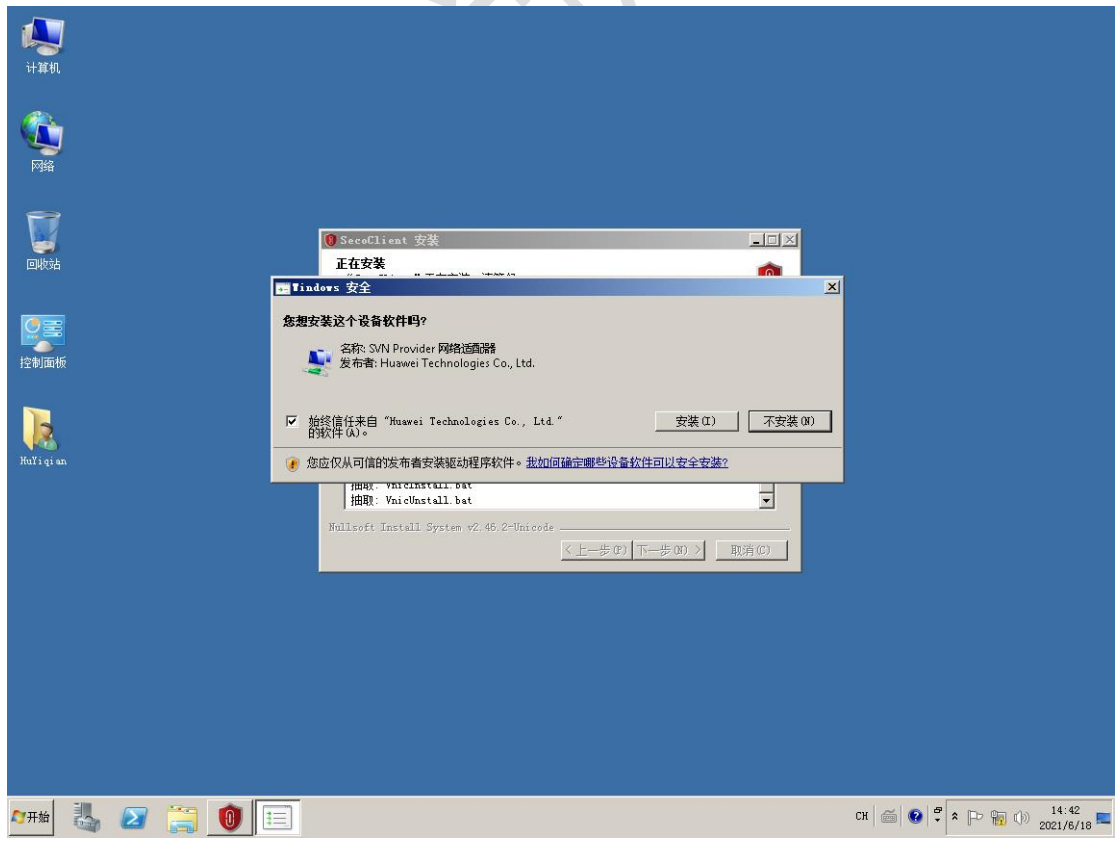
在客户端上安装 secoclient【VPN 客户端软件】

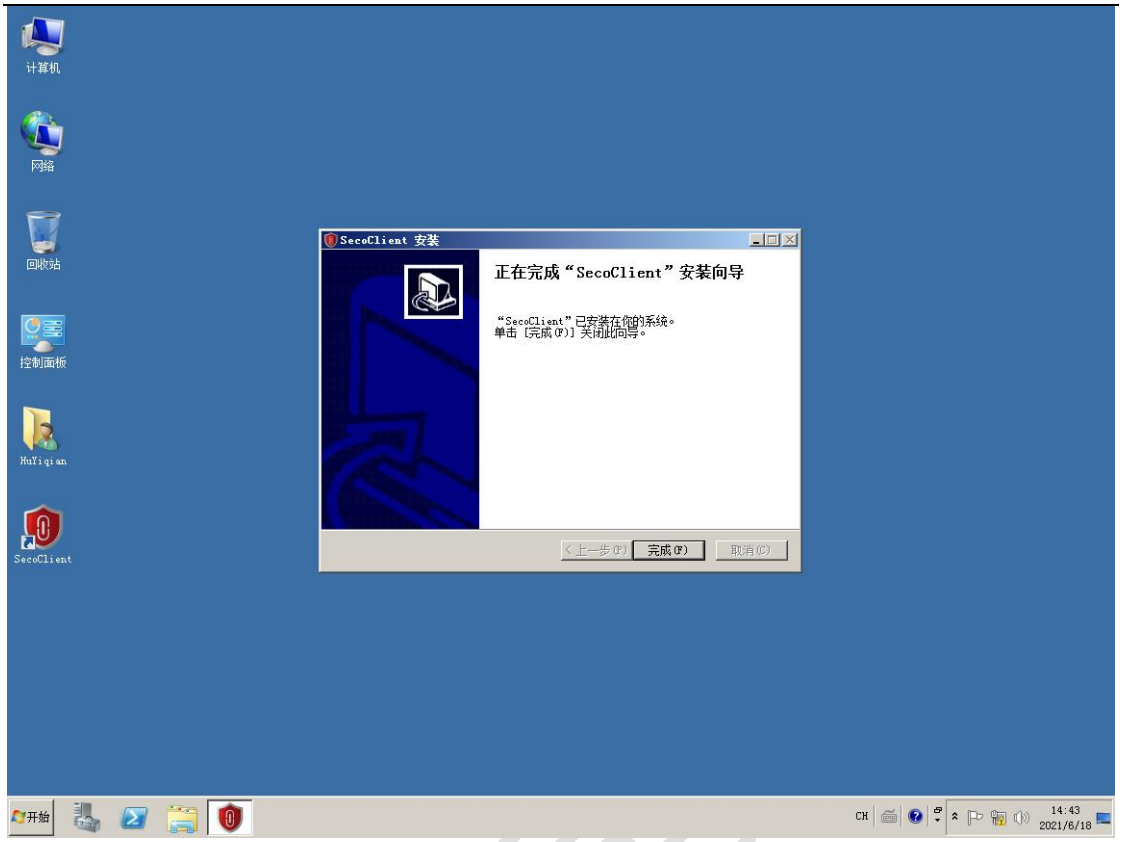
注：客户端使用的操作系统最低版本要求为 Windows Vista

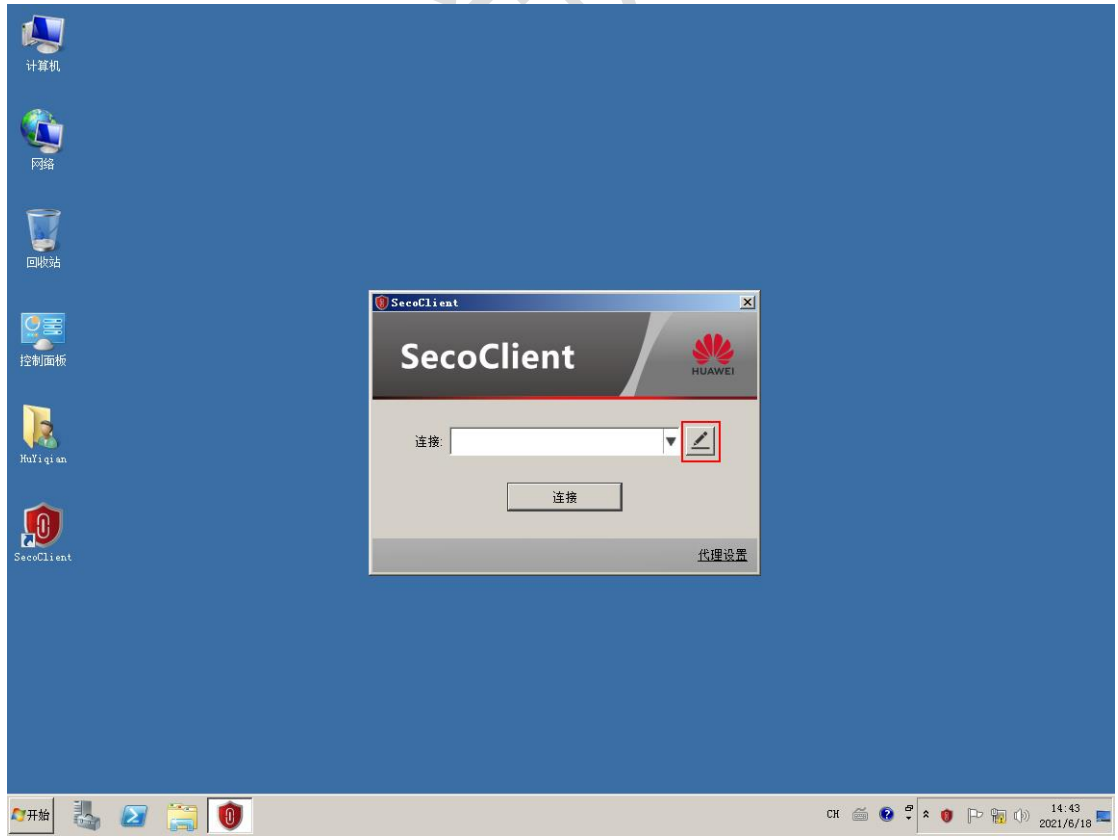




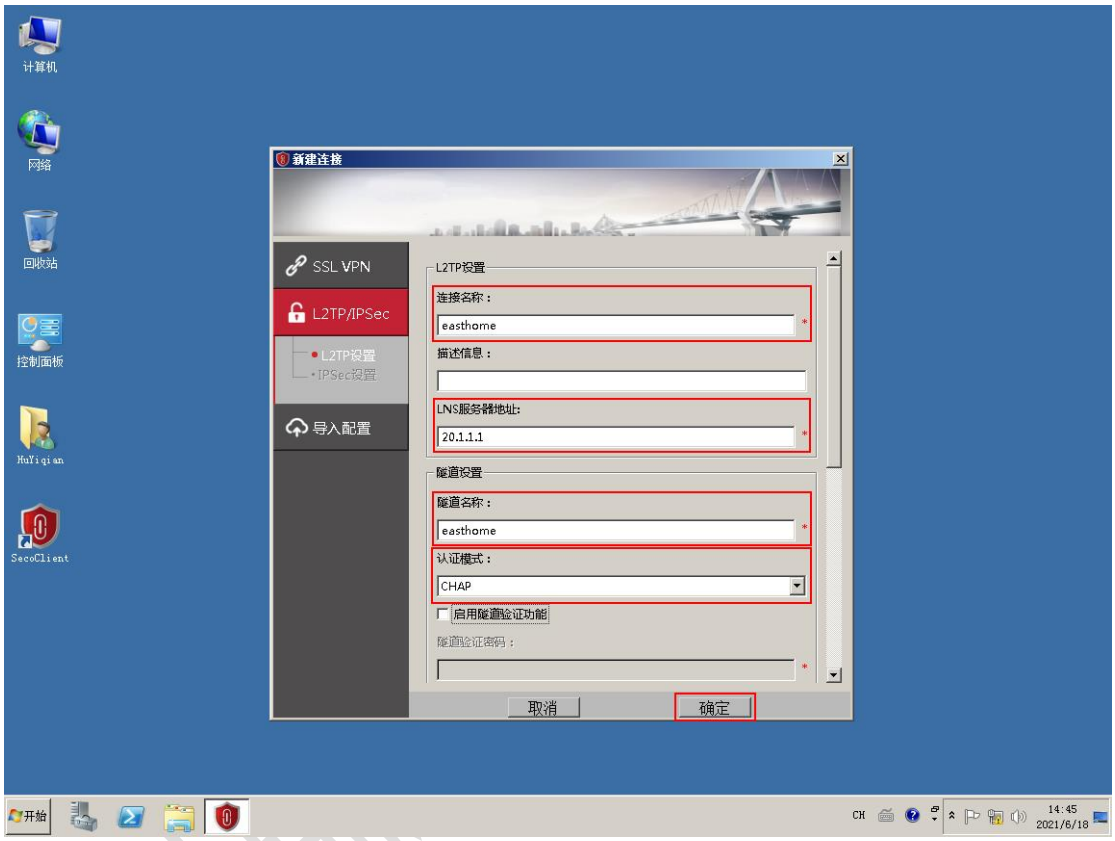

计算机
网络
回收站
控制面板
HuYiqian
SecoClient 安装
许可证协议
在安装“SecoClient”之前，请阅读授权协议。
按 [PgDn] 阅读“授权协议”的其余部分。
华为技术有限公司
软件最终用户许可协议
重要提示：本协议是您（个人、公司、或其他组织）与华为技术有限公司（以下简称“华为”）签订的关于本软件的最终用户许可协议。本协议中的“软件”包括以印刷件、电子文档或其他方式体现的计算机程序及其用户手册、维护手册等相关文档（以下统称“软件”）。
如果你接受协议中的条款，单击 [我接受(I)] 继续安装。如果你选定 [取消(C)]，安装程序将会关闭。必须接受协议才能安装“SecoClient”。
Nullsoft Install System v2.46.2-Unicode
< 上一步(P)
我接受(I)
取消(C)
开始
CH
14:41
2021/6/18


计算机
网络
回收站
控制面板
HuYiqian
SecoClient 安装
正在安装
Windows 安全
您想安装这个设备软件吗?
名称: SVN Provider 网络适配器
发布者: Huawei Technologies Co., Ltd.
始终信任来自“Huawei Technologies Co., Ltd.”的软件(A)。
安装(I)
不安装(N)
您应仅从可信的发布者安装驱动程序软件。我如何确定哪些设备软件可以安全安装?
抽取: VnicUnstall.bat
Nullsoft Install System v2.46.2-Unicode
< 上一步(P)
下一步(N) >
取消(C)
开始
CH
14:42
2021/6/18

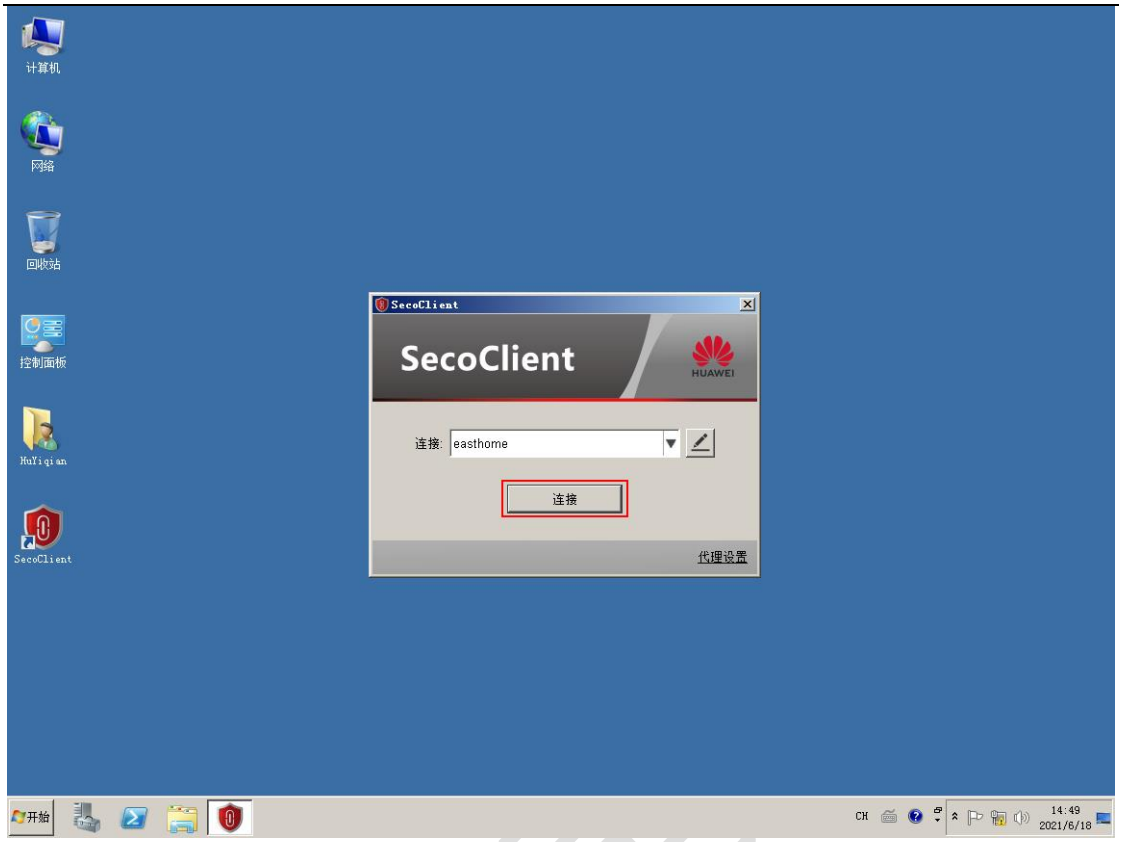

计算机
网络
回收站
控制面板
HuYiqian
SecoClient
SecoClient 安装
正在完成“SecoClient”安装向导
“SecoClient”已安装在你的系统。
单击 [完成(F)] 关闭此向导。
< 上一步(B)
完成(F)
取消(C)
开始
CH
14:43
2021/6/18

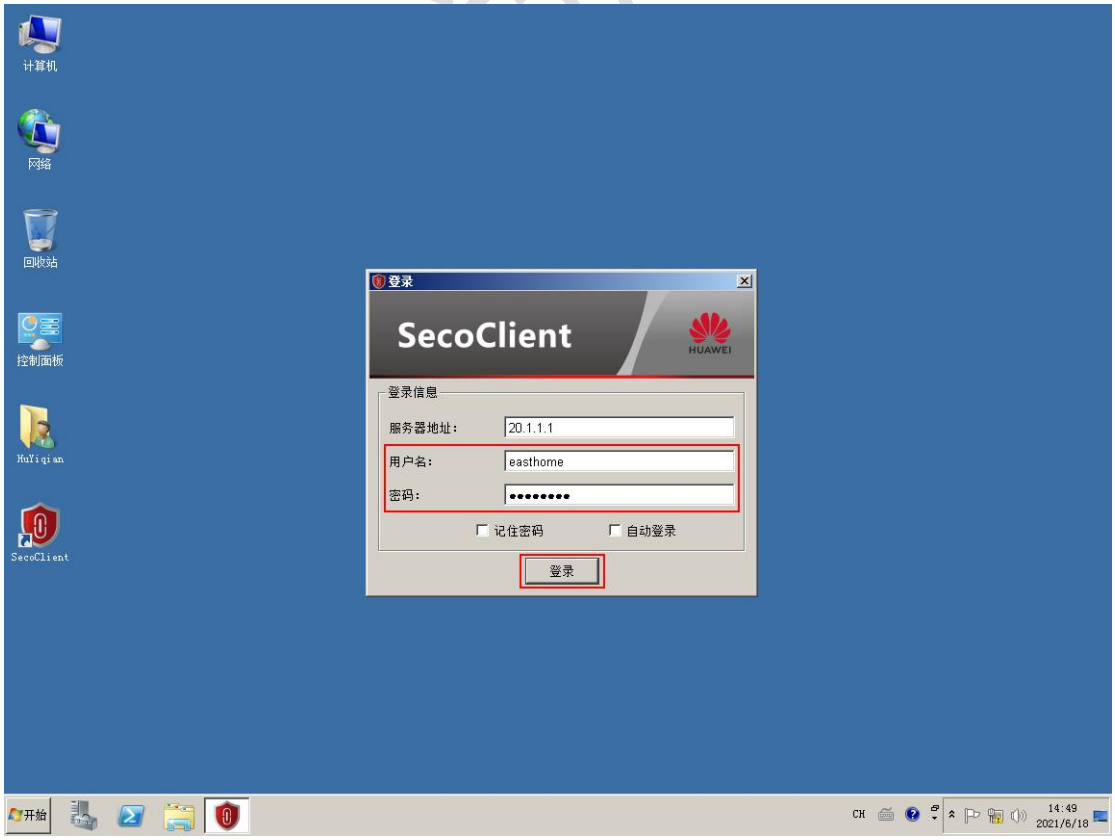

计算机
网络
回收站
控制面板
HuYiqian
SecoClient
SecoClient
SecoClient
HUAWEI
连接:
连接
代理设置
开始
CH
14:43
2021/6/18

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)】

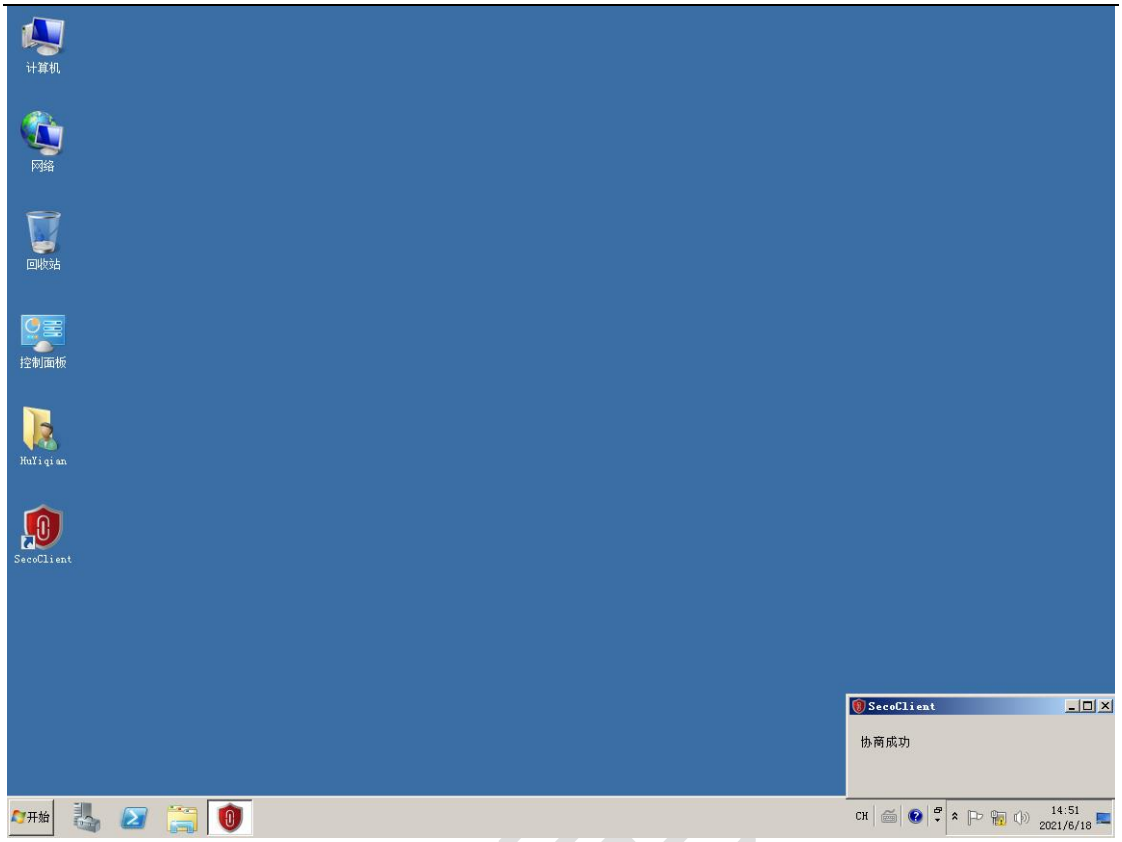


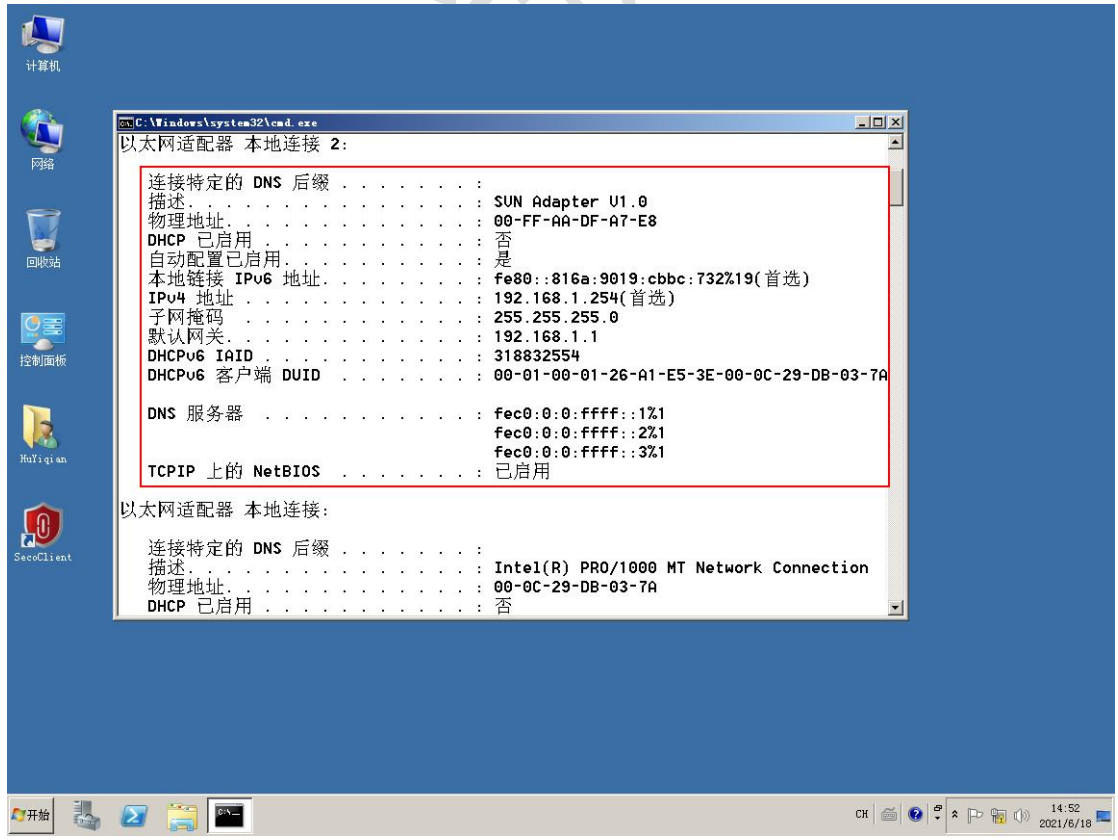
全部填写完毕后点击【确定】





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：

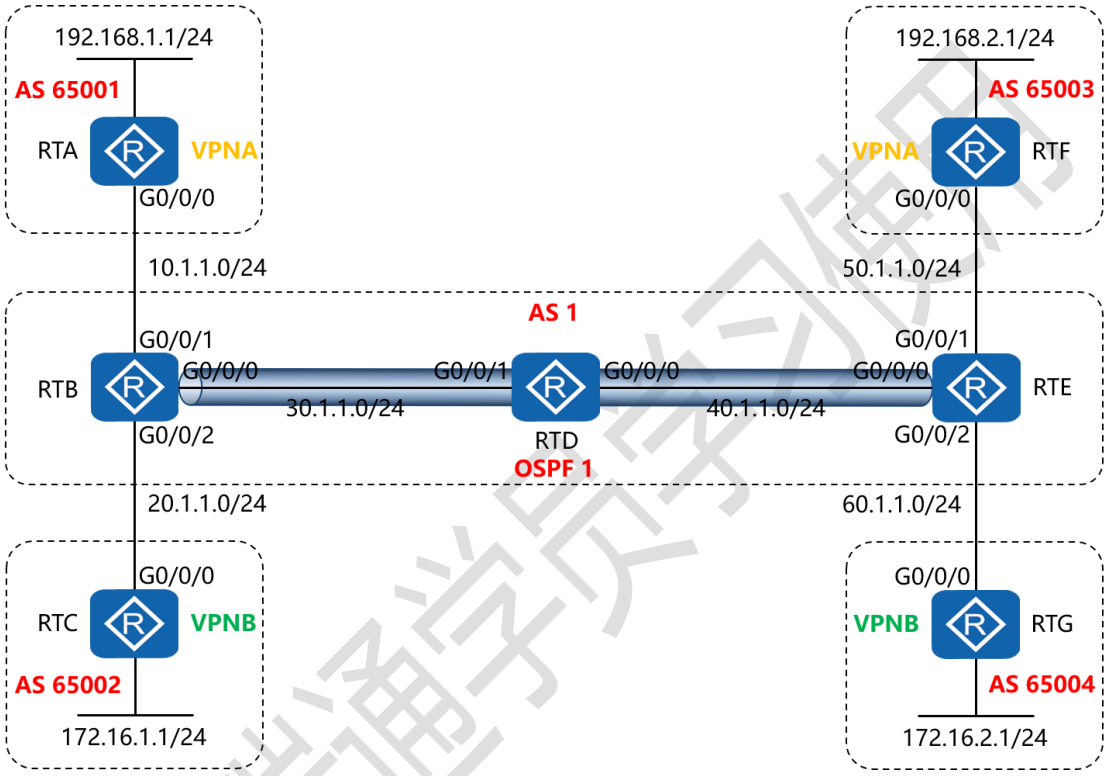
```
[Hub]display l2tp tunnel

 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]
```

