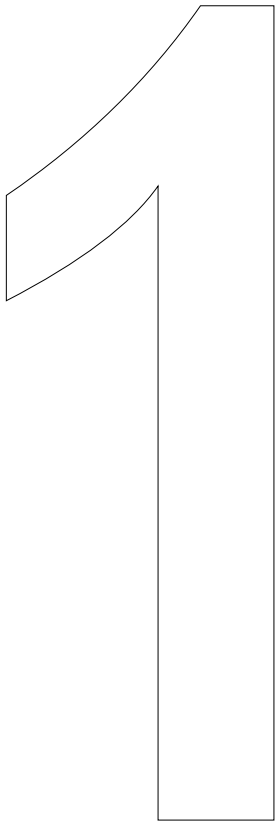
2022/ 集美工业学校

网络基础配置活页式教程

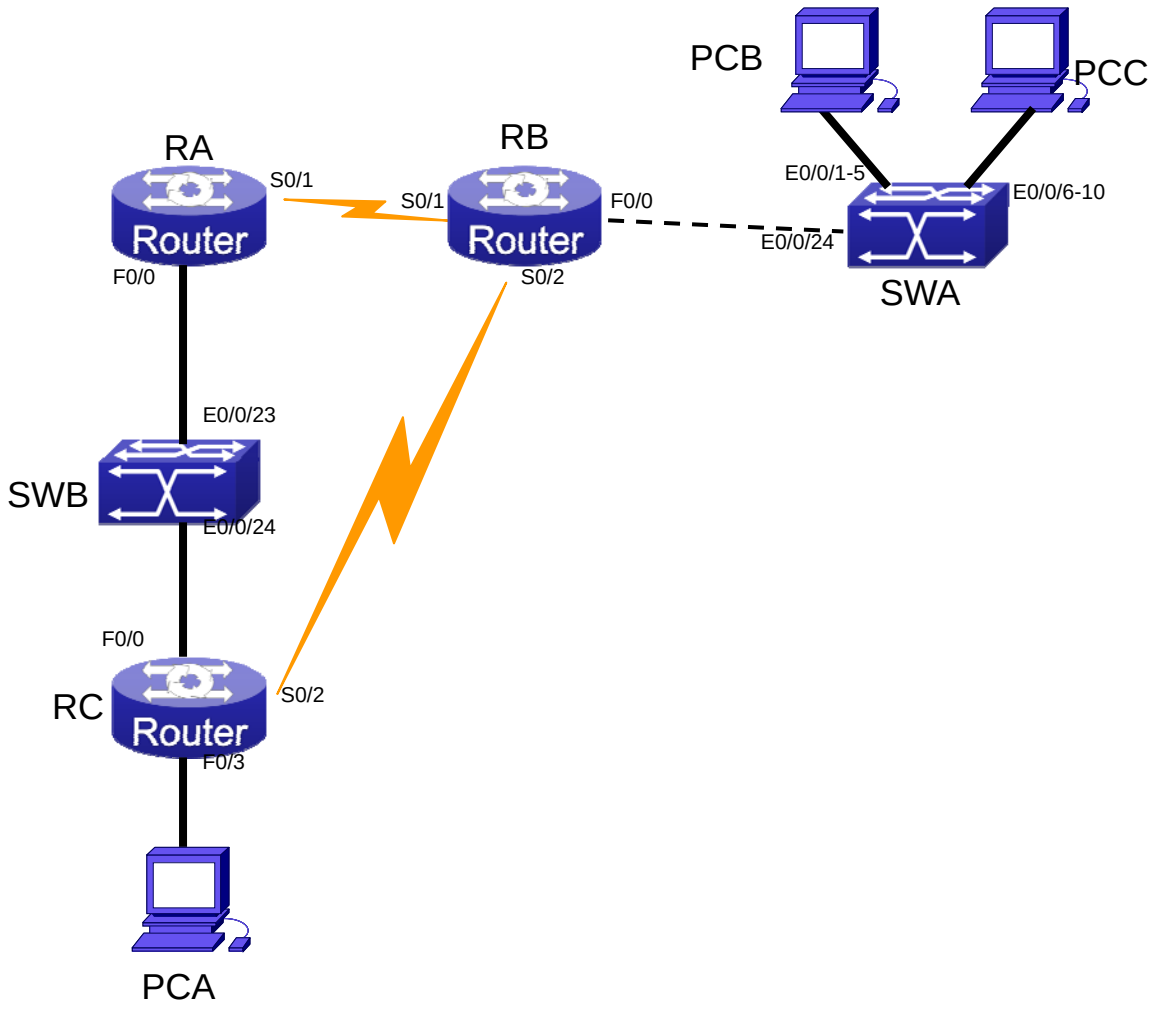
主编：刘炎火

参编：田原、詹志桢、兰一栋

基于“一学二练三优化”范式的教材改革实践



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC

S0/2	202.106.1.2/28	
F0/0	192.168.1.1/24	
F0/3	192.168.10.254/24	
RB		
S0/1	210.216.1.2/28	
S0/2	202.106.1.1/28	
F0/0	10.1.1.1/24	
RA		
S0/1	210.216.1.1/28	
F0/0	192.168.2.2/24	
SWA		
VLAN100	0/0/24	10.1.1.2/24
VLAN20	0/0/1-5	10.1.10.254/24
VLAN30	0/0/6-10	10.1.20.254/24
SWB		
VLAN100	0/0/23	192.168.2.1/24
VLAN200	0/0/24	192.168.1.2/24
PCA	192.168.10.1/24	
PCB	10.1.10.1/24	
PCC	10.1.20.1/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. RB 与 RA 之间配置 ipsec vpn：

A. RA 与 RB 之间 IKE 方式协商安全联盟主动模式；

B. IKE 策略采用 md5 hash 算法；

C. transform-set（协议变换集）名称为 lin，加密验证方式为：ah-sha-hmac、esp-des，共享密钥为：1234567

D. 加密映射表进行协商的安全联盟的生命周期为 86400 秒

2. RA 与 RB 之间配置 ppp 协议：

采用 chap 认证，启用 AAA 验证方法，本地认证；

RB 与 RC 之间配置 ppp 协议：

采用 pap 认证，设置双向认证，启用 AAA 验证方法，本地认证。

3. 不允许 PCC 访问 PCA：

A. 可在任意设备上进行配置

B. 限制使用标准 ACL 进行配置。

4. 将 PCB 与 PCC 进行 MAC 地址绑定：

A. 使 PCB 与 PCC 换到其他端口是无法通信,并且 PCC 所连接的端口其他 PC 机连接上也无法通信。

5. 全网配置 RIP v2 路由协议，使全网能够互通。

6. 策略路由：

A. 所有数据相互通信优先通过 SWA-RB-RA-SWB-RC 路线；

B. SWA-RB-RC 路线作为冗余线路。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接时的情况
debug crypto isakmp
查看第二阶段连接时的情况
debug crypto ipsec

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示以建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由

Show ip route
查看 rip 路由协议状态，能够看到所使用的版本等信息
Show ip rip protocol
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证策略路由

可使用 show running-config 进行配置查看，也可使用 taceroute 命令在 PC 机上进行验证，若正确会遵循题目要求中的线路进行路由，若不正确则会走另外一条线路。（必须在全网互通的前提下）
在网络设备上可以使用 tracert 命令进行数据路由的查看。

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
   E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。
2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. match address 后面的名字注意要写正确，需要和对应的 ACL 列表名相同
5. 在三层交换机上配置 RIP 路由协议时，宣告时注意子网掩码的写法
6. RA 与 RB 做 CHAP，主要注意 CHAP 的三次握手，用户名的交互认证。别忘了起 AAA 认证
7. 路由 RIP 主要声名直连网段。注意声名 RIP 版本
8. 端口锁定可以使用端口安全与 AM，端口安全可以使用静态与动态，本例中使用静态端口安全
9. 配置策略路由需要先建立访问列表，或者用已有的也可以，在建立 route-map 里面指明下一跳，在调用先前建立好的访问列表，最后绑定到端口上。
10. 配置策略路由后，观察 SWB 交换机，注意 SWB 到达 SWA 两个出口的跳数一致，所以从 PCA 到达 SWA 的数据经过 SWB 时数据应该会有部分丢失 ;解决的思路为让 SWB 认为 SWB-RC-RB-SWA 这条线路的跳数比 SWB-RA-RB-SWA 的跳数大，建议在 RC 的路由模式配置度量值偏移。

六、 配置参考

RA 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp for_chap local
!
username RB password 0 123456
crypto isakmp key 1234567 210.216.1.2 255.255.255.255
!
!
crypto isakmp policy 10
 hash md5
!
crypto ipsec transform-set lin
 transform-type ah-sha-hmac esp-des
!
crypto map lin2 10 ipsec-isakmp
 set peer 210.216.1.2
 set security-association lifetime seconds 86400
 set transform-set lin
 match address for_vpn
!
!
interface FastEthernet0/0
 ip address 192.168.2.2 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
```

```
interface Serial0/1
 ip address 210.216.1.1 255.255.255.240
 no ip directed-broadcast
 crypto map lin2
 encapsulation ppp
 ppp authentication chap for_chap
 ppp chap hostname RA
 physical-layer speed 64000

!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 210.216.1.0 255.255.255.240
 network 192.168.2.0 255.255.255.0
!
!
ip access-list extended for_vpn
 permit ip any any
!
!
RA#
```

RB 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
```

```
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp for_ppp local
!
username RA password 0 123456
!
crypto isakmp key 1234567 210.216.1.1 255.255.255.255
!
!
crypto isakmp policy 10
 hash md5
!
crypto ipsec transform-set lin
 transform-type ah-sha-hmac esp-des
!
crypto map lin2 10 ipsec-isakmp
 set peer 210.216.1.1
 set security-association lifetime seconds 86400
 set transform-set lin
 match address for_vpn
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip policy route-map for_rmap
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 210.216.1.2 255.255.255.240
 no ip directed-broadcast
 crypto map lin2
 encapsulation ppp
 ppp authentication chap for_ppp
 ppp chap hostname RB
 physical-layer speed 64000
```

```
!
interface Serial0/2
 ip address 202.106.1.1 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap for_ppp
 ppp pap sent-username RB password 0 123456
 physical-layer speed 64000
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 210.216.1.0 255.255.255.240
 network 202.106.1.0 255.255.255.240
 network 10.1.1.0 255.255.255.0
!
!
ip access-list extended for_vpn
 permit ip any any
!
!
route-map for_rmap 10 permit
 match ip address for_vpn
 set ip next-hop 210.216.1.1
!
!
RB#
```

RC 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
```

```
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication ppp for_pap local
!
username RB password 0 123456
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
 ip access-group for_acl in
!
interface FastEthernet0/3
 ip address 192.168.10.254 255.255.255.0
 no ip directed-broadcast
 ip policy route-map for_rmap
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap for_pap
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 202.106.1.0 255.255.255.240
 network 192.168.1.0 255.255.255.0
```

```
 network 192.168.10.0 255.255.255.0
!
!
ip access-list standard for_acl
 deny     10.1.20.0 255.255.255.0
 permit any
!
!
route-map for_rmap 1 permit
 match ip address for_acl
 set ip next-hop 192.168.1.2
!
!
RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
vlan 1
!
vlan 20
!
vlan 30
!
vlan 100
!
!
Interface Ethernet0/0/1
 switchport access vlan 20
 switchport port-security
 switchport port-security mac-address aa-bb-cc-dd-ee-ff
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
 switchport access vlan 20
!
Interface Ethernet0/0/4
```

```
 switchport access vlan 20
!
Interface Ethernet0/0/5
 switchport access vlan 20
!
Interface Ethernet0/0/6
 switchport access vlan 30
 switchport port-security
 switchport port-security lock
 switchport port-security mac-address aa-aa-aa-aa-aa-aa
!
Interface Ethernet0/0/7
 switchport access vlan 30
!
Interface Ethernet0/0/8
 switchport access vlan 30
!
Interface Ethernet0/0/9
 switchport access vlan 30
!
Interface Ethernet0/0/10
switchport access vlan 30
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
```

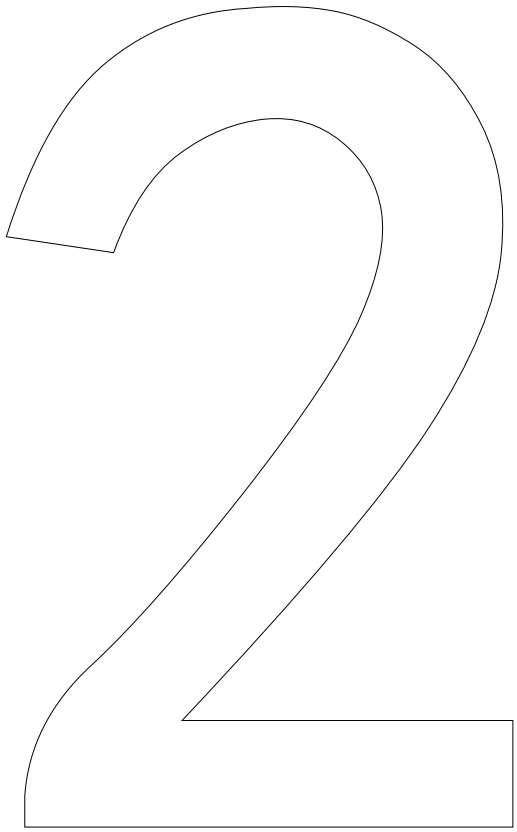
```
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan20
ip address 10.1.10.254 255.255.255.0
!
interface Vlan30
ip address 10.1.20.254 255.255.255.0
!
interface Vlan100
ip address 10.1.1.2 255.255.255.0
!
router rip
network 10.1.1.0/24
network 10.1.10.0/24
network 10.1.20.0/24
!
no login
!
end
SWA#
```

SWB 交换机：

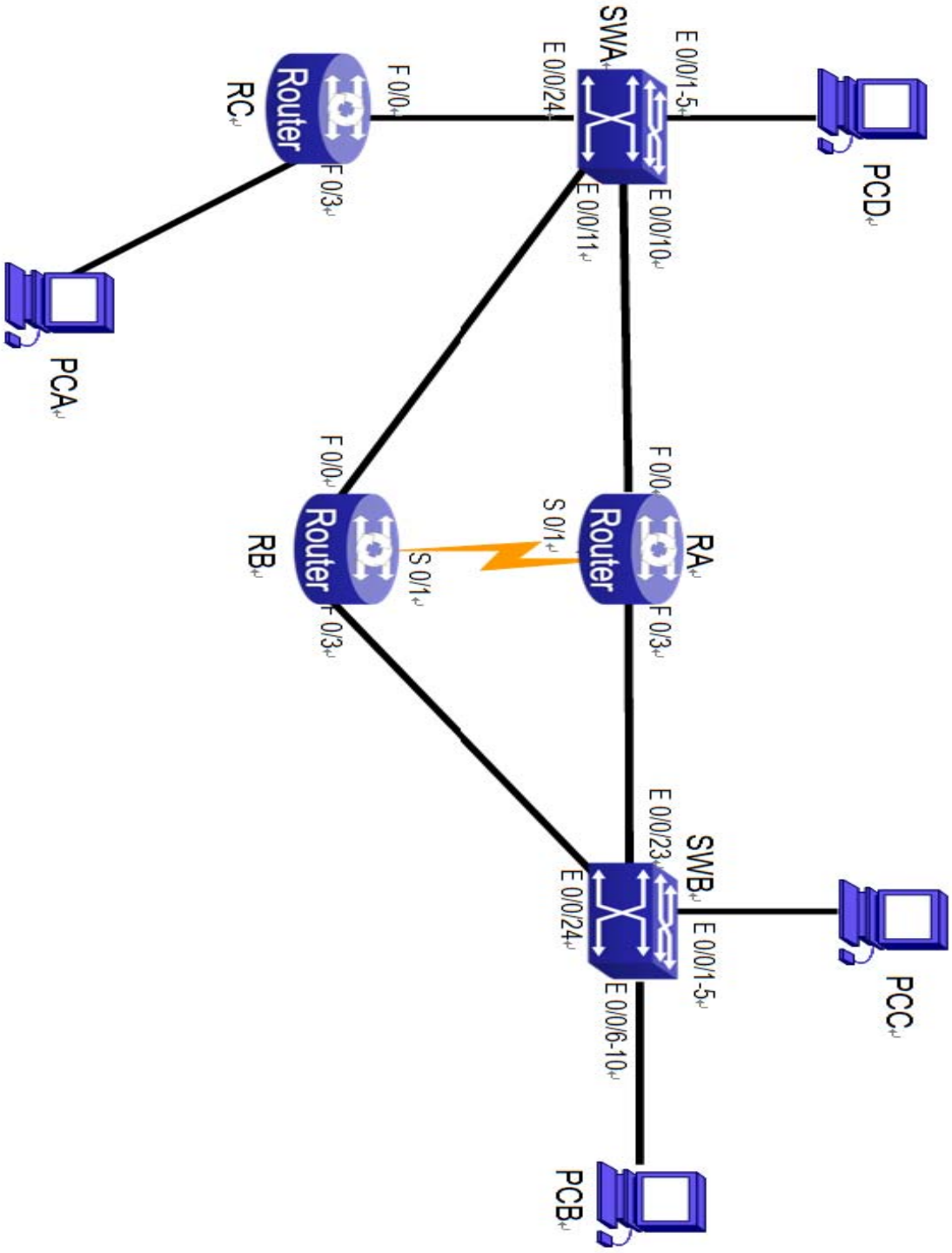
```
sho run
!
no service password-encryption
!
hostname SWB
```