六十二、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：

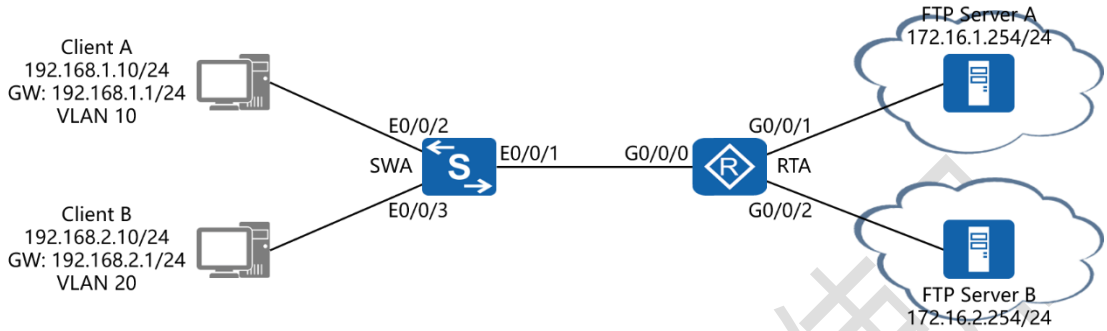
```
[RTC]ping -a 172.16.1.1 172.16.2.1
  PING 172.16.2.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.1: bytes=56 Sequence=1 ttl=252 time=40 ms
    Reply from 172.16.2.1: bytes=56 Sequence=2 ttl=252 time=60 ms
    Reply from 172.16.2.1: bytes=56 Sequence=3 ttl=252 time=40 ms
    Reply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

六十三、配置 VRF 实验组网

一、实验拓扑：



二、实验目的：

通过在 RTA 上配置 VRF，实现 192.168.1.0/24 网段内的 Client A 只能与 FTP Server A 通讯；192.168.2.0/24 网段内的 Client B 只能与 FTP Server B 通讯；令两个网络相互隔离，不可互访

三、实验步骤：

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

ip vpn-instance *east*　　#创建并进入 VPN 实例视图

ipv4-family　　#开启 VPN 实例的 IPv4 类型的路由通告和数据转发功能

ip vpn-instance *home*　　#创建并进入 VPN 实例视图

ipv4-family　　#开启 VPN 实例的 IPv4 类型的路由通告和数据转发功能

interface G0/0/0.1 #进入第 1 个子接口

ip binding vpn-instance *east* 将该子接口与 VPN 实例 east 做绑定

dot1q termination vid 10 #配置其 VLAN 的封装方式为 802.1Q，并且令该子接口为 VLAN 10 的主机提供路由转发服务

ip address 192.168.1.1 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

interface G0/0/0.2 #进入第 2 个子接口

ip binding vpn-instance *home* 将该子接口与 VPN 实例 home 做绑定

dot1q termination vid 20 #配置其 VLAN 的封装方式为 802.1Q，并且令该子接口为 VLAN 20 的主机提供路由转发服务

ip address 192.168.2.1 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

interface G0/0/1 #进入相应的接口

ip binding vpn-instance *east* 将该接口与 VPN 实例 east 做绑定

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

interface G0/0/2 #进入相应的接口

ip binding vpn-instance *home*　　将该接口与 VPN 实例 home 做绑定

ip address 172.16.2.1 24　　#配置接口的 IP 地址及子网掩码

SWA:

system-view

sysname SWA

vlan 10　　#创建 VLAN 10

vlan 20　　#创建 VLAN 20

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

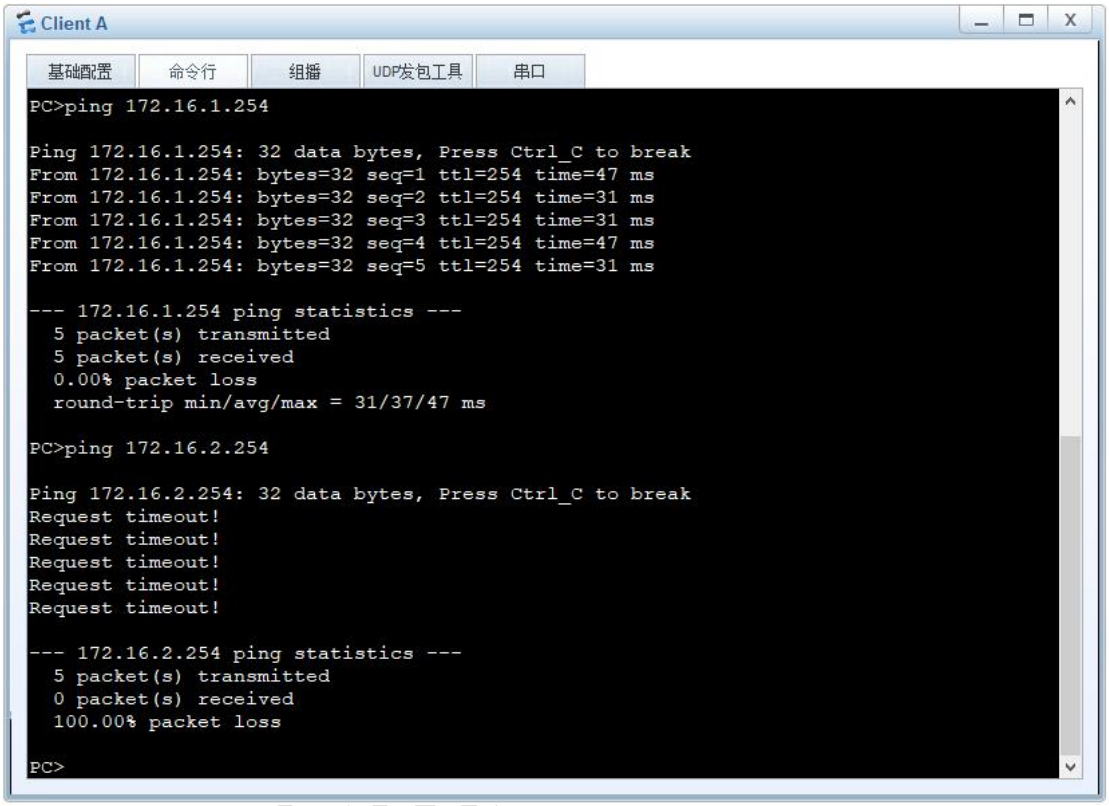
interface E0/0/3　　#进入相应端口

port link-type access　　#将端口类型配置为接入模式

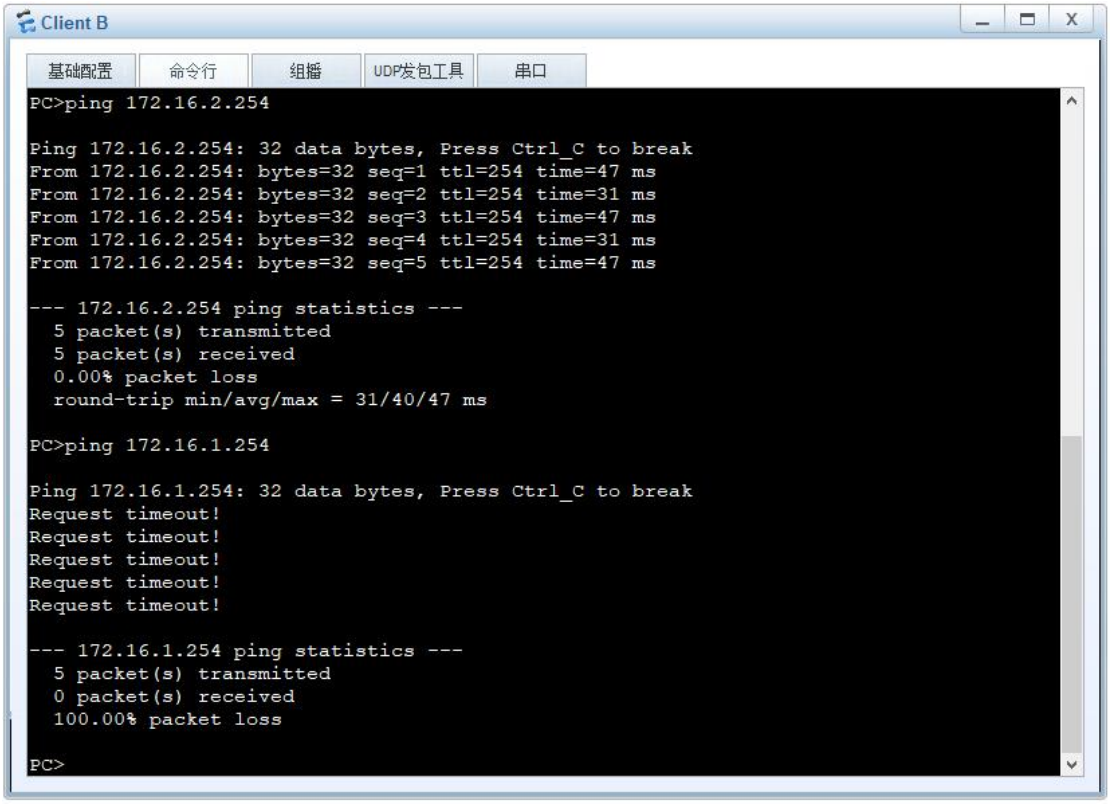
port default vlan 20　　#将端口加入 VLAN 20

测试：

在 Client A 上分别测试与 FTP Server A 与 FTP Server B 的连通性：

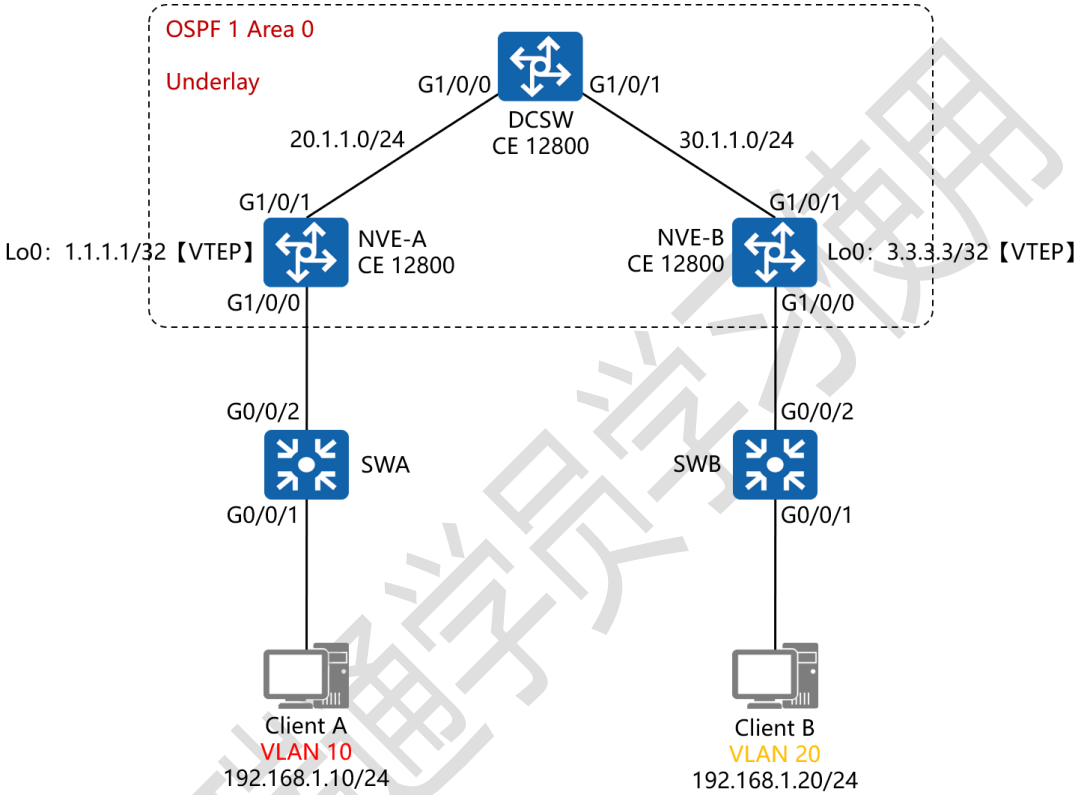


在 Client B 上分别测试与 FTP Server A 与 FTP Server B 的连通性：



六十四、配置 VXLAN 构建大二层实验组网

一、实验拓扑：



二、实验目的：

通过 OSPFv2 的配置令设备 NVE-A、NVE-B 与 Internet 相互联通，构建基于 IPv4 的 underlay 网络；NVE-A 与 NVE-B 作为网络虚拟化边界节点，充当 VXLAN 隧道的两个端点；同时 NVE-A 与 NVE-B 的环回接口【Lo0】作为隧道的源地址，即 VTEP；Client A【192.168.1.10/24】与 Client B【192.168.1.20/24】虽属同一网段，但由于不在同一个广播域【且 VLAN 不同】，因此无法直接互通，此时需要在 NVE-A 与

NVE-B 之间建立 VXLAN 静态隧道，令 Client A 与 Client B 认为其在同一个广播域中【实现大二层概念】，从而完成相互通讯

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

interface G0/0/1　　#进入相应的端口

port link-type access　　#将端口的链路类型配置为接入模式

port default vlan 10　　#将端口加入进 VLAN 10

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　　#进入系统视图模式

sysname SWB　　#给设备命名

vlan 20　　#创建 VLAN 10

interface G0/0/1　　#进入相应的端口

port link-type access　　#将端口的链路类型配置为接入模式

port default vlan 20　　#将端口加入进 VLAN 20

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

NVE-A:

system-view immediately　　#进入系统视图模式并令配置立即生效

sysname NVE-A　　#给设备命名

interface G1/0/1　　#进入相应接口

undo portswitch　　#关闭二层端口功能，开启三层接口功能

undo shutdown　　#开启接口

ip address 20.1.1.1 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 1.1.1.1 0.0.0.0　　#通告环回接口地址

network 20.1.1.0 0.0.0.255 #通告其直连网段

bridge-domain 10 #创建本地桥接域

vxlan vni 10 #创建 VXLAN，其 VNI 编号为 10

interface G1/0/0 #进入相应接口

undo shutdown #开启接口

interface G1/0/0.1 mode l2 #创建二层子接口

encapsulation dot1q vid 10 #收到 tag 为 VLAN 10 的数据帧后使用 802.1Q 的方式进行封装

bridge-domain 10 #将 tag 为 VLAN 10 的数据帧封装好后与 VNI 10 进行绑定

interface nve 1 #创建并进入 NVE 接口

source 1.1.1.1 #指定 VTEP 接口

vni 10 head-end peer-list 3.3.3.3 #在 VNI 10 下指定对端 NVE 设备的 VTEP 地址

Internet:

system-view immediately

sysname Internet

interface G1/0/0

undo portswitch

undo shutdown

ip address 20.1.1.2 24

```
interface G1/0/1
undo portswitch
undo shutdown
ip address 30.1.1.1 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 2.2.2.2 0.0.0.0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
```

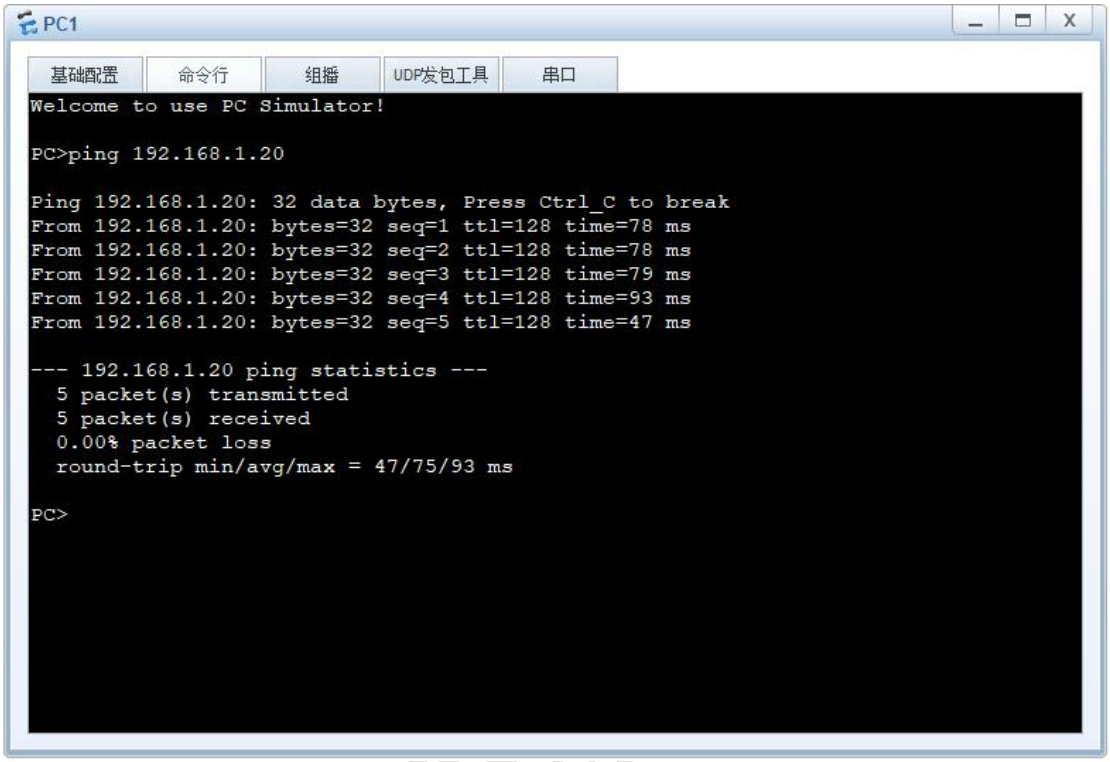
NVE-B:

```
system-view immediately
sysname NVE-B
interface G1/0/1
undo portswitch
undo shutdown
ip address 30.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
```

```
area 0
network 3.3.3.3 0.0.0.0
network 30.1.1.0 0.0.0.255
bridge-domain 10
vxlan vni 10
interface G1/0/0
undo shutdown
interface G1/0/0.1 mode l2
encapsulation dot1q vid 20
bridge-domain 10
interface nve 1
source 3.3.3.3
vni 10 head-end peer-list 1.1.1.1
```

测试：

检测 Client A 与 Client B 之间的网络连通性：



网络正常通讯，由此证明 VXLAN 静态隧道建立成功

在 NVE-A 上查看 VXLAN 隧道的建立：

```
[NVE-A]display vxlan tunnel
Number of vxlan tunnel : 1
Tunnel ID   Source               Destination          State  Type     Uptime
-----------------------------------------------------------------------------
---
4026531841  1.1.1.1              3.3.3.3              up     static   00:09:16

[NVE-A]
```

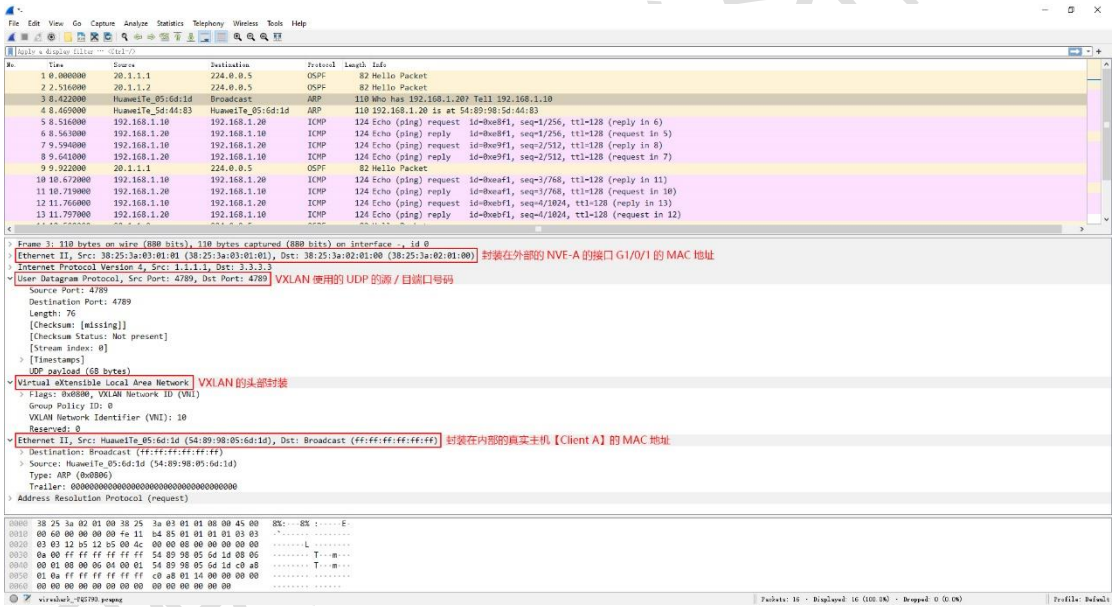
在 NVE-A 上查看 VXLAN 的对等体：

```
[NVE-A]display vxlan peer
Number of peers : 1
Vni ID    Source               Destination          Type      Out Vni ID
-----------------------------------------------------------------------------
10        1.1.1.1              3.3.3.3              static    10
[NVE-A]
```

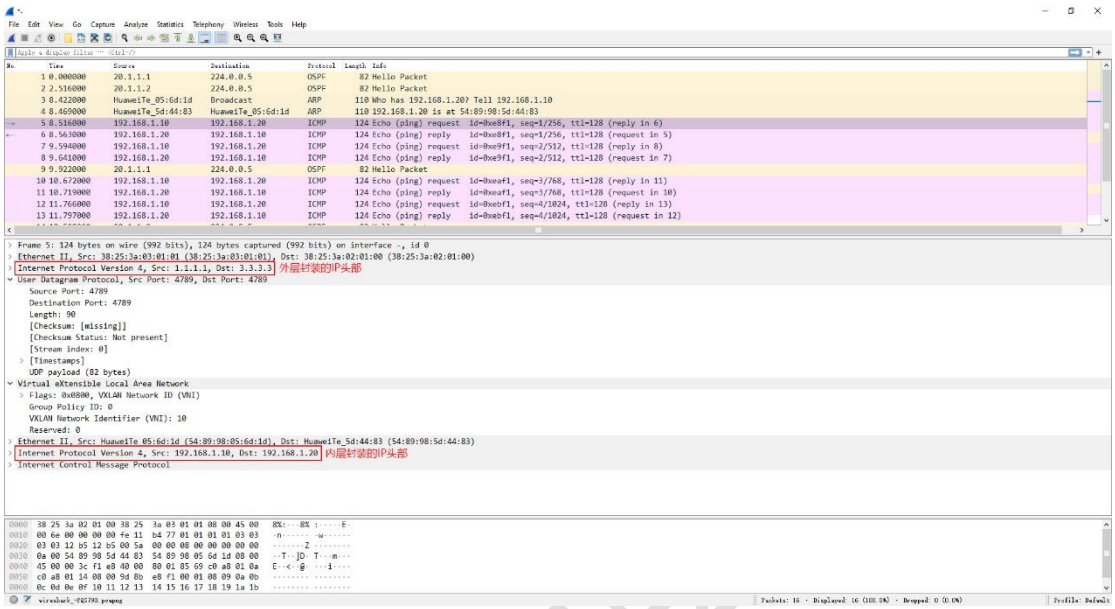
在 NVE-A 上查看 VXLAN 的 VNI 信息：

```
[NVE-A]display vxlan vni
Number of vxlan vni : 1
VNI                 BD-ID                State
--------------------------------------------------
10                  10                   up
[NVE-A]
```

当 Client A 访问 Client B 时，在 NVE-A 的接口 G1/0/1 上抓取 ARP 广播请求报文：

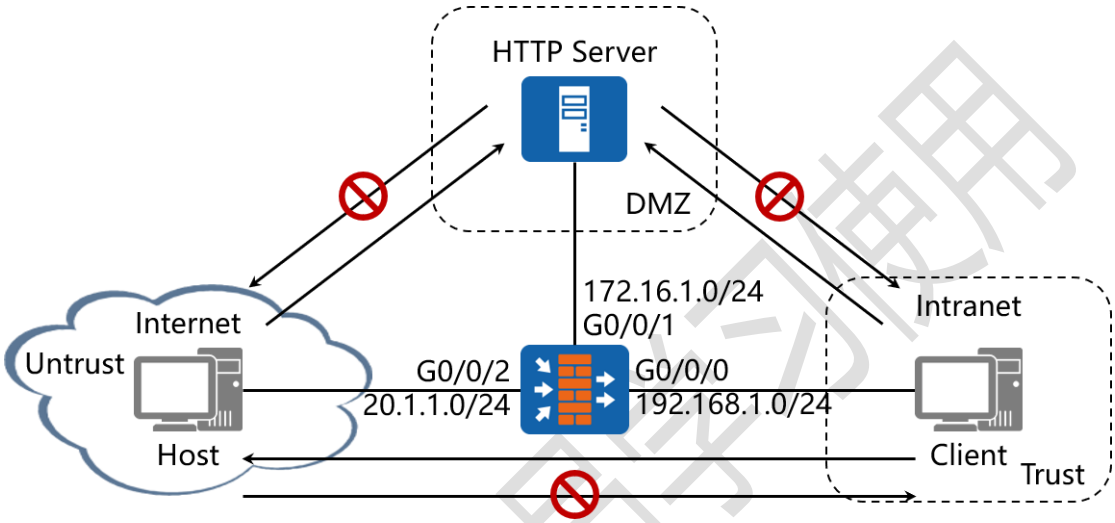


当 Client A 访问 Client B 时，在 NVE-A 的接口 G1/0/1 上抓取 ICMP 请求报文：



六十五、配置状态化包过滤实验组网【USG5500】

一、实验拓扑：



二、实验目的：

通过 USG5500 状态化包过滤的配置，令外部主机无法访问内部客户端，但可以访问 DMZ 区域中的 HTTP Server，内部客户端可以访问外部主机，也可以访问 DMZ 区域中的 HTTP Server，DMZ 区域中的 HTTP Server 不能访问外部主机与内部客户端

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G0/0/1 #进入相应接口

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

interface G0/0/2 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

firewall zone trust #进入防火墙信任区域

set priority 85 #配置该区域安全级别为 85

add interface G0/0/0 #将接口 G0/0/0 加入进该区域

firewall zone dmz #进入防火墙 dmz 区域

set priority 50 #配置该区域安全级别为 50

add interface G0/0/1 #将接口 G0/0/1 加入进该区域

firewall zone untrust #进入防火墙非信任区域

set priority 5 #配置该区域安全级别为 5

add interface G0/0/2 #将接口 G0/0/2 加入进该区域

policy interzone trust dmz outbound #配置从信任区域访问 dmz 区域的外出策略

policy 0 #进入策略配置模式并指定策略编号

policy service service-set icmp #指定策略匹配的协议为 ICMP

action permit #定义其动作为允许

policy interzone trust untrust outbound #配置从信任区域访问非信任区域的外出策略

policy 0 #进入策略配置模式并指定策略编号

policy service service-set icmp #指定策略匹配的协议为 ICMP

action permit #定义其动作为允许

policy interzone untrust dmz inbound #配置从非信任区域访问 dmz 区域的进入策略

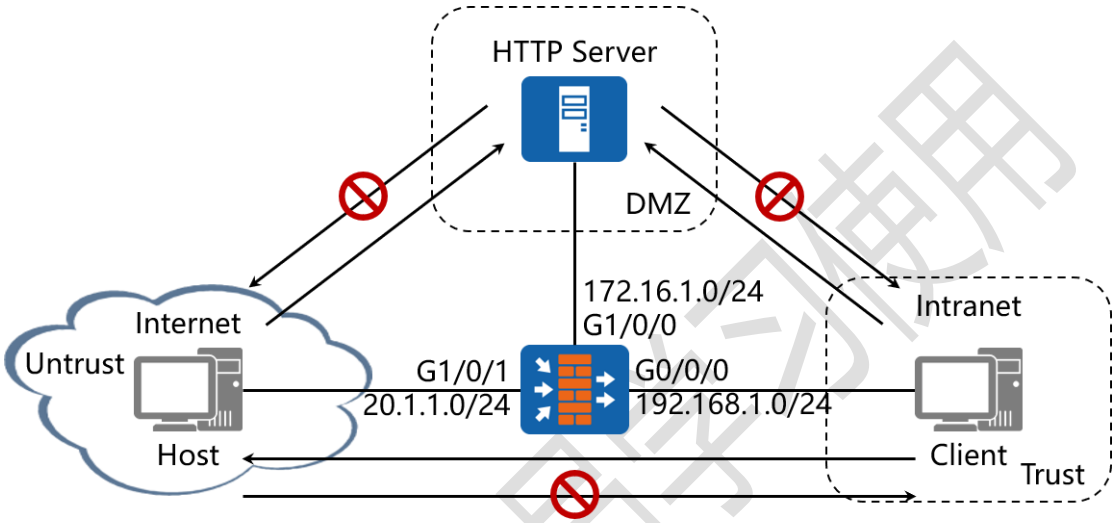
policy 0 #进入策略配置模式并指定策略编号

policy service service-set icmp #指定策略匹配的协议为 ICMP

action permit #定义其动作为允许

六十六、配置状态化包过滤实验组网【USG6000V1】

一、实验拓扑：



二、实验目的：

通过 USG6000V1 状态化包过滤的配置，令外部主机无法访问内部客户端，但可以访问 DMZ 区域中的 HTTP Server，内部客户端可以访问外部主机，也可以访问 DMZ 区域中的 HTTP Server，DMZ 区域中的 HTTP Server 不能访问外部主机与内部客户端

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G1/0/0      #进入相应接口
ip address 172.16.1.1 24      #配置 IP 地址及子网掩码
interface G1/0/1      #进入相应接口
ip address 20.1.1.1 24      #配置 IP 地址及子网掩码
firewall zone trust      #进入防火墙信任区域
set priority 85      #配置该区域安全级别为 85
add interface G0/0/0      #将接口 G0/0/0 加入进该区域
firewall zone dmz      #进入防火墙 dmz 区域
set priority 50      #配置该区域安全级别为 50
add interface G1/0/0      #将接口 G1/0/0 加入进该区域
firewall zone untrust      #进入防火墙非信任区域
set priority 5      #配置该区域安全级别为 5
add interface G1/0/1      #将接口 G1/0/1 加入进该区域
security-policy      #配置安全策略
rule name insidetooutside      #定义该安全策略规则名称
source-zone trust      #指定源区域为 trust
destination-zone untrust      #指定目标区域为 untrust
source-address 192.168.1.0 24      #指定源 IP 网段及掩码
service icmp      #定义匹配的服务为 ICMP 协议
action permit      #定义动作为允许操作
security-policy      #配置安全策略
```

rule name *insidetodmz* #定义该安全策略规则名称

source-zone trust #指定源区域为 trust

destination-zone dmz #指定目标区域为 dmz

source-address 192.168.1.0 24 #指定源 IP 网段及掩码

service icmp #定义匹配的服务为 ICMP 协议

action permit #定义动作为允许操作

security-policy #配置安全策略

rule name *outsidetodmz* #定义该安全策略规则名称

source-zone untrust #指定源区域为 untrust

destination-zone dmz #指定目标区域为 dmz

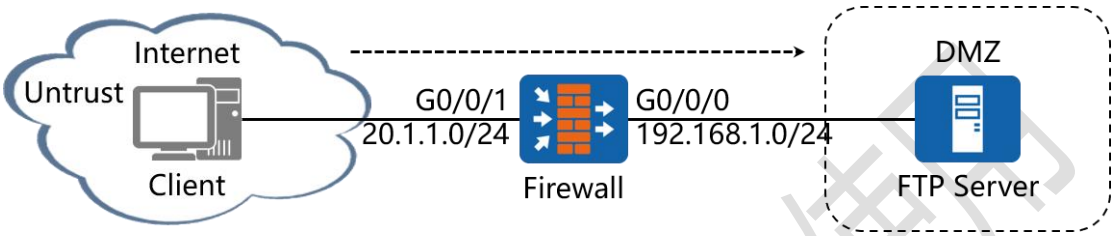
source-address 20.1.1.0 24 #指定源 IP 网段及掩码

service icmp #定义匹配的服务为 ICMP 协议

action permit #定义动作为允许操作

六十七、配置 Server-map 实验组网【USG5500】

一、实验拓扑：



二、实验目的：

在 USG5500 防火墙上配置基于 ASPF 的过滤策略，通过会话表项中的 5 元组信息匹配 FTP 流量，令处于 Untrust 区域中的 Client 能够访问 DMZ 区域中的 FTP Server

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 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

firewall zone dmz　　#进入防火墙 dmz 区域

set priority 50　　#配置该区域安全级别为 50

add interface G0/0/0　　#将接口 G0/0/0 加入进该区域

firewall zone untrust　　#进入防火墙非信任区域

set priority 5　　#配置该区域安全级别为 5

add interface G0/0/1　　#将接口 G0/0/1 加入进该区域

policy interzone untrust dmz inbound　　#配置从非信任区域访问 dmz 区域的进入策略

policy 0　　#进入策略配置模式并指定策略编号

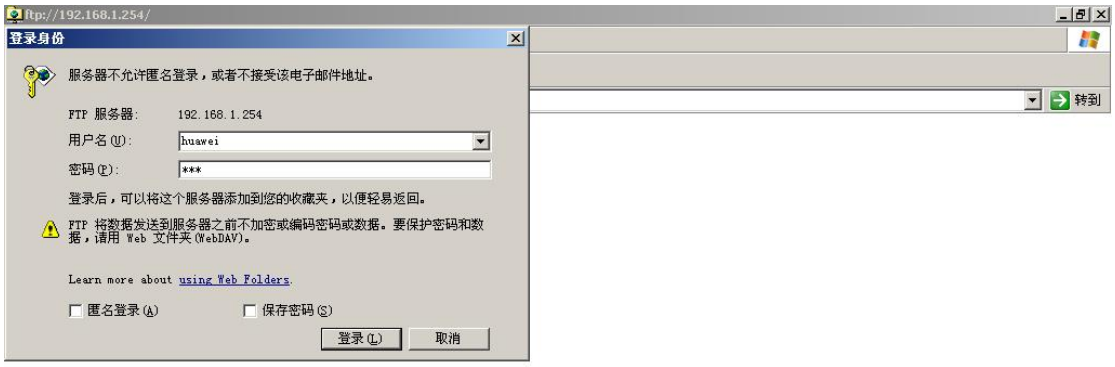
policy destination 192.168.1.0 mask 24　　#指定目的网段与子网掩码

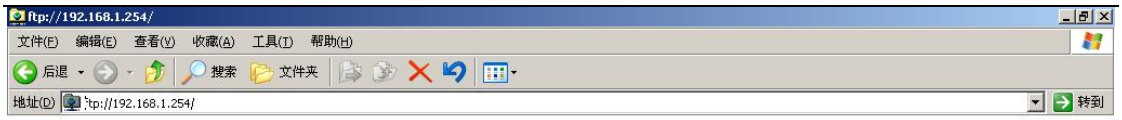
policy service service-set ftp　　#指定策略匹配的协议为 FTP

action permit　　#定义其动作为允许

测试：

将 FTP Server 与 Client 的 FTP 模式更改为主动模式（PORT 模式），在 Client 上访问 FTP Server：





在正确输入完用户名及密钥之后，无法获取目录列表

产生上述问题的原因在于，Client 向 FTP Server 的 21 号端口发起连接建立控制通道，之后通过 PORT 命令协商 Client 使用的数据传输端口号，在协商成功后，FTP Server 主动向 Client 的这个端口号发起数据连接，然而每次数据传输都会协商不同的端口号码

在防火墙上，管理员配置的安全策略仅开放了 FTP 协议，也就是 21 号端口，当 Client 向 FTP Server 发起控制连接时建立了会话，而 FTP Server 向 Client 发起数据连接的源/目的端口号分别为 20 与临时协商的端口号 X，这显然不是此条连接的后续报文，因此无法命中此会话转发

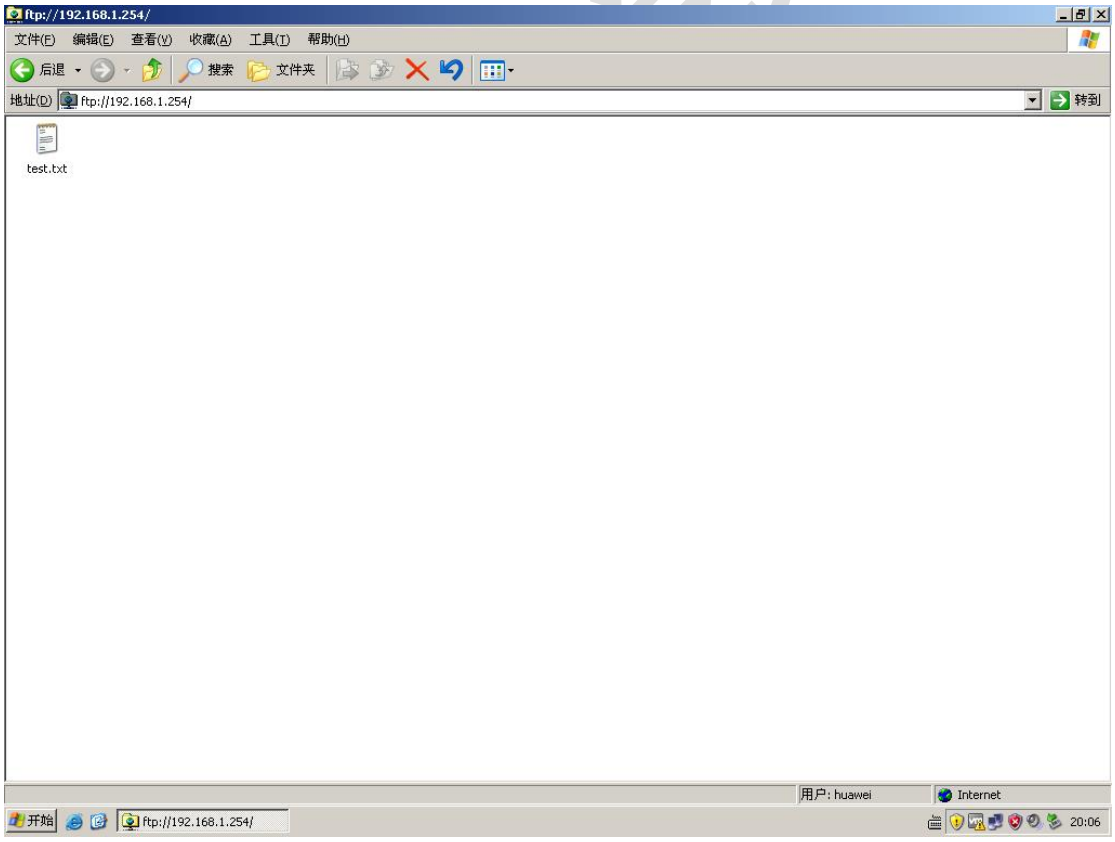
若在 FTP Server 到 Client 的方向也配置了安全策略，则必须开放 Client 的所有端口号码，将会产生很大的安全隐患

此时的解决方案是，在防火墙上开启 ASPF 功能

firewall interzone untrust dmz　　# 在非信任区域访问 DMZ 区域的方向上开启 ASPF 功能

detect ftp　　#令 ASPF 功能发现 FTP 会话

再次使用 Client 访问 FTP Server：



结果发现已经可以正常访问 FTP Server

在防火墙上查看 Server-map 表项：

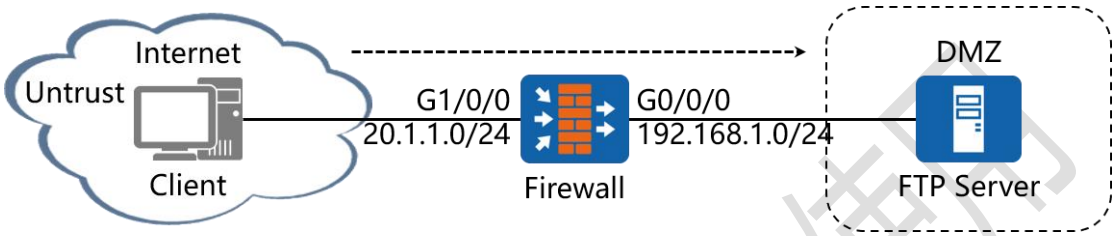
```
[Firewall]display firewall server-map
20:09:17  2019/12/25
 server-map item(s)
 --------------------------------------------------------------------------------
 ASPF, 192.168.1.254 -> 20.1.1.10:1055[any], Zone: ---
   Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:56, Addr-Pool: ---
   VPN: public -> public

[Firewall]
```

在防火墙上查看会话表项：

```
[Firewall]display firewall session table
20:10:48  2019/12/25
 Current Total Sessions : 4
  ftp  VPN:public --> public 20.1.1.10:1045-->192.168.1.254:21
  ftp  VPN:public --> public 20.1.1.10:1049+->192.168.1.254:21
  ftp  VPN:public --> public 20.1.1.10:1053+->192.168.1.254:21
  ftp  VPN:public --> public 20.1.1.10:1054+->192.168.1.254:21
[Firewall]
```

六十八、配置 Server-map 实验组网【USG6000V1】

一、实验拓扑：



二、实验目的：

在 USG6000V1 防火墙上配置基于 ASPF 的过滤策略，通过会话表项中的 5 元组信息匹配 FTP 流量，令处于 Untrust 区域中的 Client 能够访问 DMZ 区域中的 FTP Server

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G1/0/0　　#进入相应接口

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

firewall zone dmz　　#进入防火墙 dmz 区域

set priority 50　　#配置该区域安全级别为 50

add interface G0/0/0 #将接口 G0/0/0 加入进该区域

firewall zone untrust #进入防火墙非信任区域

set priority 5 #配置该区域安全级别为 5

add interface G1/0/0 #将接口 G1/0/0 加入进该区域

undo firewall detect ftp #关闭防火墙 FTP 检测功能

security-policy #配置安全策略

rule name *outsidetodmz* #定义该安全策略规则名称

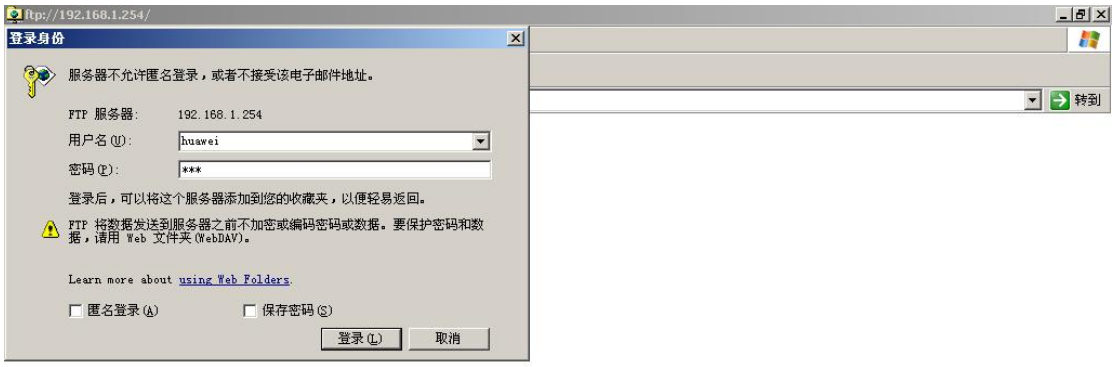
destination-address 192.168.1.0 24 #指定目标地址与子网掩码

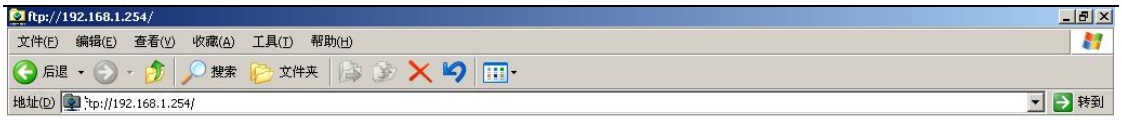
service ftp #定义匹配的服务为 FTP 协议

action permit #定义动作为允许操作

测试：

将 FTP Server 与 Client 的 FTP 模式更改为主动模式（PORT 模式），在 Client 上访问 FTP Server：





在正确输入完用户名及密钥之后，无法获取目录列表

产生上述问题的原因在于，Client 向 FTP Server 的 21 号端口发起连接建立控制通道，之后通过 PORT 命令协商 Client 使用的数据传输端口号，在协商成功后，FTP Server 主动向 Client 的这个端口号发起数据连接，然而每次数据传输都会协商不同的端口号码

在防火墙上，管理员配置的安全策略仅开放了 FTP 协议，也就是 21 号端口，当 Client 向 FTP Server 发起控制连接时建立了会话，而 FTP Server 向 Client 发起数据连接的源/目的端口号分别为 20 与临时协商的端口号 X，这显然不是此条连接的后续报文，因此无法命中此会话转发

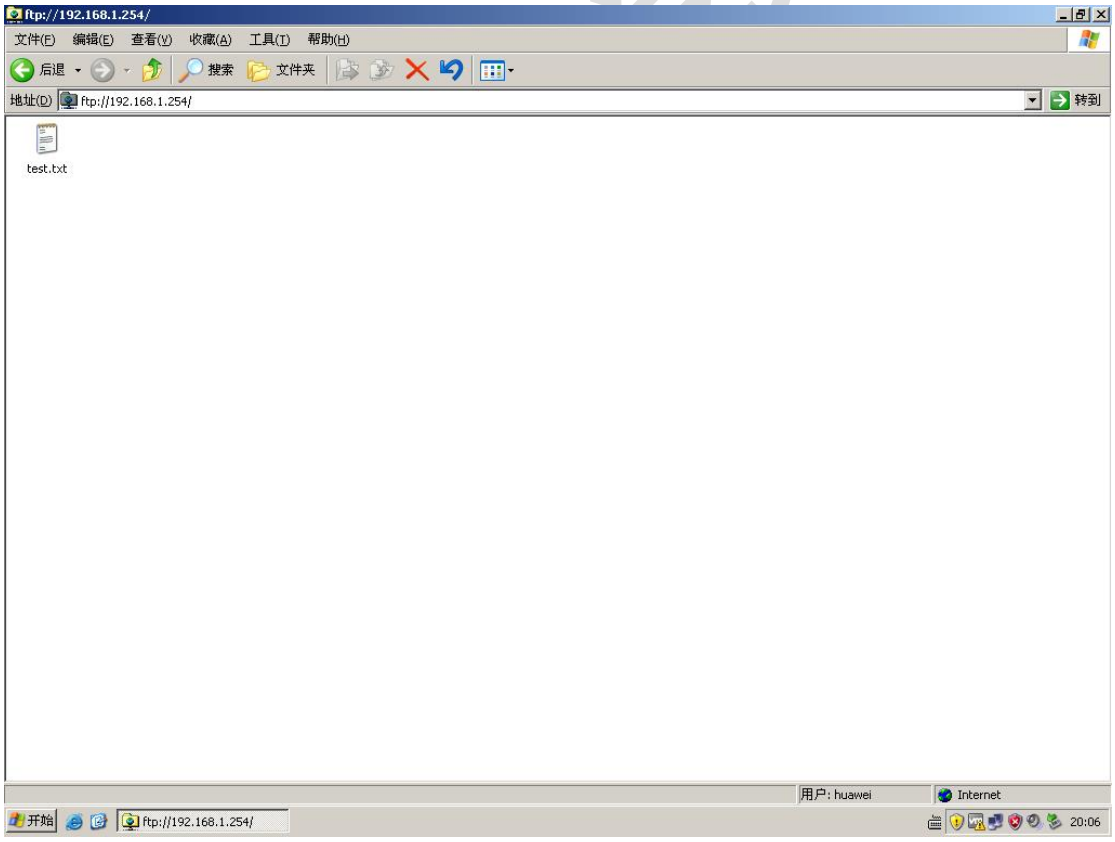
若在 FTP Server 到 Client 的方向也配置了安全策略，则必须开放 Client 的所有端口号码，将会产生很大的安全隐患

此时的解决方案是，在防火墙上开启 ASPF 功能

firewall interzone untrust dmz　　# 在非信任区域访问 DMZ 区域的方向上开启 ASPF 功能

detect ftp　　#令 ASPF 功能发现 FTP 会话

再次使用 Client 访问 FTP Server：



结果发现已经可以正常访问 FTP Server

在防火墙上查看 Server-map 表项：

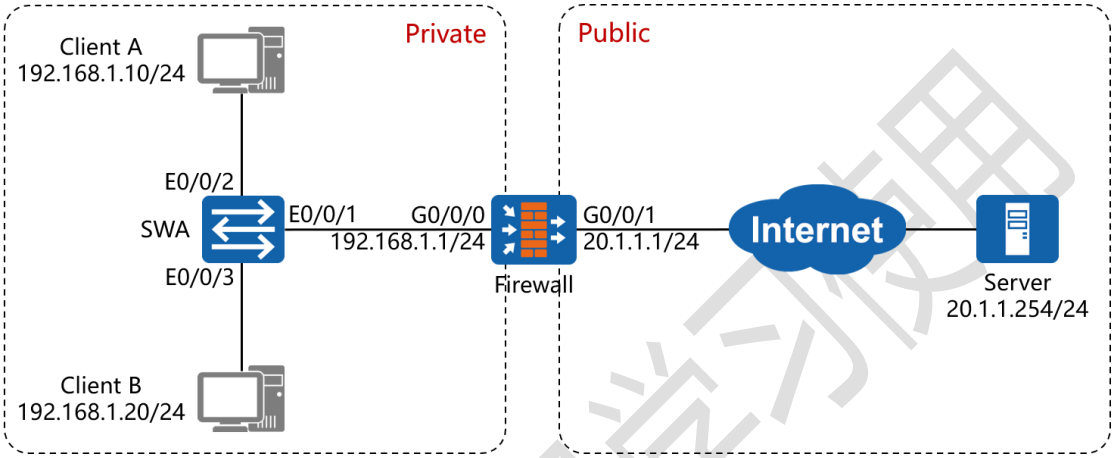
```
[Firewall]display firewall server-map
2020-01-11 08:22:48.740
 Current Total Server-map : 1
 Type: ASPF,  192.168.1.254 -> 20.1.1.10:1056,  Zone:---
 Protocol: tcp(Appro: ftp-data),  Left-Time:00:00:10
 Vpn: public -> public

[Firewall]
```

在防火墙上查看会话表项：

```
[Firewall]display firewall session table
2020-01-11 08:25:10.270
 Current Total Sessions : 6
 ftp  VPN: public --> public  20.1.1.10:1057 +-> 192.168.1.254:21
 ftp-data  VPN: public --> public  192.168.1.254:20 --> 20.1.1.10:1060
 ftp  VPN: public --> public  20.1.1.10:1050 +-> 192.168.1.254:21
 ftp  VPN: public --> public  20.1.1.10:1059 +-> 192.168.1.254:21
 ftp  VPN: public --> public  20.1.1.10:1054 +-> 192.168.1.254:21
 ftp  VPN: public --> public  20.1.1.10:1058 +-> 192.168.1.254:21
[Firewall]
```

六十九、配置基于 USG5500 防火墙的 NAPT 实验组网

一、实验拓扑：



二、实验目的：

网络边界部署 USG5500 Firewall 作为安全网关，使私网中 192.168.1.0/24 网段的用户可以正常访问 Internet 中的 Server，在 Firewall 上配置源 NAT 策略

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 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

firewall zone trust　　#进入防火墙信任区域

set priority 85　　#配置该区域安全级别为 85

add interface G0/0/0　　#将接口 G0/0/0 加入进该区域

firewall zone untrust　　#进入防火墙非信任区域

set priority 5　　#配置该区域安全级别为 5

add interface G0/0/1　　#将接口 G0/0/1 加入进该区域

policy interzone trust untrust outbound　　#配置从信任区域访问非信任区域的外出策略

policy 0　　#进入策略配置模式并指定策略编号

policy source 192.168.1.0 mask 24　　#指定源网段与子网掩码

action permit　　#定义其动作为允许

nat address-group 1 *napt* 20.1.1.2 20.1.1.3　　#配置 NAT 地址池，指定地址池的起始地址与结束地址

nat-policy interzone trust untrust outbound　　#配置从信任区域访问非信任区域的外出方向的 NAT 策略

policy 0　　#进入策略配置模式并指定策略编号

action source-nat　　#指定动作使用源 NAT

address-group *napt*　　#调用 NAT 地址池

ip route-static 0.0.0.0 0.0.0.0 20.1.1.254　　#配置缺省路由

ip route-static 20.1.1.2 255.255.255.255 Null 0　　#为防止

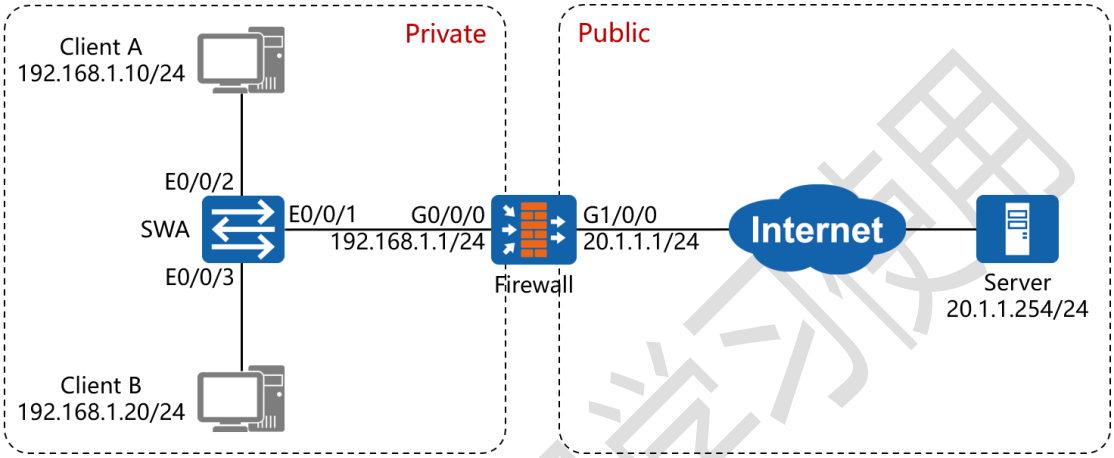
路由黑洞，配置空接口路由

ip route-static 20.1.1.3 255.255.255.255 Null 0　　#为防止

路由黑洞，配置空接口路由

七十、配置基于 USG6000V1 防火墙的 NAPT 实验组网

一、实验拓扑：



二、实验目的：

网络边界部署 USG6000V1 Firewall 作为安全网关，使私网中 192.168.1.0/24 网段的用户可以正常访问 Internet 中的 Server，在 Firewall 上配置源 NAT 策略

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G1/0/0　　#进入相应接口

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

firewall zone trust　　#进入防火墙信任区域

set priority 85　　#配置该区域安全级别为 85

add interface G0/0/0　　#将接口 G0/0/0 加入进该区域

firewall zone untrust　　#进入防火墙非信任区域

set priority 5　　#配置该区域安全级别为 5

add interface G1/0/0　　#将接口 G1/0/0 加入进该区域

security-policy　　#配置安全策略

rule name *NAPT*　　#定义策略名称

source-zone trust　　#指定源为信任区域

destination-zone untrust　　#指定目标为非信任区域

source-address 192.168.1.0 24　　#指定源 IP 地址与子网掩码

action permit　　#指定动作为允许

nat address-group *1*　　#配置 NAT 地址池

section 0 20.1.1.2 20.1.1.3　　#指定用于转换的公网地址

nat-policy　　#配置源 NAT 策略

rule name *NAPTPolicy*　　#定义源 NAT 策略名称

source-zone trust　　#指定源为信任区域

destination-zone untrust　　#指定目标为非信任区域

source-address 192.168.1.0 24　　#指定源 IP 地址与子网掩码

action source-nat address-group *1*　#指定动作按照 NAT 地址池 1 中配置的地址进行转换

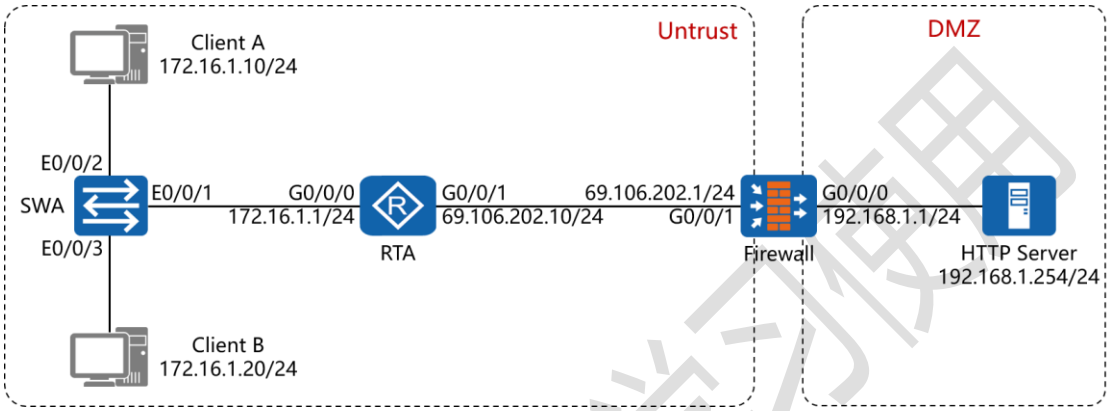
ip route-static 0.0.0.0 0.0.0.0 20.1.1.254　#配置缺省路由

ip route-static 20.1.1.2 255.255.255.255 Null 0　#为防止路由黑洞，配置空接口路由

ip route-static 20.1.1.3 255.255.255.255 Null 0　#为防止路由黑洞，配置空接口路由

七十一、配置基于 USG5500 防火墙的 NAT Server 实验组网

一、实验拓扑：



二、实验目的：

网络边界部署 USG5500 Firewall 作为安全网关，令 DMZ 区域中的 Web Server 能够对外提供服务，需在 Firewall 上配置服务器静态映射功能；除公网接口的 IP 地址外，使用地址【69.106.202.2】作为内网服务器对外提供服务的地址

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G0/0/1　　#进入相应接口

ip address 69.106.202.1 24 #配置 IP 地址及子网掩码

firewall zone untrust #进入防火墙非信任区域

set priority 5 #配置该区域安全级别为 5

add interface G0/0/1 #将接口 G0/0/1 加入进该区域

firewall zone dmz #进入防火墙 DMZ 区域

set priority 50 #配置该区域安全级别为 50

add interface G0/0/0 #将接口 G0/0/0 加入进该区域

policy interzone untrust dmz inbound #配置从非信任区域访问 DMZ 区域的进入策略

policy 0 #进入策略配置模式并指定策略编号

policy destination 192.168.1.0 mask 24 #指定目的网段与子网掩码

policy service service-set http #策略匹配 HTTP 协议

action permit #定义其动作为允许

nat server 1 protocol tcp global 69.106.202.2 8080 inside 192.168.1.254 80 no-reverse #将内部服务器地址与端口映射至外部公网地址与端口

ip route-static 0.0.0.0 0.0.0.0 69.106.202.10 #配置缺省路由

ip route-static 69.106.202.2 255.255.255.255 Null 0 #为防止路由黑洞，配置空接口路由

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

acl 2001　　#创建标准访问控制列表

rule 5 permit source 172.16.1.0 0.0.0.255　　#匹配内部源网段

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

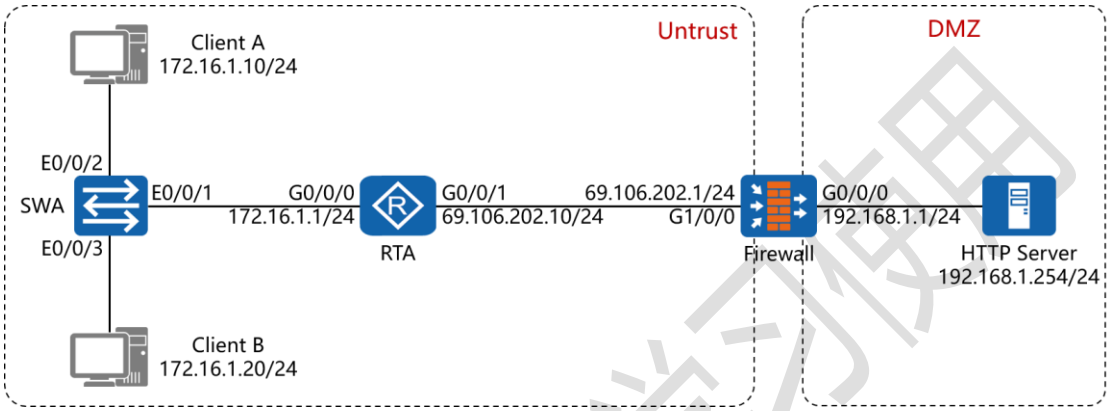
interface G0/0/1　　#进入相应接口

ip address 69.106.202.10 24　　#配置 IP 地址及子网掩码

nat outbound 2001　　#在外部接口的出方向上调用访问控制列表

七十二、配置基于 USG6000V1 防火墙的 NAT Server 实验组网

一、实验拓扑：



二、实验目的：

网络边界部署 USG6000V1 Firewall 作为安全网关，令 DMZ 区域中的 Web Server 能够对外提供服务，需在 Firewall 上配置服务器静态映射功能；除公网接口的 IP 地址外，使用地址【69.106.202.2】作为内网服务器对外提供服务的地址

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#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 G1/0/0　　#进入相应接口

ip address 69.106.202.1 24　　#配置 IP 地址及子网掩码

firewall zone untrust　#进入防火墙非信任区域

set priority 5　　#配置该区域安全级别为 5

add interface G1/0/0　　#将接口 G1/0/加入进该区域

firewall zone dmz　#进入防火墙 DMZ 区域

set priority 50　#配置该区域安全级别为 50

add interface G0/0/0　　#将接口 G0/0/0 加入进该区域

security-policy　#配置安全策略

rule name *NATSERVER*　　#指定安全策略名称

source-zone untrust　#指定源为信任区域

destination-zone dmz　　#指定目标为 DMZ 区域

destination-address 192.168.1.0 24　#指定目标的 IP 地址及子网掩码

action permit　　#指定动作为允许

nat server *natserver* protocol tcp global 69.106.202.2 www inside 192.168.1.254 www no-reverse　　#将内部服务器地址与端口映射至外部公网地址与端口

ip route-static 0.0.0.0 0.0.0.0 69.106.202.10　　#配置缺省路由

ip route-static 69.106.202.2 255.255.255.255 Null 0　　#为防止路由黑洞，配置空接口路由

RTA:

system-view　　#进入系统视图模式

sysname RTA　　#给设备命名

acl 2001　　#创建标准访问控制列表

rule 5 permit source 172.16.1.0 0.0.0.255　　#匹配内部源网段

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

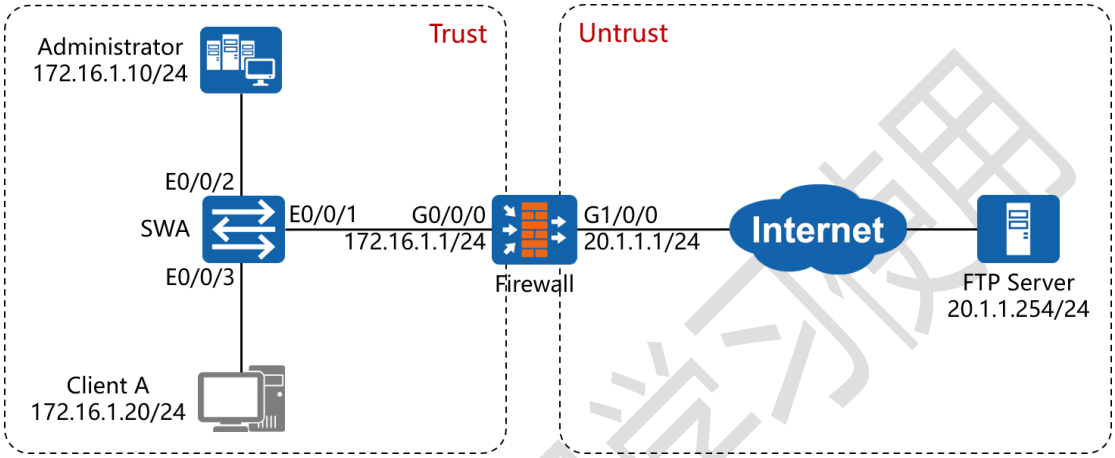
interface G0/0/1　　#进入相应接口

ip address 69.106.202.10 24　　#配置 IP 地址及子网掩码

nat outbound 2001　　#在外部接口的出方向上调用访问控制列表

七十三、配置基于 USG6000V1 防火墙的 Web 管理实验组网

一、实验拓扑：



二、实验目的：

网络边界部署 USG6000V1 Firewall 作为安全网关，令管理员通过登录防火墙 Web 页面的方式对其进行管理，使内部的 Client A 能够访问 FTP Server，但无法 ping 通 FTP Server

三、实验步骤：

Firewall:

system-view　　#进入系统视图模式

sysname Firewall　　#给设备命名

interface G0/0/0　　#进入相应接口

undo ip binding vpn-instance default　　#删除默认绑定的 VPN 实例

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

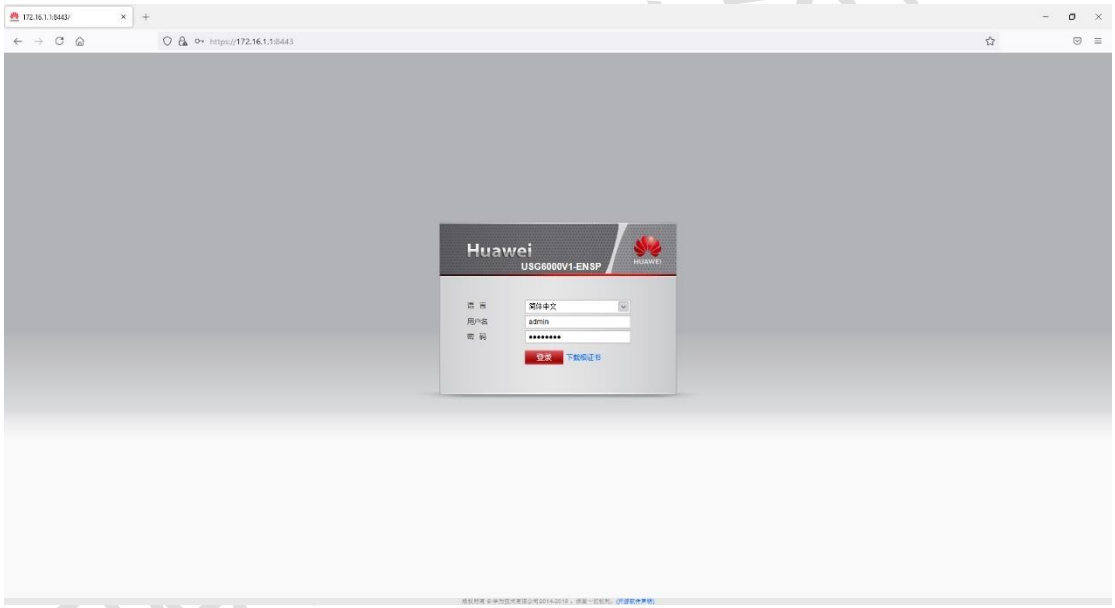
service-manage all permit　　#允许通过该接口对防火墙的所有服务进行管理

service-manage enable　　#开启服务管理功能

web-manager enable　　#开启 Web 管理功能

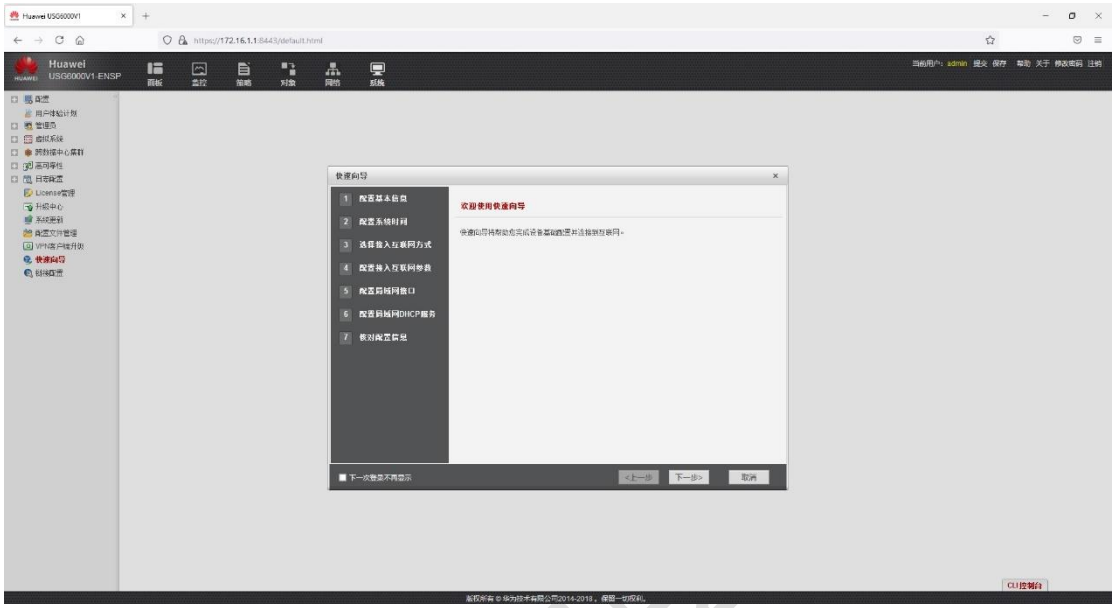
Administrator:

打开 Web 浏览器，输入 https://172.16.1.1:8443

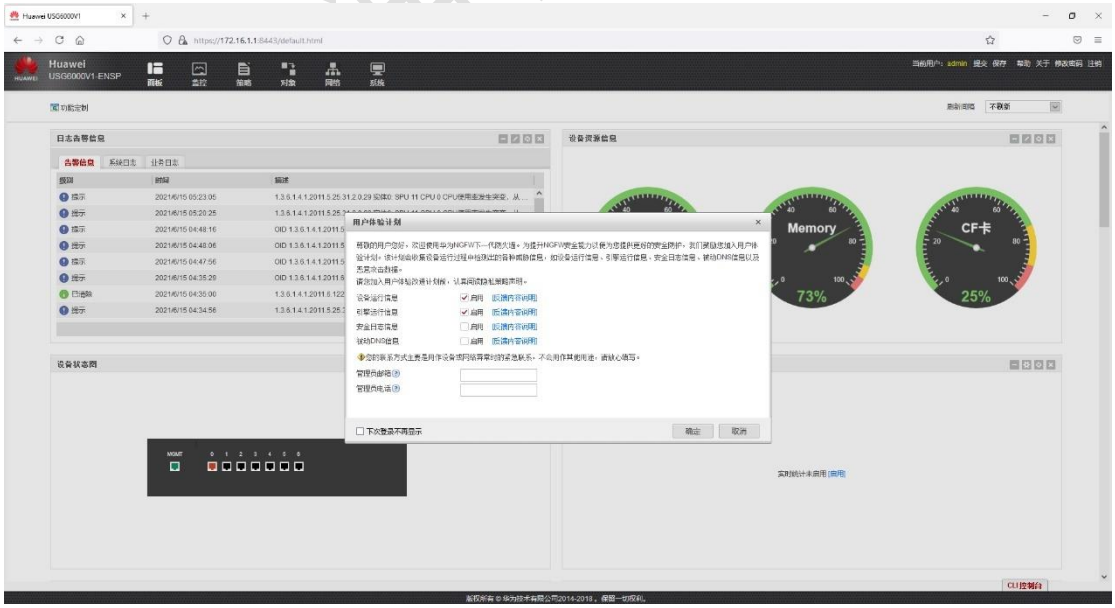


输入用户名及密钥，登录设备

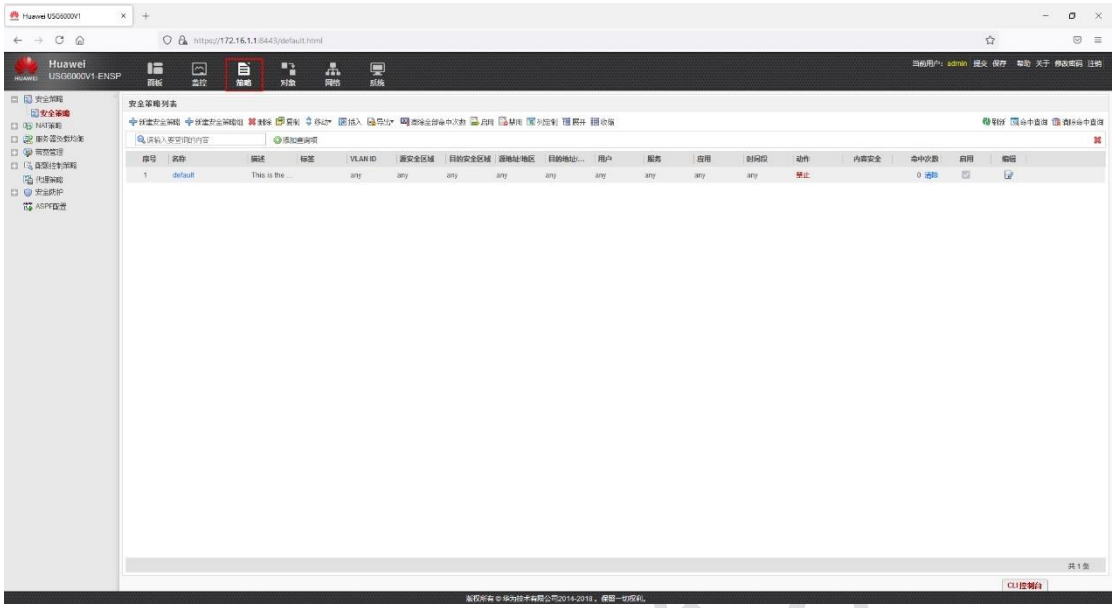
首次进入会开启【快速向导】，可不使用，勾选【下一次登录不再显示】或直接【取消】



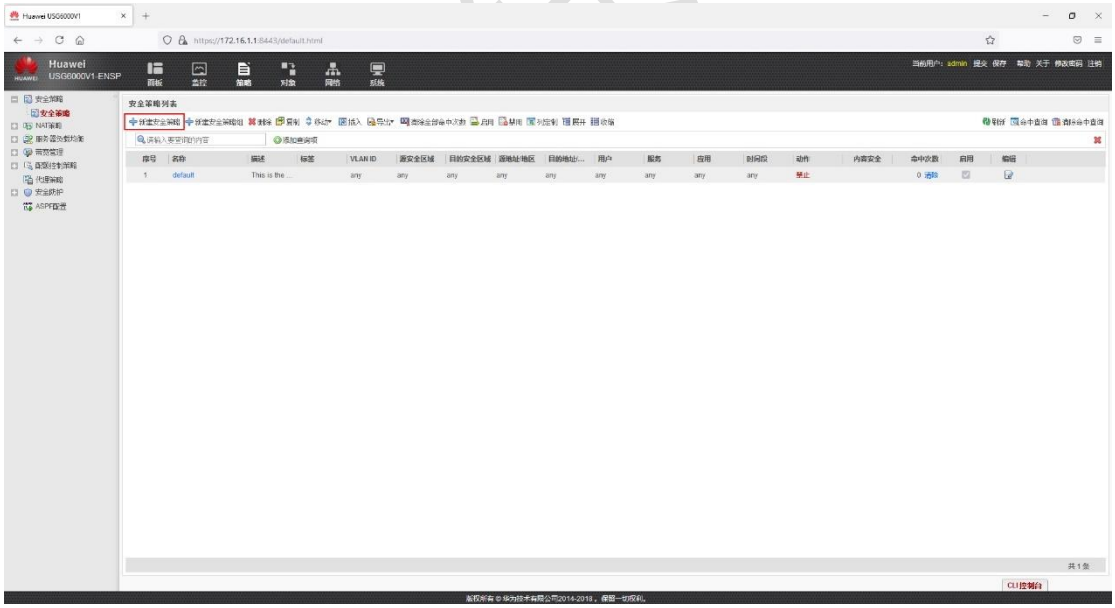
之后弹出【用户体验计划】，管理员可根据企业实际情况选择【参与】或【不参与】



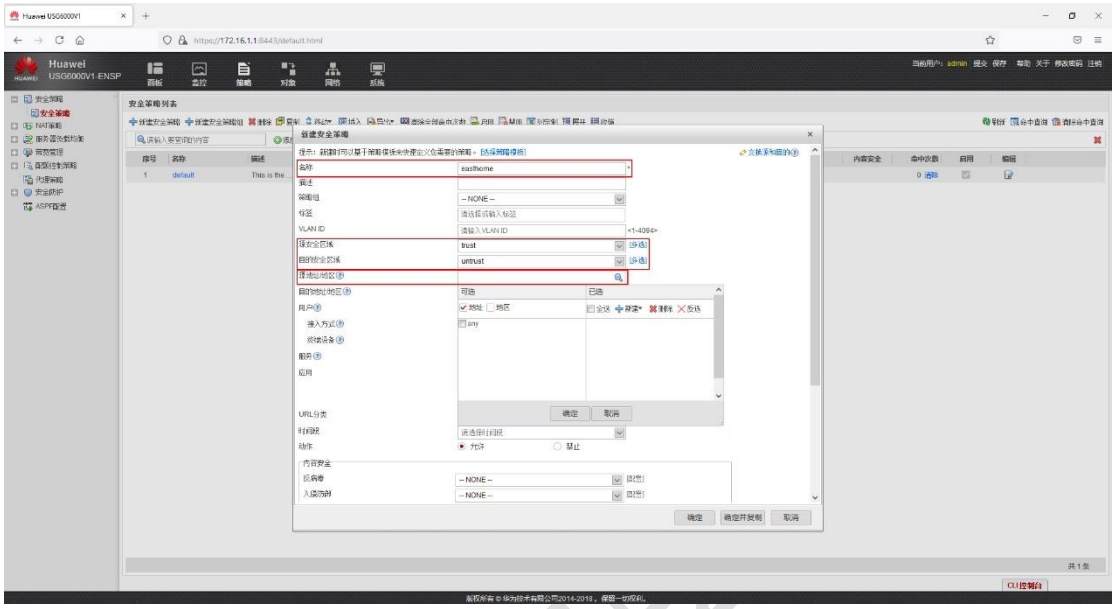
单击【策略】



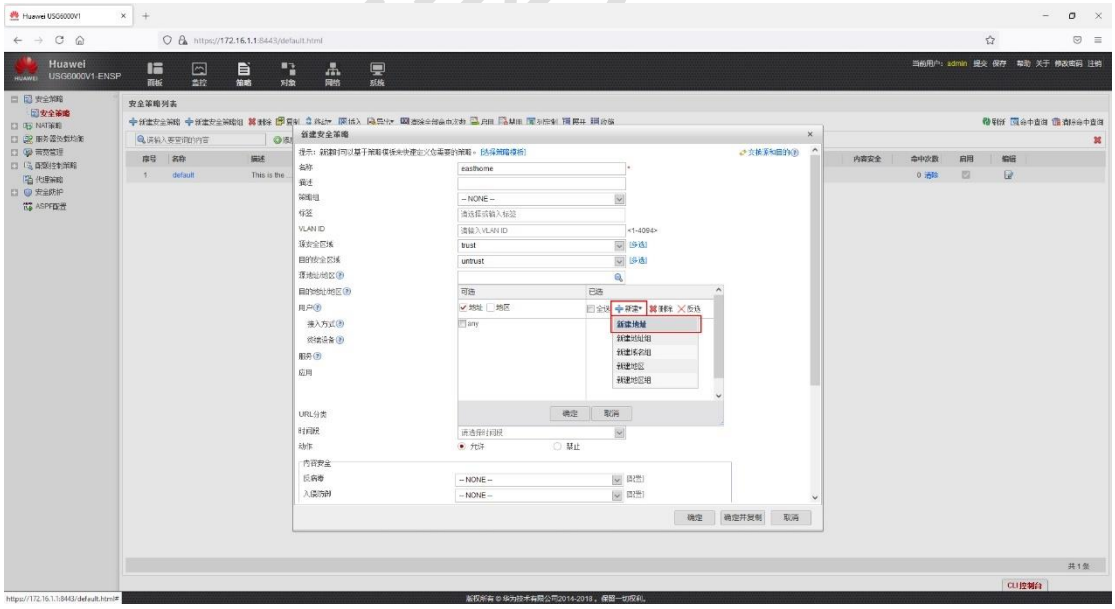
点击【新建安全策略】



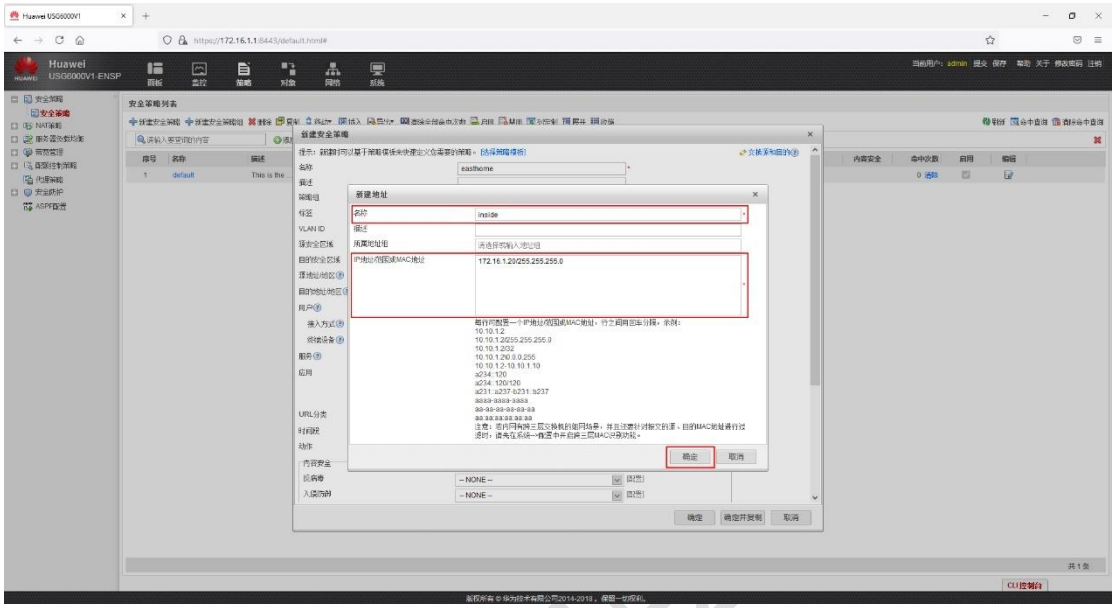
填写策略名称【easthome】，选择【源安全区域】与【目的安全区域】；之后在【源地址/地区】的空白处单击左键



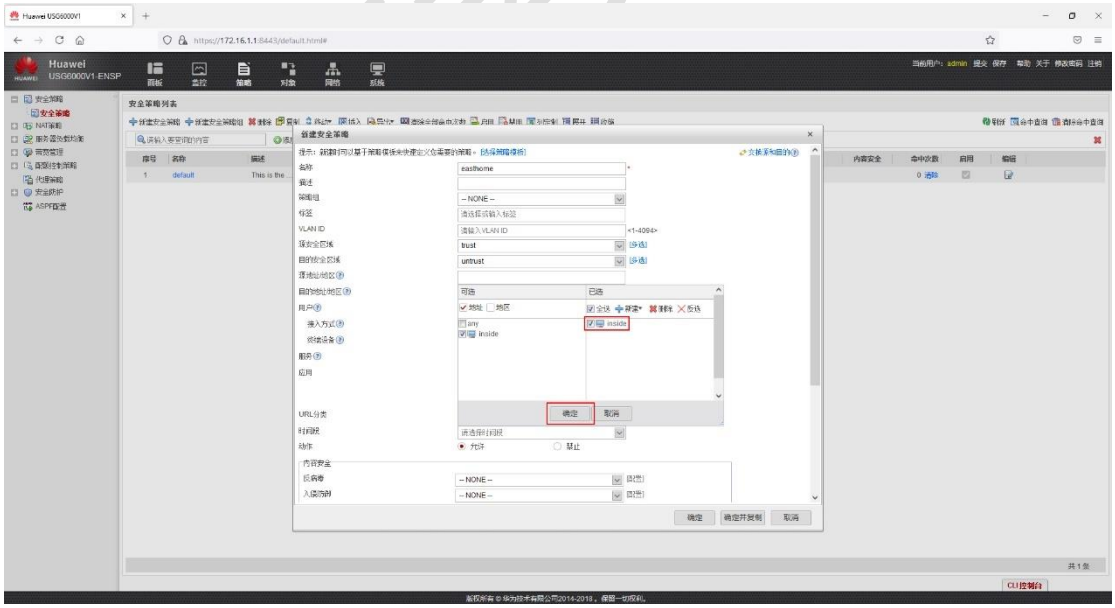
点击【新建】，选择【新建地址】



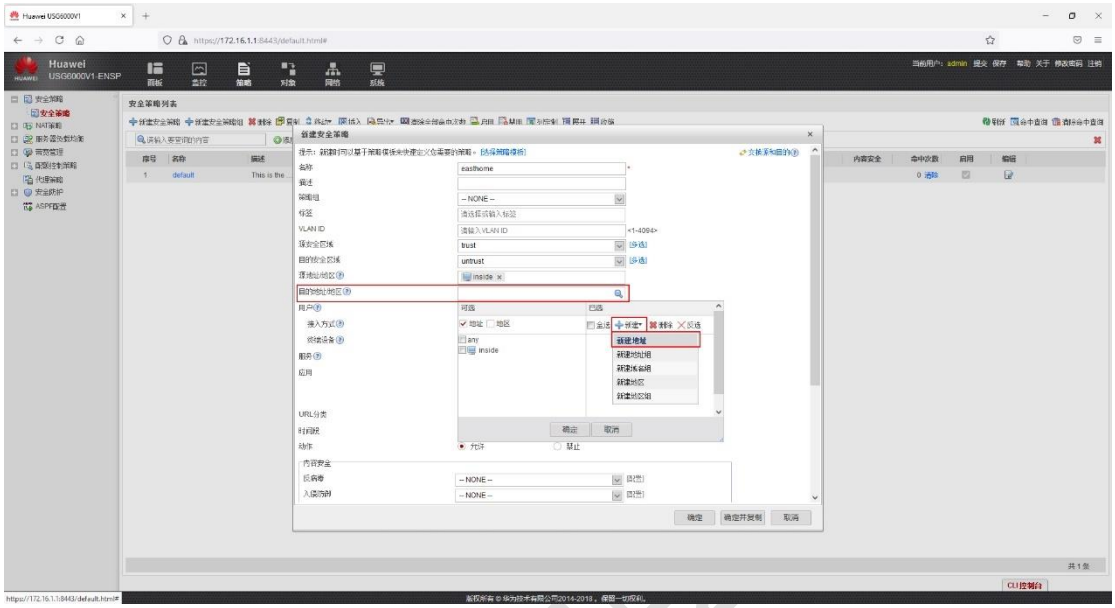
填写名称及内部主机 Client A 的 IP 地址与子网掩码，之后单击【确定】



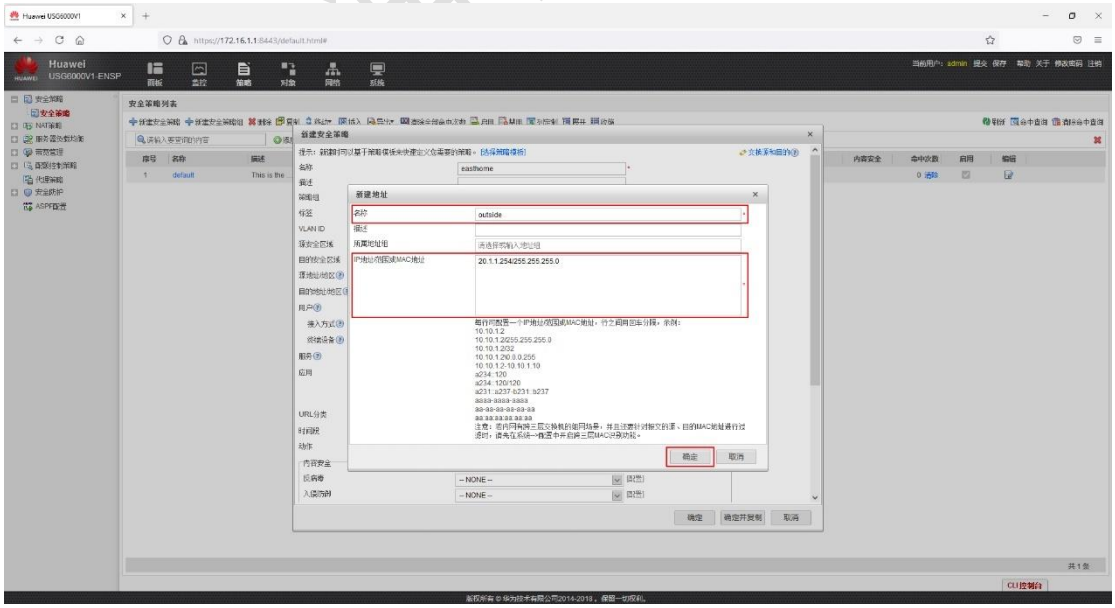
勾选新建好的【源地址】选项并点击【确定】



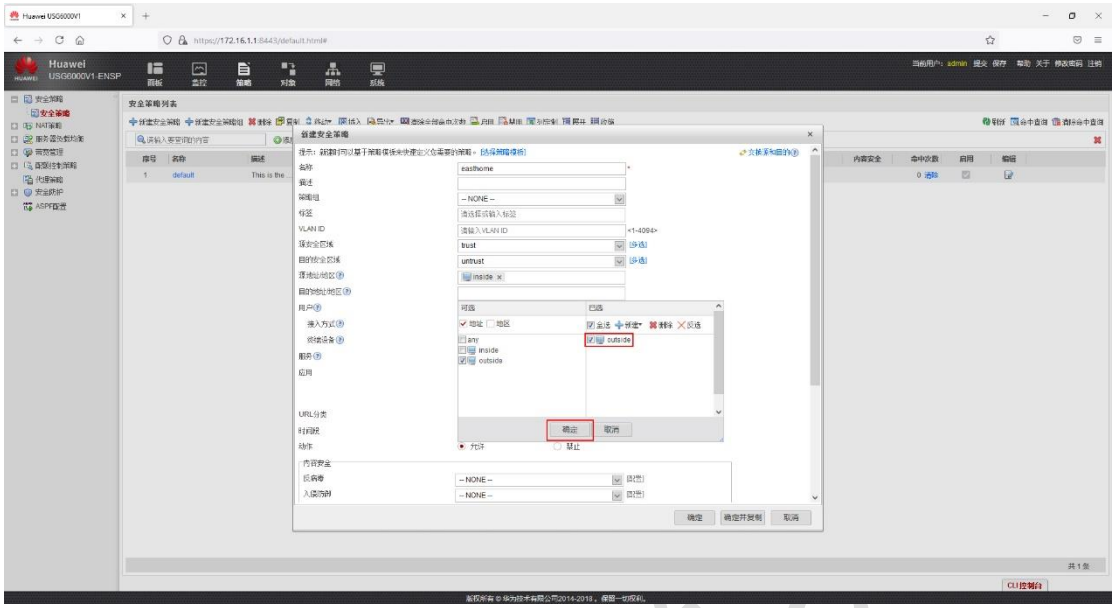
在【目的地址/地区】空白处单击左键，之后点击【新建】，选择【新建地址】



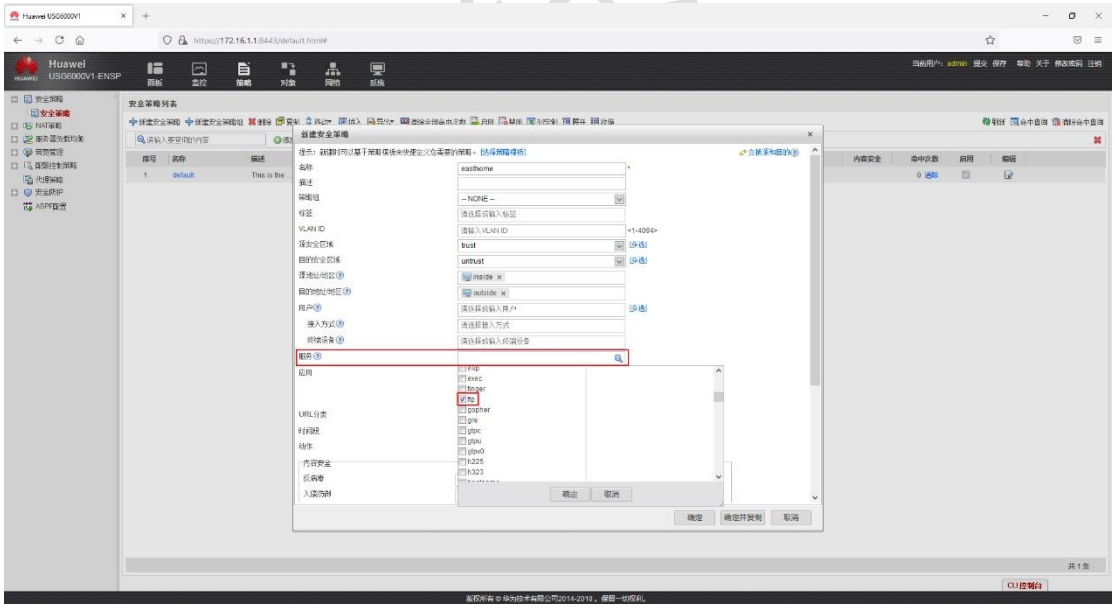
填写名称及外部的 FTP Server 的 IP 地址与子网掩码，之后单击【确定】



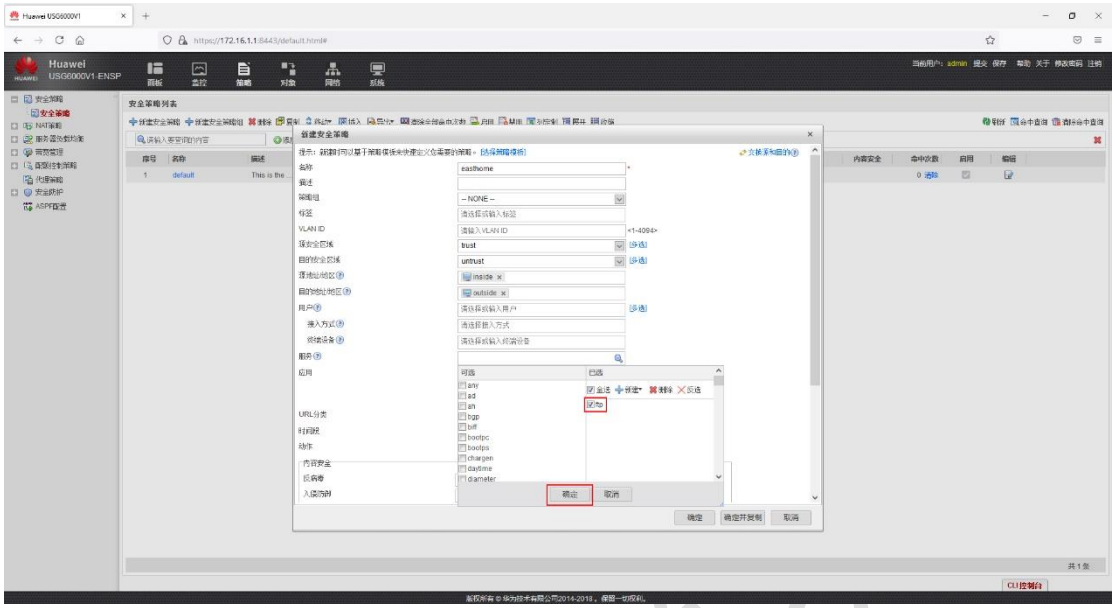
勾选新建好的【目的地址】选项并点击【确定】



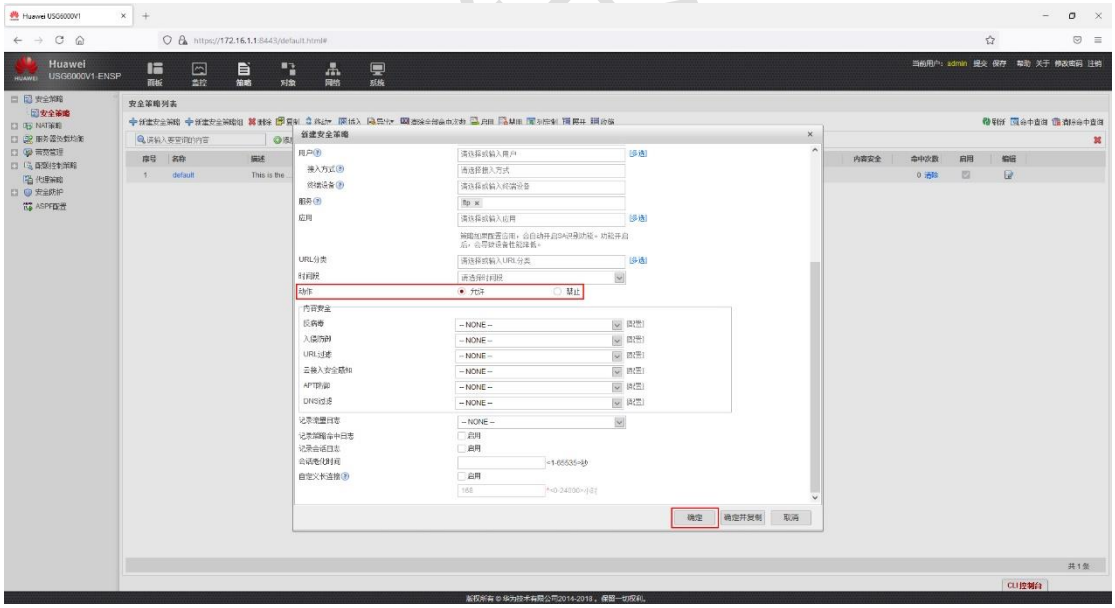
在【服务】的空白处单击左键，在弹出的下拉菜单中勾选【ftp】



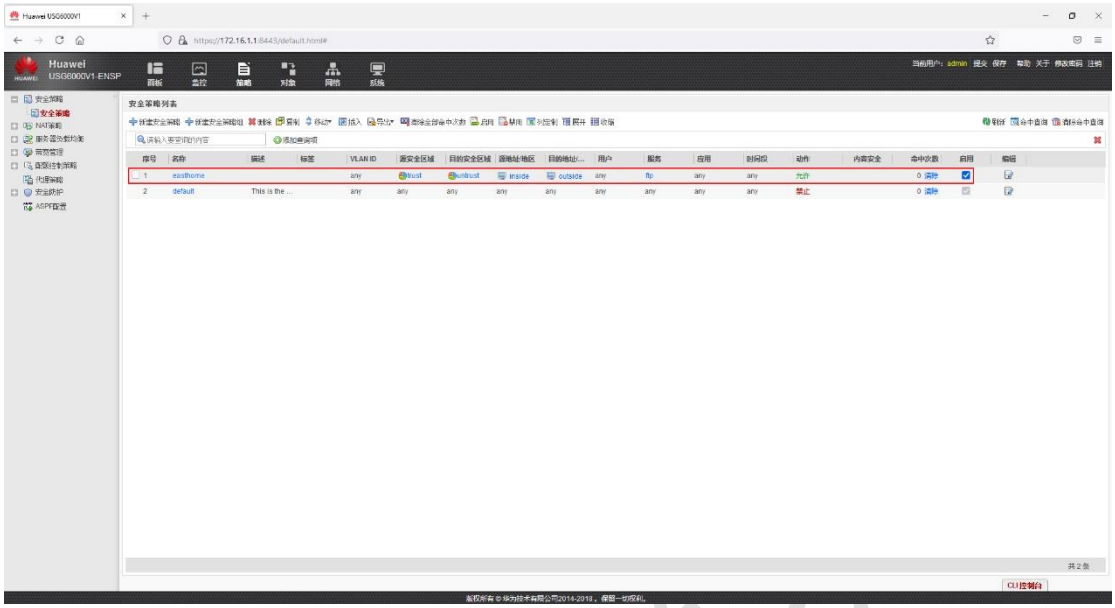
在右侧同样需要勾选【ftp】，之后单击【确定】



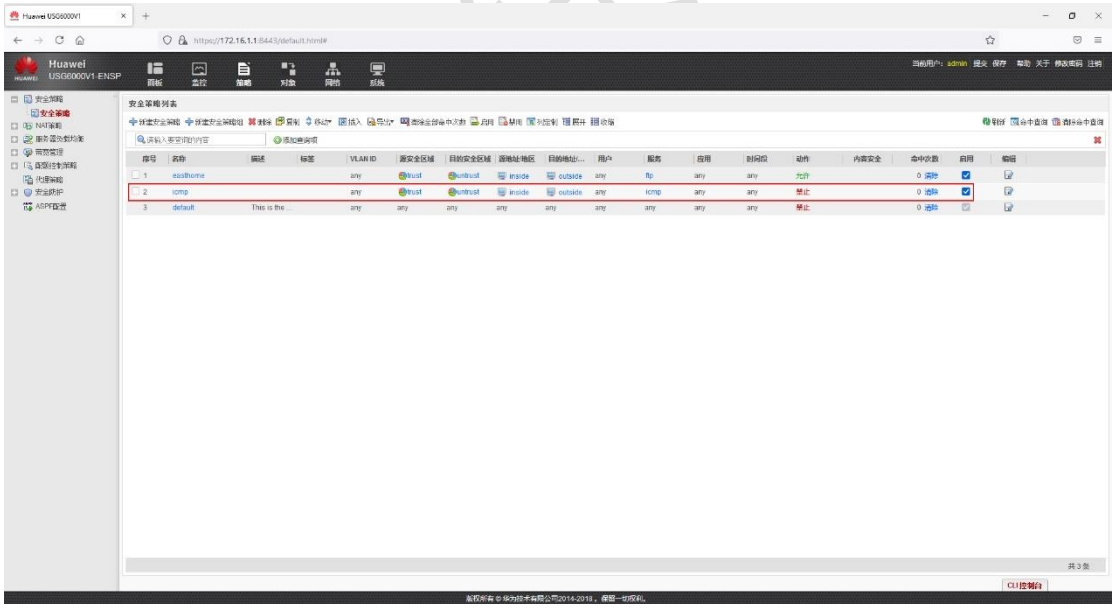
在【动作】处选择【允许】，并单击【确定】



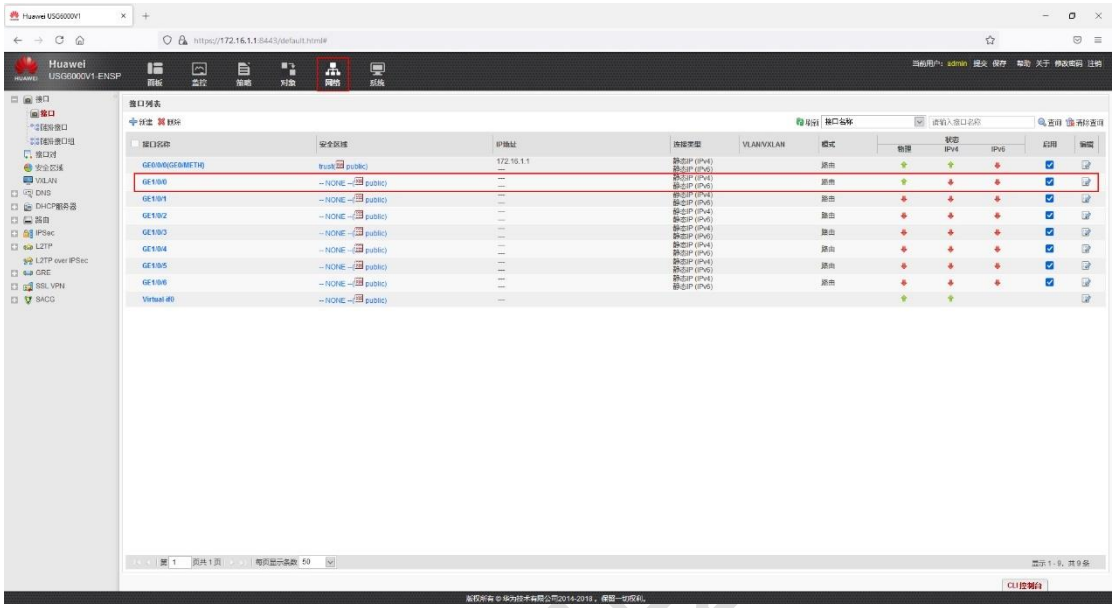
此时已创建完针对 FTP 流量的允许访问策略



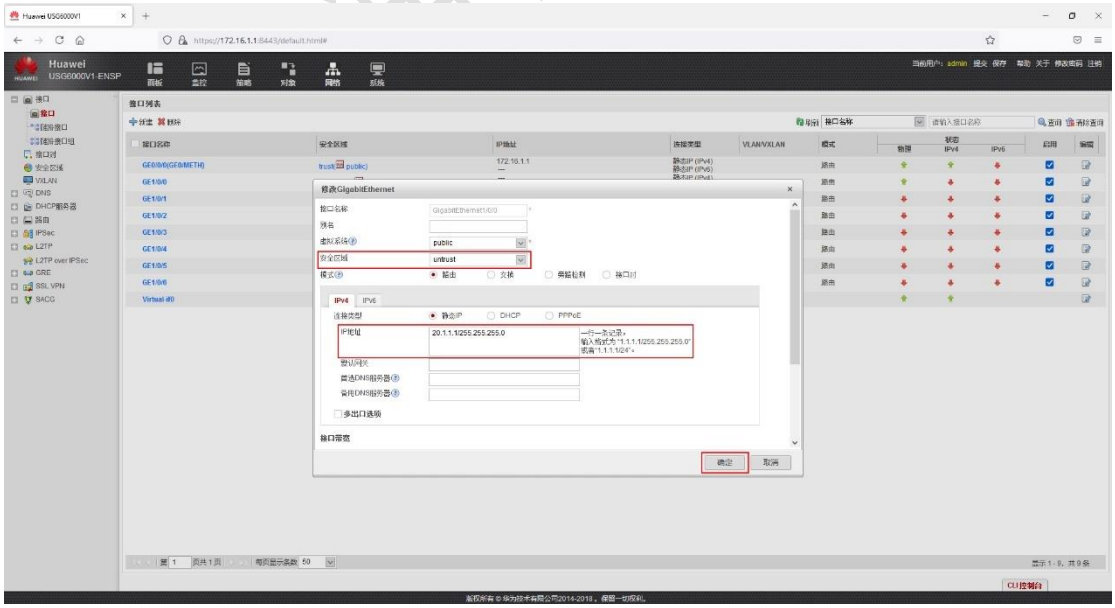
以同样的方式再创建一个针对 ICMP 流量的拒绝访问策略



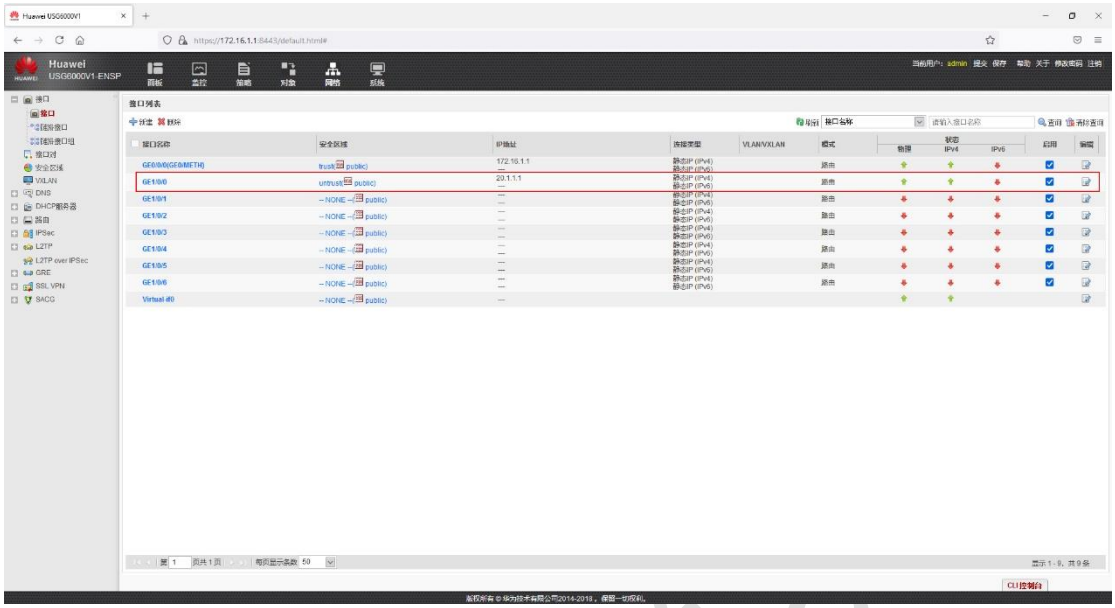
此时，防火墙的 G1/0/0 接口还没有配置 IP 地址，也没有划分所属的区域，因此需要点击【网络】，在【接口】下进行【编辑】