```
!
vlan 1
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
!
Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
```

```
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan100
 ip address 192.168.2.1 255.255.255.0
!
interface Vlan200
 ip address 192.168.1.2 255.255.255.0
!
router rip
 network 192.168.1.0/24
 network 192.168.2.0/24
!
no login
!
end


SWB#
```



一、 拓扑图


SWA
E 0/0/1-5
E 0/0/24
E 0/0/11
E 0/0/10
PCD
RC
Router
F 0/0
F 0/3
PCA
F 0/0
S 0/1
RB
Router
S 0/1
F 0/3
F 0/0
RA
Router
F 0/3
SWB
E 0/0/23
E 0/0/24
E 0/0/1-5
E 0/0/6-10
PCC
PCB

二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
F0/0	202.106.1.10/24	
F0/3	192.168.30.1/24	
RB		
F0/0	172.16.1.3/24	
F0/3.1	192.168.10.254/24	
F0/3.2	192.168.20.254/24	
S0/1	100.1.1.2/30	
RA		
F0/0	172.16.1.2/24	
F0/3.1	192.168.10.253/24	
F0/3.2	192.168.20.253/24	
S0/1	100.1.1.1/30	
SWA		
VLAN40	0/0/1-5	192.168.40.1/24
VLAN100	0/0/24	202.106.1.11/24
VLAN200	0/0/10-11	172.16.1.1/24
SWB		
VLAN10	0/0/1-5	
VLAN20	0/0/6-10	
PCA	192.168.30.10/24	
PCB	192.168.10.10/24	
PCC	192.168.20.10/24	
PCD	192.168.40.10/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. RA 的 F0/3 接口、RB 的 F0/3 接口上配置单臂路由；
2. RA 与 RB 之间配置 vrrp：
   A. 侦听下一跳端口、递减为 20；
   B. 分别为 VLAN10 与 VLAN20 设置不同的 VRRP；
   C. VLAN10 的虚拟 IP 为 192.168.10.1/24；
   D. VLAN20 的虚拟 IP 为 192.168.20.1/24；
   E. VLAN10 优先 RA 通过，VLAN20 优先 RB 通过。
3. 全网使用 RIPv2 路由协议，使全网络能够相互通信。
4. 在所有设备上开启 telnet 服务，使网络内所有的 pc 均可进行远程控制。
5. 在 RC 上配置 NAT，使 PCA 的私有地址转换为公网地址访问 PCA 与 PCB。

四、 验证思路

1. 查看配置文件

   Show running-config 确保配置是否正确

2. 验证 VRRP

   查看本设备 VRRP 运行状况,配置成功会出现本台设备 vrrp 的相关信息，如主次关系、优先级、虚拟 ip、对端 ip 等信息
   Show vrrp detail
   查看 vrrp 协商主次关系过程（须在配置 VRRP 前配置）
   debug vrrp
   从内网持续 Ping 外网某 PC，拔下 VRRP 出口任意条链路，都不会影响内网和外网间通信

3. 查看全网互通

   查看路由表，是否学到全网路由
   Show ip route
   查看 rip 路由协议状态，能够看到所使用的版本等信息

Show ip rip protocol
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

4. 验证 telnet 服务

可使用 ping 命令测试主机与网络中各个设备的连通情况，如果连通使用 telnet 命令进行验证，也可使用 show running-cnfig 命令验证。

5. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需要先通信）
show ip nat translations

五、 注意事项

1. 单臂路由上注意路由器的接口封装 802.1q 协议，交换机与路由器连接端口上注意开启 TRUNK 模式。
2. 由于 VLAN10 的数据优先 RA 通过，VLAN20 的数据优先 RB 通过，所以需要在 RA 上降低 VLAN20 的 VRRP 优先级，RB 上降低 VLAN10 的 VRRP 优先级；或提高 RA 上 VLAN10 的 VRRP 优先级，RB 上 VLAN20 的 VRRP 优先级
3. 路由器上配置 RIP 路由协议主要宣告直连网段。注意 RIP 路由协议的版本与自动汇总，三层交换机上注意宣告直连时子网掩码的写法。
4. 在路由器上配置 telnet 服务时注意开启 AAA 服务本地认证，且需要配置 enable 密码 ,才可正常访问 ,配置 enable 密码也需要开启 AAA 服务本地认证 ,两个 AAA 本地认证注意区分。在 VTY 中注意引用 AAA 列表。注：配置 AAA 服务时可以使用默认 default，也可以自命名。
5. 配置 nat 时请注意路由器的 inside 口和 outside 口，注意数据流的方向。
6. Nat 可以使用静态 NAT、动态 NAT 与端口转换 NAT，在本例中将静态、动态与 PAT 结合的配置分别显示，注意区分。

六、 配置参考

RA 路由器：

sho run
正在收集配置...

```
当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication login dcnu local
aaa authentication enable default enable
!
username admin password 0 admin
enable password 0 enbpasswd level 15
!
interface FastEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3.1
 ip address 192.168.10.253 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 10
 bandwidth 100000
 delay 1
 vrrp track interface FastEthernet0/0 20
 vrrp 10 associate 192.168.10.1 255.255.255.0
 vrrp 10 track interface FastEthernet0/0 20
!
interface FastEthernet0/3.2
 ip address 192.168.20.253 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 20
 bandwidth 100000
```

```
 delay 1
 vrrp 20 associate 192.168.20.1 255.255.255.0
 vrrp 20 priority 90
 vrrp 20 track interface FastEthernet0/0 20
!
interface Serial0/1
 ip address 100.1.1.1 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
!
line vty 0
 login authentication dcnu
!
line vty 1
 login authentication dcnu
!
line vty 2
 login authentication dcnu
!
line vty 3
 login authentication dcnu
!
line vty 4
 login authentication dcnu
!
!
router rip
 version 2
 no auto-summary
 network 100.1.1.0 255.255.255.252
 network 172.16.1.0 255.255.255.0
 network 192.168.10.0 255.255.255.0
 network 192.168.20.0 255.255.255.0
!
```

```
!
RA#
```

RB 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication login dcnu local
aaa authentication enable default enable
!
username admin password 0 admin
enable password 0 passwd2 level 15
!
interface FastEthernet0/0
 ip address 172.16.1.3 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3.1
 ip address 192.168.10.254 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 10
 bandwidth 100000
 delay 1
 vrrp 10 associate 192.168.10.1 255.255.255.0
 vrrp 10 priority 90
```

```
 vrrp 10 track interface FastEthernet0/0 20
!
interface FastEthernet0/3.2
 ip address 192.168.20.254 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 20
 bandwidth 100000
 delay 1
 vrrp 20 associate 192.168.20.1 255.255.255.0
 vrrp 20 track interface FastEthernet0/0 20
!
interface Serial0/1
 ip address 100.1.1.2 255.255.255.252
 no ip directed-broadcast
 physical-layer speed 64000
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
!
line vty 0
 login authentication dcnu
!
line vty 1
 login authentication dcnu
!
line vty 2
 login authentication dcnu
!
line vty 3
 login authentication dcnu
!
line vty 4
 login authentication dcnu
!
!
router rip
```

```
 version 2
 no auto-summary
 network 172.16.1.0 255.255.255.0
 network 192.168.10.0 255.255.255.0
 network 100.1.1.0 255.255.255.252
 network 192.168.20.0 255.255.255.0
!
!
RB#
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication login dcnu local
aaa authentication enable default enable
!
username admin password 0 admin
enable password 0 passwd3 level 15
!
interface FastEthernet0/0
 ip address 202.106.1.10 255.255.255.0
 no ip directed-broadcast
 ip nat outside
!
interface FastEthernet0/3
 ip address 192.168.30.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
```

```
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
!
line vty 0
 login authentication dcnu
!
line vty 1
 login authentication dcnu
!
line vty 2
 login authentication dcnu
!
line vty 3
 login authentication dcnu
!
line vty 4
 login authentication dcnu
!
!
router rip
 version 2
 no auto-summary
 network 202.106.1.0 255.255.255.0
!
ip route default FastEthernet0/0
!
!
ip access-list standard lin
 permit any
!
!
```

```
ip nat inside source static 192.168.30.1 202.106.1.10
ip nat inside source list lin interface FastEthernet0/0
!
RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
enable password admin
!
!
telnet-user admin password 0 admin
!
vlan 1
!
vlan 40
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
switchport access vlan 40
!
Interface Ethernet0/0/2
switchport access vlan 40
!
Interface Ethernet0/0/3
switchport access vlan 40
!
Interface Ethernet0/0/4
switchport access vlan 40
!
Interface Ethernet0/0/5
switchport access vlan 40
!
Interface Ethernet0/0/6
!
```

```
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
switchport access vlan 200
!
Interface Ethernet0/0/11
switchport access vlan 200
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
```

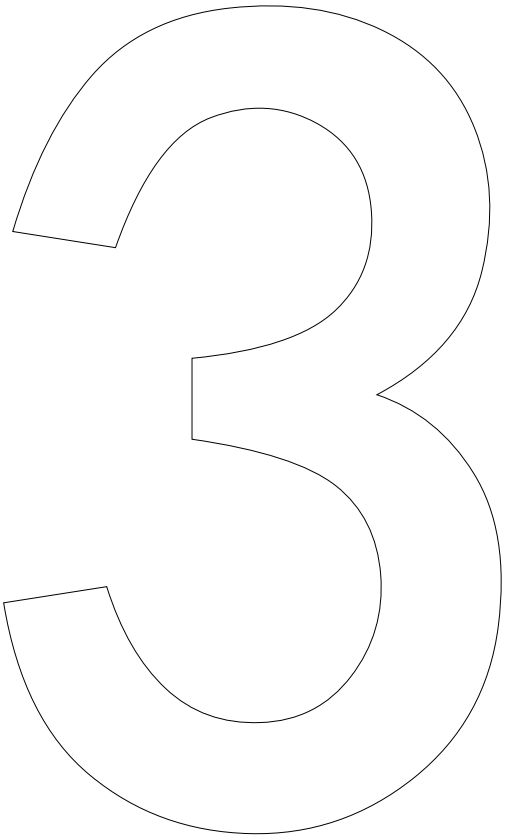
```
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan40
ip address 192.168.40.1 255.255.255.0
!
interface Vlan100
ip address 202.106.1.11 255.255.255.0
!
interface Vlan200
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.1.0/24
network 192.168.40.0/24
network 202.106.1.0/24
!
no login
!
end
SWA#
```

SWB 交换机：

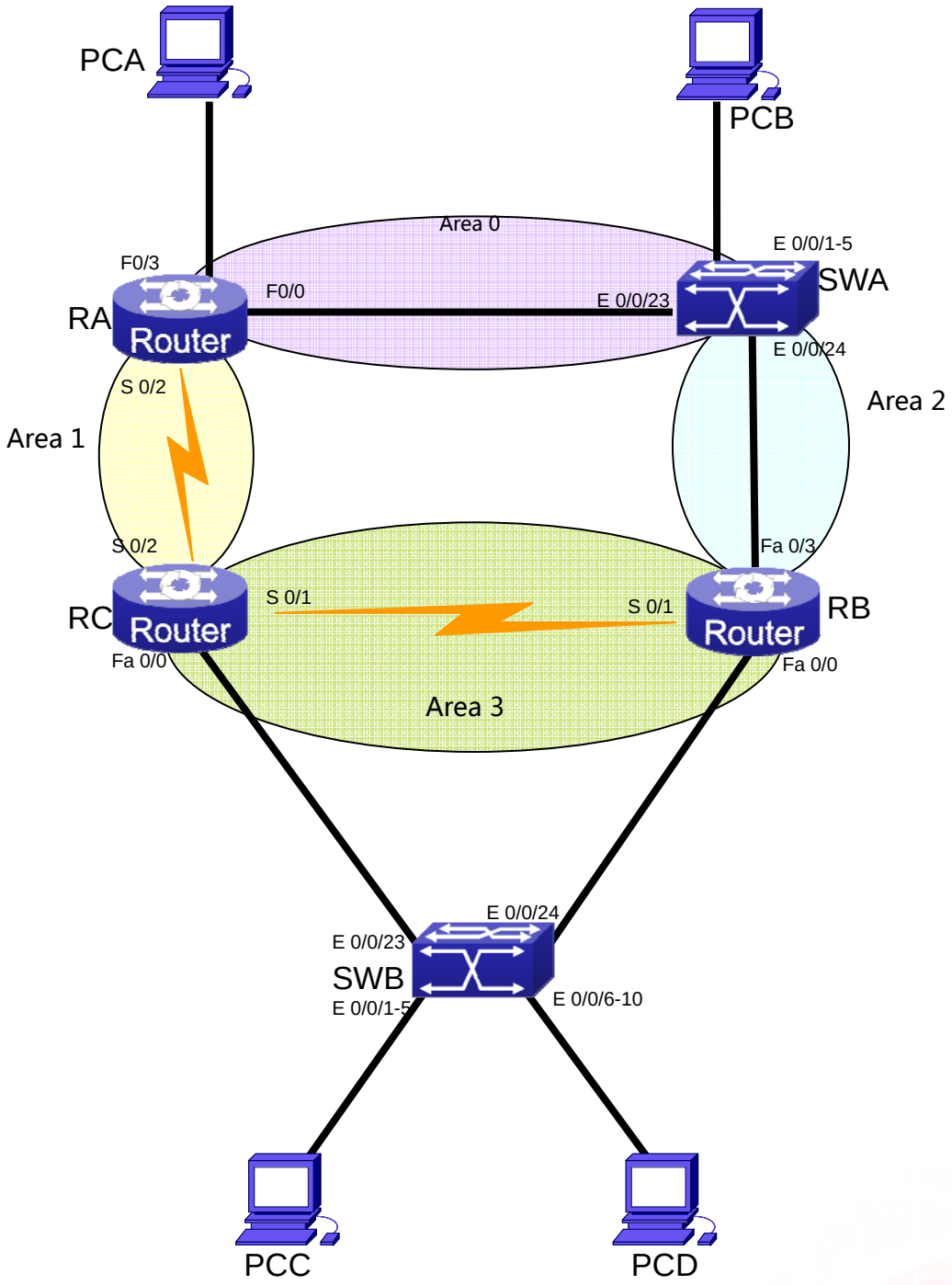
```
sho run
!
no service password-encryption
!
hostname SWB
!
enable password admin
!
!
telnet-user admin password 0 admin
!
vlan 1
!
vlan 10
!
vlan 20
!
Interface Ethernet0/0/1
switchport access vlan 10
```

```
!
Interface Ethernet0/0/2
switchport access vlan 10
!
Interface Ethernet0/0/3
switchport access vlan 10
!
Interface Ethernet0/0/4
switchport access vlan 10
!
Interface Ethernet0/0/5
switchport access vlan 10
!
Interface Ethernet0/0/6
switchport access vlan 20
!
Interface Ethernet0/0/7
switchport access vlan 20
!
Interface Ethernet0/0/8
switchport access vlan 20
!
Interface Ethernet0/0/9
switchport access vlan 20
!
Interface Ethernet0/0/10
switchport access vlan 20
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
```

```
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
switchport mode trunk
!
Interface Ethernet0/0/24
 switchport mode trunk
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
no login
!
end
SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
F0/0	172.16.1.3/24	
S0/1	100.1.2.1/30	
S0/2	100.1.3.1/30	
RB		
F0/0	172.16.1.4/24	
F0/3	100.1.4.1/30	
S0/1	100.1.2.2/30	
RA		
F0/0	100.1.5.1/30	
F0/3	192.168.10.1/24	
S0/2	100.1.3.2/30	
SWA		
VLAN20	0/0/1-5	192.168.20.1/24
VLAN100	0/0/23	100.1.5.2/30
VLAN200	0/0/24	100.1.4.2/30
SWB		
VLAN30	0/0/1-5	192.168.30.1/24
VLAN40	0/0/6-10	192.168.40.1/24
VLAN100	0/0/23-24	172.16.1.2/24
PCA	192.168.10.10/24	
PCB	192.168.20.10/24	
PCC	192.168.30.10/24	
PCD	192.168.40.10/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. RC 的 f0/0 与 RB 的 F0/0 接口配置 vrrp 协议：

A. 虚拟 IP 为 172.16.1.1/24,并且设置下一跳跟踪端口；

B. RB 路由器为主路由器。

2. 全网络配置 ospf 路由协议；

根据图中所示划分区域。

3. 在区域 3 和区域 0 之间配置虚链路，使全网络互通。

4. 配置访问控制列表：

A. 使 PCA 可以 ping 通 PCC，PCC 不能 ping 通 PCA；

B. PCB 可以访问任何人，PCD 不能访问 PCB。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VRRP

查看本设备 VRRP 运行状况,配置成功会出现本台设备 vrp 的相关信息，如主次关系、优先级、虚拟 ip、对端 ip 等信息
Show vrrp detail
查看 vrrp 协商主次关系过程（须在配置 VRRP 前配置）
debug vrrp
从内网持续 ping 外网某站点，拆除 VRRP 协议相关任意链路，不影响 ping 结果

3. 验证 OSPF 路由协议

查看 OSPF 路由协议状态，可以看到 OSPF 进程号、route id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
查看虚链路状态信息

Show ip ospf virtual-link

4. 验证访问控制列表

查看访问控制类表的配置
Show ip access-list lin
PC 之间相互 ping 命令也可验证访问控制列表是否成功。

五、 注意事项

1. OSPF 的 Route ID 由设备上的 loopback 端口决定，如果没有 loopback 端口，则由 IP 地址最大的物理端口决定
2. OSPF 进行宣告时注意子网掩码与网段所归属的区域
3. 在三层交换上宣告直连网段时注意使用子网屏蔽码代替原来子网掩码的位置
4. 配置虚链路时注意两个区域中间所经过的区域，注意对方路由器的 Route ID
5. ICMP 协议的 echo（request）消息的类型号为 8，echo reply 消息的类型号为 0

六、 配置参考

RA 路由器：