在【安全区域】处选择【untrust】，并按照格式配置该接口的 IP 地址与子网掩码，之后单击【确定】

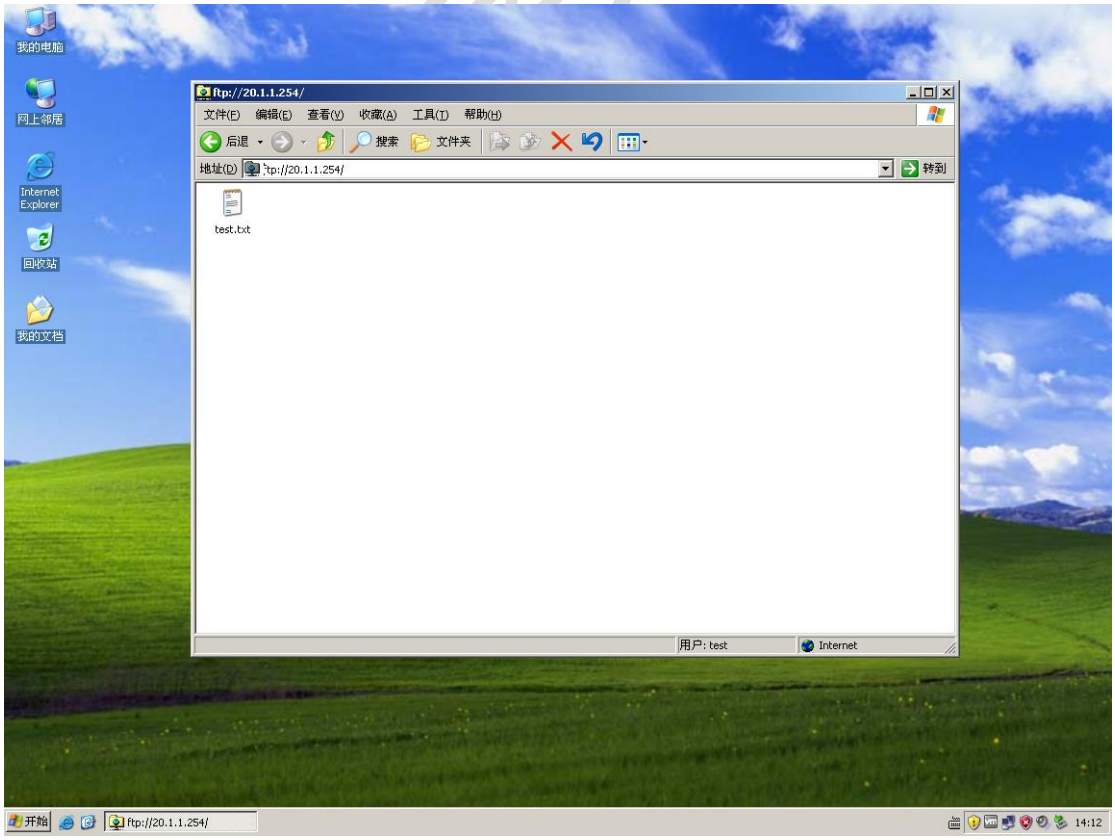


检查接口配置是否有误

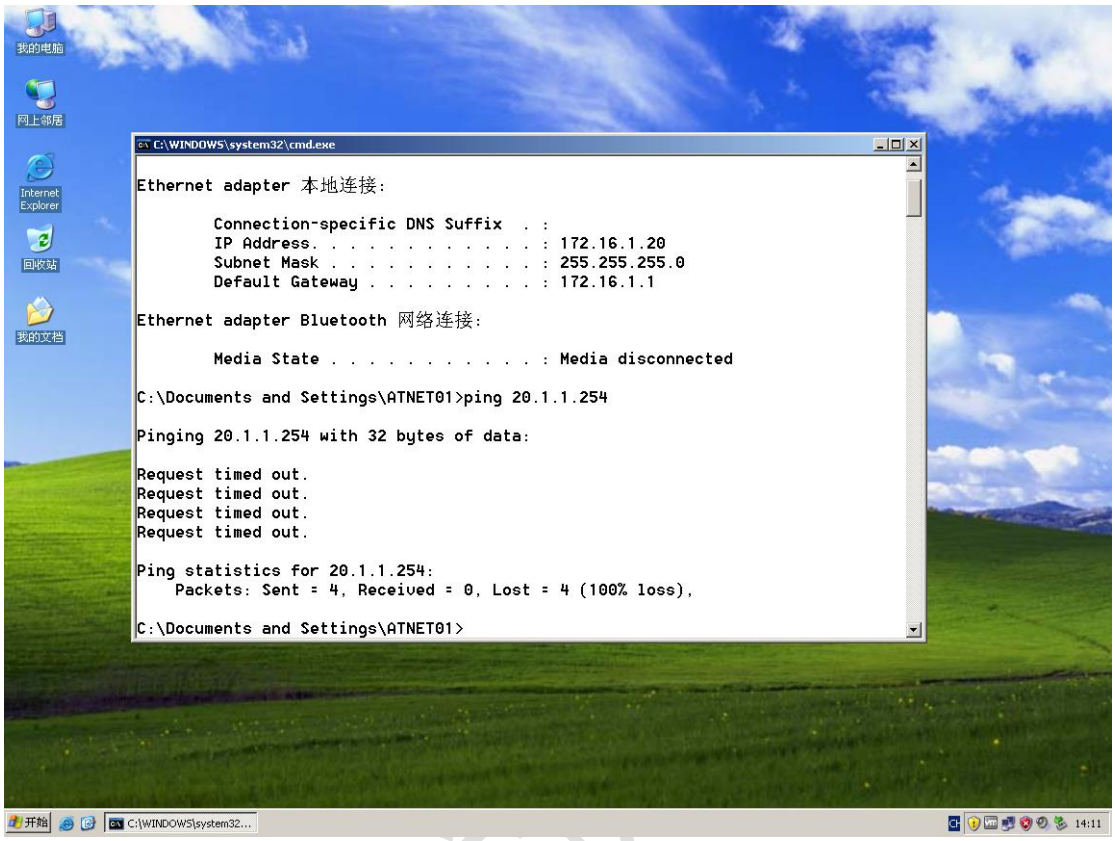


测试：

Client A 可正常访问 FTP Server：

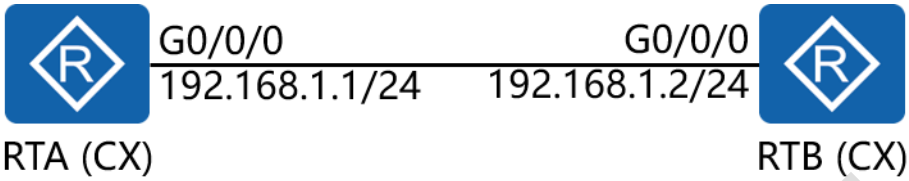


在 Client A 上检测与 FTP Server 的连通性，发现无法 ping 通：



七十四、配置 NTP 实验组网

一、实验拓扑：



二、实验目的：

将 RTA 配置成为 NTP Master，令 RTB 作为 Client 从 RTA 上同步时钟

三、实验步骤：

RTA:

system-view immediately　#进入系统视图模式并令配置立即生效

sysname Master　#给设备命名

ntp-service refclock-master　#配置本地时钟作为参考时钟

ntp-service authentication enable　#开启 NTP 认证功能

ntp-service source-interface Ethernet1/0/0　#配置 NTP 时钟源为本地接口 Ethernet1/0/0

ntp-service authentication-keyid 1 authentication-mode md5 cipher *P@ssw0rd*　#配置 NTP 服务器服务认证密钥

ntp-service reliable authentication-keyid 1　#配置可信

密钥号

undo ntp-service disable　　#开启 NTP 服务器功能

interface Ethernet1/0/0　　#进入相应接口

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

RTB:

system-view immediately

sysname Client

ntp-service authentication enable

ntp-service authentication-keyid 1 authentication-mode

md5 cipher *P@ssw0rd*

ntp-service reliable authentication-keyid 1

undo ntp-service disable

interface Ethernet1/0/0

ip address 192.168.1.2 24

测试：

更改 RTA 的时钟时间：

clock datetime 21:00:00 2021-07-01

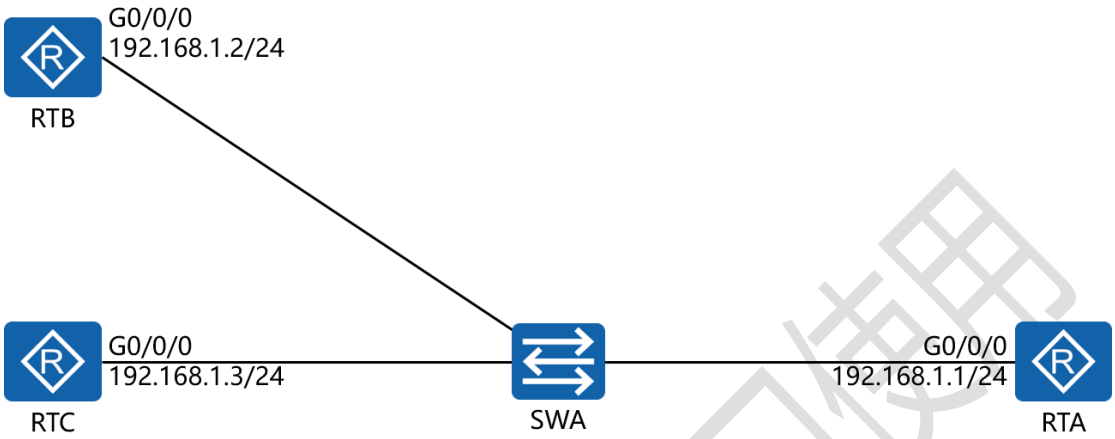
```
<Master>display clock
2021-07-01 21:03:17
Thursday
Time Zone(DefaultZoneName) : UTC
<Master>
```

查看 RTB 的时钟时间：

```
[Client]display clock
2021-07-01 21:03:29
Thursday
Time Zone(DefaultZoneName) : UTC
[Client]
```

七十五、配置 SSH 远程登录实验组网

一、实验拓扑：



二、实验目的：

配置并使用 STelnet 以安全的方式远程登录设备，在 RTA 上创建 2 个登录用户：east 与 home，令 RTB 使用用户 east，通过 password 认证方式登录 RTA；令 RTC 使用用户 home 通过 RSA 认证方式登录 RTA；同时配置安全策略，保证只允许 RTB 与 RTC 登录设备

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

rsa local-key-pair create　　#生成本地 RSA 主机密钥对与

服务器密钥对；若 RSA 密钥已存在，则系统将提示管理员确认是否替换原有密钥；输入【y】后会提示管理员输入主机密钥的位数；服务器密钥对与主机密钥对的最小长度为 512 位，最大长度为 2048 位，缺省长度为 2048 位

The key name will be: Host

% RSA keys defined for Host already exist.

Confirm to replace them? (y/n)[n]:y

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Input the bits in the modulus[default = 512]:2048

Generating keys...

.....

.....

.....+++

.....+++

.....++++++++

.++++++++

user-interface vty 0 4 #进入用户登录视图界面

authentication-mode aaa #配置认证模式为 AAA

protocol inbound ssh #入站协议允许 SSH

aaa　　#进入 AAA 的配置模式

local-user *east* password cipher *P@ssw0rd*　　#创建用户及登录密钥

local-user *east* privilege level 15　　#设置用户的级别为 15

local-user *home* password cipher *P@ssw0rd*　　#创建用户及登录密钥

local-user *home* privilege level 15　　#设置用户的级别为 15

ssh user *east* authentication-type password　　#设置用户 east 的认证类型为密钥型认证

ssh user *home* authentication-type rsa　　#设置用户 home 的认证类型为 RSA 认证

stelnet server enable　　#开启 STelnet 服务

aaa　　#进入 AAA 的配置模式

local-user *east* service-type ssh　　#设置用户 east 的服务类型为 SSH

local-user *home* service-type ssh　　#设置用户 home 的服务类型为 SSH

ssh server port *1025*　　#更改 SSH 的服务端口号码

RTC:

system-view

```
sysname RTC
interface G0/0/0
ip address 192.168.1.3 24
rsa local-key-pair create
The key name will be: Host
% RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
Input the bits in the modulus[default = 512]:2048
Generating keys...
.....
.....
.....+++
.....+++
.....++++++++
.++++++++
display rsa local-key-pair public      #查看 RTC 生成的 RSA 密钥对的公钥部分
Key code:
30820109
```

02820100

C26E4E3D C26A16FC D9B0F1E9 4B820FE8 51124585
73CADEB2 726E7424 99469D94 B0D487E8 0ED67787
6B742E0C BC249E4D D8D29999 1767E5FE F4CFF205
2CEB82CC 8F4045A7 A3D9B57F 5400B36E 370A44D9
A3AE3225 17A8DCE9 97F1AA4C C516CF0F
DC372CD6
95641839 424AD90E C96874AF FAB7CFB6 BF99E821
A63718EF 2ABC167E E34D93B7 00BA2780 92DA8688
36679812 C48F496B DBB6BB7A 0E3A8858 6DFBDF42
05EC0DEE 26A825CC 9E5577BE B6C0D9EF EBE419E0
D4F17D2F 837A4A52 7F8844E9 6FE97402 57E35D5C
53BDC944 9A6D73D7 CA1BF090 F240BDF2 ED76C2FE
0A27BC9C 887CDD67 5943C84A 7111BAD4
526BEF6B
B4567330 E12C410F CD62907B 8DC0BFA5
0203
010001

==========

==========

Time of Key pair created: 2021-06-16 10:07:56-08:00

Key name: Server

Key type: RSA encryption Key

==========

==========

Key code:

3067

0260

A7DF1302 A6FC8B70 126086A4 9579681A EC5F2651

4DDEB703 0F0E43E0 659DAFA9 2E886979 F088FA93

6783783C 854B0447 38C3B791 FCC5C1DC 45E9FAE6

ABB6AEC7 AEBDCED6 3E7A13E1 C243CE7A

45C7CCD3

B55B2F92 C46C9FF5 21834E08 681CB891

0203

010001

RTA:

rsa peer-public-key *easthome* #创建并进入 RSA 对等体公钥配置视图

public-key-code begin #指定此处为公钥代码起始点

30820109

02820100

C26E4E3D C26A16FC D9B0F1E9 4B820FE8 51124585

73CADEB2 726E7424 99469D94 B0D487E8 0ED67787

6B742E0C BC249E4D D8D29999 1767E5FE F4CFF205

2CEB82CC 8F4045A7 A3D9B57F 5400B36E 370A44D9

A3AE3225 17A8DCE9 97F1AA4C C516CF0F

DC372CD6

95641839 424AD90E C96874AF FAB7CFB6 BF99E821

A63718EF 2ABC167E E34D93B7 00BA2780 92DA8688

36679812 C48F496B DBB6BB7A 0E3A8858 6DFBDF42

05EC0DEE 26A825CC 9E5577BE B6C0D9EF EBE419E0

D4F17D2F 837A4A52 7F8844E9 6FE97402 57E35D5C

53BDC944 9A6D73D7 CA1BF090 F240BDF2 ED76C2FE

0A27BC9C 887CDD67 5943C84A 7111BAD4

526BEF6B

B4567330 E12C410F CD62907B 8DC0BFA5

0203

010001 #将 RTC 上产生的 RSA 公钥配置到服务器端

public-key-code end #指定此处为公钥代码结束点

peer-public-key end #对等体公钥配置结束

ssh user *home* assign rsa-key *easthome* #为 SSH 用户

home 绑定 STelnet 客户端的 RSA 公钥

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 192.168.1.2 24

ssh client first-time enable　#开启 SSH 客户端首次认证功能

stelnet 192.168.1.1 1025

Please input the username:*east*

Trying 192.168.1.1 ...

Press CTRL+K to abort

Connected to 192.168.1.1 ...

The server is not authenticated. Continue to access it?(y/n)[n]:y

Jun 16 2021 10:21:52-08:00

RTB %%01SSH/4/CONTINUE_KEYEXCHANGE(l)[1]:The server had not been authenticated in the process of exchanging keys. When deciding whether to continue, the user chose Y.

[RTB]

Save the server's public key? (y/n)[n]:y

The server's public key will be saved with the name 192.168.1.1. Please wait...

Jun 16 2021 10:21:56-08:00

RTB %%01SSH/4/SAVE_PUBLICKEY(l)[2]:When deciding whether to save the server's public key 192.168.1.1, the user chose Y.

[RTB]

Enter password:*P@ssw0rd*

<RTA>　　#显示登录成功

RTC:

system-view

ssh client first-time enable

stelnet 192.168.1.1 1025

Please input the username:*home*

Trying 192.168.1.1 ...

Press CTRL+K to abort

Connected to 192.168.1.1 ...

The server is not authenticated. Continue to access it? (y/n)[n]:y

Jun 16 2021 10:25:42-08:00

RTC %%01SSH/4/CONTINUE_KEYEXCHANGE(l)[1]:The server had not been authenticated in the process of exchanging keys. When deciding whether to continue, the user chose Y.

[RTC]

Save the server's public key? (y/n)[n]:y

The server's public key will be saved with the name 192.168.1.1. Please wait...

Jun 16 2021 10:25:44-08:00

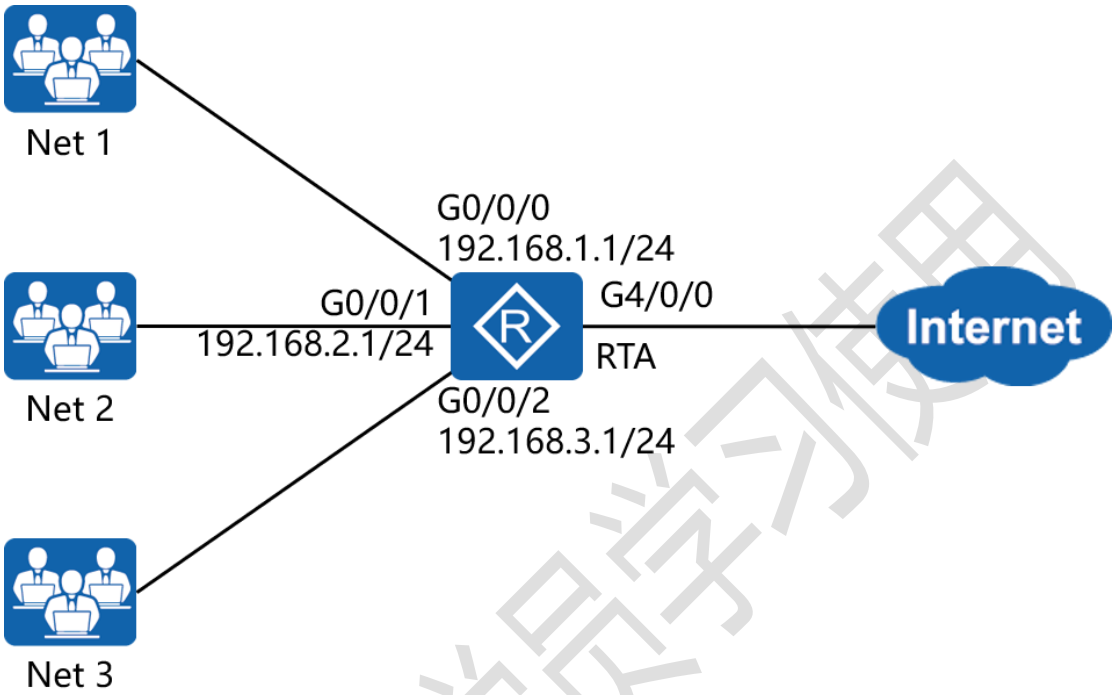
RTC %%01SSH/4/SAVE_PUBLICKEY(l)[2]:When deciding whether to save the server's public key 192.168.1.1, the user chose Y.

[RTC]

<RTA>　　#显示登录成功

七十六、配置本机防攻击实验组网

一、实验拓扑：



二、实验目的：

位于不同局域网内的用户通过 RTA 访问 Internet；为分析 RTA 受攻击情况，现需要配置攻击溯源检查功能记录攻击源信息；管理员发现存在以下现象：

1、通过攻击溯源检查功能分析可知，Net 1 中的某个用户经常发生攻击行为；

2、RTA 收到大量的 ARP Reply 报文，影响 CPU 的正常工作；

3、RTA 无法提供 FTP 服务；

4、局域网用户通过 DHCP 方式动态获取 IP 地址，但 RTA 未优先处理上送 CPU 的 DHCP 报文；

5、RTA 收到大量的 Telnet 报文

管理员需要通过在 RTA 上配置本机防攻击以便解决上述问题

三、实验步骤：

RTA:

system-view

sysname RTA

acl 4001 #创建基于 MAC 地址的访问控制列表

rule permit source-mac 5489-985C-476F #匹配攻击者的源 MAC 地址

cpu-defend policy *easthome* #创建防攻击策略

auto-defend enable #开启攻击溯源检查功能

auto-defend threshold 50 #配置攻击溯源检查阈值为 50

blacklist 1 acl 4001 #将 ACL 4001 匹配的源 MAC 地址配置在黑名单中

packet-type arp-reply rate-limit 1 #配置 ARP Reply 报文上送 CPU 的速率限制为 1pps

application-apperceive packet-type ftp rate-limit 2000 #配置 FTP 协议动态链路保护功能的速率限制值为 2000pps

cpu-defend application-apperceive ftp enable #全局下开启 FTP 协议动态链路保护功能

cpu-defend policy *easthome* #进入防攻击策略配置模式

packet-type dhcp-client priority 3 #将上报的 DHCP 报文优先级配置为 3，令 CPU 优先处理此类报文

cpu-defend-policy *easthome* #在全局下应用防攻击策略

undo telnet server enable #关闭 Telnet 服务功能

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 192.168.1.254 #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

interface G0/0/1 #进入相应接口

ip address 192.168.2.1 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 192.168.2.254 #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

interface G0/0/2 #进入相应接口

ip address 192.168.3.1 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 192.168.3.254 #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

测试：

在 RTA 上查看配置的防攻击策略信息

```
[RTA]display cpu-defend policy easthome
 Related slot : <0>
 BlackList Status :
   Slot<0> : Success
 Configuration :
   Blacklist 1 ACL number : 4001
   Packet-type arp-reply rate-limit : 1(pps)
   Packet-type dhcp-client priority : 3
   Rate-limit all-packets : 1500(pps)(default)
   Application-apperceive packet-type ftp : 2000(pps)
   Application-apperceive packet-type tftp : 2000(pps)
[RTA]
```

在网络中没有 ARP-Reply 攻击时，查看上送到 RTA 主控板的报文的统计信息：

```
[RTA]display cpu-defend statistics
Statistics on on main board.
-------------------------------------------------------------------------
Packet Type                Pass Packets         Drop Packets
-------------------------------------------------------------------------
8021X                                 0                    0
arp-miss                              0                    0
arp-reply                             1                    0
arp-request                           4                    0
bfd                                   0                    0
bgp                                   0                    0
bgp4plus                              0                    0
capwap                                0                    0
dhcp-client                           0                    0
dhcp-server                           0                    0
dhcpv6-reply                          0                    0
dhcpv6-request                        0                    0
dlsw                                  0                    0
dns                                   0                    0
eoam-3ah                              0                    0
eoam-3ah-test                         0                    0
fib-hit                               0                    0
fr                                    0                    0
ftp-client                            0                    0
ftp-server                            0                    0
  ---- More ----
```

当网络中出现了大量的 ARP-Reply 报文时，系统会弹出提示信息，表明丢弃了这些报文：

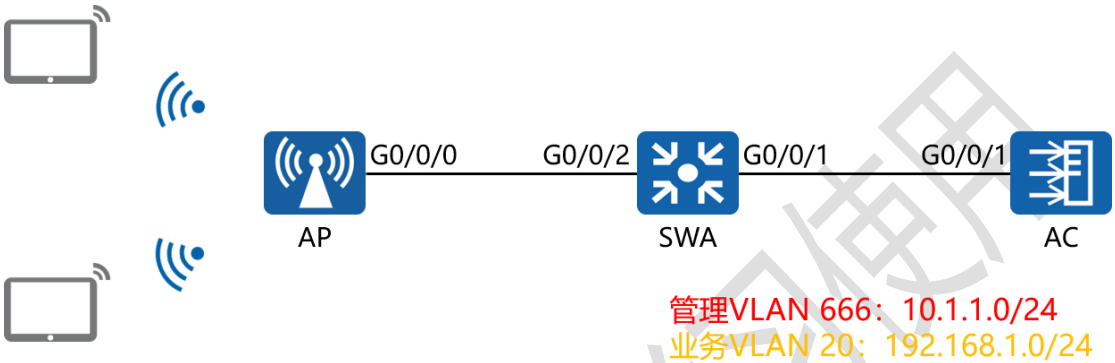
```
Jun 16 2021 11:14:53-08:00 RTA %%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l)[2]:Invalid
 source mac address.(SourceMAC=1122-3344-5566, SourceIP=100.2.168.192, SourceInt
erface=GigabitEthernet0/0/1, DropTime=2021/06/16 11:14:53)fw-dns
```

此时再次查看上送到 RTA 主控板的报文的统计信息，此时发现存在大量的 ARP-Reply 丢弃报文，表明设备已经对 ARP-Reply 报文进行了速率限制

```
[RTA]display cpu-defend statistics
Statistics on on main board.
------------------------------------------------------------------------------
Packet Type                Pass Packets        Drop Packets
------------------------------------------------------------------------------
8021X                                 0                   0
arp-miss                              0                   0
arp-reply                           449                41096
arp-request                           4                   0
bfd                                   0                   0
bgp                                   0                   0
bgp4plus                              0                   0
capwap                                0                   0
dhcp-client                           0                   0
dhcp-server                           0                   0
dhcpv6-reply                          0                   0
dhcpv6-request                        0                   0
dlsw                                  0                   0
dns                                   0                   0
eoam-3ah                              0                   0
eoam-3ah-test                         0                   0
fib-hit                               0                   0
fr                                    0                   0
ftp-client                            0                   0
ftp-server                            0                   0
  ---- More ----
```

七十七、配置 WLAN VLAN Pool 实验组网

一、实验拓扑：



二、实验目的：

通过在 AC 上配置 VLAN Pool，令 VLAN Pool 中包含 2 个业务 VLAN，从而实现一个 SSID 对应多个业务 VLAN 的方案；基于 HASH 分配算法将大量用户分散到不同的 VLAN 中，以划分广播域，减少广播风暴

三、实验步骤：

AC:

system-view　　#进入系统视图模式

sysname AC　　#给设备命名

vlan batch 20 30 666　　#创建 VLAN 20、30 及 666

dhcp enable　　#开启 DHCP 功能

ip pool vlan20　　#创建并进入 vlan20 地址池

network 192.168.1.0 mask 24 #配置分配的网段及子网掩码

gateway-list 192.168.1.1 #配置分配的网关地址

dns-list 202.106.0.20 #配置分配的 DNS 地址

ip pool vlan30 #创建并进入 vlan30 地址池

network 172.16.1.0 mask 24 #配置分配的网段及子网掩码

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

ip pool vlan666 #创建并进入 vlan666 地址池

network 10.1.1.0 mask 24 #配置分配的网段及子网掩码

gateway-list 10.1.1.1 #配置分配的网关地址

interface vlan 20 #进入 VLAN 20 的接口配置模式

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

dhcp select global #开启基于全局的 DHCP 功能

interface vlan 30 #进入 VLAN 30 的接口配置模式

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

dhcp select global #开启基于全局的 DHCP 功能

interface vlan 666 #进入 VLAN 666 的接口配置模式

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

dhcp select global #开启基于全局的 DHCP 功能

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 #允许传递所有 VLAN 标记的数据帧

capwap source interface Vlanif 666 #指定 AC 与 AP 建立 CAPWAP 隧道的源接口

wlan #进入 WLAN 的配置模式

security-profile name *Huawei-AP3030* #创建并进入安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip #指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030* #创建并进入SSID模板视图

ssid Huawei-AP3030 #指定SSID的名称

vlan pool *easthome* #创建并进入VLAN Pool

vlan 20 30 #指定VLAN Pool中包含的业务VLAN

assignment hash #配置基于HASH分配算法

wlan #进入WLAN的配置模式

vap-profile name *Huawei-AP3030* #创建并进入VAP模板视图

service-vlan vlan-pool *easthome* #配置VAP的业务VLAN使用VLAN Pool中的VLAN

ssid-profile *Huawei-AP3030* #绑定SSID模板

security-profile *Huawei-AP3030* #绑定安全模板

ap-group name *Huawei-AP3030* #创建并进入AP组

radio 0 #指定射频ID

vap-profile *Huawei-AP3030* wlan 1 #将VAP与WLAN配置做绑定

ap-id 1 type-id 45 ap-mac 00e0-fcd7-2d20 #配置第一台AP的ID值，类型值，以及AP的MAC地址

ap-name AP1 #为第一台AP命名

ap-group *Huawei-AP3030* #将AP加入进AP组

SWA:

system-view

sysname SWA

vlan batch 20 30 666

interface G0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface G0/0/2

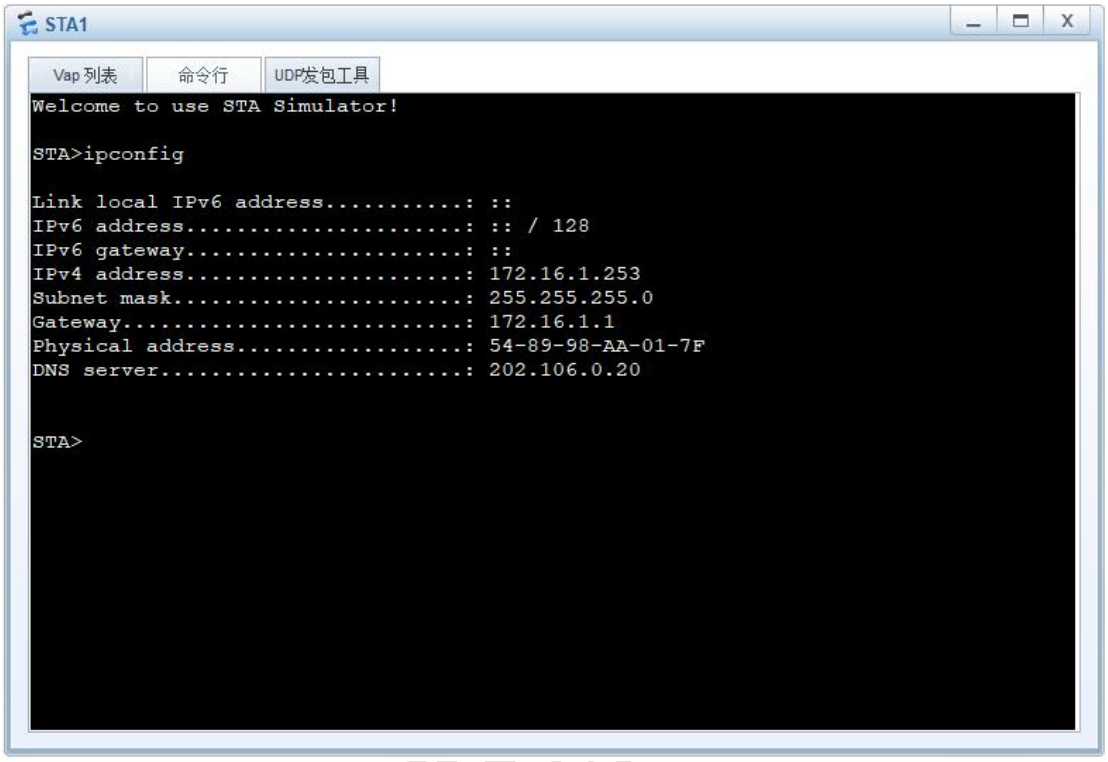
port link-type trunk

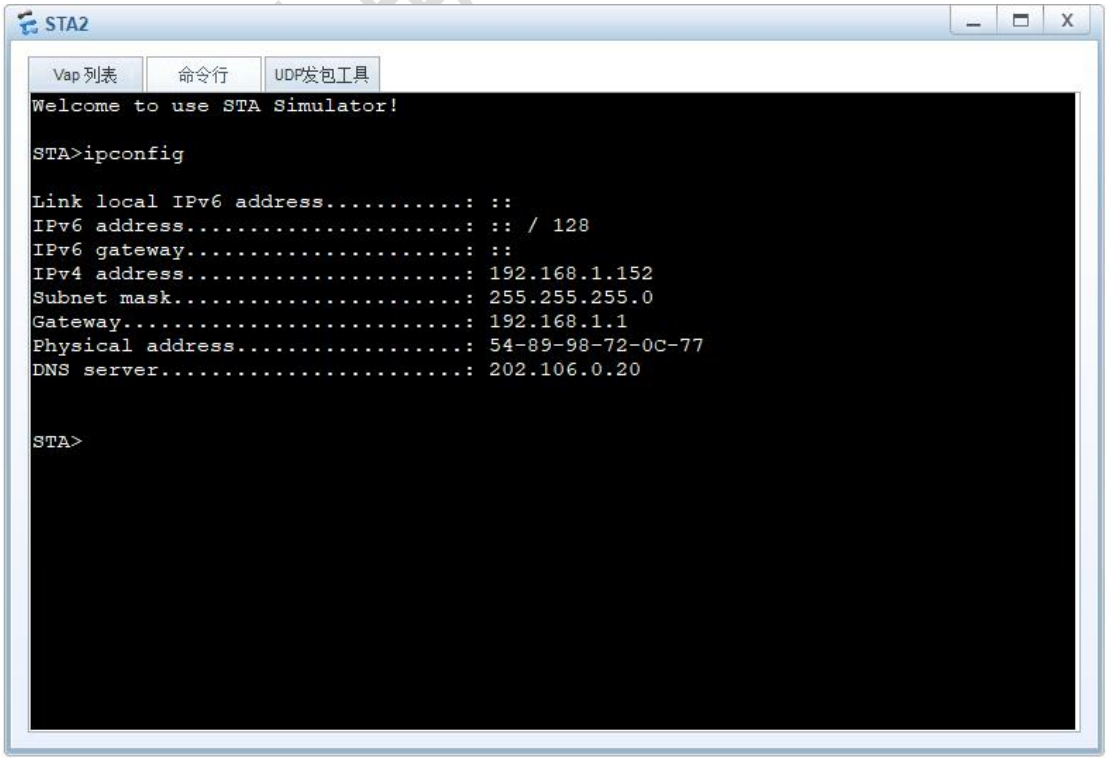
port trunk allow-pass vlan all

port trunk pvid vlan 666

测试：

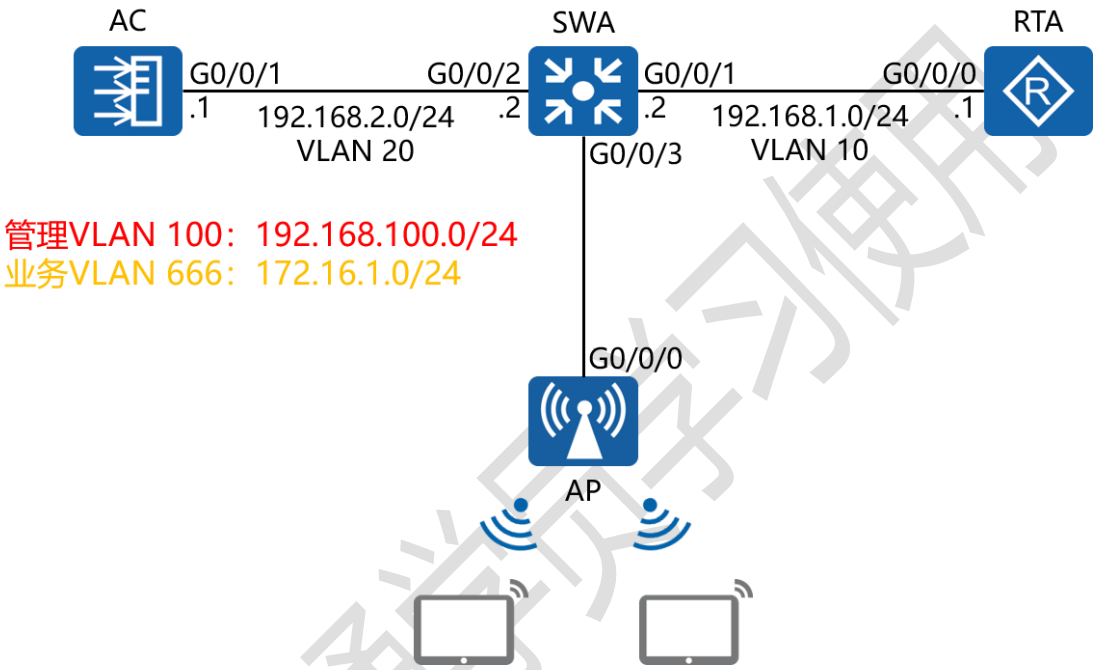
使用 2 台 STA 设备连接 AP，查看这 2 台 STA 所获取的 IP 地址





七十八、配置 WLAN DHCP 中继代理实验组网

一、实验拓扑：



二、实验目的：

AC 与 AP 之间为三层组网，将 RTA 配置为 DHCP 服务器，为 AP 下发管理 VLAN 与业务 VLAN 的 IP 地址；在三层组网环境中，AP 无法通过发送广播请求报文的方式发现 AC，因此需要配置 DHCP 服务器向 AP 回应的报文中携带 Option 43 字段来通告 AC 的 IP 地址，令 AP 能够以单播的方式与 AC 之间建立 CAPWAP 隧道

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　　#进入相应的接口

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

dhcp select global　　#开启基于全局的 DHCP 功能

ip pool vlan100　　#创建并进入 vlan100 地址池

network 192.168.100.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 192.168.100.254　　#配置分配的网关地址

option 43 sub-option 2 ip-address 192.168.2.1　　#配置 option 43 参数，携带 AC 的 IP 地址

ip pool vlan666　　#创建并进入 vlan666 地址池

network 172.16.1.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 172.16.1.1　　#配置分配的网关地址

ip route-static 0.0.0.0 0.0.0.0 192.168.1.2　　#配置缺省路由

SWA:

system-view

```
sysname SWA
vlan batch 10 20 100 666        #创建 VLAN 10、20、100 及 666
dhcp enable
interface vlan 10
ip address 192.168.1.2 24
interface vlan 20
ip address 192.168.2.2 24
interface vlan 100
ip address 192.168.100.254 24
dhcp select relay        #开启 DHCP 中继代理功能
dhcp relay server-ip 192.168.1.1        #指定 DHCP 服务器的 IP 地址
interface vlan 666
ip address 172.16.1.1 24
dhcp select relay        #开启 DHCP 中继代理功能
dhcp relay server-ip 192.168.1.1        #指定 DHCP 服务器的 IP 地址
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 pvid vlan 100

port trunk allow-pass vlan all

AC:

system-view

sysname AC

vlan batch 20 100 666

interface Vlanif20

ip address 192.168.2.1 24

interface G0/0/1

port link-type access

port default vlan 20

ip route-static 0.0.0.0 0 192.168.2.2

capwap source interface vlanif20 #指定AC与AP建立CAPWAP 隧道的源接口

wlan #进入 WLAN 的配置模式

security-profile name *Huawei-AP3030* #创建并进入安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

#指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030*　　#创建并进入SSID模板视图

ssid Huawei-AP3030　　#指定SSID的名称

vap-profile name *Huawei-AP3030*　　#创建并进入VAP模板视图

service-vlan vlan-id 666　　#配置VAP的业务VLAN为VLAN 666

ssid-profile *Huawei-AP3030*　　#绑定SSID模板

security-profile *Huawei-AP3030*　　#绑定安全模板

ap-group name *Huawei-AP3030*　　#创建并进入AP组

radio 0　　#指定射频ID

vap-profile *Huawei-AP3030* wlan 1　　#将VAP与WLAN配置做绑定

ap-id 1 type-id 45 ap-mac 00E0-FC48-4D40　　#配置第一台AP的ID值，类型值，以及AP的MAC地址

ap-name AP1　　#为第一台AP命名

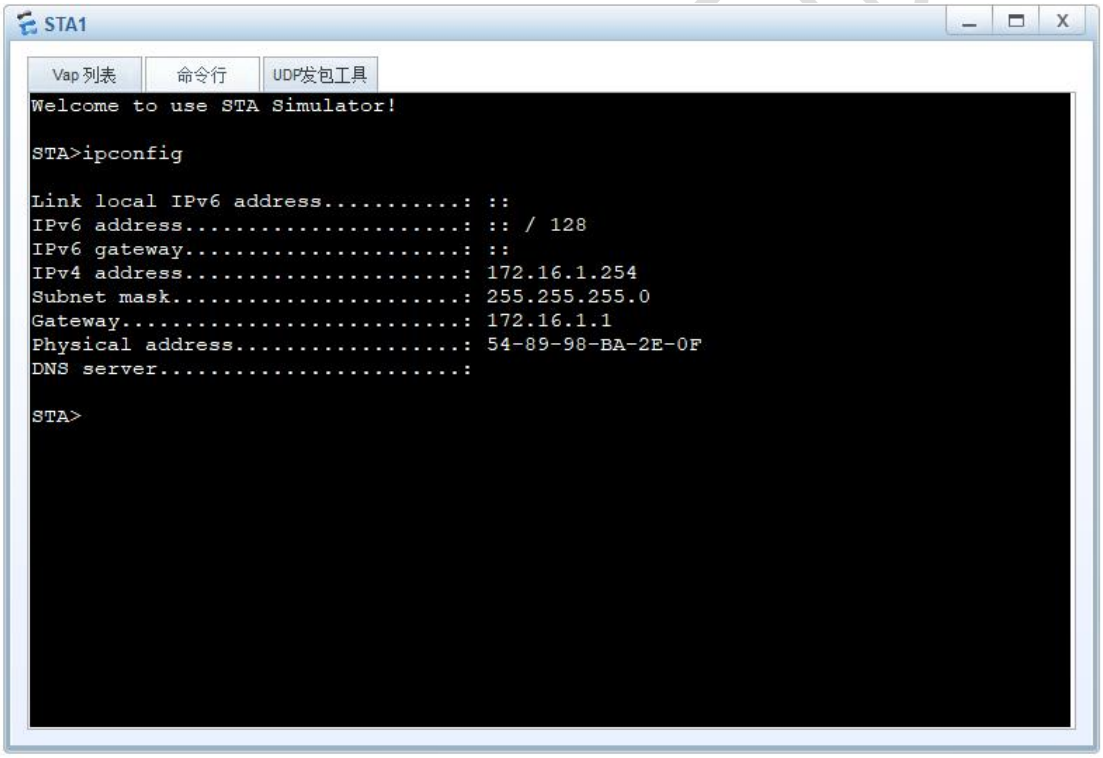
ap-group *Huawei-AP3030*　　#将AP加入进AP组

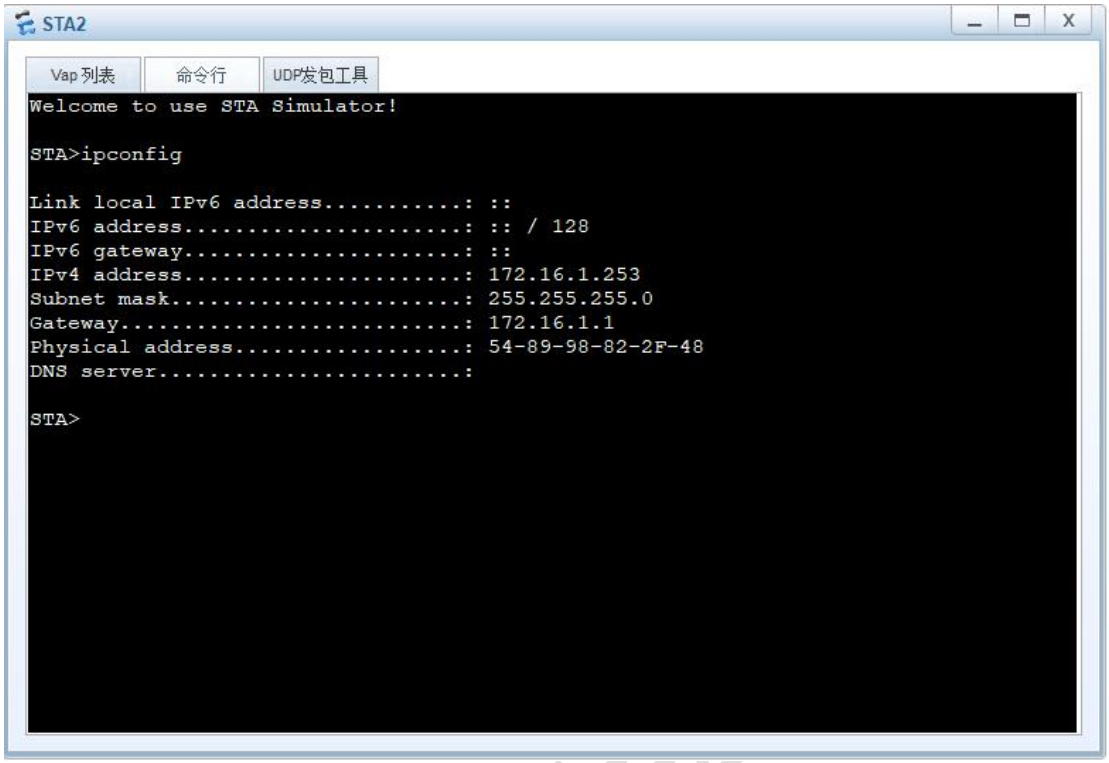
测试：

在 AP 上查看获得的管理 IP 地址：

```
[AP1]display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                          VLAN
--------------------------------------------------------------------------------
192.168.100.253 00e0-fc0a-3010            I -  Vlanif1
192.168.100.254 4c1f-cc80-5903  18        D-0  GE0/0/0
                                          1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0     Interface:1
[AP1]
```

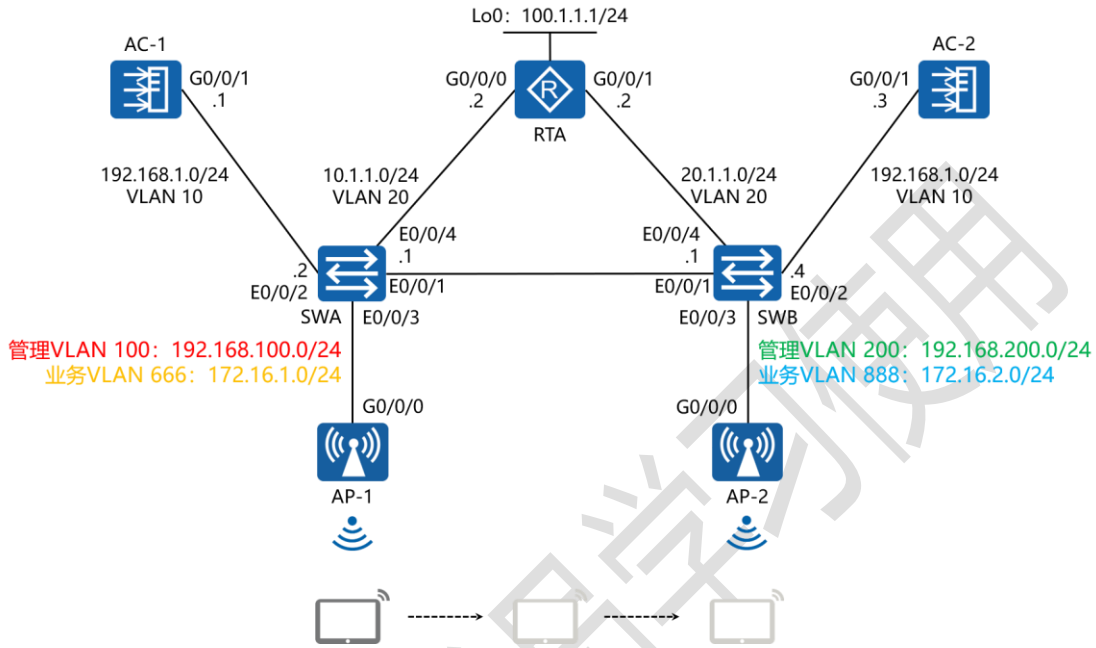
检测 STA 设备获取的业务 IP 地址：




STA2
Vap 列表
命令行
UDP发包工具
Welcome to use STA Simulator!
STA>ipconfig
Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 172.16.1.253
Subnet mask.....: 255.255.255.0
Gateway.....: 172.16.1.1
Physical address.....: 54-89-98-82-2F-48
DNS server.....:
STA>

七十九、配置 WLAN 漫游实验组网

一、实验拓扑：



二、实验目的：

令 AC-1 与 AC-2 共同组成漫游组，STA 设备最初通过连接 AP-1 来访问整个网络，当 STA 设备逐步向 AP-2 移动时，通过 AC-1 与 AC-2 的漫游组配置，令 STA 设备的 IP 地址不更换，同时保证其业务的连续性

三、实验步骤：

AC-1:

system-view　　#进入系统视图模式

sysname AC-1　　#给设备命名

vlan batch 10 100 666　　#创建 VLAN 10、100 及 666

dhcp enable　　#开启 DHCP 功能

ip pool vlan100　　#创建并进入vlan100地址池

network 192.168.100.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 192.168.100.254　　#配置分配的网关地址

option 43 sub-option 2 ip-address 192.168.1.1　　#配置option 43参数，携带AC的IP地址

ip pool vlan666　　#创建并进入vlan666地址池

network 172.16.1.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 172.16.1.1　　#配置分配的网关地址

interface Vlanif10　　#进入vlan 10接口配置模式

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

dhcp select global　　#开启基于全局的 DHCP 功能

interface G0/0/1　　#进入相应的端口

port link-type access　　#配置端口的链路类型为接入模式

port default vlan 10　　#将端口加入进 vlan 10

capwap source interface vlanif10　　#指定AC与AP建立CAPWAP 隧道的源接口

wlan　　#进入 WLAN 的配置模式

security-profile name *Huawei-AP3030*　　#创建并进入

安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

#指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030*　　#创建并进入SSID模板视图

ssid Huawei-AP3030　　#指定SSID的名称

vap-profile name *Huawei-AP3030*　　#创建并进入VAP模板视图

service-vlan vlan-id 666　　#配置VAP的业务VLAN为VLAN 666

ssid-profile *Huawei-AP3030*　　#绑定SSID模板

security-profile *Huawei-AP3030*　　#绑定安全模板

ap-group name *Huawei-AP3030*　　#创建并进入AP组

radio 0　　#指定射频ID

vap-profile *Huawei-AP3030* wlan 1　　#将VAP与WLAN配置做绑定

ap-id 1 type-id 45 ap-mac 00E0-FC48-4D40　　#配置第一台AP的ID值，类型值，以及AP的MAC地址

ap-name AP-1　　#为第一台AP命名

ap-group *Huawei-AP3030*　　#将AP加入进AP组

ospf 1　　#进入 OSPF 配置模式

area 0　　#进入区域 0

network 192.168.1.0 0.0.0.255 #通告自身直连的网段

SWA:

system-view

sysname SWA

vlan batch 10 20 100 666

dhcp enable

interface Vlanif10

ip address 192.168.1.2 24

interface vlanif20

ip address 10.1.1.1 24

interface Vlanif100

ip address 192.168.100.254 24

dhcp select relay

dhcp relay server-ip 192.168.1.1

interface Vlanif666

ip address 172.16.1.1 24

dhcp select relay

dhcp relay server-ip 192.168.1.1

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 trunk
port trunk pvid vlan 100
port trunk allow-pass vlan all
interface E0/0/4
port link-type access
port default vlan 20
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
network 192.168.100.0 0.0.0.255
network 10.1.1.0 0.0.0.255
```

AC-2:

```
system-view
sysname AC-2
vlan batch 10 200 888
dhcp enable
```

```
ip pool vlan200
network 192.168.200.0 mask 24
gateway-list 192.168.200.254
option 43 sub-option 2 ip-address 192.168.1.3
ip pool vlan888
network 172.16.2.0 mask 24
gateway-list 172.16.2.1
interface Vlanif10
ip address 192.168.1.3 24
dhcp select global
interface G0/0/1
port link-type access
port default vlan 10
capwap source interface vlanif10
wlan
security-profile name Huawei-AP3030
security wpa2 psk pass-phrase P@ssw0rd aes-tkip
ssid-profile name Huawei-AP3030
ssid Huawei-AP3030
vap-profile name Huawei-AP3030
service-vlan vlan-id 888
ssid-profile Huawei-AP3030
```

security-profile *Huawei-AP3030*

ap-group name *Huawei-AP3030*

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-id 1 type-id 45 ap-mac 00E0-FC48-4D40

ap-name AP-2

ap-group *Huawei-AP3030*

ospf 1

area 0

network 192.168.1.0 0.0.0.255

SWB:

system-view

sysname SWB

vlan batch 10 20 200 888

dhcp enable

interface Vlanif10

ip address 192.168.1.4 24

interface Vlanif20

ip address 20.1.1.1 24

interface Vlanif200

ip address 192.168.200.254 24

```
dhcp select relay
dhcp relay server-ip 192.168.1.3
interface Vlanif888
ip address 172.16.2.1 24
dhcp select relay
dhcp relay server-ip 192.168.1.3
interface Ethernet0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface Ethernet0/0/2
port link-type access
port default vlan 10
interface Ethernet0/0/3
port link-type trunk
port trunk pvid vlan 200
port trunk allow-pass vlan all
interface Ethernet0/0/4
port link-type access
port default vlan 20
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
```

network 172.16.2.0 0.0.0.255

network 192.168.200.0 0.0.0.255

network 20.1.1.0 0.0.0.255

RTA:

system-view

sysname RTA

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 100.1.1.1 24

ospf 1

area 0.0.0.0

network 10.1.1.0 0.0.0.255

network 20.1.1.0 0.0.0.255

network 100.1.1.0 0.0.0.255

完成上述配置后，STA 设备可通过 AP-1 或 AP-2 获取信号连接网络，但无法实现漫游，因此需要在 AC-1 与 AC-2 上配置漫游组：

AC-1:

```
wlan
mobility-group name eaashome      #创建漫游组并命名
member ip-address 192.168.1.1     #向漫游组中添加成员
member ip-address 192.168.1.3     #向漫游组中添加成员
```

AC-2:

```
wlan
mobility-group name eaashome
member ip-address 192.168.1.1
member ip-address 192.168.1.3
```

注：完成上述配置后，需要保存 AC-1 与 AC-2 的配置并重启设备，否则漫游无法生效

测试：

当 AC-1 与 AC-2 重启完成后，令 STA 设备逐步从 AP-1 漫游至 AP-2，再由 AP-2 漫游回 AP-1 后，在 AC-1 上查看 STA 设备的漫游轨迹：

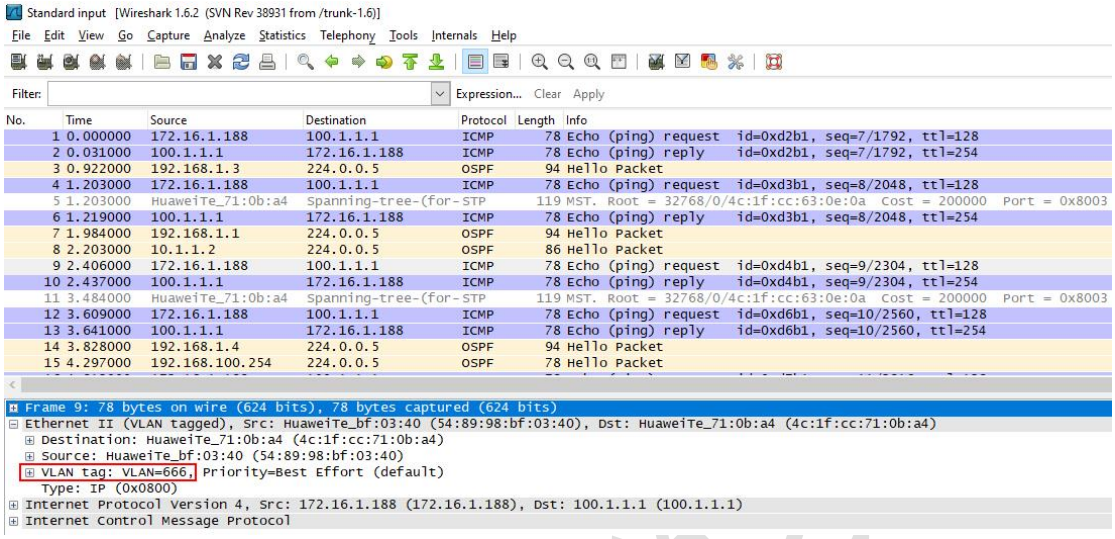
```
[AC-1]display station roam-track sta-mac 5489-98BF-0340
Access SSID:Huawei-AP3030
Rx/Tx: link receive rate/link transmit rate(Mbps)
z: Zero Roam c:PMK Cache Roam r:802.11r Roam
--------------------------------------------------------------------------------
L2/L3           AC IP                 AP name             Radio ID
BSSID           TIME                  In/Out RSSI         Out Rx/Tx
--------------------------------------------------------------------------------
--              192.168.1.1           AP-1                0
00e0-fcb6-26e0  2021/06/16 11:56:31   -95/-95             0/0
L3              192.168.1.3           AP-2                0
00e0-fc77-6800  2021/06/16 11:56:52   -95/-95             0/0
L2              192.168.1.1           AP-1                0
00e0-fcb6-26e0  2021/06/16 11:57:30   -95/-               -/-
--------------------------------------------------------------------------------
Number: 2
[AC-1]
```

同时查看 STA 设备的 IP 地址，发现从 AP-1 漫游至 AP-2 后，其 IP 地址并没有发生变化，由此证明漫游配置成功

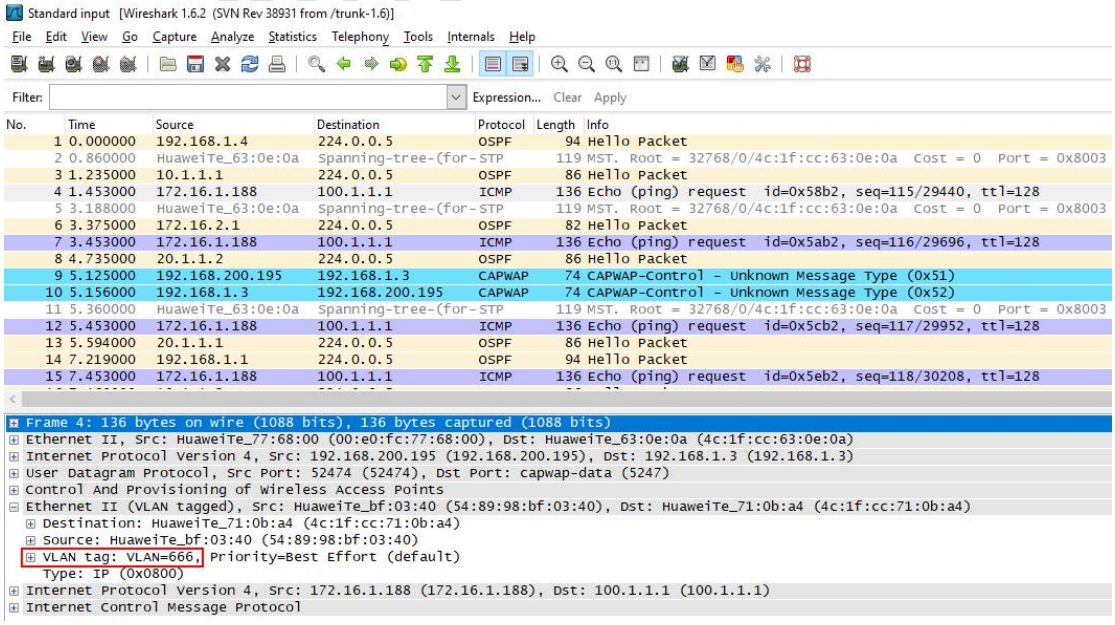
但在测试连通性时发现，STA 连接在 AP-1 上时，可正常 ping 通 RTA 的 Loopback 0 接口地址（100.1.1.1），但漫游至 AP-2 上时，网络连通性中断

导致网络中断的原因是 AC 间的三层漫游使用了以 HAP 为家乡代理的方式，当 STA 设备连接在 AP-2 上时，业务数据发送至 AP-2【FAP】，AP-2【FAP】将数据传送至 AC-2【FAC】，AC-2【FAC】又将数据传送至 AC-1【HAC】，AC-1【HAC】再将数据传送至 AP-1【HAP】，再由 HAP 经过 SWA 上送至 RTA

STA 设备连接到 AP-1 上时，其发送的业务数据的二层封装中，VLAN 为 666



当 STA 设备从 AP-1 漫游至 AP-2 上时，其发送的业务数据的外部二层封装中，VLAN 依旧为 666，但 SWB 与 AC-2 上并没有配置 VLAN 666，因此无法识别 VLAN 666 封装的数据，最终导致网络无法正常通讯



解决方案为：在 SWB 与 AC-2 上创建 VLAN 666

注:若 STA 设备初始连接的 AP 为 AP-2(也就是说 AP-2 为 HAP)，则 STP 设备漫游至 AP-1 上时，其业务数据的二层封装中 VLAN 为 888，而 SWA 与 AC-1 上也没有配置 VLAN 888，因此业务数据也会中断，故而需要在 SWA 与 AC-1 上也创建 VLAN 888

AC-1:

vlan 888

SWA:

vlan 888

AC-2:

vlan 666

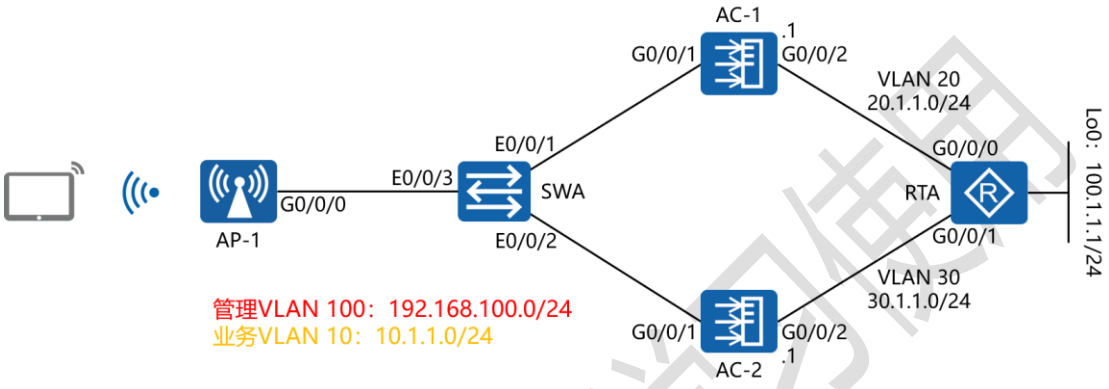
SWB:

vlan 666

完成上述配置后，当 STA 设备从 AP-1 漫游至 AP-2 上时，业务数据不会中断，可保证网络的持续连通性

八十、配置 WLAN VRRP 双机热备实验组网

一、实验拓扑：



二、实验目的：

通过在 AC-1 与 AC-2 上配置基于 VRRP 的双机热备，主 AC【AC-1】备份 AP 信息、STA 信息与 CAPWAP 链路信息，并通过 HSB 主备服务将信息同步给备份 AC【AC-2】，实现在 AC-1 失效时网络自动切换至 AC-2，保证业务的连续性

三、实验步骤：

AC-1:

system-view　　#进入系统视图模式

sysname AC-1　　#给设备命名

vlan batch 10 20 100　　#创建 VLAN 10、20 及 100

dhcp enable　　#开启 DHCP 功能

ip pool vlan10　　#创建并进入 vlan10 地址池

network 10.1.1.0 mask 24 #配置分配的网段及子网掩码

gateway-list 10.1.1.254 #配置分配的网关地址

excluede-ip-address 10.1.1.2 #排除掉不分配的地址

ip pool vlan100 #创建并进入 vlan100 地址池

network 192.168.100.0 mask 24 #配置分配的网段及子网掩码

gateway-list 192.168.100.254 #配置分配的网关地址

excluded-ip-address 192.168.100.2 #排除掉不分配的地址

interface vlan 10 #进入 vlan 10 接口配置模式

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

dhcp select global #开启基于全局的 DHCP 功能

vrrp vrid 48 virtual-ip 10.1.1.254 #创建 VRRP 组，指定组号与虚拟 IP 地址

vrrp vrid 48 priority 200 #配置当前 AC 的 VRRP 优先级

vrrp vrid 48 track interface G0/0/2 reduced 60 # 配置VRRP端口跟踪,并指定在被跟踪的端口G0/0/2失效时，令当前 VRRP 路由器的优先级降低 60

vrrp vrid 48 track interface Vlanif20 reduced 60 # 配置 VRRP 端口跟踪，并指定在被跟踪的接口 VLAN 20 失

效时，令当前 VRRP 路由器的优先级降低 60

interface vlan 20　　#进入 vlan 20 接口配置模式

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

interface vlan 100　　#进入 vlan 100 接口配置模式

ip address 192.168.100.1 24　　#配置 IP 地址及子网掩码

vrrp vrid 47 virtual-ip 192.168.100.254　　#创建 VRRP 组，指定组号与虚拟 IP 地址

vrrp vrid 47 priority 200　　#配置当前 AC 的 VRRP 优先级

vrrp vrid 47 track interface G0/0/2 reduced 60　　#配置VRRP端口跟踪,并指定在被跟踪的端口G0/0/2失效时，令当前 VRRP 路由器的优先级降低 60

vrrp vrid 47 track interface Vlanif20 reduced 60　　#配置 VRRP 端口跟踪，并指定在被跟踪的接口 VLAN 20 失效时，令当前 VRRP 路由器的优先级降低 60

dhcp select global　　#开启基于全局的 DHCP 功能

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　　#允许传递所有 VLAN 标记的数据帧

interface G0/0/2　　#进入相应的端口

port link-type access　　#将端口配置为接入模式

port default vlan 20　　#将端口加入进 VLAN 20

capwap source ip-address 192.168.100.254　　# 指 定 AC 与 AP 建立 CAPWAP 隧道的源 IP 地址

wlan　　#进入 WLAN 的配置模式

security-profile name *Huawei-AP3030*　　#创建并进入安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip #指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030*　　#创建并进入SSID模板视图

ssid Huawei-AP3030　　#指定SSID的名称

vap-profile name *Huawei-AP3030*　　#创建并进入VAP模板视图

service-vlan vlan-id 10　　#配置VAP的业务VLAN为VLAN 10

ssid-profile *Huawei-AP3030*　　#绑定SSID模板

security-profile *Huawei-AP3030*　　#绑定安全模板

ap-group name *Huawei-AP3030*　　#创建并进入AP组

radio 0　　#指定射频ID

vap-profile *Huawei-AP3030* wlan 1　　#将VAP与WLAN配置做绑定

ap-id 1 type-id 45 ap-mac 00e0-fcd7-2d20 #配置第一台AP的ID值，类型值，以及AP的MAC地址

ap-name AP1 #为第一台AP命名

ap-group *Huawei-AP3030* #将AP加入进AP组

hsb-service 0 #创建HSB主备服务并进入HSB主备服务视图

service-ip-port local-ip 192.168.100.1 peer-ip 192.168.100.2 local-data-port 10241 peer-data-port 10241 #配置建立HSB主备备份通道的IP地址与端口号

hsb-group 0 #创建HSB备份组并进入HSB备份组视图

bind-service 0 #配置HSB备份组绑定的HSB主备服务

track vrrp vrid 47 interface Vlanif100 #配置HSB备份组绑定的VRRP备份组

hsb-service-type access-user hsb-group 0 #配置准入控制用户绑定HSB备份组

hsb-service-type dhcp hsb-group 0 配置DHCP业务绑定HSB备份组

hsb-service-type ap hsb-group 0 配置WLAN业务绑定HSB备份组

hsb-group 0 #进入HSB备份组视图

hsb enable #开启HSB备份组

ospf 1 #进入OSPF配置模式

area 0.0.0.0 #进入区域0

network 10.1.1.0 0.0.0.255 #通告自身直连的网段

network 20.1.1.0 0.0.0.255 #通告自身直连的网段

network 192.168.100.0 0.0.0.255 #通告自身直连的网段

AC-2:

system-view

sysname AC-2

vlan batch 10 30 100

dhcp enable

ip pool vlan10

network 10.1.1.0 mask 24

gateway-list 10.1.1.254

excluded-ip-address 10.1.1.1

ip pool vlan100

network 192.168.100.0 mask 24

gateway-list 192.168.100.254

excluded-ip-address 192.168.100.1

interface vlan 10

ip address 10.1.1.2 24

dhcp select global

```
vrrp vrid 48 virtual-ip 10.1.1.254
vrrp vrid 48 priority 150
interface vlan 30
ip address 30.1.1.1 24
interface vlan 100
ip address 192.168.100.2 24
vrrp vrid 47 virtual-ip 192.168.100.254
vrrp vrid 47 priority 150
dhcp select global
interface G0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface G0/0/2
port link-type access
port default vlan 30
capwap source ip-address 192.168.100.254
wlan
security-profile name Huawei-AP3030
security wpa2 psk pass-phrase P@ssw0rd aes-tkip
ssid-profile name Huawei-AP3030
ssid Huawei-AP3030
vap-profile name Huawei-AP3030
```

service-vlan vlan-id 10

ssid-profile *Huawei-AP3030*

security-profile *Huawei-AP3030*

ap-group name *Huawei-AP3030*

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-id 1 type-id 45 ap-mac 00e0-fcd7-2d20

ap-name AP1

ap-group *Huawei-AP3030*

hsb-service 0

service-ip-port local-ip 192.168.100.2 peer-ip

192.168.100.1 local-data-port 10241 peer-data-port

10241

hsb-group 0

bind-service 0

track vrrp vrid 47 interface Vlanif100

hsb-service-type access-user hsb-group 0

hsb-service-type dhcp hsb-group 0

hsb-service-type ap hsb-group 0

hsb-group 0

hsb enable

ospf 1

area 0.0.0.0

network 10.1.1.0 0.0.0.255

network 30.1.1.0 0.0.0.255

network 192.168.100.0 0.0.0.255

SWA:

system-view

sysname SWA

vlan batch 10 100

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 trunk

port trunk allow-pass vlan all

port trunk pvid vlan 100

RTA:

system-view

sysname RTA

interface G0/0/0

ip address 20.1.1.2 24

interface G0/0/1

ip address 30.1.1.2 24

interface LoopBack0

ip address 100.1.1.1 24

ospf 1

area 0.0.0.0

network 20.1.1.0 0.0.0.255

network 30.1.1.0 0.0.0.255

network 100.1.1.0 0.0.0.255

测试：

在 AC-1 上查看主备服务的建立情况：

```
[AC-1]display hsb-service 0
Hot Standby Service Information:
-------------------------------------------------------------
  Local IP Address        : 192.168.100.1
  Peer IP Address         : 192.168.100.2
  Source Port             : 10241
  Destination Port        : 10241
  Keep Alive Times        : 5
  Keep Alive Interval     : 3
  Service State           : Connected
  Service Batch Modules   :
-------------------------------------------------------------
[AC-1]
```