```
sho run
Building configuration...
Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 100.1.5.1 255.255.255.252
 no ip directed-broadcast
```

```
!
interface FastEthernet0/3
 ip address 192.168.10.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 100.1.3.2 255.255.255.252
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 192.168.10.0 255.255.255.0 area 0
 network 100.1.5.0 255.255.255.252 area 0
 network 100.1.3.0 255.255.255.252 area 1
 area 1 virtual-link 172.16.1.3
!
!
RA#
```

RB 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
```

```
hostname RB
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 172.16.1.4 255.255.255.0
 no ip directed-broadcast
 vrrp 10 associate 172.16.1.1 255.255.255.0
 vrrp 10 priority 90
 vrrp 10 track interface FastEthernet0/3 20
!
interface FastEthernet0/3
 ip address 100.1.4.1 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/1
 ip address 100.1.2.2 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 172.16.1.0 255.255.255.0 area 3
 network 100.1.2.0 255.255.255.252 area 3
 network 100.1.4.0 255.255.255.252 area 2
 area 2 virtual-link 192.168.20.1
!
!
RB#
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 172.16.1.3 255.255.255.0
 no ip directed-broadcast
 vrrp 10 associate 172.16.1.1 255.255.255.0
 vrrp 10 track interface Serial0/2 20
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 100.1.2.1 255.255.255.252
 no ip directed-broadcast
 physical-layer speed 64000
!
interface Serial0/2
 ip address 100.1.3.1 255.255.255.252
 no ip directed-broadcast
 physical-layer speed 64000
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
```

```
!
router ospf 1
 network 100.1.2.0 255.255.255.252 area 3
 network 172.16.1.0 255.255.255.0 area 3
 network 100.1.3.0 255.255.255.252 area 1
 area 1 virtual-link 192.168.10.1
!
!
RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
vlan 1
!
vlan 20
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
 switchport access vlan 20
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
 switchport access vlan 20
!
Interface Ethernet0/0/4
 switchport access vlan 20
!
Interface Ethernet0/0/5
 switchport access vlan 20
!
Interface Ethernet0/0/6
!
```

```
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
```

```
!
Interface Ethernet0/0/28
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip address 100.1.5.2 255.255.255.252
!
interface Vlan200
 ip address 100.1.4.2 255.255.255.252
!
router ospf 1
 network 100.1.4.0 0.0.0.3 area 2
 network 100.1.5.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 area 2 virtual-link 172.16.1.4
!
no login
!
end
SWA#
```

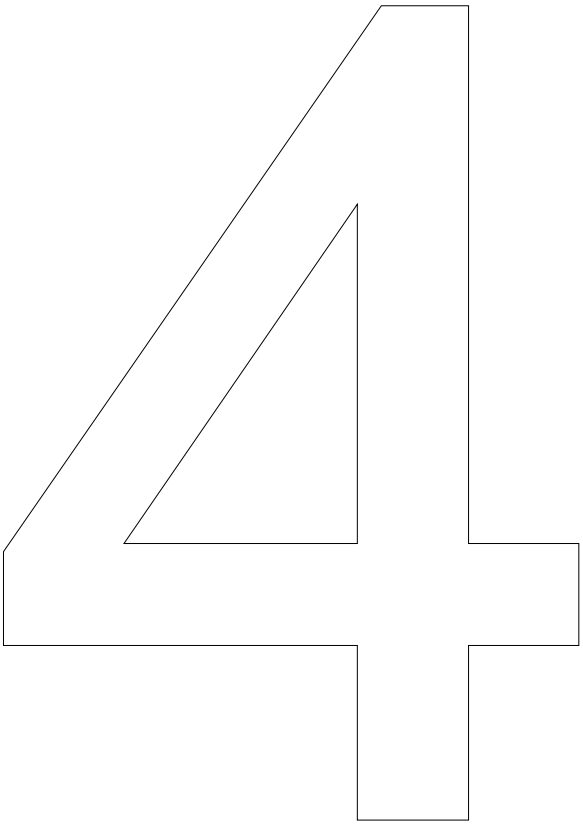
SWB 交换机：

```
ho run
!
no service password-encryption
!
hostname SWB
!
vlan 1
!
vlan 30
!
vlan 40
!
vlan 100
!
firewall enable
!
ip access-list extended lin2
   deny igmp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 8
```

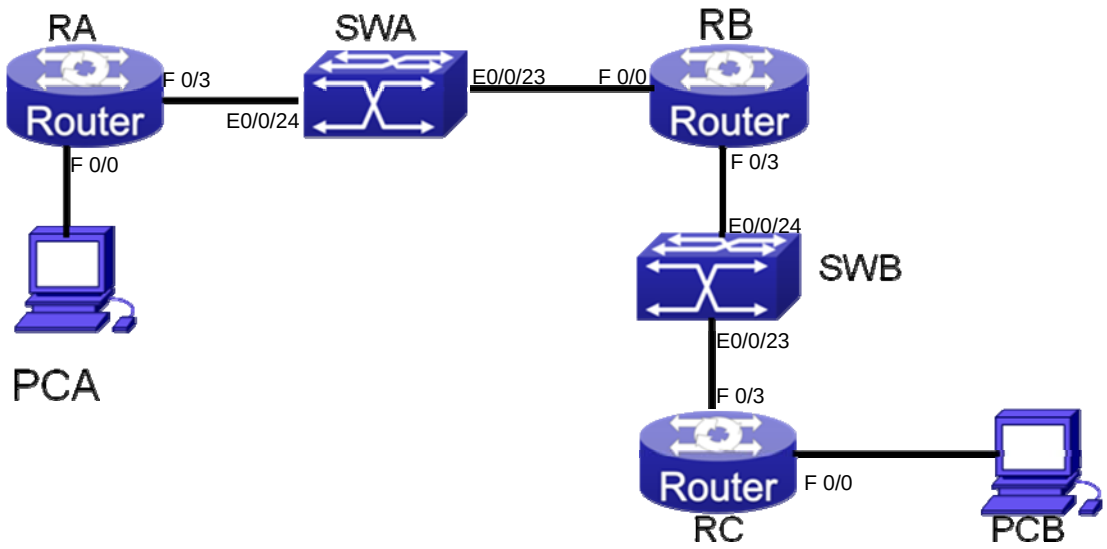
```
   permit ip any-source any-destination
ip access-list extended lin1
   deny igmp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 8
   permit ip any-source any-destination
!
Interface Ethernet0/0/1
ip access-group lin1 in
 switchport access vlan 30
!
Interface Ethernet0/0/2
 switchport access vlan 30
!
Interface Ethernet0/0/3
 switchport access vlan 30
!
Interface Ethernet0/0/4
 switchport access vlan 30
!
Interface Ethernet0/0/5
 switchport access vlan 30
!
Interface Ethernet0/0/6
 ip access-group lin2 in
 switchport access vlan 40
!
Interface Ethernet0/0/7
 switchport access vlan 40
!
Interface Ethernet0/0/8
 switchport access vlan 40
!
Interface Ethernet0/0/9
 switchport access vlan 40
!
Interface Ethernet0/0/10
 switchport access vlan 40
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
```

```
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
!
 interface Vlan40
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan100
 ip address 172.16.1.2 255.255.255.0
!
router ospf 1
 network 172.16.1.0 0.0.0.255 area 3
```

```
 network 192.168.30.0 0.0.0.255 area 3
 network 192.168.40.0 0.0.0.255 area 3
!
no login
!
end
SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
F0/0	192.168.20.1/24	
F0/3	172.16.4.2/30	
RB		
F0/0	172.16.2.2/30	
F0/3	172.16.3.1/30	
RA		
F0/0	192.168.10.1/24	
F0/3	172.16.1.1/30	
SWA		
VLAN100	0/0/24	172.16.1.2/30
VLAN200	0/0/23	172.16.2.1/30

SWB		
VLAN300	0/0/24	172.16.3.2/30
VLAN400	0/0/23	172.16.4.1/30
PCA	192.168.10.10/24	
PCB	192.168.20.10/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 在 RA、SWA、RB 运行 ospf 动态路由协议：

采用单区域；

2. 在 RB、SWB、RC 运行 rip 动态路由协议：

采用版本二；

3. 使整个网络可以相互通信

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 rip 路由协议状态，能够看到所使用的版本、路由重分发等信息
Show ip rip protocol
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离、路由重分发等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database

查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

五、 注意事项

1. OSPF 注意宣告直连网段和区域 ID
2. RIP 注意宣告直连网段和版本号
3. 路由再发布注意 ,在 RIP 路由模式中发布 OSPF ,发布的时候注意 OSPF 的进程号；在 OSPF 路由模式发布 RIP

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 172.16.1.1 255.255.255.252
```

```
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Serial1/0
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 192.168.10.0 255.255.255.0 area 0
 network 172.16.1.0 255.255.255.252 area 0
!
!
RA_config#
```

RB 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
```

```
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 172.16.2.2 255.255.255.252
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 172.16.3.1 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Serial1/0
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 network 172.16.3.0 255.255.255.252
 redistribute connect
 redistribute ospf 1

!
router ospf 1
```

```
 network 172.16.2.0 255.255.255.252 area 0
 redistribute connect
 redistribute rip
!
!
RB_config#
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 172.16.4.2 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
```

```
 no ip directed-broadcast
!
interface Serial1/0
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
no ip directed-broadcast
!
!
router rip
 version 2
 network 172.16.4.0 255.255.255.252
 network 192.168.20.0 255.255.255.0

!
!
RC_config#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
vlan 1
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
!
Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
```

!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22

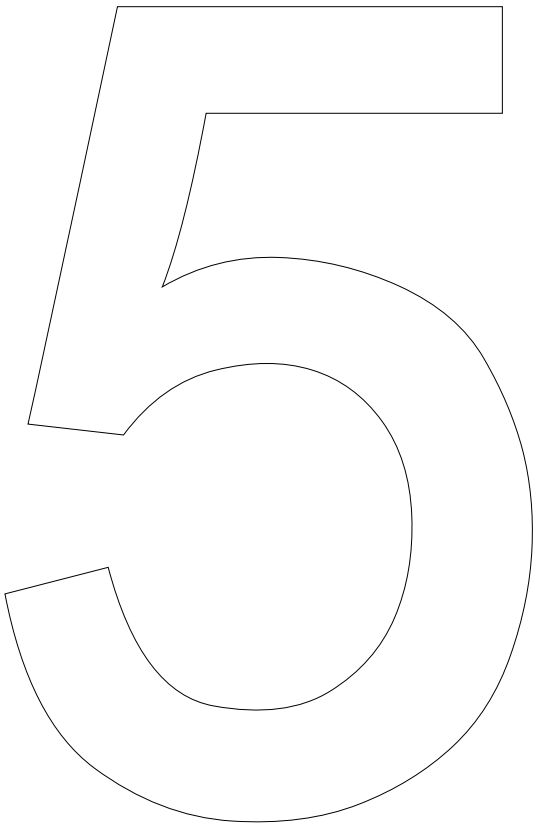
```
!
Interface Ethernet0/0/23
 switchport access vlan 200
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
interface Vlan100
 ip address 172.16.1.2 255.255.255.252
!
interface Vlan200
 ip address 172.16.2.1 255.255.255.252
!
router ospf 1
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
!
no login
!
end

SWA#
```

SWB 交换机：

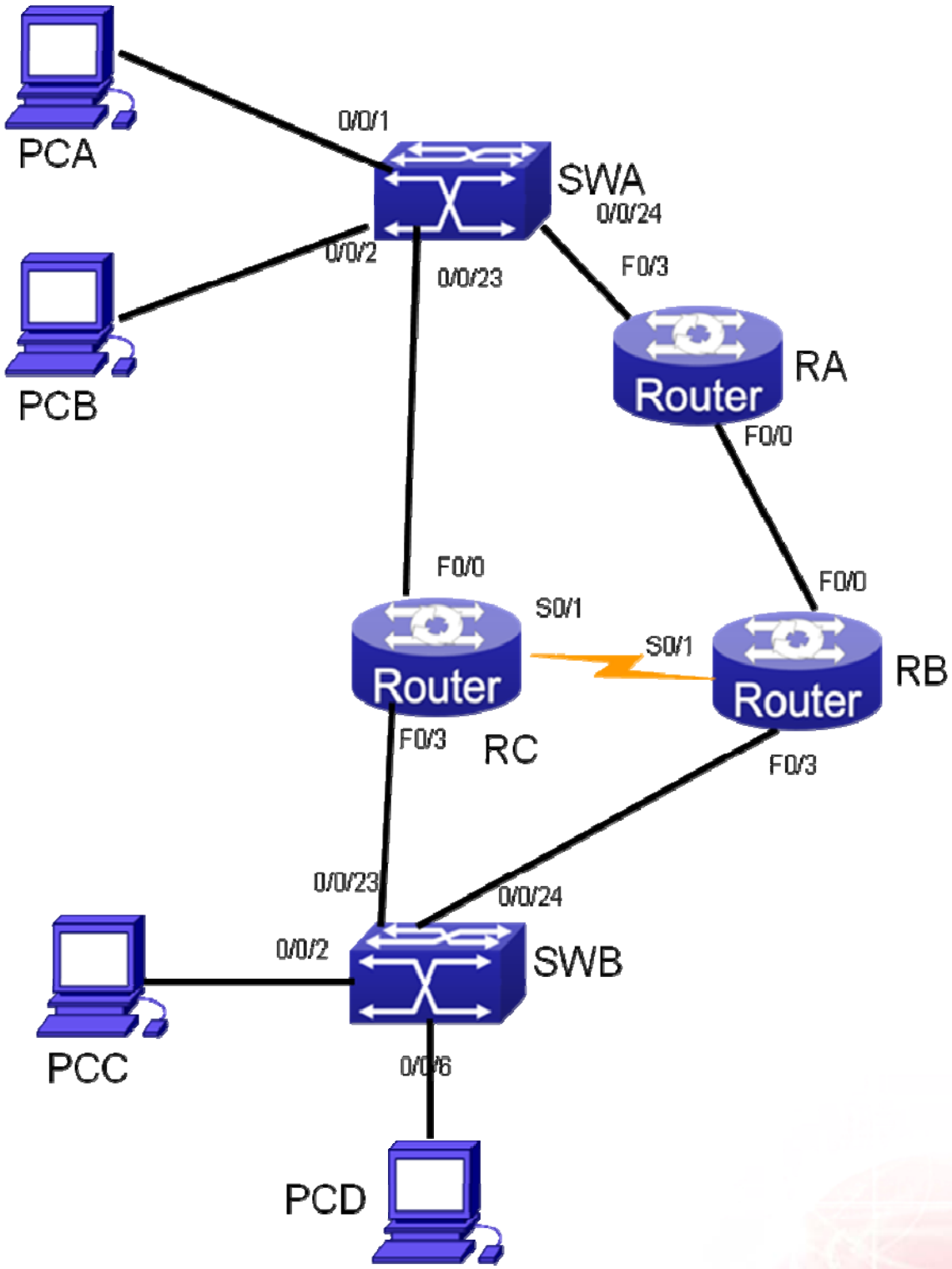
```
WB#sho run
!
no service password-encryption
!
hostname SWB
!
vlan 1
!
vlan 300
!
vlan 400
!
Interface Ethernet0/0/1
!
```

Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!

```
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 400
!
Interface Ethernet0/0/24
 switchport access vlan 300
!
interface Vlan300
 ip address 172.16.3.2 255.255.255.252
!
interface Vlan400
 ip address 172.16.4.1 255.255.255.252
!
router rip
 network 172.16.3.0/30
 network 172.16.4.0/30
!
no login
!
end

SWB(config)#
```



一、 拓扑图



二、 环境准备

3. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

4. IP 地址规划

RC		
S0/1	210.216.1.2/28	
F0/0	11.1.1.2/24	
F0/3	200.1.10.1/24	
RB		
S0/1	210.216.1.1/28	
F0/0	202.106.1.2/28	
F0/3	100.101.1.1/24	
RA		
F0/3	10.1.1.1/24	
F0/0	202.106.1.1/28	
SWA		
VLAN10	0/0/1	192.168.10.1/24
VLAN20	0/0/2	192.168.20.1/24
VLAN100	0/0/23	11.1.1.1/24
VLAN200	0/0/24	10.1.1.2/24
SWB		
VLAN100	0/0/23	200.1.10.2/24
VLAN200	0/0/24	100.101.1.2/24
VLAN30	0/0/1-5	192.168.30.1/24
VLAN40	0/0/6-10	192.168.40.1/24
PCA		
PCB		
PCC		
PCD		

5. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. SWA 与 SWB 配置 DHCP：

A. SWA 为其 VLAN10、VLAN20 分配 ip 地址分别为 192.168.10.0、192.168.20.0 网段；SWB 为其 VLAN30、VLAN40 分配 ip 地址分别为 192.168.30.0、192.168.40.0 网段；

B. 网关地址为端口所在 vlan 地址；

C. DNS 全部设置为 202.106.0.20

2. PCA 可以访问 PCD 的主页，不可以访问其他任何服务；PCB 工作日上午 8：30 至下午 5：00 可以访问 PCC，其余时间不可以访问。

3. 全网络运行 ospf 动态路由协议：

A. SWA、RC、SWB 在区域 0 中；

B. SWA、RA、RB、SWB 在区域 1 中；

C. RB 和 RC 在区域 2 中;

D. 在区域 2 中设置 MD5 加密认证。

4. PCA 网段与 PCC 网段通信时：

A. 必须以 SWA-RA-RB-SWB 线路进行双向数据转发；

B. 在 SWA 与 SWB 上进行配置.

5. RA 与 RB 之间配置 ipsce vpn：

A. RA 与 RB 之间 IKE 方式协商安全联盟，协商模式为野蛮模式；

B. IKE 策略采用 sha hash 算法；

C. transform-set（协议变换集）名称为 lin，加密验证方式为：ah-md5-hmac esp-3des esp-md5-hmac，共享密钥为：1234567

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 DHCP 服务器

查看 DHCP 服务器的地址分配情况、连接信息等

show ip dhcp server statistics

3. 验证访问控制列表

查看配置状态
show access-lists

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证路由选路

可使用 show running-config 进行配置查看，也可使用 tacert 命令在 PC 机上进行验证 ,若正确会遵循题目要求中的线路进行路由 ,若不正确则会走另外一条线路。（必须在全网互通的前提下）
在网络设备上可以使用 traceroute 命令进行数据路由的查看。

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表和 IKE 预共享密钥；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
   E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。
2. IPSEC IKE 默认开启主动模式
3. crypto map 的名字必须与接口上应用的名字一致
4. DHCP 注意配置好为不同网段分发的 IP。
5. 时间访问列表，注意配置完后要修改交换机的 CLOCK，或者 NTP 服务器。
6. OSPF 注意声明好直链网段和区域 ID，认证的时候注意两端的加密密钥要一致。
7. VPN 要注意两端的加密算法要一致，注意把做完的加密映射表绑定到端口。

8. 选择特定路径时需要注意，由于三层交换的 route-map 只支持 BGP，所以需要采用其他的方法，本例中采用修改接口 BW 值的方法，用来影响修改 ospf 的 cost 值，也可采用静态路由浮动的方法。

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!

!
gbsc group default
!
!
crypto isakmp key 1234567 202.106.1.2 255.255.255.255
!
!
crypto isakmp policy 10
!
crypto ipsec transform-set lin
 transform-type ah-md5-hmac esp-3des esp-md5-hmac
!
crypto map lin-map 10 ipsec-isakmp
 mode aggressive
 set peer 202.106.1.2
 set pfs group1
 set security-association lifetime seconds 86400
 set transform-set lin
 match address vpn-acl
!
!
```

```
interface FastEthernet0/0
 ip address 202.106.1.1 255.255.255.240
 no ip directed-broadcast
 crypto map lin-map
 bandwidth 500
!
interface FastEthernet0/3
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 bandwidth 500
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 202.106.1.0 255.255.255.240 area 1
 network 10.1.1.0 255.255.255.0 area 1
!
!
ip access-list extended vpn-acl
 permit ip any any
!
!
RA#
```

RB 路由器：

```
RB#sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
```

```
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
crypto isakmp key 1234567 202.106.1.1 255.255.255.255
!
!
crypto isakmp policy 10
!
crypto ipsec transform-set lin
 transform-type ah-md5-hmac esp-3des esp-md5-hmac
!
crypto map lin-map 10 ipsec-isakmp
 mode aggressive
 set peer 202.106.1.1
 set pfs group1
 set security-association lifetime seconds 86400
 set transform-set lin
 match address vpn-acl
!
!
interface FastEthernet0/0
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
 crypto map lin-map
 bandwidth 500
!
interface FastEthernet0/3
 ip address 100.101.1.1 255.255.255.0
 no ip directed-broadcast
 bandwidth 500
!
interface Serial0/1
 ip address 210.216.1.1 255.255.255.240
 no ip directed-broadcast
 physical-layer speed 64000
 ip ospf authentication message-digest
```

```
 ip ospf message-digest-key 8 md5 lin
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 100.101.1.0 255.255.255.0 area 1
 network 202.106.1.0 255.255.255.240 area 1
 network 210.216.1.0 255.255.255.240 area 2
 area 2 authentication message-digest
!
!
ip access-list extended vpn-acl
 permit ip any any
!
!
RB#
```

RC 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 11.1.1.2 255.255.255.0
```

```
 no ip directed-broadcast
 bandwidth 100
!
interface FastEthernet0/3
 ip address 200.1.10.1 255.255.255.0
 no ip directed-broadcast
 bandwidth 100
!
interface Serial0/1
 ip address 210.216.1.2 255.255.255.240
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 8 md5 lin
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 200.1.10.0 255.255.255.0 area 0
 network 216.216.1.0 255.255.255.240 area 2
 network 11.1.1.0 255.255.255.0 area 0
 area 2 authentication message-digest
!
!
RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
vendorlocation China
vendorContact 800-810-9119
!
!
service dhcp
```

```
!
ip dhcp pool lin2
 network-address 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 202.106.0.20
!
ip dhcp pool lin1
 network-address 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 202.106.0.20
!
!
vlan 1
!
lan 10
!
vlan 20
!
vlan 100
!
vlan 200
!
time-range lin
 periodic daily 8:30:0 to 17:0:0
!
firewall enable
!
ip access-list extended lin-acl2
   permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 time-range lin
   permit ip any-source any-destination
ip access-list extended lin-acl1
   permit tcp 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255 d-port 80
   deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
   permit ip any-source any-destination
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
nterface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
!
```

```
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13

Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 bandwidth control 100 both
 switchport access vlan 100
!
Interface Ethernet0/0/24
```

```
 bandwidth control 500 both
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip address 11.1.1.1 255.255.255.0
!
interface Vlan200
 ip address 10.1.1.2 255.255.255.0
!
router ospf 1
network 10.1.1.0 0.0.0.255 area 1
 network 11.1.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
no login
!
end

SWA#
```

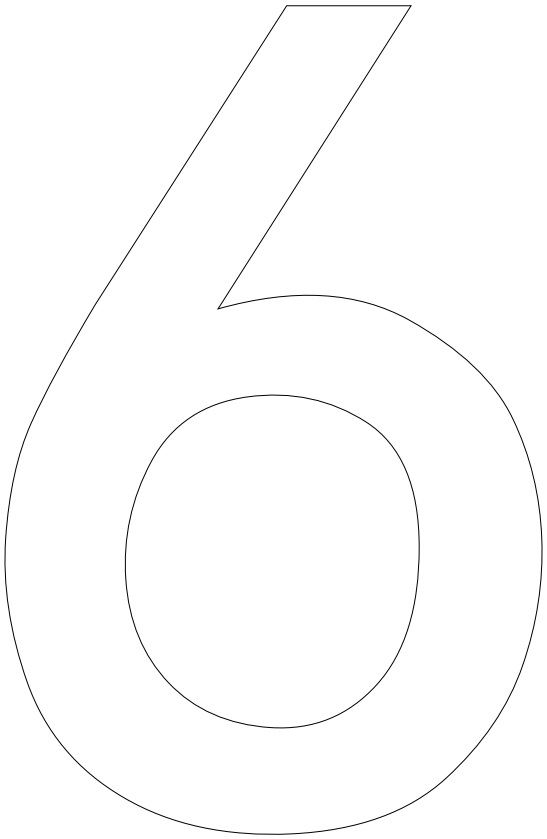
SWB 交换机：

```
sho run
!
no service password-encryption
!
hostname SWB
vendorlocation China
vendorContact 800-810-9119
```

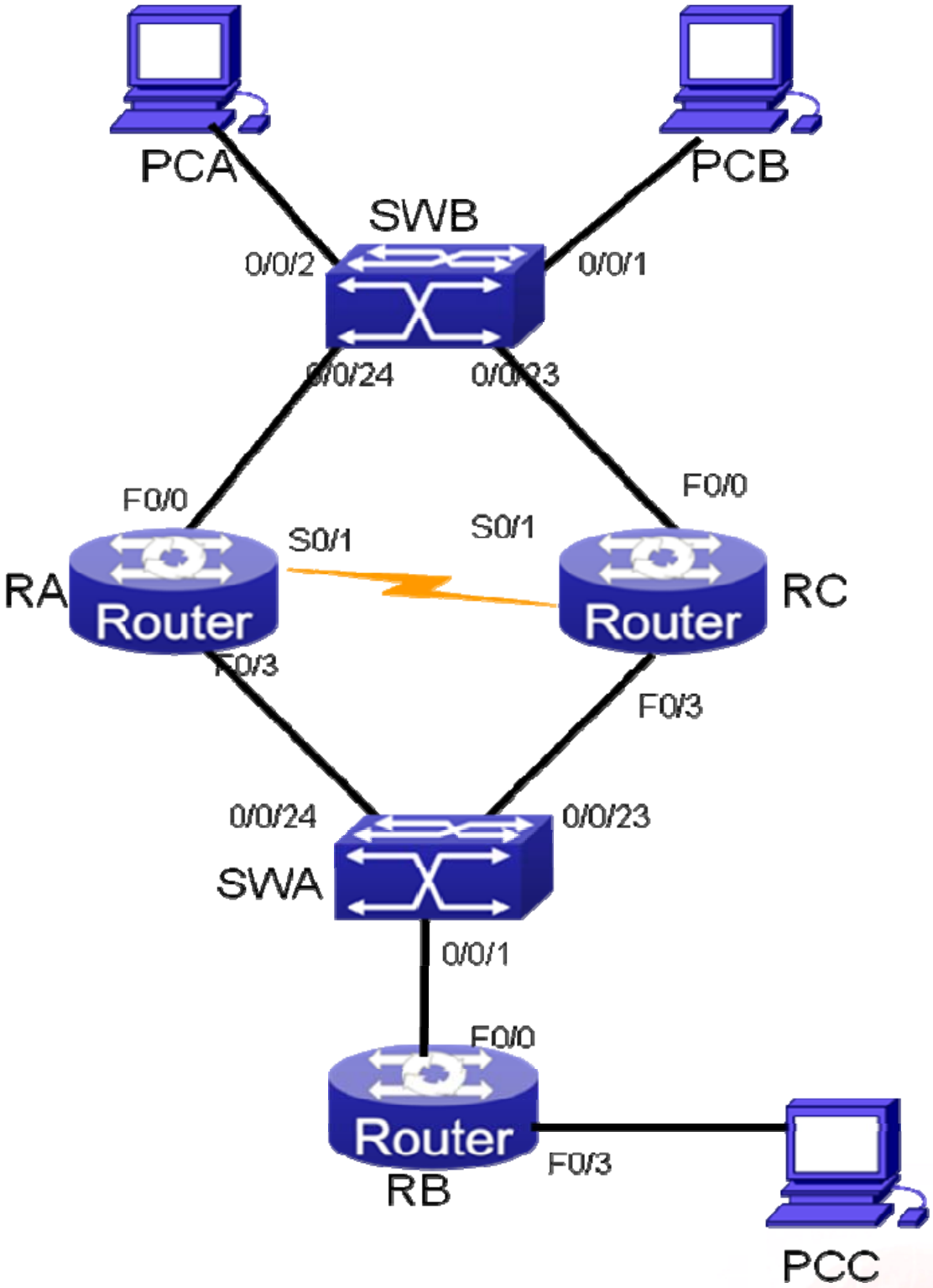
```
!
!
service dhcp
!
ip dhcp pool lin4
 network-address 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 202.106.0.20
!
ip dhcp pool lin3
 network-address 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 202.106.0.20
!
!
vlan 1
!
vlan 30
!
vlan 40
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
 switchport access vlan 30
!
Interface Ethernet0/0/2
 switchport access vlan 30
!
Interface Ethernet0/0/3
 switchport access vlan 30
!
Interface Ethernet0/0/4
 switchport access vlan 30
!
Interface Ethernet0/0/5
 switchport access vlan 30
!
Interface Ethernet0/0/6
switchport access vlan 40
!
```

```
Interface Ethernet0/0/7
 switchport access vlan 40
!
Interface Ethernet0/0/8
 switchport access vlan 40
!
Interface Ethernet0/0/9
 switchport access vlan 40
!
Interface Ethernet0/0/10
 switchport access vlan 40
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 bandwidth control 100 both
 switchport access vlan 100
!
Interface Ethernet0/0/24
 bandwidth control 500 both
 switchport access vlan 200
```

```
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan100
 ip address 200.1.10.2 255.255.255.0
!
interface Vlan200
 ip address 100.101.1.2 255.255.255.0
!
router ospf 1
 network 100.101.1.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 200.1.10.0 0.0.0.255 area 0
!
no login
!
end

SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
S0/1	200.1.10.2/28	
F0/0	192.168.10.6/30	
F0/3	100.1.1.1/24	
RB		
F0/3	10.1.10.2/24	
F0/0	10.1.10.2/24	
RA		
F0/3	100.1.1.2/24	
F0/0	192.168.10.2/30	
S0/1	200.1.10.1/28	
SWA		
VLAN100	0/0/23-24	100.1.1.3/24
VLAN300	0/0/1	10.1.10.1/24
SWB		
VLAN100	0/0/23	192.168.10.5/30
VLAN200	0/0/24	192.168.10.1/30
VLAN10	0/0/1-5	192.168.20.1/24
PCA	192.168.20.10/24	
PCB	192.168.20.20/24	
PCC	11.1.1.10/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. RA、RC 与 SWA 之间配置 vrrp 协议：

A. 虚拟 ip 为 100.1.1.254；

B. 正常情况下，RC 为主路由器，RA 为辅路由器。

2. 全网开启组播路由协议：

A. 要求使用 DVMRP；

B. 要求 PCC 发送的组播数据包 PCA 与 PCB 能接收到，可借助第三方组播发送软件；

3. 在 RA 与 RC 之间开启 PPP 协议 ,使之能够相互通信：

采用 CHAP 单方向验证。

4. 在 SWB 上绑定 PCA 与 PCB 的 MAC 地址：

A. 让其 PC 无法使用其他端口进行通信，更改 MAC 地址后也无法通信；

B. 关闭自动学习功能，每个端口最多学习 5 个 MAC 地址。

5. 在 RA 与 RB 上开启 telnet 与 ssh 服务 ,使网络内的 PC 能够通过 telnet 与 ssh 方式进行登录。

6. 设置 enable 密码，使用 aaa 服务器本地验证。

7. 全网络配置静态路由使之相互通信。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证组播

显示 DVMRP 路由组播信息

Show mroute dvmrp

也可在 PC 上开启组播软件，进行数据传输，若其他 PC 可以接收到此数据，证明成功。推荐使用 Mcast 软件（可在神州数码网络大学 BBS 下载）

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。

Show ppp status

查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示以建立连接，否则则不停认证。

Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证端口绑定

可使用 show running-config 进行配置查看，也可将 PC 从当前交换机端口换至其他端口验证，如果换至其他端口无法通信，说明配置成功。

五、 注意事项

1. 注意路由器与交换机开启组播的命令不同，验证也稍有区别。
2. 在路由器上开启 SSH 的方法与在交换机不同 ,但同样需要开启 AAA 服务本地认证。

六、 配置参考

RA 路由器：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
ip multicast-routing
!
!
gbsc group default
!
!
aaa authentication login telnet local
aaa authentication login ssh local
aaa authentication enable default enable
aaa authentication ppp default local
```