在 AC-1 上查看 HSB 备份组的运行情况：

```
[AC-1]display hsb-group 0
Hot Standby Group Information:
-------------------------------------------------------------
  HSB-group ID                  : 0
  Vrrp Group ID                 : 47
  Vrrp Interface                : Vlanif100
  Service Index                 : 0
  Group Vrrp Status             : Master
  Group Status                  : Active
  Group Backup Process          : Realtime
  Peer Group Device Name        : AC6605
  Peer Group Software Version   : V200R007C10SPC300B220
  Group Backup Modules          : Access-user
                                  DHCP
                                  AP
-------------------------------------------------------------
[AC-1]
```

在 AP1 上查看 CAPWAP 隧道的建立情况，发现 AP1 只与虚拟 AC【192.168.100.254】建立了一条隧道，并未与 2 台真实的物理 AC 建立隧道：

```
[AP1]display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
192.168.100.98  00e0-fc5e-0f80           I -  Vlanif1
192.168.100.254 0000-5e00-012f  20       D-0  GE0/0/0
                                          1
------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0     Interface:1
[AP1]
```

在 AC-1 与 AC-2 均处于正常工作状态下时，查看 AC-1 与 AC-2 的 VRRP 情况：

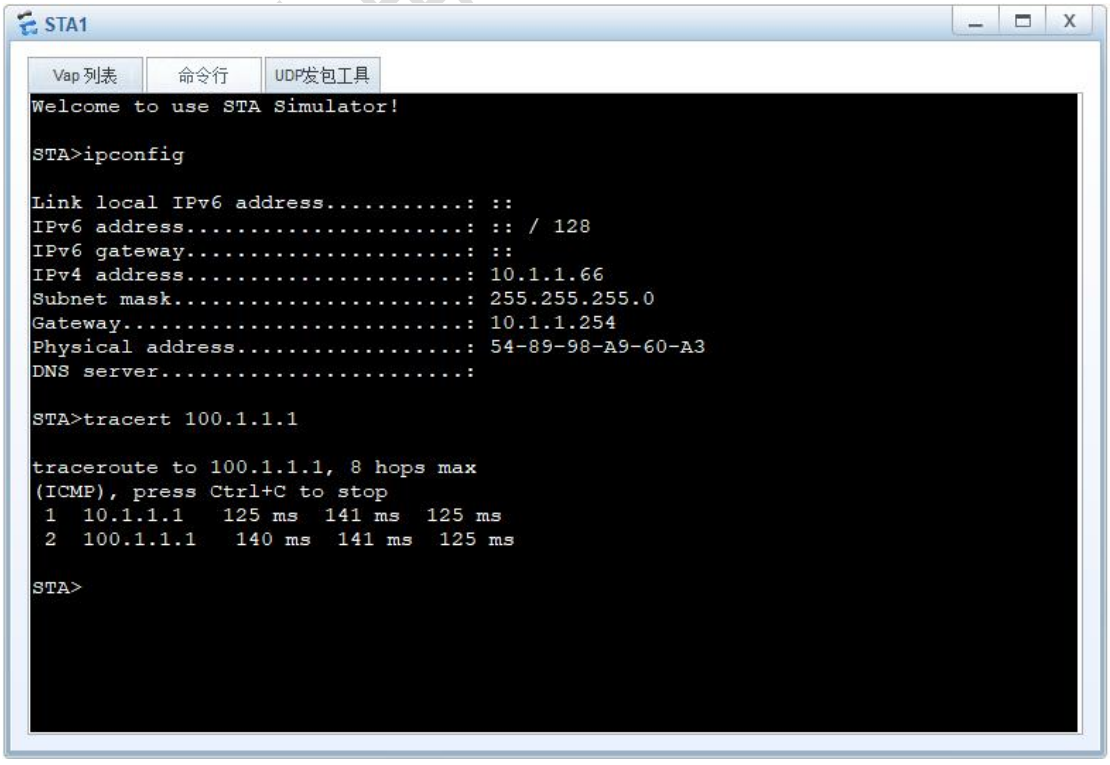
```
[AC-1]display vrrp 47
  Vlanif100 | Virtual Router 47
    State : Master
    Virtual IP : 192.168.100.254
    Master IP : 192.168.100.1
    PriorityRun : 200
    PriorityConfig : 200
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-012f
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/2   Priority reduced : 60
    IF state : UP
    Track IF : Vlanif20   Priority reduced : 60
    IF state : UP
    Create time : 2021-06-17 06:26:01 UTC-05:13
    Last change time : 2021-06-17 07:20:53 UTC-05:13

[AC-1]
```

```
[AC-1]display vrrp 48
  Vlanif10 | Virtual Router 48
    State : Master
    Virtual IP : 10.1.1.254
    Master IP : 10.1.1.1
    PriorityRun : 200
    PriorityConfig : 200
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0130
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/2   Priority reduced : 60
    IF state : UP
    Track IF : Vlanif20   Priority reduced : 60
    IF state : UP
    Create time : 2021-06-17 06:25:31 UTC-05:13
    Last change time : 2021-06-17 07:20:52 UTC-05:13

[AC-1]
```

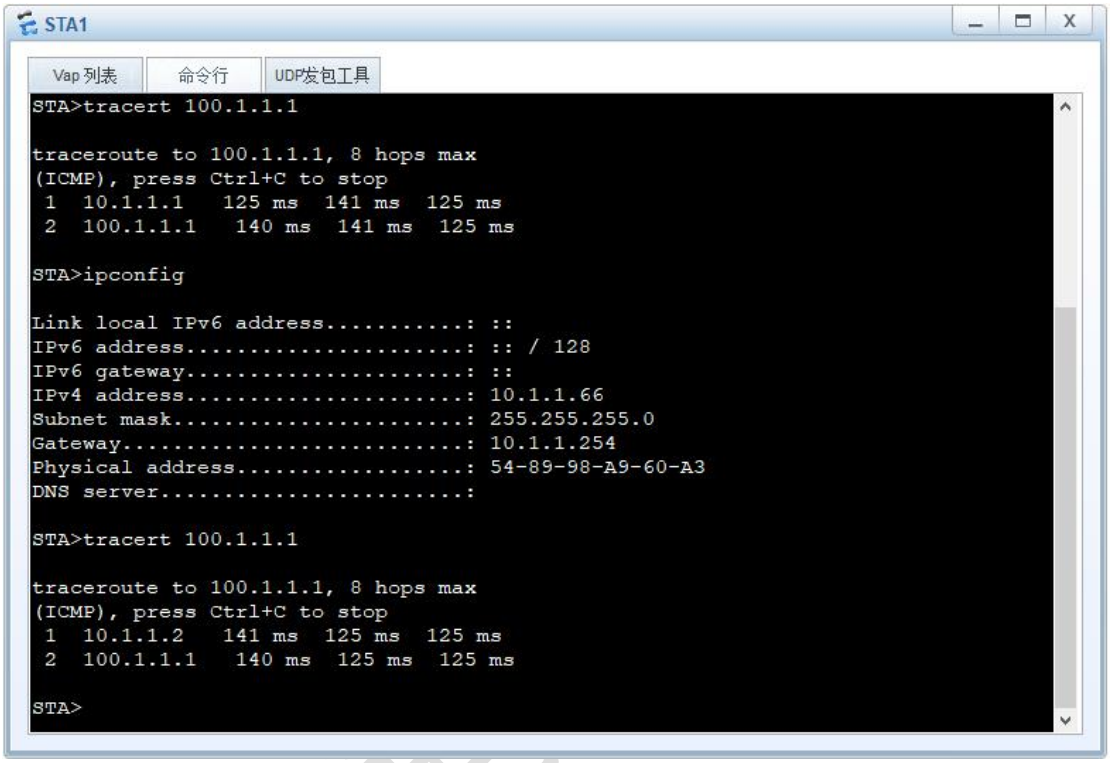
```
[AC-2]display vrrp 47
  Vlanif100 | Virtual Router 47
    State : Backup
    Virtual IP : 192.168.100.254
    Master IP : 192.168.100.1
    PriorityRun : 150
    PriorityConfig : 150
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-012f
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2021-06-17 06:59:38 UTC-05:13
    Last change time : 2021-06-17 07:20:53 UTC-05:13

[AC-2]
```

```
[AC-2]display vrrp 48
  Vlanif10 | Virtual Router 48
    State : Backup
    Virtual IP : 10.1.1.254
    Master IP : 10.1.1.1
    PriorityRun : 150
    PriorityConfig : 150
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0130
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2021-06-17 06:59:12 UTC-05:13
    Last change time : 2021-06-17 07:20:53 UTC-05:13

[AC-2]
```

在 STA 设备上查看其获取的 IP 地址，同时测试与目标网络的连通性，并观察所经过的路径：



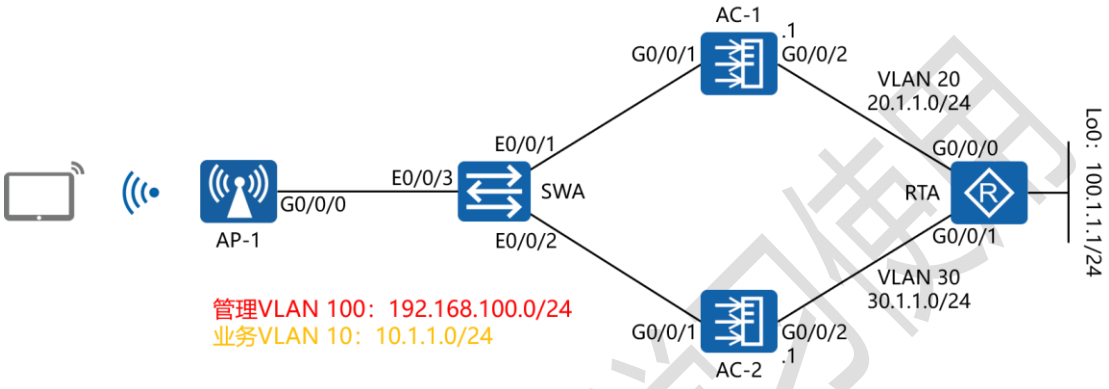
在 AC-1 设备失效时（此处将 AC-1 的 G0/0/2 端口手工 down 掉，模拟上行链路失效），再次检测 STA 设备所获取的 IP 地址，同时测试与目标网络的连通性，并再次观察所经过的路径：



经过测试发现，STA 设备的 IP 地址并没有更换，但到达目标网络所经过的路径已经切换至 AC-2

八十一、配置 WLAN 双链路热备份实验组网

一、实验拓扑：



二、实验目的：

通过在 AC-1 与 AC-2 上配置双链路热备份，令 AP-1 分别与主、备 AC 同时建立 CAPWAP 隧道，一条为主用链路，令一条为备份链路；主 AC【AC-1】仅备份 STA 信息，并通过 HSB 主备服务将信息同步给备份 AC【AC-2】；实现在 AC-1 失效时网络自动切换至 AC-2

三、实验步骤：

AC-1:

system-view　　#进入系统视图模式

sysname AC-1　　#给设备命名

vlan batch 10 20 100　　#创建 VLAN 10、20 及 100

dhcp enable　　#开启 DHCP 功能

ip pool vlan10 #创建并进入 vlan10 地址池

network 10.1.1.0 mask 24 #配置分配的网段及子网掩码

gateway-list 10.1.1.254 #配置分配的网关地址

excluede-ip-address 10.1.1.2 #排除掉不分配的地址

ip pool vlan100 #创建并进入 vlan100 地址池

network 192.168.100.0 mask 24 #配置分配的网段及子网掩码

gateway-list 192.168.100.1 #配置分配的网关地址

excluded-ip-address 192.168.100.2 #排除掉不分配的地址

interface vlan 10 #进入 vlan 10 接口配置模式

ip address 10.1.1.1 24 #配置 IP 地址及子网掩码

dhcp select global #开启基于全局的 DHCP 功能

vrrp vrid 47 virtual-ip 10.1.1.254 #创建 VRRP 组，指定组号与虚拟 IP 地址

vrrp vrid 47 priority 200 #配置当前 AC 的 VRRP 优先级

vrrp vrid 47 track interface G0/0/2 reduced 60 # 配置VRRP端口跟踪,并指定在被跟踪的端口G0/0/2失效时，令当前 VRRP 路由器的优先级降低 60

vrrp vrid 47 track interface Vlanif20 reduced 60 #

配置 VRRP 端口跟踪，并指定在被跟踪的接口 VLAN 20 失效时，令当前 VRRP 路由器的优先级降低 60

interface vlan 20 #进入 vlan 20 接口配置模式

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

interface vlan 100 #进入 vlan 100 接口配置模式

ip address 192.168.100.1 24 #配置 IP 地址及子网掩码

dhcp select global #开启基于全局的 DHCP 功能

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 #允许传递所有 VLAN 标记的数据帧

interface G0/0/2 #进入相应的端口

port link-type access #将端口配置为接入模式

port default vlan 20 #将端口加入进 VLAN 20

capwap source interface Vlanif 100 #指定 AC 与 AP 建立 CAPWAP 隧道的源接口

wlan #进入 WLAN 的配置模式

ac protect enable #开启双链路备份功能

ac protect protect-ac 192.168.100.2 priority 1 # 配置备份 AC 的 IP 地址与本 AC 的优先级 1

security-profile name *Huawei-AP3030* #创建并进入

安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

#指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030*　　#创建并进入SSID模板视图

ssid Huawei-AP3030　　#指定SSID的名称

vap-profile name *Huawei-AP3030*　　#创建并进入VAP模板视图

service-vlan vlan-id 10　　#配置VAP的业务VLAN为VLAN 10

ssid-profile *Huawei-AP3030*　　#绑定SSID模板

security-profile *Huawei-AP3030*　　#绑定安全模板

ap-group name *Huawei-AP3030*　　#创建并进入AP组

radio 0　　#指定射频ID

vap-profile *Huawei-AP3030* wlan 1　　#将VAP与WLAN配置做绑定

ap-id 1 type-id 45 ap-mac 00e0-fcd7-2d20　　#配置第一台AP的ID值，类型值，以及AP的MAC地址

ap-name AP1　　#为第一台AP命名

ap-group *Huawei-AP3030*　　#将AP加入进AP组

hsb-service 0　　#创建HSB主备服务并进入HSB主备服务视图

service-ip-port local-ip 192.168.100.1 peer-ip 192.168.100.2 local-data-port 10241 peer-data-port 10241 #配置建立HSB主备备份通道的IP地址与端口号

hsb-group 0 #创建HSB备份组并进入HSB备份组视图

bind-service 0 #配置HSB备份组绑定的HSB主备服务

hsb-service-type access-user hsb-service 0 #配置准入控制用户绑定HSB备份通道

hsb-service-type dhcp hsb-group 0 配置DHCP业务绑定HSB备份组

hsb-service-type ap hsb-service 0 配置WLAN业务绑定HSB备份通道

hsb-group 0 #进入HSB备份组视图

hsb enable #开启HSB备份组

ospf 1 #进入OSPF配置模式

area 0.0.0.0 #进入区域0

network 10.1.1.0 0.0.0.255 #通告自身直连的网段

network 20.1.1.0 0.0.0.255 #通告自身直连的网段

network 192.168.100.0 0.0.0.255 #通告自身直连的网段

AC-2:

system-view

```
sysname AC-2
vlan batch 10 30 100
dhcp enable
ip pool vlan10
network 10.1.1.0 mask 24
gateway-list 10.1.1.254
excluded-ip-address 10.1.1.1
ip pool vlan100
network 192.168.100.0 mask 24
gateway-list 192.168.100.2
excluded-ip-address 192.168.100.1
interface vlan 10
ip address 10.1.1.2 24
dhcp select global
vrrp vrid 47 virtual-ip 10.1.1.254
vrrp vrid 47 priority 150
interface vlan 30
ip address 30.1.1.1 24
interface vlan 100
ip address 192.168.100.2 24
dhcp select global
interface G0/0/1
```

port link-type trunk

port trunk allow-pass vlan all

interface G0/0/2

port link-type access

port default vlan 30

capwap source interface Vlanif 100

wlan

ac protect enable

ac protect protect-ac 192.168.100.1 priority 2

security-profile name *Huawei-AP3030*

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

ssid-profile name *Huawei-AP3030*

ssid Huawei-AP3030

vap-profile name *Huawei-AP3030*

service-vlan vlan-id 10

ssid-profile *Huawei-AP3030*

security-profile *Huawei-AP3030*

ap-group name *Huawei-AP3030*

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-id 1 type-id 45 ap-mac 00e0-fcd7-2d20

ap-name AP1

ap-group *Huawei-AP3030*

hsb-service 0

service-ip-port local-ip 192.168.100.2 peer-ip 192.168.100.1 local-data-port 10241 peer-data-port 10241

hsb-group 0

bind-service 0

hsb-service-type access-user hsb-service 0

hsb-service-type dhcp hsb-group 0

hsb-service-type ap hsb-service 0

hsb-group 0

hsb enable

ospf 1

area 0.0.0.0

network 10.1.1.0 0.0.0.255

network 30.1.1.0 0.0.0.255

network 192.168.100.0 0.0.0.255

SWA:

system-view

sysname SWA

vlan batch 10 100

```
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 trunk
port trunk allow-pass vlan all
port trunk pvid vlan 100
```

RTA:

```
system-view
sysname RTA
interface G0/0/0
ip address 20.1.1.2 24
interface G0/0/1
ip address 30.1.1.2 24
interface LoopBack0
ip address 100.1.1.1 24
ospf 1
area 0.0.0.0
```

network 20.1.1.0 0.0.0.255

network 30.1.1.0 0.0.0.255

network 100.1.1.0 0.0.0.255

测试：

当 AC-1 与 AC-2 均处于正常工作状态时，在 AP1 上查看 CAPWAP 隧道的建立情况，发现 AP1 同时与 AC-1、AC-2 建立了 2 条 CAPWAP 隧道：

```
[AP1]display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                          VLAN
--------------------------------------------------------------------------------
192.168.100.217 00e0-fc5e-0f80            I -  Vlanif1
192.168.100.1   00e0-fc50-0889  20        D-0  GE0/0/0
                                          1
192.168.100.2   00e0-fc7a-0ab7  20        D-0  GE0/0/0
                                          1
--------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0     Interface:1
[AP1]
```

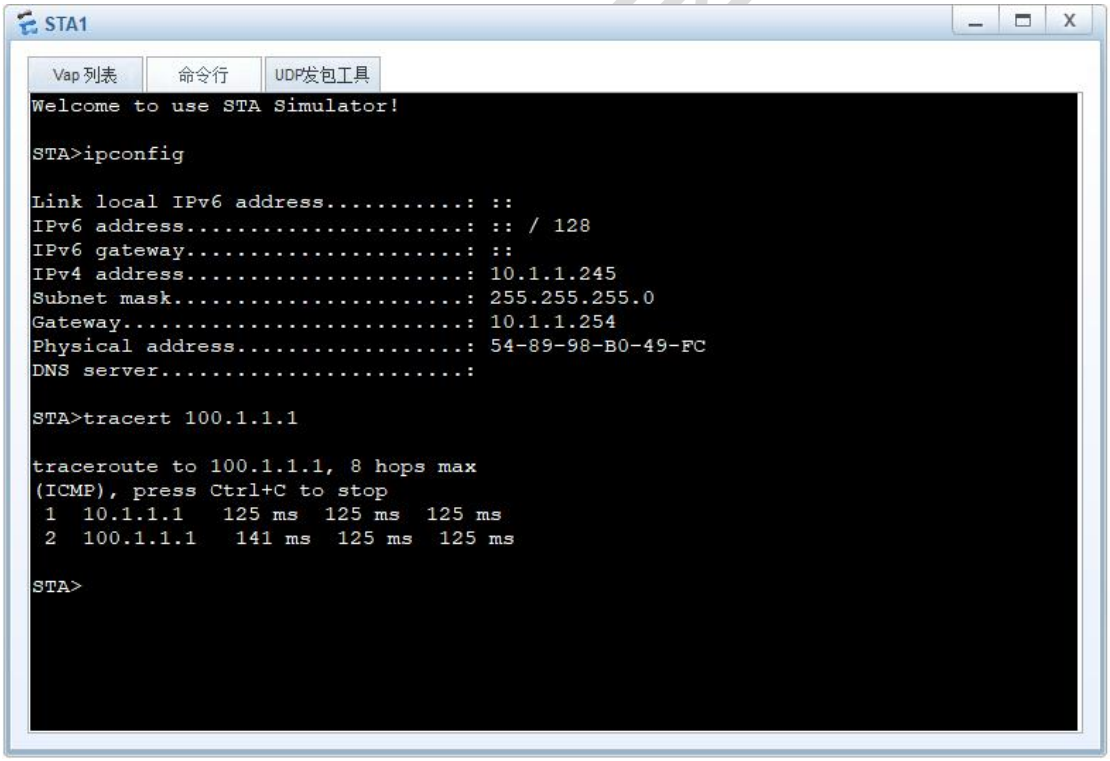
在 AC-1、AC-2 上查看与 AP 建立的 CAPWAP 隧道关系：

```
[AC-1]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal          [1]
--------------------------------------------------------------------------------
------------------
ID   MAC            Name Group         IP              Type            State STA
 Uptime
--------------------------------------------------------------------------------
------------------
1    00e0-fc5e-0f80 AP1  Huawei-AP3030 192.168.100.217 AP3030DN        nor   1
 1M:52S
--------------------------------------------------------------------------------
------------------
Total: 1
[AC-1]
```

```
[AC-2]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
stdby: standby         [1]
--------------------------------------------------------------------------------
------------------
ID   MAC            Name Group         IP              Type            State STA
 Uptime
--------------------------------------------------------------------------------
------------------
1    00e0-fc5e-0f80 AP1  Huawei-AP3030 192.168.100.217 AP3030DN        stdby 1
 -
--------------------------------------------------------------------------------
------------------
Total: 1
[AC-2]
```

从输出结果可以很明显的看到，AC-1 为主 AC，AC-2 为备 AC

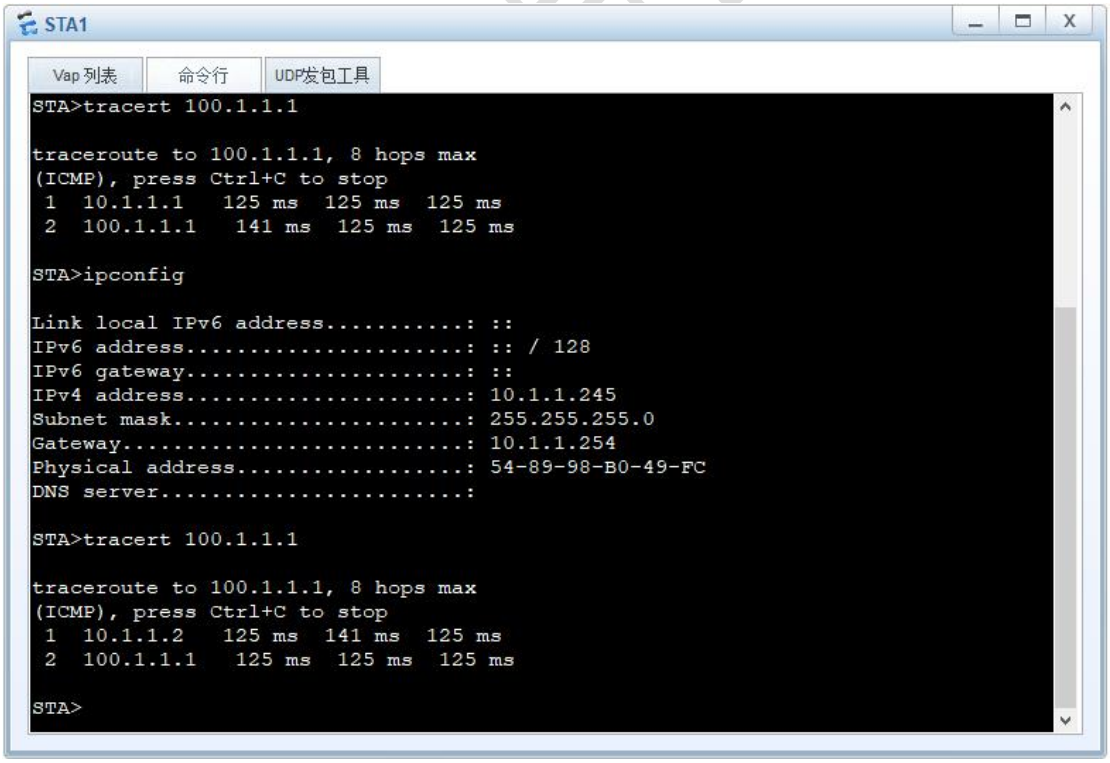
在 STA 设备上查看其获取的 IP 地址，同时测试与目标网络的连通性，并观察所经过的路径：



在 AC-1 设备失效时 (此处将 AC-1 设备关机，模拟设备失效)，观察 AC-2 需要多久才能够从 stdby 状态变为 nor 状态(25s x 3)：

```
[AC-2]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor   : normal          [1]
------------------------------------------------------------------------------
------------------
ID   MAC            Name Group         IP              Type            State STA
 Uptime
------------------------------------------------------------------------------
------------------
1    00e0-fc5e-0f80 AP1  Huawei-AP3030 192.168.100.217 AP3030DN       nor   1
 2S
------------------------------------------------------------------------------
------------------
Total: 1
[AC-2]
```

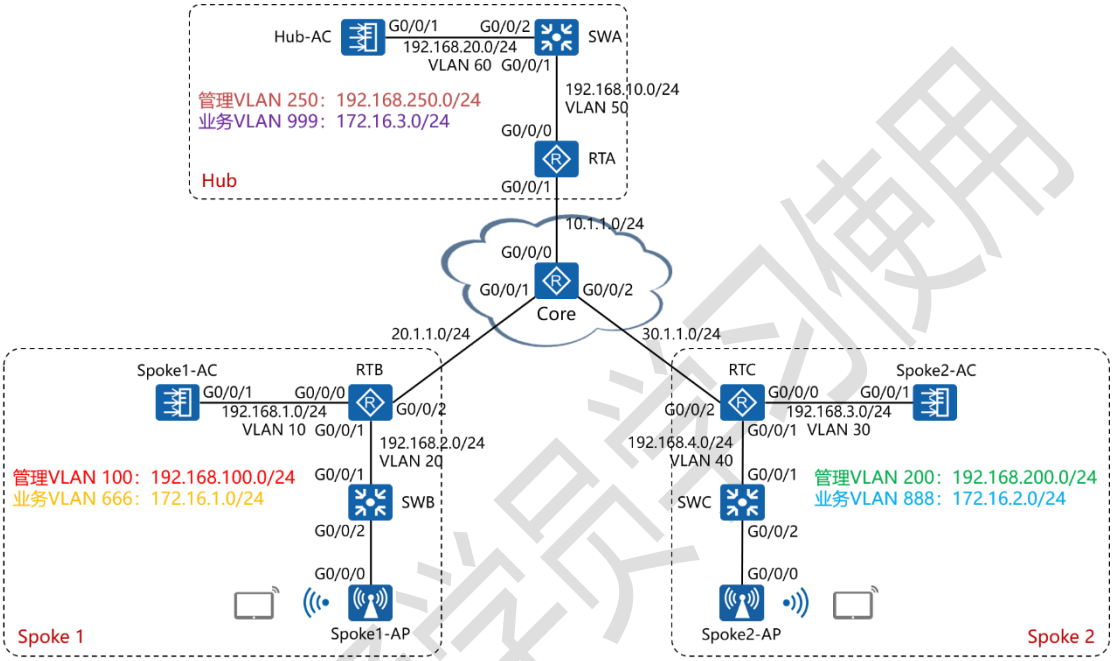
再次检测 STA 设备所获取的 IP 地址，同时测试与目标网络的连通性，并再次观察所经过的路径：



经过测试发现，STA 设备的 IP 地址并未更换(已为业务 VLAN 10 配置了 VRRP)，但到达目标网络所经过的路径已经切换至 AC-2

八十二、配置 WLAN N+1 备份实验组网

一、实验拓扑：



二、实验目的：

Spoke 1 中的 Spoke1-AP 首选与 Spoke1-AC 建立 CAPWAP 隧道；Spoke 2 中的 Spoke2-AP 首选与 Spoke2-AC 建立 CAPWAP 隧道；当主 AC【Spoke1-AC 或 Spoke2-AC】失效时，令 Hub 中的备份 AC【Hub-AC】重新与 Spoke1-AP 或 Spoke2-AP 建立 CAPWAP 隧道，接替主 AC 的工作；并且在主 AC【Spoke1-AC 或 Spoke2-AC】恢复后，能够自动的进行主备回切

三、实验步骤：

RTB:

system-view　　#进入系统视图模式

sysname RTB　　#给设备命名

dhcp enable　　#开启 DHCP 功能

ip pool vlan100　　#创建并进入 vlan100 地址池

network 192.168.100.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 192.168.100.254　　#配置分配的网关地址

option 43 sub-option 2 ip-address 192.168.1.2　　#配置 option 43 参数，携带 AC 的 IP 地址

ip pool vlan666　　#创建并进入 vlan666 地址池

network 172.16.1.0 mask 24　　#配置分配的网段及子网掩码

gateway-list 172.16.1.1　　#配置分配的网关地址

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

interface G0/0/1　　#进入相应的接口

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

dhcp select global　　#开启基于全局的 DHCP 功能

interface G0/0/2　　#进入相应的接口

ip address 20.1.1.2 24　　#配置 IP 地址及子网掩码

ospf 1 #进入 OSPF 配置模式

area 0 #进入区域 0

network 192.168.1.0 0.0.0.255 #通告自身直连的网段

network 192.168.2.0 0.0.0.255 #通告自身直连的网段

SWB:

system-view

sysname SWB

vlan batch 20 100 666 #创建 VLAN 20、100 及 666

dhcp enable

interface vlan 20

ip address 192.168.2.2 24

interface vlan 100

ip address 192.168.100.254 24

dhcp select relay #开启 DHCP 中继代理功能

dhcp relay server-ip 192.168.2.1 #指定 DHCP 服务器的 IP 地址

interface vlan 666

ip address 172.16.1.1 24

dhcp select relay #开启 DHCP 中继代理功能

dhcp relay server-ip 192.168.2.1 #指定 DHCP 服务器的 IP 地址

```
interface G0/0/1
port link-type access
port default vlan 20
interface G0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan all
ospf 1
area 0
network 192.168.2.0 0.0.0.255
network 192.168.100.0 0.0.0.255
network 172.16.1.0 0.0.0.255
```

Spoke1-AC:

```
system-view
sysname Spoke1-AC
vlan batch 10 100 666
interface Vlanif10
ip address 192.168.1.2 24
interface G0/0/1
port link-type access
port default vlan 10
```

capwap source interface vlanif10 #指定 AC 与 AP 建立 CAPWAP 隧道的源接口

wlan #进入 WLAN 的配置模式

security-profile name *Huawei-AP3030* #创建并进入安全模板视图

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip #指定加密使用的方式及密钥

ssid-profile name *Huawei-AP3030* #创建并进入 SSID 模板视图

ssid Huawei-AP3030 #指定 SSID 的名称

vap-profile name *Huawei-AP3030* #创建并进入 VAP 模板视图

service-vlan vlan-id 666 #配置 VAP 的业务 VLAN 为 VLAN 666

ssid-profile *Huawei-AP3030* #绑定 SSID 模板

security-profile *Huawei-AP3030* #绑定安全模板

ap-group name *Huawei-AP3030* #创建并进入 AP 组

radio 0 #指定射频 ID

vap-profile *Huawei-AP3030* wlan 1 #将 VAP 与 WLAN 配置做绑定

ap-id 1 type-id 45 ap-mac 00E0-FC89-33A0 #配置 Spoke1-AP 的 ID 值，类型值，以及 AP 的 MAC 地址

ap-name Spoke1-AP　　#为 Spoke1-AP 命名

ap-group *Huawei-AP3030*　　#将 AP 加入进 AP 组

ospf 1

area 0

network 192.168.1.0 0.0.0.255

RTC:

system-view

sysname RTC

dhcp enable

ip pool vlan200

network 192.168.200.0 mask 24

gateway-list 192.168.200.254

option 43 sub-option 2 ip-address 192.168.3.2

ip pool vlan888

network 172.16.2.0 mask 24

gateway-list 172.16.2.1

interface G0/0/0

ip address 192.168.3.1 24

interface G0/0/1

ip address 192.168.4.1 24

dhcp select global

```
interface G0/0/2
ip address 30.1.1.2 24
ospf 1
area 0
network 192.168.3.0 0.0.0.255
network 192.168.4.0 0.0.0.255
```

SWC:

```
system-view
sysname SWC
vlan batch 40 200 888
dhcp enable
interface vlan 40
ip address 192.168.4.2 24
interface vlan 200
ip address 192.168.200.254 24
dhcp select relay
dhcp relay server-ip 192.168.4.1
interface vlan 888
ip address 172.16.2.1 24
dhcp select relay
dhcp relay server-ip 192.168.4.1
```

```
interface G0/0/1
port link-type access
port default vlan 40
interface G0/0/2
port link-type trunk
port trunk pvid vlan 200
port trunk allow-pass vlan all
ospf 1
area 0
network 192.168.4.0 0.0.0.255
network 192.168.200.0 0.0.0.255
network 172.16.2.0 0.0.0.255
```