```
!
username admin password 0 admin
username telnet password 0 admin
username ssh password 0 admin
enable password 0 123456 level 15
!
!
interface Null0
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.252
 no ip directed-broadcast
 ip dvmrp
!
interface FastEthernet0/3
 ip address 100.1.1.2 255.255.255.0
 no ip directed-broadcast
 ip dvmrp
 vrrp priority 254
 vrrp 1 associate 100.1.1.254 255.255.255.0
!
interface Serial0/1
 ip address 200.1.10.1 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname admin
 ppp chap password 0 admin
 physical-layer speed 64000
 ip dvmrp
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
line vty 0
 login authentication telnet
!
```

```
line vty 1
 login authentication telnet
!
line vty 2
 login authentication telnet
!
line vty 3
 login authentication telnet
!
line vty 4
 login authentication telnet
!
!
ip sshd auth-method ssh
ip sshd enable
!
!
ip route 10.1.10.0 255.255.255.0 100.1.1.3
ip route 11.1.1.0 255.255.255.0 100.1.1.3
ip route 192.168.10.4 255.255.255.252 192.168.10.1
ip route 192.168.10.4 255.255.255.252 200.1.10.2
ip route 192.168.20.0 255.255.255.0 192.168.10.1
!
!
RA_config#
```

RB 路由器：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
ip multicast-routing
!
!
```

```
gbsc group default
!
!
interface Null0
!
interface FastEthernet0/0
 ip address 10.1.10.2 255.255.255.0
 no ip directed-broadcast
 ip dvmrp
!
interface FastEthernet0/3
 ip address 11.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip dvmrp
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
no ip address
 no ip directed-broadcast
!
!
ip route 100.1.1.0 255.255.255.0 10.1.10.1
ip route 192.168.10.0 255.255.255.252 10.1.10.1
ip route 192.168.10.4 255.255.255.252 10.1.10.1
ip route 192.168.20.0 255.255.255.0 10.1.10.1
ip route 200.1.10.0 255.255.255.240 10.1.10.1
!
!
RB#
```

RC 路由器：

```
SHO RUN
Building configuration...

Current configuration:
!
```

```
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
ip multicast-routing
!
!
gbsc group default
!
!
aaa authentication login telnet local
aaa authentication login ssh local
aaa authentication enable default enable
aaa authentication ppp default local
!
username admin password 0 admin
username telnet password 0 admin
username ssh password 0 admin
enable password 0 123456 level 15
!
!
interface Null0
!
interface FastEthernet0/0
 ip address 192.168.10.6 255.255.255.252
 no ip directed-broadcast
 ip dvmrp
!
interface FastEthernet0/3
 ip address 100.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip dvmrp
 vrrp 1 associate 100.1.1.254 255.255.255.0
!
interface Serial0/1
 ip address 200.1.10.2 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp chap password 0 admin
```

```
 ip dvmrp
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
line vty 0
 login authentication telnet
!
line vty 1
 login authentication telnet
!
line vty 2
 login authentication telnet
!
line vty 3
 login authentication telnet
!
line vty 4
 login authentication telnet
!
!
ip sshd auth-method ssh
ip sshd enable
!
!
!
ip route 10.1.10.0 255.255.255.0 100.1.1.3
ip route 11.1.1.0 255.255.255.0 100.1.1.3
ip route 192.168.10.0 255.255.255.252 192.168.10.5
ip route 192.168.10.0 255.255.255.252 200.1.10.1
ip route 192.168.20.0 255.255.255.0 192.168.10.5
!
!
RC_config#
```

SWA 交换机：

```
Vty connection is timed out.
enter any key to start?
SWA>ENA
SWA#SHO RUN
!
no service password-encryption
!
hostname SWA
!
vlan 1
!
vlan 100
!
vlan 300
!
Interface Ethernet0/0/1
 switchport access vlan 300
!
Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
```

```
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 100
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan100
ip dvmrp enable
 ip address 100.1.1.3 255.255.255.0
!
interface Vlan300
 ip dvmrp enable
 ip address 10.1.10.1 255.255.255.0
!
ip dvmrp multicast-routing
!
router vrrp 1
 virtual-ip 100.1.1.254
 interface Vlan100
```

```
 enable
!
ip route 11.1.1.0/24 10.1.10.2
ip route 192.168.10.0/30 10.1.1.254
ip route 192.168.10.0/30 100.1.1.254
ip route 192.168.10.4/30 10.1.1.254
ip route 192.168.10.4/30 100.1.1.254
ip route 192.168.20.0/24 10.1.1.254
ip route 192.168.20.0/24 100.1.1.1
ip route 200.1.10.0/28 10.1.1.254
!
no login
!
end

SWA#
```

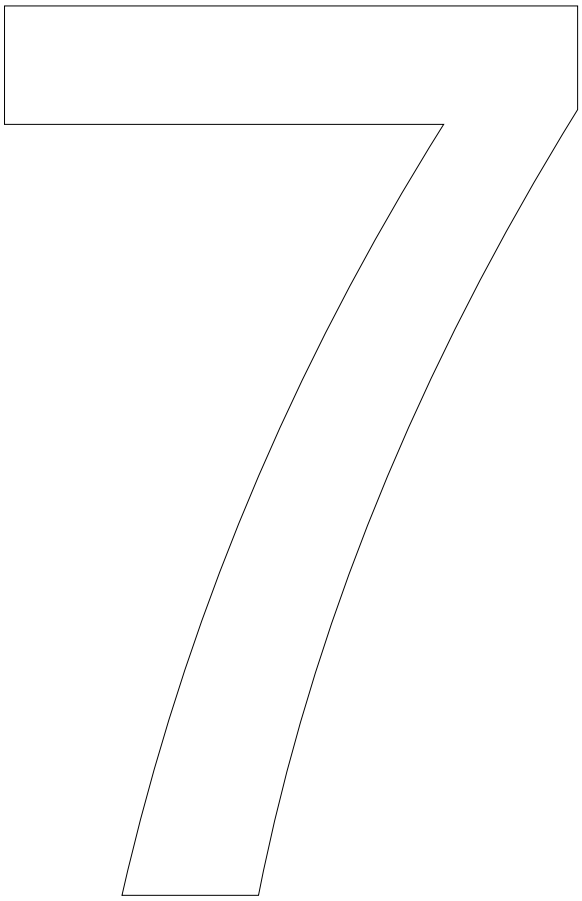
SWB 交换机：

```
sho run
!
no service password-encryption
!
hostname SWB
vendorlocation China
vendorContact 800-810-9119
!
!
!
vlan 1
!
vlan 10
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address 00-0b-cd-4a-97-08
 switchport port-security lock
!
```

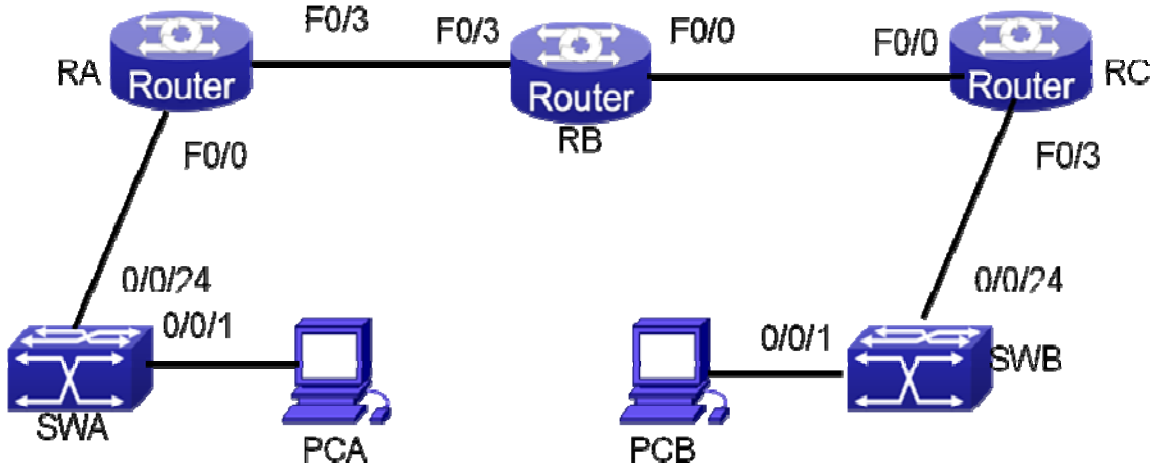
```
Interface Ethernet0/0/2
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address 00-15-58-e9-7c-dd
 switchport port-security lock
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
```

```
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip dvmrp enable
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip dvmrp enable
 ip address 192.168.10.5 255.255.255.252
!
interface Vlan200
 ip dvmrp enable
 ip address 192.168.10.1 255.255.255.252
!
ip dvmrp multicast-routing
!
ip route 10.1.10.0/24 192.168.10.2
ip route 10.1.10.0/24 192.168.10.6
ip route 11.1.1.0/24 192.168.10.2
ip route 11.1.1.0/24 192.168.10.6
ip route 100.1.1.0/24 192.168.10.2
ip route 100.1.1.0/24 192.168.10.6
ip route 200.1.10.0/28 192.168.10.2
ip route 200.1.10.0/28 192.168.10.6
```

```
!
no login
!
end
SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
F0/0	202.106.1.2/24	
F0/3	10.1.10.2/24	
RB		
F0/3	210.216.1.2/24	
F0/0	202.106.1.1/24	
RA		
F0/3	210.216.1.1/24	
F0/0	100.1.1.2/24	
SWA		
VLAN100	0/0/24	100.1.1.1/24
VLAN10	0/0/1-5	192.168.10.1/24
SWB		
VLAN20	0/0/1-3	192.168.20.1/24
VLAN100	0/0/24	10.1.10.1/24
PCA	192.168.10.10/24	

PCB	192.168.20.10/24

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 全网运行 RIPv2 动态路由协议:

A. RA 与 RB 之间开启明文认证；

B. RC 与 SWB 之间开启 MD5 认证

2. RA 与 RC 之间设置 GREoverIPsecVPN：

A. IPSEC VPN 为传输模式，

B. RA 与 RB 之间 IKE 方式协商安全联盟，主动模式；

C. IKE 策略采用 md5 hash 算法；

D. transform-set（协议变换集）名称为 lin，加密验证方式为：ah-sha-hmac、esp-des，共享密钥为：1234567

E. 加密映射表进行协商的安全联盟的生命周期为 86400 秒；

F. GRE 最大传输单元为 1476

3. 在 SWA 上的端口 e0/0/2 上，将属于 PCA 的报文带宽限制为 10M 比特/秒，突发值设为 4M 字节，超过带宽的该网段内的报文一律丢弃

4. SWB 上设置 enable 密码，telnat、web 服务与其用户名密码

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec
查看隧道情况
Show ip int tunnel

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 rip 路由协议状态，能够看到所使用的版本等信息
Show ip rip protocol
查看 rip 验证信息，需进入端口，能够看到端口所开启的 rip 认证种类及口令
Show ip rip interface
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证服务质量

查看 QoS 端口信息
Show mls qos interface
也可以设置一个 FTP 服务器，在 FTP server 端放置文件大小约为 14M 的测试文件，在端口应用 QOS 策略前后观察客户端下载同一文件所用时间，直观观察速率变化

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；

B. 配置变换集；
C. 创建策略表；
D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。

2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. GREoverIPsecVPN 注意：先配置 GRE，然后再将 IPsec 绑定在 GRE 的隧道端口中。

六、 配置参考

RA 路由器：

```
show run
RA#show running-config
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
ip fast-switch enable
!
gbsc group default
!
!
crypto isakmp key digitalchina 202.106.1.2 255.255.255.255
!
!
crypto isakmp policy 1
 group 2
 lifetime 36000
!
crypto ipsec transform-set one
```

```
 transform-type ah-sha-hmac esp-des
!
crypto map pp 1 ipsec-isakmp
 set peer 202.106.1.2
 set pfs group2
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface Tunnel0
 mtu 1476
 ip address 1.1.1.1 255.255.255.0
 no ip directed-broadcast
 crypto map pp
 tunnel source 210.216.1.1
 tunnel destination 202.106.1.2
!
interface FastEthernet0/0
 ip address 100.1.1.2 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 210.216.1.1 255.255.255.0
 no ip directed-broadcast
 ip rip authentication simple
 ip rip password panpan
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
```

```
 no auto-summary
 network 210.216.1.0 255.255.255.0
 network 100.1.1.0 255.255.255.0
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RA#
```

RB 路由器：

```
show run
RB#show running-config
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 202.106.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 210.216.1.2 255.255.255.0
 no ip directed-broadcast
 ip rip authentication simple
 ip rip password panpan
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
```

```
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 210.216.1.0 255.255.255.0
 network 202.106.1.0 255.255.255.0
!
!
RB#
```

RC 路由器：

```
RC#show running-config
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
ip fast-switch enable
!
gbsc group default
!
!
crypto isakmp key digitalchina 210.216.1.1 255.255.255.255
!
!
crypto isakmp policy 1
```

```
 group 2
 lifetime 36000
!
crypto ipsec transform-set one
 transform-type ah-sha-hmac esp-des
!
crypto map pp 1 ipsec-isakmp
 set peer 210.216.1.1
 set pfs group2
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface Tunnel0
 mtu 1476
 ip address 1.1.1.2 255.255.255.0
 no ip directed-broadcast
 crypto map pp
 tunnel source 202.106.1.2
 tunnel destination 210.216.1.1
!
interface FastEthernet0/0
 ip address 202.106.1.2 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 10.1.10.2 255.255.255.0
 no ip directed-broadcast
 ip rip authentication message-digest
 ip rip message-digest-key 1 md5 123
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
```

```
!
!
router rip
 version 2
 no auto-summary
 network 202.106.1.0 255.255.255.0
 network 10.1.10.0 255.255.255.0
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RC#
```

SWA 交换机：

```
SWA#show run
SWA#show running-config
!
no service password-encryption
!
hostname SWA
vendorlocation China
vendorContact 800-810-9119
!
!
!
vlan 1
!
vlan 10
!
vlan 100
!
firewall enable
!
ip access-list extended qos_acl
   permit ip any-source any-destination
!
mls qos
class-map qos_class
 match access-group qos_acl
!
```

```
policy-map qos_policy
 class qos_class
  police 10024 4096 exceed-action drop
 exit
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
Interface Ethernet0/0/2
 service-policy input qos_policy
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
```

```
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan100
 ip address 100.1.1.1 255.255.255.0
!
router rip
 network 100.1.1.0/24
 network 192.168.10.0/24
!
no login
!
end
SWA#
```

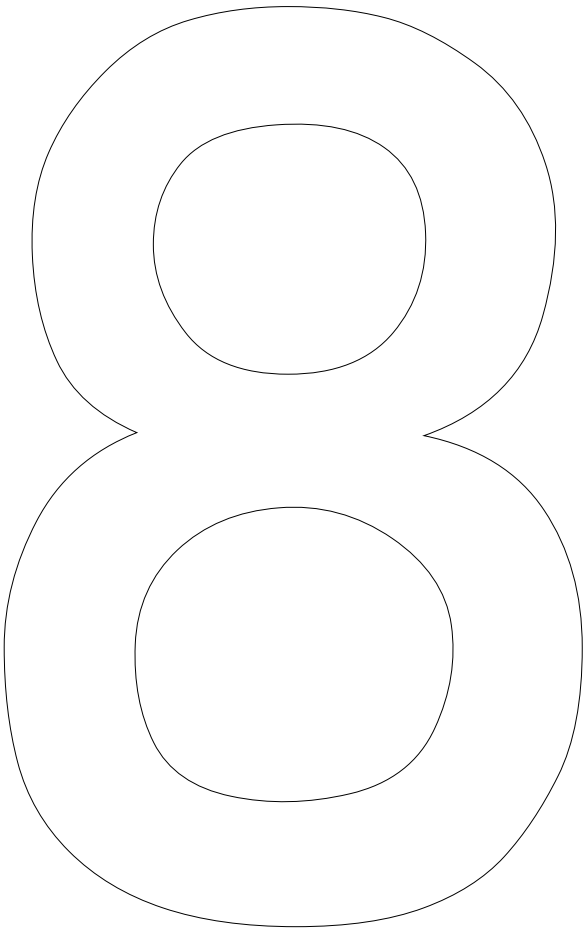
SWB 交换机：

```
SWB#show running-config
```

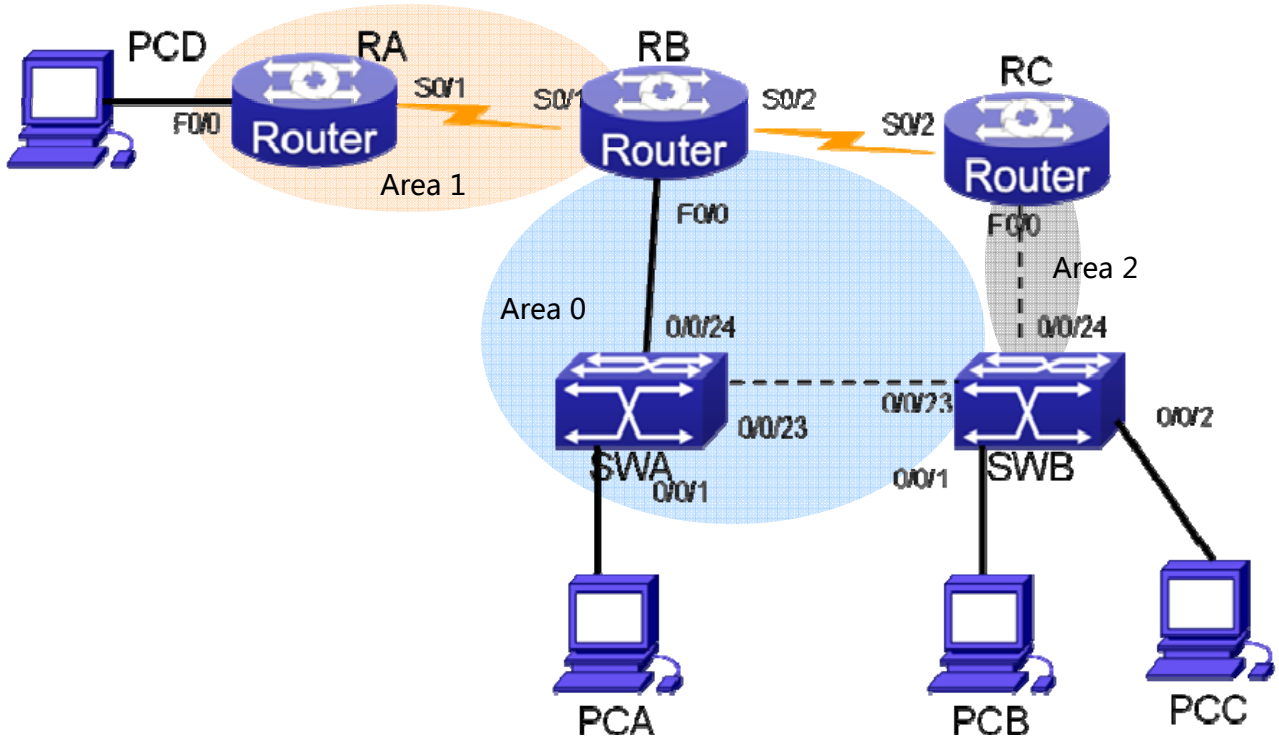
```
!
no service password-encryption
!
hostname SWB
vendorlocation China
vendorContact 800-810-9119
!
!
ip http server
web-user aaa password 0 aaa
web-user panpan password 0 admin
web-user admin password 0 admin
!
telnet-user admin password 0 admin
!
!
vlan 1
!
vlan 20
!
vlan 100
!
Interface Ethernet0/0/1
 switchport access vlan 20
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
 switchport access vlan 20
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
```

```
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
key chain 1
 key 123
!
interface Vlan20
```

```
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip rip authentication mode md5
 ip rip authentication key-chain 1
 ip address 10.1.10.1 255.255.255.0
!
router rip
 network 10.1.10.0/24
 network 192.168.20.0/24
!
no login
!
end
SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC	
S0/2	202.106.1.2/28
F0/0	192.168.1.1/24
RB	
S0/1	210.216.1.2/28
S0/2	202.106.1.1/28
F0/0	10.1.1.1/24
RA	
S0/1	210.216.1.1/28
F0/0	192.168.10.1/24
SWA	

VLAN300	0/0/24	10.1.1.2/24
VLAN30	0/0/1-5	192.168.30.1/24
VLAN100	0/0/23	101.1.1.1/30；
SWB		
VLAN20	0/0/1-2	192.168.20.1/24
VLAN 200	0/0/24	192.168.1.2/24
VLAN100	0/0/23	101.1.1.2/30
PCA		
PCB		
PCC		
PCD	192.168.10.2/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 在 RA-RB-RC 链路上使用 hdlc 协议
2. 在 RC 与 RB 之间配置 IPsecVPN ,RA 与 RB 之间运行 GRE VPN
3. 全网运行多区域 ospf 动态路由协议
4. 在 SWB 上设置 DHCP 服务：
   A. 为 PCB、PCC 分配 IP 地址；
   B. 在 SWA 上设置 DHCP 中继服务，为 PCA 分配 IP 地址
5. 在交换机上划分相应的 VLAN，并将端口加入，SWB 的 PCC 端口可以监听 PCB 端口的所有进入的数据。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec

3. 验证 HDLC 连接

查看端口状态，可以显示出当前串行链路接口所使用的封装协议，以及当前链路状态
Show interface ser0/1
查看 HDLC 数据连接过程
debug hdlc packet

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、route id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证 DHCP 服务

查看 DHCP 服务器的地址分配情况、连接信息等
show ip dhcp server statistics
查看 DHCP 服务分配 IP 地址的过程
debug ip dhcp server packets
查看 DHCP 中继的转发过程
debug ip dhcp relay packet

也可以直接在 PC 上观察是否正确的获得 TCP 信息

6. 验证端口镜像

可以在 PCC 上安装抓包软件，再重其他设备向 PCB 发送信息，观察 PCC 所在的端口是否将数据转发过来。

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
   E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。
2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. DHCP 注意配置好为不同网段分发的 IP。
5. OSPF 注意声明好直链网段和区域 ID，认证的时候注意两端的加密密钥要一致。
6. VPN 要注意两端的加密算法要一致，注意把做完的加密映射表绑定到端口。
7. 配置 DHCP 中继时，注意在全局模式开启转发协议，否则无法配置 DHCP 中继。
8. DHCP 中继的 helper-address 的地址要指向正确，是 SWA 与 SWB 所直连的端口 IP 地址。
9. 在 SWA 需要中继的端口注意配置 IP 地址，此 IP 地址为 PC 自动获得的 IP 地址的网关
10. 在 SWA 的下发 IP 地址的端口配置 DHCP 中继，在其他端口配置无效
11. 若长时间无法获得 IP 地址 ,且配置没有错误 ,可在 DHCP 服务器配置一跳指向 PCA 网段的静态路由（不推荐）

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
```

```
!
hostname RA
!
!
gbsc group default
!
!
interface Tunnel0
 mtu 1476
 ip address 1.1.1.2 255.255.255.0
 no ip directed-broadcast
 tunnel source 210.216.1.1
 tunnel destination 210.216.1.2
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 210.216.1.1 255.255.255.240
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 192.168.10.0 255.255.255.0 area 1
 network 210.216.1.0 255.255.255.240 area 1
!
!
RA#
```

RB 路由器：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!

!
crypto isakmp key digitalchina 202.106.1.2 255.255.255.255
!
!
crypto isakmp policy 10
 group 2
 lifetime 36000
!
crypto ipsec transform-set one
 transform-type ah-sha-hmac esp-des
!
crypto map pp 10 ipsec-isakmp
 set peer 202.106.1.2
 set pfs group2
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface Tunnel0
 mtu 1476
 ip address 1.1.1.1 255.255.255.0
 no ip directed-broadcast
 tunnel source 210.216.1.2
 tunnel destination 210.216.1.1
!
interface FastEthernet0/0
```

```
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 210.216.1.2 255.255.255.240
 no ip directed-broadcast
 physical-layer speed 64000
!
interface Serial0/2
 ip address 202.106.1.1 255.255.255.240
 no ip directed-broadcast
 crypto map pp
 physical-layer speed 64000
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 210.216.1.0 255.255.255.240 area 1
 network 202.106.1.0 255.255.255.240 area 0
 network 10.1.1.0 255.255.255.0 area 0
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RB#
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
```

```
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
crypto isakmp key digitalchina 202.106.1.1 255.255.255.255
!
!
crypto isakmp policy 10
 group 2
 lifetime 36000
!
crypto ipsec transform-set one
 transform-type ah-sha-hmac esp-des
!
crypto map pp 10 ipsec-isakmp
 set peer 202.106.1.1
 set pfs group2
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
 crypto map pp
```

```
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 202.106.1.0 255.255.255.240 area 0
 network 192.168.1.0 255.255.255.0 area 2
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
vendorlocation China
vendorContact 800-810-9119
!
!
service dhcp
!
ip forward-protocol udp bootps
!

vlan 1
!
vlan 30
!
vlan 100
!
vlan 300
!
no ip forwarding
!
Interface Ethernet0/0/1
```

```
 switchport access vlan 30
!
Interface Ethernet0/0/2
 switchport access vlan 30
!
Interface Ethernet0/0/3
 switchport access vlan 30
!
Interface Ethernet0/0/4
 switchport access vlan 30
!
Interface Ethernet0/0/5
 switchport access vlan 30
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
```

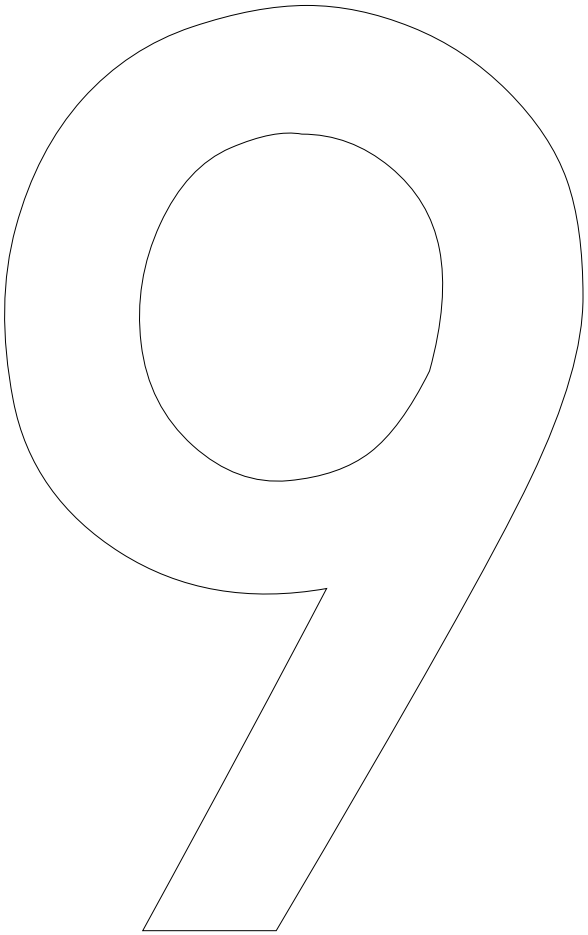
```
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
 ip dhcp snooping trust
!
Interface Ethernet0/0/24
 switchport access vlan 300
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan30
ip address 192.168.30.1 255.0.0.0
   !forward protocol udp 68(active)!
    ip helper-address 101.1.1.2
!
interface Vlan100
 ip address 101.1.1.1 255.255.255.252
!
interface Vlan300
 ip address 10.1.1.2 255.255.255.0
!
ip igmp snooping
!
router ospf 10
 network 10.1.1.0 0.0.0.255 area 0
 network 101.1.1.0 0.0.0.3 area 0
!
!
no login
!
end

SWA#
```

SWB 交换机：

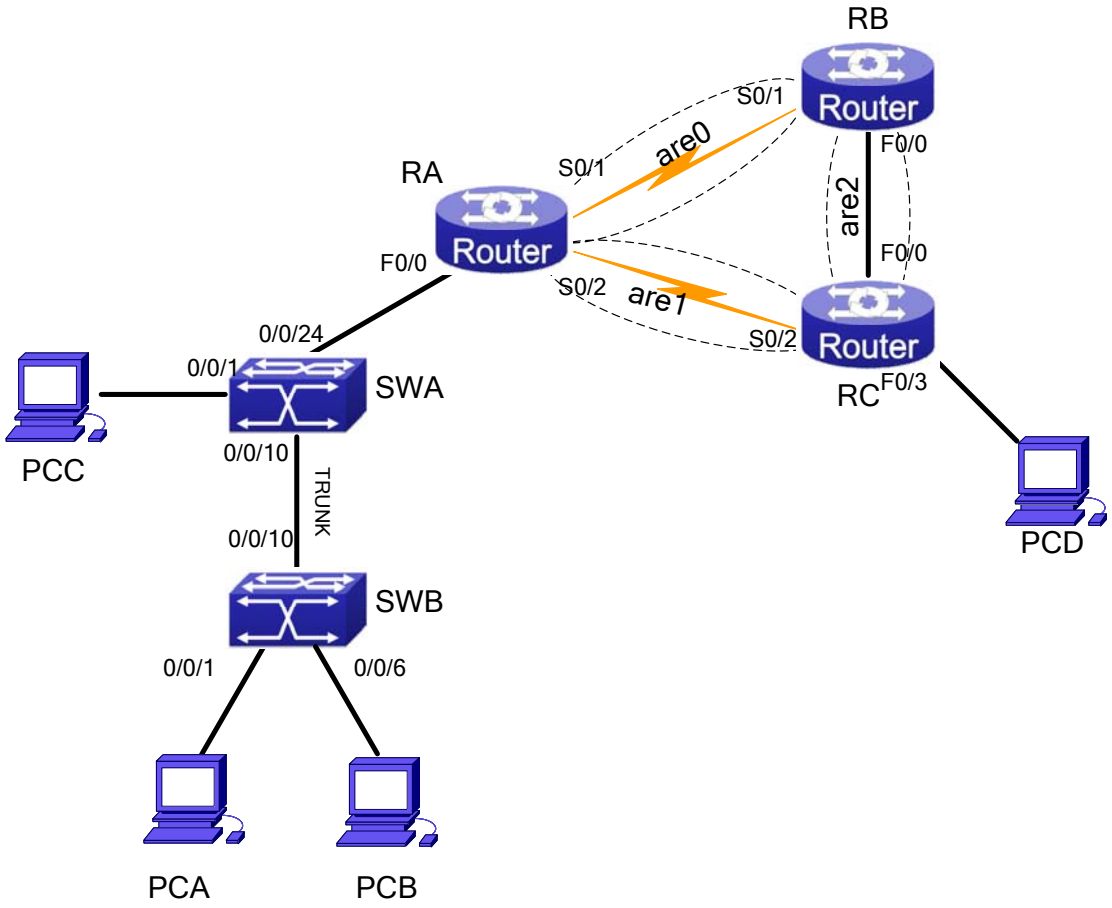
```
SWB#sho run
!
no service password-encryption
!
hostname SWB
!
service dhcp
!
ip dhcp pool pool-A
 network-address 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 202.106.0.20
!
ip dhcp pool pool-B
 network-address 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 202.106.0.20
!
monitor session 1 source interface Ethernet0/0/1 rx
monitor session 1 source interface Ethernet0/0/1 tx
monitor session 1 destination interface Ethernet0/0/2
!
vlan 1
!
lan 20
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
 switchport access vlan 20
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
```

```
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
nterface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
```

```
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip address 101.1.1.2 255.255.255.252
!
Interface Vlan200
 ip address 192.168.1.2 255.255.255.0
!
router ospf 10
 network 101.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 2
 network 192.168.20.0 0.0.0.255 area 0
!
!
no login
!
end

SWB#
```



一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC	
S0/2	184.11.1.2/28
F0/0	210.11.10.2/28
F0/3	192.168.100.254/24
RB	
S0/1	202.106.1.2/28
F0/0	210.11.10.1/28
RA	
S0/1	202.106.1.1/28

S0/2	184.11.1.1/28	
F0/0	172.168.1.1/24	
SWA		
VLAN88	0/0/24	172.168.1.2/24
VLAN10	0/0/1-5	192.168.10.254/24
VLAN20	0/0/6-9	192.168.20.254/24
VLAN30	0/0/11-15	192.168.30.254/24
SWB		
VLAN10	0/0/1-5	
VLAN20	0/0/6-10	
PCA	192.168.10.1/24	
PCB	192.168.20.254/24	
PCC	192.168.30.1/24	
PCD	192.168.100.2/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 在 RA、RB、RC 间采用多区域 ospf：