Spoke2-AC:

```
system-view
sysname Spoke2-AC
vlan batch 30 200 888
interface Vlanif30
ip address 192.168.3.2 24
interface G0/0/1
port link-type access
port default vlan 30
```

capwap source interface vlanif30

wlan

security-profile name *Huawei-AP3030*

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

ssid-profile name *Huawei-AP3030*

ssid Huawei-AP3030

vap-profile name *Huawei-AP3030*

service-vlan vlan-id 888

ssid-profile *Huawei-AP3030*

security-profile *Huawei-AP3030*

ap-group name *Huawei-AP3030*

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-id 1 type-id 45 ap-mac 00E0-FCD7-3520

ap-name Spoke2-AP

ap-group *Huawei-AP3030*

ospf 1

area 0

network 192.168.3.0 0.0.0.255

RTA:

system-view

```
sysname RTA
dhcp enable
ip pool vlan250
network 192.168.250.0 mask 24
gateway-list 192.168.250.254
option 43 sub-option 2 ip-address 192.168.20.1
ip pool vlan999
network 172.16.3.0 mask 24
gateway-list 172.16.3.1
interface G0/0/0
ip address 192.168.10.1 24
dhcp select global
interface G0/0/1
ip address 10.1.1.2 24
ospf 1
area 0
network 192.168.10.0 0.0.0.255
```

SWA:

```
system-view
sysname SWA
vlan batch 50 60 250 999
```

```
dhcp enable
interface vlan 50
ip address 192.168.10.2 24
interface vlan 60
ip address 192.168.20.2 24
interface vlan 250
ip address 192.168.250.254 24
dhcp select relay
dhcp relay server-ip 192.168.10.1
interface vlan 999
ip address 172.16.3.1 24
dhcp select relay
dhcp relay server-ip 192.168.10.1
interface G0/0/1
port link-type access
port default vlan 50
interface G0/0/2
port link-type access
port default vlan 60
ospf 1
area 0
network 192.168.10.0 0.0.0.255
```

network 192.168.20.0 0.0.0.255

network 192.168.250.0 0.0.0.255

network 172.16.3.0 0.0.0.255

Hub-AC:

system-view

sysname Hub-AC

vlan batch 60 250 999

interface Vlanif60

ip address 192.168.20.1 24

interface G0/0/1

port link-type access

port default vlan 60

capwap source interface vlanif60

wlan

security-profile name *Huawei-AP3030*

security wpa2 psk pass-phrase *P@ssw0rd* aes-tkip

ssid-profile name *Huawei-AP3030*

ssid Huawei-AP3030

vap-profile name *Huawei-AP3030*

service-vlan vlan-id 999

ssid-profile *Huawei-AP3030*

security-profile *Huawei-AP3030*

ap-group name *Spoke1* #分别创建 2 个不同的 AP 组，用来关联 2 个不同的 AP

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-group name *Spoke2* #分别创建 2 个不同的 AP 组，用来关联 2 个不同的 AP

radio 0

vap-profile *Huawei-AP3030* wlan 1

ap-id 1 type-id 45 ap-mac 00E0-FC89-33A0 #配置 Spoke1-AP 的 ID 值，类型值，以及 AP 的 MAC 地址

ap-name Spoke1-AP

ap-group *Spoke1* #将 Spoke1-AP 加入进对应的 AP 组

ap-id 2 type-id 45 ap-mac 00E0-FCD7-3520 #配置 Spoke2-AP 的 ID 值，类型值，以及 AP 的 MAC 地址

ap-name Spoke2-AP

ap-group *Spoke2* #将 Spoke2-AP 加入进对应的 AP 组

ospf 1

area 0

network 192.168.20.0 0.0.0.255

Core:

system-view

sysname Core

interface G0/0/0

ip address 10.1.1.1 24

interface G0/0/1

ip address 20.1.1.1 24

interface G0/0/2

ip address 30.1.1.1 24

rip 1 #进入 RIP 配置模式

version 2 #使用版本 2

network 10.0.0.0 #通告自身直连的主网网段

network 20.0.0.0 #通告自身直连的主网网段

network 30.0.0.0 #通告自身直连的主网网段

undo summary #关闭自动汇总

为实现全网全通，本实验采用在 RTA、RTB、RTC 上配置双向重注入，令 OSPF 与 RIP 的路由条目相互学习：

RTA:

rip 1

version 2

network 10.0.0.0

undo summary

import-route ospf 1 cost 3　　#将 OSPF 1 的路由以 3 条的代价值注入进 RIP 进程中

ospf 1

import-route rip 1 type 1 cost 4　　#将 RIP 1 的路由以外部类型 1 的形式，且以代价值 4 注入进 OSPF 进程中

RTB:

rip 1

version 2

network 20.0.0.0

undo summary

import-route ospf 1 cost 3

ospf 1

import-route rip 1 type 1 cost 4

RTC:

rip 1

version 2

network 30.0.0.0

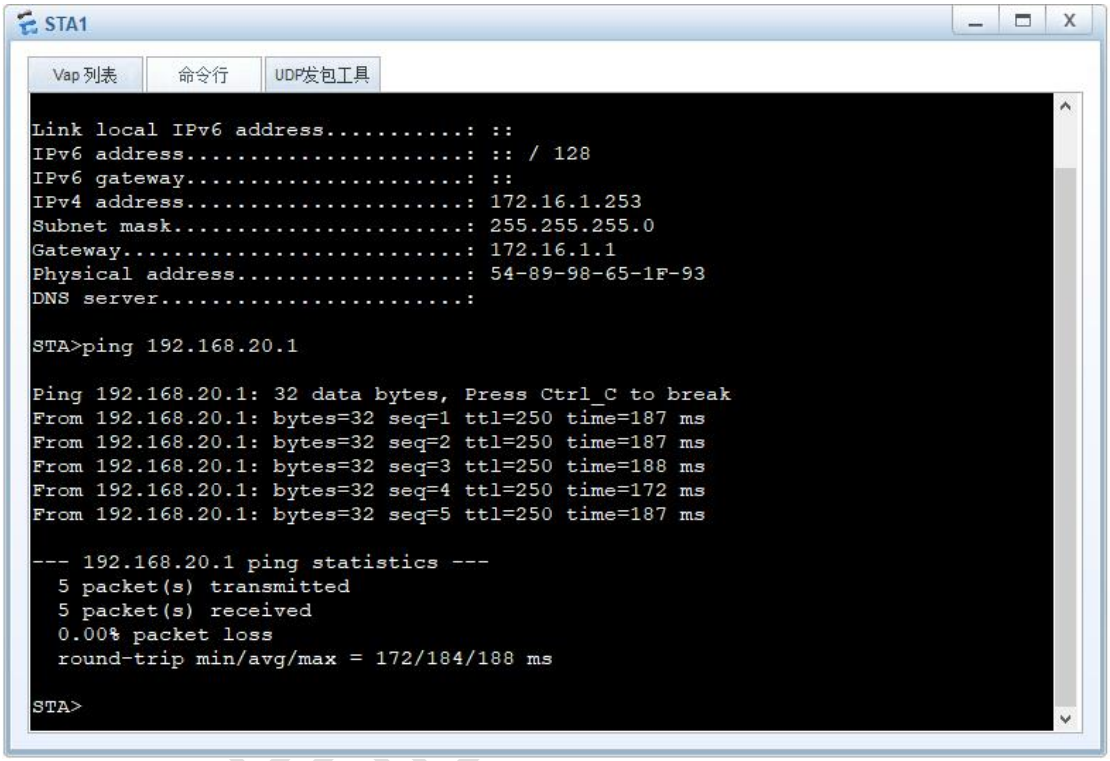
undo summary

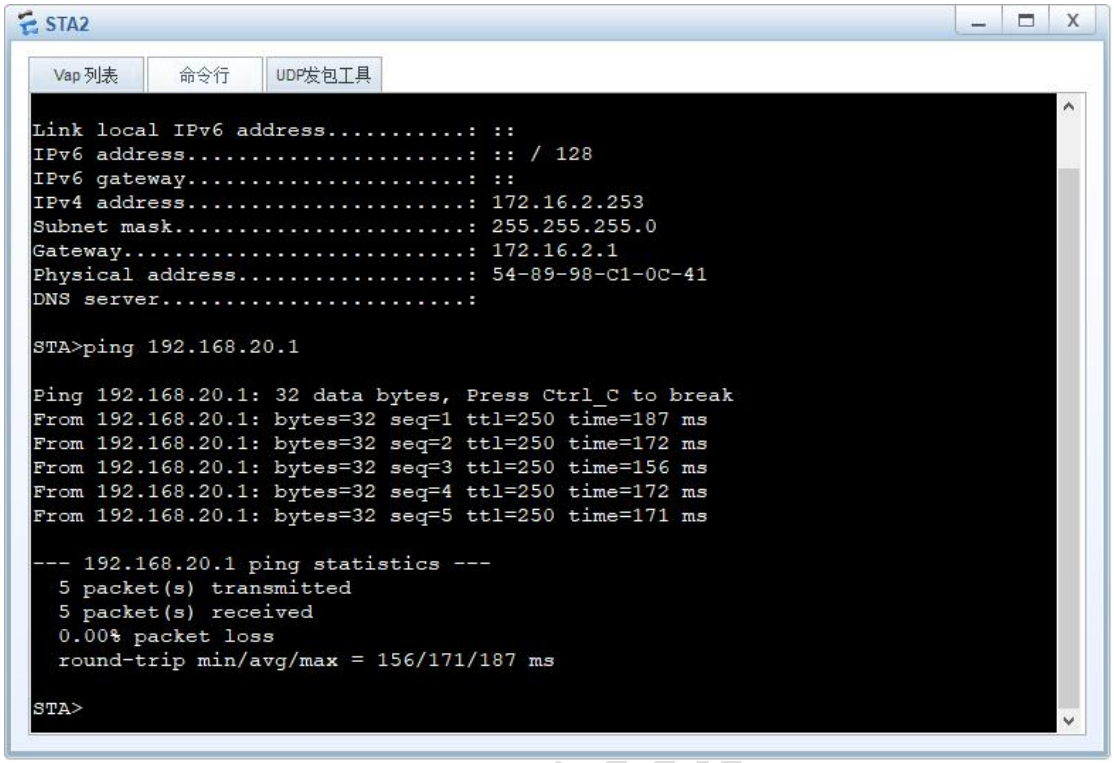
import-route ospf 1 cost 3

ospf 1

import-route rip 1 type 1 cost 4

完成上述配置后，在2台STA设备上测试与Hub-AC的连通性：





在确保全网全通后，需要在 Spoke1-AC、Spoke2-AC 与 Hub-AC 上配置 N+1 备份：

Spoke1-AC:

wlan　　#进入 WLAN 的配置模式

ap-system-profile name *Spoke1*　　#创建 AP 系统模板，并进入模板视图

primary-access ip-address 192.168.1.2　　#配置优选 AC 的 IP 地址

backup-access ip-address 192.168.20.1　　#配置备选 AC 的 IP 地址

ap-group name Huawei-AP3030

ap-system-profile *Spoke1*　　#在 AP 组中引用 AP 系统模板

Spoke2-AC:

wlan

ap-system-profile name *Spoke2*

primary-access ip-address 192.168.3.2

backup-access ip-address 192.168.20.1

ap-group name Huawei-AP3030

ap-system-profile *Spoke2*

Hub-AC:

wlan

ap-system-profile name *Spoke1*

primary-access ip-address 192.168.1.2

backup-access ip-address 192.168.20.1

ap-system-profile name *Spoke2*

primary-access ip-address 192.168.3.2

backup-access ip-address 192.168.20.1

ap-group name Spoke1

ap-system-profile *Spoke1*

ap-group name Spoke2

ap-system-profile *Spoke2*

Spoke1-AC:

wlan

undo ac protect enable　　#关闭全局双链路备份功能并开启 N+1 备份功能

ap-reset all　　#重启 AP，令 N+1 备份功能生效

Spoke2-AC:

wlan

undo ac protect enable

ap-reset all

Hub-AC:

wlan

undo ac protect restore disable　　#开启全局回切功能

undo ac protect enable

ap-reset all

测试：

分别在 Spoke1-AC、Spoke2-AC 与 Hub-AC 上查看 N+1 备份的信息：

```
[Spoke1-AC]display ac protect
------------------------------------------------------------
Protect state               : disable
Protect AC                  : -
Priority                    : 0
Protect restore             : enable
Coldbackup kickoff station: disable
------------------------------------------------------------
[Spoke1-AC]
```

```
[Spoke1-AC]display ap-system-profile name Spoke1
------------------------------------------------------------------------------
AC priority                                    : -
Protect AC IP address                          : -
Primary AC                                     : 192.168.1.2
Backup AC                                      : 192.168.20.1
AP management VLAN                             : -
Keep service                                   : disable
Keep service allow new access                  : disable
Temporary management switch                    : disable
Mesh role                                      : mesh-node
STA access mode                                : disable
STA whitelist profile                          : -
STA blacklist profile                          : -
EAPOL start mode                               : multicast
EAPOL start transform                          : equal-bssid
EAPOL response mode                            : unicast learning
EAPOL response transform                       : equal-bssid
AP LLDP message transmission delay time(s)     : 2
AP LLDP message transmission hold multiplier   : 4
AP LLDP message transmission interval time(s)  : 30
AP LLDP restart delay time(s)                  : 2
AP LLDP admin status                           : txrx
AP LLDP report interval time(s)                : 30
AP high temperature threshold(degree C)        : -
  ---- More ----
```

```
[Spoke2-AC]display ac protect
------------------------------------------------------------
Protect state               : disable
Protect AC                  : -
Priority                    : 0
Protect restore             : enable
Coldbackup kickoff station: disable
------------------------------------------------------------
[Spoke2-AC]
```

```
[Spoke2-AC]display ap-system-profile name Spoke2
------------------------------------------------------------------------------
AC priority                                     : -
Protect AC IP address                           : -
Primary AC                                      : 192.168.3.2
Backup AC                                       : 192.168.20.1
AP management VLAN                              : -
Keep service                                    : disable
Keep service allow new access                   : disable
Temporary management switch                     : disable
Mesh role                                       : mesh-node
STA access mode                                 : disable
STA whitelist profile                           : -
STA blacklist profile                           : -
EAPOL start mode                                : multicast
EAPOL start transform                           : equal-bssid
EAPOL response mode                             : unicast learning
EAPOL response transform                        : equal-bssid
AP LLDP message transmission delay time(s)      : 2
AP LLDP message transmission hold multiplier    : 4
AP LLDP message transmission interval time(s)   : 30
AP LLDP restart delay time(s)                   : 2
AP LLDP admin status                            : txrx
AP LLDP report interval time(s)                 : 30
AP high temperature threshold(degree C)         : -
  ---- More ----
```

```
[Hub-AC]display ac protect
------------------------------------------------------------------
Protect state                : disable
Protect AC                   : -
Priority                     : 0
Protect restore              : enable
Coldbackup kickoff station: disable
------------------------------------------------------------------
[Hub-AC]
```

```
[Hub-AC]display ap-system-profile name Spoke1
------------------------------------------------------------------------------
AC priority                                    : -
Protect AC IP address                          : -
Primary AC                                     : 192.168.1.2
Backup AC                                      : 192.168.20.1
AP management VLAN                             : -
Keep service                                   : disable
Keep service allow new access                  : disable
Temporary management switch                    : disable
Mesh role                                      : mesh-node
STA access mode                                : disable
STA whitelist profile                          : -
STA blacklist profile                          : -
EAPOL start mode                               : multicast
EAPOL start transform                          : equal-bssid
EAPOL response mode                            : unicast learning
EAPOL response transform                       : equal-bssid
AP LLDP message transmission delay time(s)     : 2
AP LLDP message transmission hold multiplier   : 4
AP LLDP message transmission interval time(s)  : 30
AP LLDP restart delay time(s)                  : 2
AP LLDP admin status                           : txrx
AP LLDP report interval time(s)                : 30
AP high temperature threshold(degree C)        : -
  ---- More ----
```

```
[Hub-AC]display ap-system-profile name Spoke2
------------------------------------------------------------------------------
AC priority                                    : -
Protect AC IP address                          : -
Primary AC                                     : 192.168.3.2
Backup AC                                      : 192.168.20.1
AP management VLAN                             : -
Keep service                                   : disable
Keep service allow new access                  : disable
Temporary management switch                    : disable
Mesh role                                      : mesh-node
STA access mode                                : disable
STA whitelist profile                          : -
STA blacklist profile                          : -
EAPOL start mode                               : multicast
EAPOL start transform                          : equal-bssid
EAPOL response mode                            : unicast learning
EAPOL response transform                       : equal-bssid
AP LLDP message transmission delay time(s)     : 2
AP LLDP message transmission hold multiplier   : 4
AP LLDP message transmission interval time(s)  : 30
AP LLDP restart delay time(s)                  : 2
AP LLDP admin status                           : txrx
AP LLDP report interval time(s)                : 30
AP high temperature threshold(degree C)        : -
  ---- More ----
```

当 Spoke1-AC 与 Spoke2-AC 正常工作时，查看 Spoke1-AC、Spoke2-AC 以及 Hub-AC 与 AP 的关联信息：

```
[Spoke1-AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor   : normal          [1]
------------------------------------------------------------------------------
------------------------
ID   MAC            Name      Group         IP              Type            Stat
e STA Uptime
------------------------------------------------------------------------------
------------------------
1    00e0-fc89-33a0 Spoke1-AP Huawei-AP3030 192.168.100.253 AP3030DN        nor
  0   16M:15S
------------------------------------------------------------------------------
------------------------
Total: 1
[Spoke1-AC]
```

```
[Spoke2-AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor   : normal          [1]
------------------------------------------------------------------------------
------------------------
ID   MAC            Name      Group         IP              Type            Stat
e STA Uptime
------------------------------------------------------------------------------
------------------------
1    00e0-fcd7-3520 Spoke2-AP Huawei-AP3030 192.168.200.253 AP3030DN        nor
  0   18M:36S
------------------------------------------------------------------------------
------------------------
Total: 1
[Spoke2-AC]
```

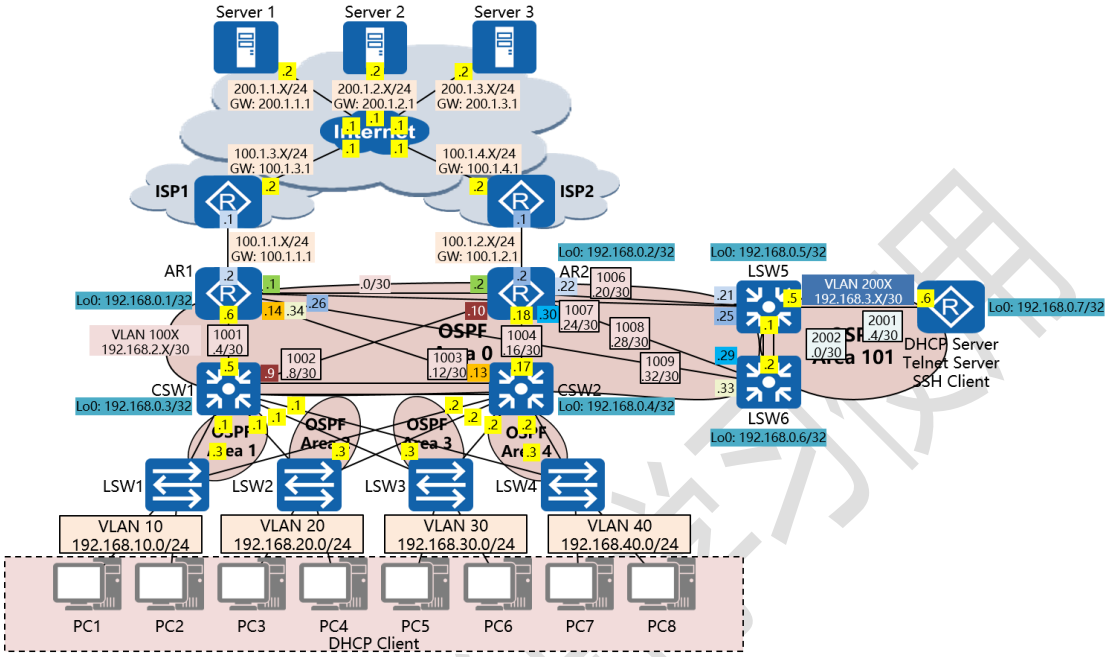
```
[Hub-AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
idle : idle             [2]
------------------------------------------------------------------------------
---
ID   MAC            Name      Group  IP Type            State STA Uptime
------------------------------------------------------------------------------
---
1    00e0-fc89-33a0 Spoke1-AP Spoke1 -  AP3030DN        idle  0   -
2    00e0-fcd7-3520 Spoke2-AP Spoke2 -  AP3030DN        idle  0   -
------------------------------------------------------------------------------
---
Total: 2
[Hub-AC]
```

当 Spoke1-AC 与 Spoke2-AC 失效时（此时将 Spoke1-AC 与 Spoke2-AC 关机，模拟设备失效），再在 Hub-AC 上查看其与 AP 的关联信息：

```
[Hub-AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal          [2]
-------------------------------------------------------------------------------
-----------------
ID   MAC            Name      Group  IP              Type            State STA U
ptime
-------------------------------------------------------------------------------
-----------------
1    00e0-fc89-33a0 Spoke1-AP Spoke1 192.168.100.253 AP3030DN        nor   1   4
7S
2    00e0-fcd7-3520 Spoke2-AP Spoke2 192.168.200.253 AP3030DN        nor   1   5
3S
-------------------------------------------------------------------------------
-----------------
Total: 2
[Hub-AC]
```

八十三、综合实验

一、实验拓扑：



二、实验目的：

根据项目需求，令全网按需通讯

三、实验步骤：

Part I VLAN 设计：

LSW1:

system-view

sysname LSW1

vlan 10

interface Ethernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface Ethernet0/0/2

port link-type trunk

port trunk allow-pass vlan 2 all

interface Ethernet0/0/3

port link-type access

port default vlan 10

interface Ethernet0/0/4

port link-type access

port default vlan 10

LSW2:

system-view

sysname LSW2

vlan 20

interface Ethernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface Ethernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

interface Ethernet0/0/3

port link-type access

port default vlan 20

interface Ethernet0/0/4

port link-type access

port default vlan 20

LSW3:

system-view

sysname LSW3

vlan 30

interface Ethernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface Ethernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

interface Ethernet0/0/3

port link-type access

port default vlan 30

interface Ethernet0/0/4

port link-type access

port default vlan 30

LSW4:

system-view

sysname LSW4

vlan 40

interface Ethernet0/0/1

port link-type trunk

port trunk allow-pass vlan 2 to 4094

interface Ethernet0/0/2

port link-type trunk

port trunk allow-pass vlan 2 to 4094

interface Ethernet0/0/3

port link-type access

port default vlan 40

interface Ethernet0/0/4

port link-type access

port default vlan 40

CSW1:

system-view

sysname CSW1

vlan 10

vlan 20

```
vlan 30
vlan 40
vlan 1001
vlan 1002
interface Eth-Trunk1
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/1
port link-type access
port default vlan 1001
interface GigabitEthernet0/0/2
eth-trunk 1
interface GigabitEthernet0/0/3
eth-trunk 1
interface GigabitEthernet0/0/4
port link-type access
port default vlan 1002
interface GigabitEthernet0/0/5
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/6
port link-type trunk
```

```
port trunk allow-pass vlan all
interface GigabitEthernet0/0/7
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan all
```

CSW2:

```
system-view
sysname CSW2
vlan 10
vlan 20
vlan 30
vlan 40
vlan 1003
vlan 1004
interface Eth-Trunk1
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/1
port link-type access
```

```
port default vlan 1004
interface GigabitEthernet0/0/2
eth-trunk 1
interface GigabitEthernet0/0/3
eth-trunk 1
interface GigabitEthernet0/0/4
port link-type access
port default vlan 1003
interface GigabitEthernet0/0/5
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/6
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/7
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan all
```

LSW5:

```
system-view
sysname LSW5
vlan 1006
vlan 1007
vlan 2001
vlan 2002
interface Eth-Trunk1
port link-type trunk
port trunk allow-pass vlan all
interface GigabitEthernet0/0/1
eth-trunk 1
interface GigabitEthernet0/0/2
eth-trunk 1
interface GigabitEthernet0/0/3
port link-type access
port default vlan 2001
interface GigabitEthernet0/0/4
port link-type access
port default vlan 1007
interface GigabitEthernet0/0/5
port link-type access
```

port default vlan 1006

LSW6:

system-view

sysname LSW6

vlan 1008

vlan 1009

vlan 2002

interface Eth-Trunk1

port link-type trunk

port trunk allow-pass vlan all

interface GigabitEthernet0/0/1

eth-trunk 1

interface GigabitEthernet0/0/2

eth-trunk 1

interface GigabitEthernet0/0/3

port link-type access

port default vlan 1009

interface GigabitEthernet0/0/4

port link-type access

port default vlan 1008

Part II MSTP 设计：

LSW1:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

LSW2:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

LSW3:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

LSW4:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

CSW1:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

stp instance 10 root primary

stp instance 20 root secondary

CSW2:

stp mode mstp

stp region-configuration

region-name easthome

revision-level 0

instance 10 vlan 10 20

instance 20 vlan 30 40

active region-configuration

stp instance 10 root secondary

stp instance 20 root primary

Part III IP 地址设计：

LSW1:

interface vlan10

ip address 192.168.10.3 24

LSW2:

interface vlan20

ip address 192.168.20.3 24

LSW3:

interface vlan30

ip address 192.168.30.3 24

LSW4:

interface vlan40

ip address 192.168.40.3 24

CSW1:

interface LoopBack0

ip address 192.168.0.3 32

interface vlan10

ip address 192.168.10.1 24

interface vlan20

ip address 192.168.20.1 24

interface vlan30

ip address 192.168.30.1 24

interface vlan40

ip address 192.168.40.1 24

interface vlan1001

ip address 192.168.2.5 30

interface vlan1002

ip address 192.168.2.9 30

CSW2:

interface LoopBack0

ip address 192.168.0.4 32

interface vlan10

ip address 192.168.10.2 24

interface vlan20

ip address 192.168.20.2 24

interface vlan30

ip address 192.168.30.2 24

interface vlan40

ip address 192.168.40.2 24

interface vlan1003

ip address 192.168.2.13 30

interface vlan1004

ip address 192.168.2.17 30

LSW5:

interface LoopBack0

ip address 192.168.0.5 32

interface vlan1006

ip address 192.168.2.21 30

interface vlan1007

ip address 192.168.2.25 30

interface vlan2001

ip address 192.168.3.5 30

interface vlan2002

ip address 192.168.3.1 30

LSW6:

interface LoopBack0

ip address 192.168.0.6 32

interface vlan1008

ip address 192.168.2.29 30

interface vlan1009

ip address 192.168.2.33 30

interface vlan2002

ip address 192.168.3.2 30

AR1:

interface LoopBack0

ip address 192.168.0.1 32

interface GigabitEthernet0/0/0

ip address 100.1.1.2 24

interface GigabitEthernet0/0/1

ip address 192.168.2.1 30

interface GigabitEthernet0/0/2

ip address 192.168.2.6 30

interface GigabitEthernet2/0/0

ip address 192.168.2.14 30

interface GigabitEthernet3/0/0

ip address 192.168.2.26 30

interface GigabitEthernet4/0/0

ip address 192.168.2.34 30

AR2:

interface LoopBack0

ip address 192.168.0.2 32

interface GigabitEthernet0/0/0

ip address 100.1.2.2 24

interface GigabitEthernet0/0/1

ip address 192.168.2.2 30

interface GigabitEthernet0/0/2

ip address 192.168.2.18 30

interface GigabitEthernet2/0/0

ip address 192.168.2.10 30

interface GigabitEthernet3/0/0

ip address 192.168.2.22 30

interface GigabitEthernet4/0/0

ip address 192.168.2.30 30

DHCP Server:

interface LoopBack0

ip address 192.168.0.7 32

interface GigabitEthernet0/0/0

ip address 192.168.3.6 30

ISP1:

interface GigabitEthernet0/0/0

ip address 100.1.3.2 24

interface GigabitEthernet0/0/1

ip address 100.1.1.1 24

ISP2:

interface GigabitEthernet0/0/0

ip address 100.1.4.2 24

interface GigabitEthernet0/0/1

ip address 100.1.2.1 24

Internet:

interface GigabitEthernet0/0/0

ip address 100.1.3.1 24

interface GigabitEthernet0/0/1

ip address 100.1.4.1 24

interface GigabitEthernet0/0/2

ip address 200.1.1.1 24

interface GigabitEthernet3/0/0

ip address 200.1.2.1 24

interface GigabitEthernet4/0/0

```
ip address 200.1.3.1 24
```

Part IV 内网路由设计：

LSW1:

ospf 1

area 1

network 192.168.10.0 0.0.0.255

LSW2:

ospf 1

area 2

network 192.168.20.0 0.0.0.255

LSW3:

ospf 1

area 3

network 192.168.30.0 0.0.0.255

LSW4:

ospf 1

area 4

network 192.168.40.0 0.0.0.255

CSW1:

ospf 1 router-id 192.168.0.3

area 0

network 192.168.2.5 0.0.0.0

network 192.168.2.9 0.0.0.0

area 1

network 192.168.10.0 0.0.0.255

area 2

network 192.168.20.0 0.0.0.255

area 3

network 192.168.30.0 0.0.0.255

area 4

network 192.168.40.0 0.0.0.255

CSW2:

ospf 1 router-id 192.168.0.4

area 0

network 192.168.2.17 0.0.0.0

network 192.168.2.13 0.0.0.0

area 1

network 192.168.10.0 0.0.0.255

area 2

network 192.168.20.0 0.0.0.255

area 3

network 192.168.30.0 0.0.0.255

area 4

network 192.168.40.0 0.0.0.255

AR1:

ospf 1 router-id 192.168.0.1

area 0

network 192.168.2.1 0.0.0.0

network 192.168.2.6 0.0.0.0

network 192.168.2.14 0.0.0.0

network 192.168.2.26 0.0.0.0

network 192.168.2.34 0.0.0.0

AR2:

ospf 1 router-id 192.168.0.2

area 0

network 192.168.2.2 0.0.0.0

network 192.168.2.10 0.0.0.0

network 192.168.2.18 0.0.0.0

network 192.168.2.22 0.0.0.0

network 192.168.2.30 0.0.0.0

LSW5:

ospf 1 router-id 192.168.0.5

area 0

network 192.168.2.25 0.0.0.0

network 192.168.2.21 0.0.0.0

area 101

network 192.168.3.5 0.0.0.0

network 192.168.3.1 0.0.0.0

LSW6:

ospf 1 router-id 192.168.0.6

area 0

network 192.168.2.33 0.0.0.0

network 192.168.2.29 0.0.0.0

area 101

network 192.168.3.2 0.0.0.0

DHCP Server:

ospf 1 router-id 192.168.0.7

area 101

network 192.168.3.6 0.0.0.0

Part V 出口路由设计：

AR1:

```
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
ospf 1 router-id 192.168.0.1
default-route-advertise always cost 1
acl number 2001
rule permit source 192.168.2.4 0.0.0.3
rule permit source 192.168.2.8 0.0.0.3
rule permit source 192.168.2.12 0.0.0.3
rule permit source 192.168.2.16 0.0.0.3
rule permit source 192.168.2.20 0.0.0.3
rule permit source 192.168.2.24 0.0.0.3
rule permit source 192.168.2.28 0.0.0.3
rule permit source 192.168.2.32 0.0.0.3
rule permit source 192.168.3.0 0.0.0.3
rule permit source 192.168.3.4 0.0.0.3
rule permit source 192.168.10.0 0.0.0.255
rule permit source 192.168.20.0 0.0.0.255
rule permit source 192.168.30.0 0.0.0.255
rule permit source 192.168.40.0 0.0.0.255
rule 1000 deny source any
interface GigabitEthernet0/0/0
```

nat outbound 2001

AR2:

ip route-static 0.0.0.0 0.0.0.0 100.1.2.1

ospf 1 router-id 192.168.0.2

default-route-advertise always cost 2

acl number 2001

rule permit source 192.168.2.4 0.0.0.3

rule permit source 192.168.2.8 0.0.0.3

rule permit source 192.168.2.12 0.0.0.3

rule permit source 192.168.2.16 0.0.0.3

rule permit source 192.168.2.20 0.0.0.3

rule permit source 192.168.2.24 0.0.0.3

rule permit source 192.168.2.28 0.0.0.3

rule permit source 192.168.2.32 0.0.0.3

rule permit source 192.168.3.0 0.0.0.3

rule permit source 192.168.3.4 0.0.0.3

rule permit source 192.168.10.0 0.0.0.255

rule permit source 192.168.20.0 0.0.0.255

rule permit source 192.168.30.0 0.0.0.255

rule permit source 192.168.40.0 0.0.0.255

rule 1000 deny source any

```
interface GigabitEthernet0/0/0
nat outbound 2001
```

Part VI WAN 模拟：

ISP1:

rip 1

version 2

network 100.0.0.0

undo summary

ISP2:

rip 1

version 2

network 100.0.0.0

undo summary

Internet:

rip 1

version 2

network 100.0.0.0

network 200.1.1.0

network 200.1.2.0

network 200.1.3.0

undo summary

Part VII VRRP 设计：

CSW1:

interface vlan10

vrrp vrid 47 virtual-ip 192.168.10.4

vrrp vrid 47 priority 200

interface vlan20

vrrp vrid 47 virtual-ip 192.168.20.4

vrrp vrid 47 priority 200

interface vlan30

vrrp vrid 47 virtual-ip 192.168.30.4

interface vlan40

vrrp vrid 47 virtual-ip 192.168.40.4

CSW2:

interface vlan10

vrrp vrid 47 virtual-ip 192.168.10.4

interface vlan20

vrrp vrid 47 virtual-ip 192.168.20.4

interface vlan30

vrrp vrid 47 virtual-ip 192.168.30.4

vrrp vrid 47 priority 200

interface vlan40

```
vrrp vrid 47 virtual-ip 192.168.40.4
vrrp vrid 47 priority 200
```

Part VIII DHCP 设计：

DHCP Server:

dhcp enable

ip pool vlan10

network 192.168.10.0 mask 255.255.255.0

gateway-list 192.168.10.4

dns-list 202.106.49.151

lease day 8

ip pool vlan20

network 192.168.20.0 mask 255.255.255.0

gateway-list 192.168.20.4

dns-list 202.106.49.151

lease day 8

ip pool vlan30

network 192.168.30.0 mask 255.255.255.0

gateway-list 192.168.30.4

dns-list 202.106.49.151

lease day 8

ip pool vlan40

network 192.168.40.0 mask 255.255.255.0

gateway-list 192.168.40.4

dns-list 202.106.49.151

lease day 8

interface GigabitEthernet0/0/0

dhcp select global

LSW1:

dhcp enable

interface vlan10

dhcp select relay

dhcp relay server-ip 192.168.3.6

LSW2:

dhcp enable

interface vlan20

dhcp select relay

dhcp relay server-ip 192.168.3.6

LSW3:

dhcp enable

interface vlan30

dhcp select relay

dhcp relay server-ip 192.168.3.6

LSW4:

dhcp enable

interface vlan40

dhcp select relay

dhcp relay server-ip 192.168.3.6