A. RA 与 RB 采用明文认证；

B. RA 与 RC 采用 md5 方法认证

2. RA、RB、RC 间采用 PPP 封装协议：

A. RA 与 RB 之间采用 chap 认证，用户名分别为 chapra、 chaprb；密码均为 digitalchina

B. RA 与 RC 之间采用 pap 双向认证，用户名分别为 papra paprb；密码均为 digitalchina

3. 在 RA 上配置 NAT，使内网用户可以访问互联网：

A. 将所有的内网用户地址转换为 RA 的 S0/1、S0/2 端口的 IP 地址；

B. 但将 PCC 地址转换为 202.106.1.3/28

4. 内网采用静态路由，使之相互通信。
5. 在 SWA 与 SWB 之间配置生成树协议；
   A. 使 SWA 设置成根网桥。
6. 在 RA 上配置策略路由：
   A. 使属于 Vlan10 的数据通过 RA-RB-RC 线路传输；
   B. 属于 Vlan20 的数据通过 RA-RC 线路传输。
7. 在 RB 与 RC 之间配置 IP SEC VPN：
   A. RC 与 RB 之间 IKE 方式协商安全联盟，主动模式；
   B. IKE 策略采用 md5 hash 算法；
   C. transform-set（协议变换集）名称为 one，加密验证方式为：ah-sha-hmac、esp-des，共享密钥为：key
   D. 加密映射表进行协商的安全联盟的生命周期为 36000 秒

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证策略路由

可使用 show running-config 进行配置查看，也可使用 taceroute 命令在 PC 机上进行验证，若正确会遵循题目要求中的线路进行路由，若不正确则会走另外一条线路。（必须在全网互通的前提下）
在网络设备上可以使用 tracert 命令进行数据路由的查看。

6. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需要先通信）
show ip nat translations

7. 验证生成树协议

查看生成树状态，可查看到交换机生成树状态，以及每个端口的转发状态、BID 等信息
Show spanning-tree

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；

E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。

2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. OSPF 注意声明好直链网段和区域 ID，认证的时候注意两端的加密密钥要一致。
5. VPN 要注意两端的加密算法要一致，注意把做完的加密映射表绑定到端口。
6. 配置策略路由需要先建立访问列表，或者用已有的也可以，在建立 route-map 里面指明下一跳，在调用先前建立好的访问列表，最后绑定到端口上。

六、 配置参考

RA 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp wanpap local
aaa authentication ppp wanchap local
!
username paprc password 0 digitalchina
username chaprb password 0 digitalchina
!
!
interface FastEthernet0/0
 ip address 172.168.1.1 255.255.255.0
```

```
 no ip directed-broadcast
 priority-group 1
 ip policy route-map wan
 ip nat inside
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 210.106.1.1 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap wanchap
 ppp chap hostname chapra
 ppp chap password 0 digitalchina
 physical-layer speed 64000
 ip ospf authentication simple
 ip ospf password wan
 ip nat outside
!
interface Serial0/2
 ip address 184.11.1.1 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap wanpap
 ppp pap sent-username papra password 0 digitalchina
 physical-layer speed 64000
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 wan
 ip nat outside
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
```

```
 network 210.106.1.0 255.255.255.240 area 0
 network 184.11.1.0 255.255.255.240 area 1
 area 184.11.1.0 authentication message-digest
 area 210.106.1.0 authentication simple
!
!
ip route 192.168.10.0 255.255.255.0 172.168.1.2
ip route 192.168.20.0 255.255.255.0 172.168.1.2
ip route 192.168.30.0 255.255.255.0 172.168.1.2
!
!
ip access-list standard acl10
 permit 192.168.10.0 255.255.255.0
 deny     any
!
ip access-list standard acl20
 permit 192.168.20.0 255.255.255.0
!
ip access-list standard wan
 permit any
!
!
route-map wan 1 permit
 match ip address acl10
 match ip next-hop 202.106.1.2
!
route-map wan 2 permit
 match ip address acl20
 match ip next-hop 184.11.1.2
!
!
ip nat outside destination static 202.106.1.3 192.168.30.1
ip nat inside source list wan interface Serial0/1
ip nat inside source list wan interface Serial0/2
!
!
RA_config#
```

RB 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp wanchap local
!
username chapra password 0 digitalchina
!
crypto isakmp key key 210.11.10.2 255.255.255.255
!
!
crypto isakmp policy 1
hash md5
!
crypto ipsec transform-set one
 transform-type ah-sha-hmac esp-des
!
crypto map pp 1 ipsec-isakmp
 set peer 210.11.10.2
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface FastEthernet0/0
 ip address 210.11.10.1 255.255.255.240
```

```
 no ip directed-broadcast
 crypto map pp
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap wanchap
 ppp chap hostname chaprb
 ppp chap password 0 digitalchina
 ip ospf authentication simple
 ip ospf password wan
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 202.106.1.0 255.255.255.240 area 0
 network 210.11.10.0 255.255.255.240 area 2
 area 202.106.1.0 authentication simple
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RB_config#
```

RC 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication ppp wanpap local
!
username papra password 0 digitalchina
!
crypto isakmp key key 210.11.10.1 255.255.255.0
!
!
crypto isakmp policy 1
hash md5
!
crypto ipsec transform-set one
 transform-type ah-sha-hmac esp-des
!
crypto map pp 1 ipsec-isakmp
 set peer 210.11.10.1
 set security-association lifetime seconds 36000
 set transform-set one
 match address vpn_acl
!
!
interface FastEthernet0/0
```

```
 ip address 210.11.10.2 255.255.255.240
 no ip directed-broadcast
 crypto map pp
!
interface FastEthernet0/3
 ip address 192.168.100.254 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 184.11.1.2 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap wanpap
 ppp pap sent-username paprc password 0 digitalchina
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 wan
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 184.11.1.0 255.255.255.240 area 1
 network 210.11.10.0 255.255.255.240 area 2
 network 192.168.100.0 255.255.255.0 area 2
 area 184.11.1.0 authentication message-digest
!
!
ip access-list extended vpn_acl
 permit ip any any
!
!
RC_config#
```

SWA 交换机：

```
SHO RUN
!
no service password-encryption
!
hostname SWA
!
spanning-tree
spanning-tree mst 0 priority 4096
!
vlan 1
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 88
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
Interface Ethernet0/0/2
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 20
!
```

```
Interface Ethernet0/0/7
 switchport access vlan 20
!
Interface Ethernet0/0/8
 switchport access vlan 20
!
Interface Ethernet0/0/9
 switchport access vlan 20
!
Interface Ethernet0/0/10
 switchport mode trunk
!
Interface Ethernet0/0/11
 switchport access vlan 30
!
Interface Ethernet0/0/12
 switchport access vlan 30
!
Interface Ethernet0/0/13
 switchport access vlan 30
!
Interface Ethernet0/0/14
 switchport access vlan 30
!
Interface Ethernet0/0/15
 switchport access vlan 30
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface thernet0/0/20
!
Interface Ethernet0/0/21
```

```
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 88
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
!
interface Vlan88
 ip address 172.168.1.2 255.255.255.0
!
ip route 0.0.0.0/0 172.168.1.1
!
no login
!
end

SWA#
```

SWB 路由器：

```
SWB#
```

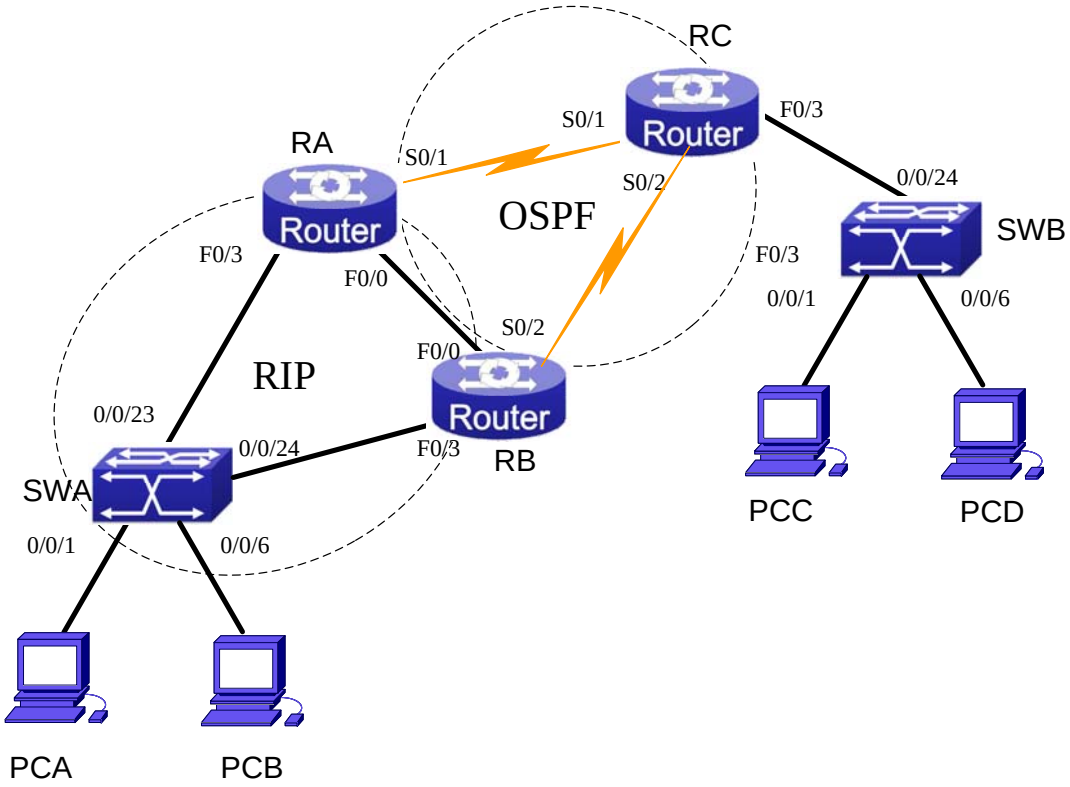
```
!
no service password-encryption
!
hostname SWB
!
spanning-tree
!
vlan 1
!
vlan 10
!
vlan 20
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
Interface Ethernet0/0/2
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10!Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 20
!
Interface Ethernet0/0/7
 switchport access vlan 20
!
Interface Ethernet0/0/8
 switchport access vlan 20
!
Interface Ethernet0/0/9
 switchport access vlan 20
!
```

```
Interface Ethernet0/0/10
 switchport mode trunk
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface thernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
!
Interface Ithernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
```

```
!
no login
!
end

SWB#
```

10

一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC	
S0/1	202.106.10.2/24
S0/2	202.106.20.2/24
F0/3	10.1.1.1/24
RB	
S0/2	202.106.20.1/24
F0/0	192.168.1.2/24
F0/3	172.16.1.253/24

RA		
S0/1	202.106.10.1/24	
F0/3	172.16.1.252/24	
F0/0	192.168.1.1/24	
SWA		
VLAN10	0/0/23-24	172.16.1.250/24
VLAN20	0/0/1-5	172.16.10.254/24
VLAN30	0/0/6-10	172.16.20.254/24
SWB		
VLAN40	0/0/24	10.1.1.2/24
VLAN50	0/0/1-5	10.1.10.254/24
VLAN60	0/0/6-10	10.1.20.254/24
PCA	172.16.10.1/24	
PCB	172.16.20.1/24	
PCC	10.1.10.1/24	
PCD	10.1.20.1/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 路由器配置单区域 OSPF 动态路由协议,使全网络能够相互通信：

RB 与 RC 之间采用 ospf md5 验证

2. 路由器相互之间采用 GRE 封装，并进行 OSPF 宣告,

隧道 ip：RA 配置 Tunnel 1,对应 S0/1：20.1.1.1/30

RC 配置 Tunnel 2，对应 S0/1：20.1.1.2/30

RB 配置 Tunnet 3，对应 s0/2：20.1.2.1/30

RC 配置 Tunnel 4，对应 S0/2：20.1.2.2/30

3. 在 RA 与 RB 之间配置 vrrp 协议：

A. 其虚拟 ip 为 172.16.1.254/24；
B. 开启跟踪端口；
C. 优先级递减为 20。

4. 在 RA 与 RC 之间配置 PPP 链路封装：

采用 chap 单向验证，RA 为主验证方,

5. 在 SWA 上配置端口镜像：

要求在 E0/0/1 能够坚挺 E0/0/6 上的所有数据。

6. 在 SWA 上配置 E0/0/7-8 端口为 10M 半双工

7. 在 SWA 上配置端口安全：

过滤掉 PCB 的 mac，使用 MAC 地址表的方法

8. 在 SWB 上配置时间访问控制列表：

要求 PCD 在工作日 9:00 到 17:00 可以连接互联网

9. 在 RC 上配置网络地址转换 ,使内网用户可以连接互联网：

使用端口转换，将内网所有 IP 地址转换为 s0/1 与 s0/2

10. 在 RA、RB、SWA 之间配置 RIPv2 动态路由协议

在 RA 与 RB 上配置路由再发布，使内网可与互联网进行通信

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示以建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 rip 路由协议状态，能够看到所使用的版本等信息
Show ip rip protocol
也可在 PC 上使用 Ping 命令进行链路连通性的测试。
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router-id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证策略路由

可使用 show running-config 进行配置查看，也可使用 taceroute 命令在 PC 机上进行验证，若正确会遵循题目要求中的线路进行路由，若不正确则会走另外一条线路。（必须在全网互通的前提下）
在网络设备上可以使用 tracert 命令进行数据路由的查看。

6. 验证 VRRP

查看本设备 VRRP 运行状况,配置成功会出现本台设备 vrp 的相关信息，如主次关系、优先级、虚拟 ip、对端 ip 等信息
Show vrrp detail
查看 vrrp 协商主次关系过程（须在配置 VRRP 前配置）
debug vrrp

7. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请

先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需要先通信）
show ip nat translations

8. 验证访问控制列表

查看访问控制类表的配置
Show ip access-list lin
PC 之间相互 ping 命令也可验证访问控制列表是否成功。

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
   E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。
2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. 时间访问列表，注意配置完后要修改交换机的 COLCK，或者 NTP 服务器。
5. OSPF 注意声明好直链网段和区域 ID，认证的时候注意两端的加密密钥要一致。
6. VPN 要注意两端的加密算法要一致，注意把做完的加密映射表绑定到端口。
7. 配置策略路由需要先建立访问列表，或者用已有的也可以，在建立 route-map 里面指明下一跳，在调用先前建立好的访问列表，最后绑定到端口上。
8. GRE 封装时注意配置虚拟端口时候源与目的。
9. 配置 VRRP 注意虚拟 IP 的统一和虚拟组的统一。

六、 配置参考

RA 路由器：

RA#sho run
正在收集配置...
当前配置:
!
!version 1.3.3F
service timestamps log date

```
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp lin local
!
username RC password 0 123546
!
!
interface Tunnel1
 mtu 1476
 ip address 20.1.1.1 255.255.255.252
 no ip directed-broadcast
 tunnel source 202.106.10.1
 tunnel destination 202.106.10.2
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 172.16.1.252 255.255.255.0
 no ip directed-broadcast
 vrrp 1 associate 172.16.1.254 255.255.255.0
 vrrp 1 track interface Serial0/1 20
!
interface Serial0/1
 ip address 202.106.10.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap lin
 ppp chap hostname RA
 ppp chap password 0 123456
```

```
 physical-layer speed 64000
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 172.16.0.0
 redistribute ospf 1
 redistribute connect
!
router ospf 1
 network 192.168.1.0 255.255.255.0 area 0
 network 20.1.1.0 255.255.255.252 area 0
 redistribute rip
 redistribute connect
!
!
```

RB 路由器：

```
RA#
RB#sho run
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
```

```
!
!
gbsc group default
!
!
interface Tunnel3
 mtu 1476
 ip address 20.1.2.1 255.255.255.252
 no ip directed-broadcast
 tunnel source 202.106.20.1
 tunnel destination 202.106.20.2
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 172.16.1.253 255.255.255.0
 no ip directed-broadcast
 duplex half
 vrrp 1 associate 172.16.1.254 255.255.255.0
 vrrp 1 priority 90
 vrrp 1 track interface Serial0/2 20
!
interface Serial0/2
 ip address 202.106.20.1 255.255.255.0
 no ip directed-broadcast
 physical-layer speed 64000
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 lin
!
!
router rip
 version 2
 no auto-summary
 network 172.16.0.0
 redistribute ospf 1
 redistribute connect
```

```
!
router ospf 1
 network 192.168.1.0 255.255.255.0 area 0
 network 20.1.2.0 255.255.255.252 area 0
 area 202.106.20.0 authentication message-digest
 redistribute rip
 redistribute connect
!
!
RB#
```

RC 路由器：

```
RC#sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication ppp default local
!
username RA password 0 123546
!
!
!
interface Tunnel2
 mtu 1476
 ip address 20.1.1.2 255.255.255.252
 no ip directed-broadcast
 tunnel source 202.106.10.2
```

```
 tunnel destination 202.106.10.1
!
interface Tunnel4
 mtu 1476
 ip address 20.1.2.2 255.255.255.252
 no ip directed-broadcast
 tunnel source 202.106.20.2
 tunnel destination 202.106.20.1
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0/1
 ip address 202.106.10.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp chap hostname RC
 ppp chap password 0 123456
 ip nat outside
!
interface Serial0/2
 ip address 202.106.20.2 255.255.255.0
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 lin
 ip nat outside
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
```

```
router ospf 1
 network 20.1.1.0 255.255.255.252 area 0
 network 20.1.2.0 255.255.255.252 area 0
 area 202.106.20.0 authentication message-digest
!
!
ip route 10.1.10.0 255.255.255.0 10.1.1.2
ip route 10.1.20.0 255.255.255.0 10.1.1.2
!
!
ip access-list standard lin
 permit 10.1.10.0 255.255.255.0
 permit 10.1.20.0 255.255.255.0
!
!
ip nat inside source list lin interface Serial0/1
ip nat inside source list lin interface Serial0/2
!
!
!
RC#
```

SWA 交换机：

```
SWA#sho run
!
no service password-encryption
!
hostname SWA
!
monitor session 1 source interface Ethernet0/0/6 rx
monitor session 1 source interface Ethernet0/0/6 tx
monitor session 1 destination interface Ethernet0/0/1
!
vlan 1
!
vlan 10
!
vlan 20
!
```

```
vlan 30
!
Interface Ethernet0/0/1
 switchport access vlan 20
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface thernet0/0/3
 switchport access vlan 20
!
Interface Ethernet0/0/4
 switchport access vlan 20
!
Interface Ethernet0/0/5
 switchport access vlan 20
!
Interface Ethernet0/0/6
 switchport access vlan 30
!
Interface Ethernet0/0/7
 speed-duplex force10-half
 switchport access vlan 30
!
Interface Ethernet0/0/8
 speed-duplex force10-half
 switchport access vlan 30
!
Interface Ethernet0/0/9
 switchport access vlan 30
!
Interface Ethernet0/0/10
 switchport access vlan 30!Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
```

```
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ithernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 10
!
Interface Ethernet0/0/24
 switchport access vlan 10
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 172.16.1.250 255.255.255.0
!
interface Vlan20
 ip address 172.16.10.254 255.255.255.0
!
```

```
interface Vlan30
 ip address 172.16.20.254 255.255.255.0
!
mac-address-table blackhole address aa-bb-cc-dd-ee-ff vlan 30
!
router rip
 network 172.16.1.0/24
 network 172.16.10.0/24
 network 172.16.20.0/24
!
no login
!
end

SWA#
```

SWB 交换机：

```
sho run
!
no service password-encryption
!
hostname SWB
!
vlan 1
!
vlan 40
!
vlan 50
!
vlan 60
!
time-range lin
 periodic weekdays 9:0:0 to 17:0:0
!
firewall enable
!
ip access-list extended lin
   permit ip 10.1.10.0 0.0.0.255 10.1.20.0 0.0.0.255
   deny ip 10.1.10.0 0.0.0.255 any-destination time-range lin
```

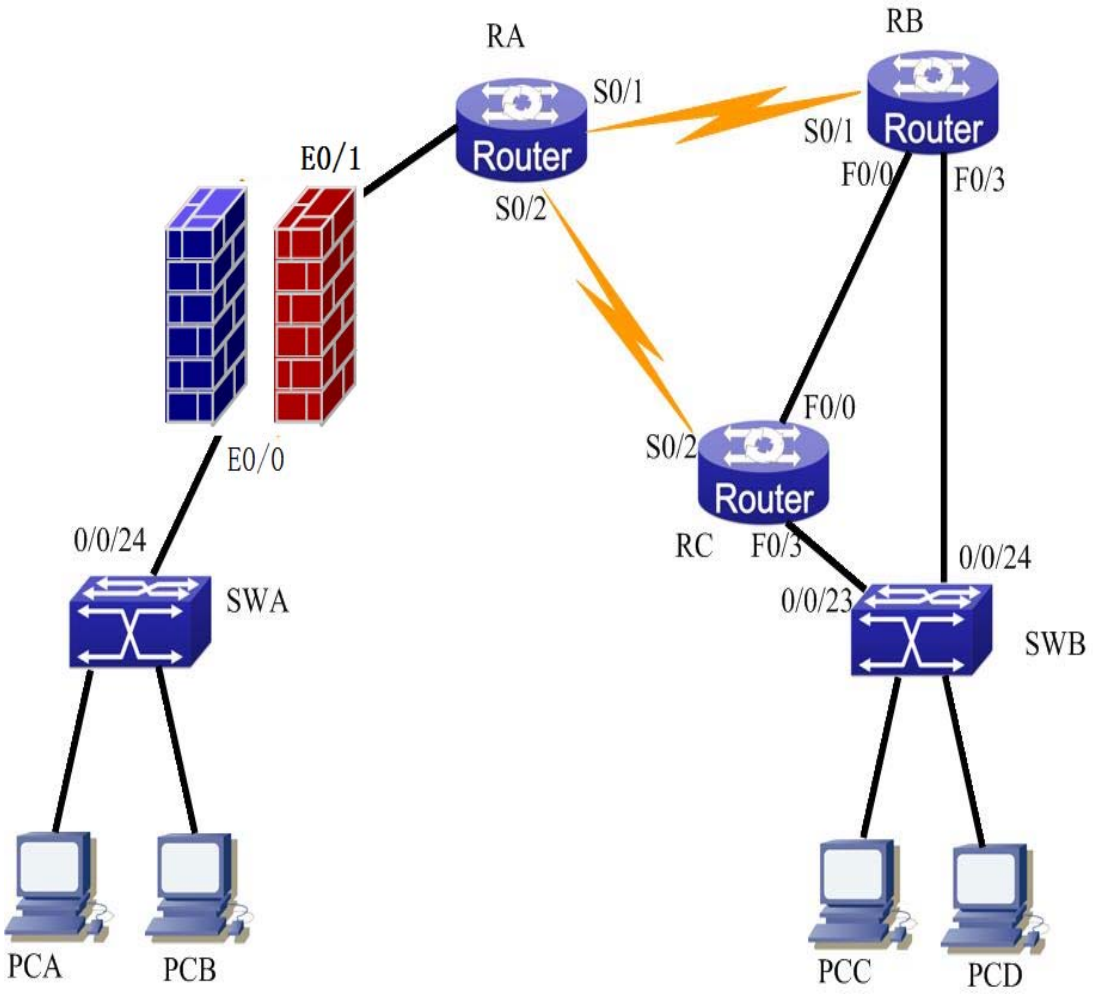
```
!
Interface Ethernet0/0/1
 switchport access vlan 50
!
Interface Ethernet0/0/2
 switchport access vlan 50
!
Interface Ethernet0/0/3
 switchport access vlan 50
!
Interface Ethernet0/0/4
 switchport access vlan 50
!
Interface Ethernet0/0/5
 switchport access vlan 50
!
Interface Ethernet0/0/6
 ip access-group lin in
 switchport access vlan 60
!
Interface Ethernet0/0/7
 switchport access vlan 60
!
Interface Ethernet0/0/8
 switchport access vlan 60
!
Interface Ithernet0/0/9
 switchport access vlan 60
!
Interface Ethernet0/0/10
 switchport access vlan 60
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
```

```
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 40
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan40
 ip address 10.1.1.2 255.255.255.0
!
interface Vlan50
 ip address 10.1.10.254 255.255.255.0
!
interface Vlan60
```

```
 ip address 10.1.20.254 255.255.255.0
!
ip route 0.0.0.0/0 10.1.1.1
!
no login
!
end

SWB#
```

11

一、拓扑图


RA
RB
S0/1
S0/1
Router
Router
E0/1
F0/0
F0/3
S0/2
F0/0
S0/2
Router
E0/0
RC
F0/3
0/0/24
0/0/24
0/0/23
SWA
SWB
PCA
PCB
PCC
PCD

二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

1 台防火墙 DCFW-1800S-V2

4 台 PC 电脑

2. IP 地址规划

RC		
S0/2	216.10.11.2/28	
F0/0	172.16.1.1/24	
F0/3	10.1.1.252/24	
RB		
S0/1	119.255.1.24/28	
F0/0	172.16.1.2/24	
F0/3	10.1.1.253/24	
RA		
S0/1	119.255.1.23/28	
S0/2	216.10.11.1/28	
F0/0	202.106.1.2/28	
SWA		
VLAN10	0/0/1-5	192.168.10.254//24
VLAN20	0/0/6-10	192.168.20.254//24
VLAN30	0/0/24	192.168.30.254//24
SWB		
VLAN50	0/0/24	10.1.1.250/24
VLAN60	0/0/1-5	10.1.10.254/24
VLAN70	0/0/6-10	10.1.20.254/24
FW		
0/0	192.168.30.253/24	
0/1	202.106.1.1/28	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 全网络运行 OSPF 动态路由协议：

A. RA、RB、RC 之间采用单区域 OSPF；

B. RA 与 RB 之间采用 OSPF MD5 验证，密码为：wan；

C. RA 与 RC 之间采用 OSPF 明文验证，密码为：123456。

2. RC 与 RB 之间采用 VRRP 进行冗余备份：

A. 虚拟 IP：10.1.1.254/24；

B. 使 RC 成为 Master,RB 成为 Backup。

3. 由 RB、RC、SWB 所组成的内网运行 RIPv2 动态路由协议：

并使之与互联网进行通信。

4. 在 RB 与 RC 上配置网络地址转换：

使 PCC 与 PCD 可以访问互联网。

5. 在防火墙上配置网络地址转换：

使 PCA 与 PCB 可以访问互联网。

6. 在防火墙与 SWA 组成的内网配置路由：

采用静态路由，并使之与互联网相互通信。

7. 在 SWA 上配置访问控制列表：

使 PCB 在工作日上午 8：00-17：00 可以访问互联网。

8. 在 SWB 上配置端口镜像：

将 0/0/24 端口上的 RX 数据全部复制到 0/0/1 端口上。

9. 路由器之间配置链路封装协议：

A. RA 与 RB 之间采用 hdlc 链路封装，时钟频率为 9600bit/s；

B. RA 与 RC 之间采用 PPP 链路封装 ,并进行 PAP 认证 ,时钟频率为 64000bit/s.

10. 在 SWA、RB、RC 上使用用明文开启 telnet 功能。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。

Show ppp status

查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。

Debug ppp authentication

3. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 rip 路由协议状态，能够看到所使用的版本等信息
Show ip rip protocol
也可在 PC 上使用 Ping 命令进行链路连通性的测试。
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

4. 验证 VRRP

查看本设备 VRRP 运行状况,配置成功会出现本台设备 vrp 的相关信息，如主次关系、优先级、虚拟 ip、对端 ip 等信息
Show vrrp detail
查看 vrrp 协商主次关系过程（须在配置 VRRP 前配置）
debug vrrp

5. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需流量触发）
show ip nat translations

6. 验证访问控制列表

查看访问控制类表的配置
Show ip access-list lin
PC 之间相互 ping 命令也可验证访问控制列表是否成功。

7. 验证端口镜像

在目的端口上的 PC 上开启抓包软件，检查是否能抓获到监控端口的地址包。

8. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。

Show ppp status

查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示以建立连接，否则则不停认证。

Debug ppp authentication

五、 注意事项

1. 时间访问列表，注意配置完后要修改交换机的 COLCK，或者 NTP 服务器。
2. OSPF 注意声明好直链网段和区域 ID，认证的时候注意两端的加密密钥要一致。
3. VRRP 注意组与虚拟 IP 的配置。
4. 注意 NAT 的内、外网端口的指定与缺省路由的配置。
5. 静态路由注意指向与回指路由。

六、 配置参考

路由器 RA：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp pap local
!
username rc password 0 123456
!
!
interface FastEthernet0/0
```

```
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 119.255.1.22 255.255.255.240
 no ip directed-broadcast
 physical-layer speed 9600
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 wan
!
interface Serial0/2
 ip address 216.10.11.1 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap pap
 ppp pap sent-username ra password 0 123456
 physical-layer speed 64000
 ip ospf authentication simple
 ip ospf password 123456
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 10
 network 119.255.1.16 255.255.255.240 area 0
 network 216.10.11.0 255.255.255.240 area 0
 network 202.106.1.0 255.255.255.240 area 0
 area 119.255.1.16 authentication message-digest
 area 216.10.11.0 authentication simple
!
!
ip route default FastEthernet0/0
ip route 192.168.10.0 255.255.255.0 FastEthernet0/0
ip route 192.168.20.0 255.255.255.0 FastEthernet0/0
ip route 192.168.30.0 255.255.255.0 FastEthernet0/0
!
!
```

RA_config#

路由器 RB：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication login telnet local
aaa authentication enable default enable
!
username admin password 0 admin
enable password 0 123456 level 15
!
!
interface FastEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface FastEthernet0/3
 ip address 10.1.1.253 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 vrrp 1 associate 10.1.1.254 255.255.255.0
!
interface Serial0/1
 ip address 119.255.1.23 255.255.255.240
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 wan
 ip nat outside
```

```
!
 interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
line vty 0
 login authentication telnet
!
!
router rip
 version 2
 no auto-summary
 network 10.1.1.0 255.255.255.0
 network 172.16.1.0 255.255.255.0
!
router ospf 10
 network 119.255.1.16 255.255.255.240 area 0
 network 172.16.1.0 255.255.255.0 area 0
 area 119.255.1.16 authentication message-digest
!
!
ip access-list standard wan
 permit any
!
!
ip nat inside source list wan interface Serial0/1
!
!
RB_config#
```

路由器 RC：

```
SHO RUN
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
```

```
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication login telnet local
aaa authentication enable default enable
aaa authentication ppp pap local
!
username ra password 0 123456
username admin password 0 123456
enable password 0 123456 level 15
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface FastEthernet0/3
 ip address 10.1.1.252 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 vrrp priority 1
 vrrp 1 associate 10.1.1.254 255.255.255.0
 vrrp 1 priority 254
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 216.10.11.2 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap pap
 ppp pap sent-username rc password 0 123456
 ip ospf authentication simple
 ip ospf password 123456
```

```
 ip nat outside
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
line vty 0
 login authentication telnet
!
!
router rip
 version 2
 no auto-summary
 network 10.1.1.0 255.255.255.0
 network 172.16.1.0 255.255.255.0

!
router ospf 10
 network 216.10.11.0 255.255.255.240 area 0
 network 172.16.1.0 255.255.255.0 area 0
 area 216.10.11.0 authentication simple
!
!
ip access-list standard wan
 permit any
!
!
ip nat inside source list wan interface Serial0/2
!
!
RC_config#
```

交换机 SWA：

```
sho run
!
no service password-encryption
!
hostname SWA
!
telnet-user admin password 0 123456
!
vlan 1
```

```
!
vlan 10
!
vlan 20
!
vlan 30
!
time-range wan
  periodic weekdays 8:0:0 to 17:0:0
!
firewall enable
!
ip access-list extended wan
    permit tcp any-source 192.168.20.0 0.0.0.255 d-port 80 time-range wan
!
Interface Ethernet0/0/1
  switchport access vlan 10
!
Interface Ethernet0/0/2
  switchport access vlan 10
!
Interface Ethernet0/0/3
  switchport access vlan 10
!
Interface Ethernet0/0/4
  switchport access vlan 10
!
Interface Ethernet0/0/5
  switchport access vlan 10
!
Interface Ethernet0/0/6
  ip access-group wan in
  switchport access vlan 20
!
Interface Ethernet0/0/7
  switchport access vlan 20
!
Interface Ethernet0/0/8
  switchport access vlan 20
!
Interface Ethernet0/0/9
  switchport access vlan 20
!
```

```
Interface Ethernet0/0/10
 switchport access vlan 20
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 30
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
!
```

```
interface Vlan20
ip address 192.168.20.254 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
!
ip route 0.0.0.0/0 192.168.30.253
ip route 202.106.1.0/28 192.168.30.253
!
no login
!
end

SWA#
```

交换机 SWB：

```
SWB#sho run
!
no service password-encryption
!
hostname SWB
!
monitor session 1 source interface Ethernet0/0/24 rx
monitor session 1 destination interface Ethernet0/0/1
!
vlan 1
!
vlan 50
!
vlan 60
!
vlan 70
!
Interface Ethernet0/0/1
 switchport access vlan 60
!
Interface Ethernet0/0/2
 switchport access vlan 60
!
Interface Ethernet0/0/3
 switchport access vlan 60
!
Interface Ethernet0/0/4
```

```
 switchport access vlan 60
!
Interface Ethernet0/0/5
 switchport access vlan 60
!
Interface Ethernet0/0/6
 switchport access vlan 70
!
Interface Ethernet0/0/7
 switchport access vlan 70
!
Interface Ethernet0/0/8
 switchport access vlan 70
!
Interface Ethernet0/0/9
 switchport access vlan 70
!
Interface Ethernet0/0/10
 switchport access vlan 70
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
```

```
!
Interface Ethernet0/0/23
 switchport access vlan 50
!
Interface Ethernet0/0/24
 switchport access vlan 50
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan50
 ip address 10.1.1.250 255.255.255.0
!
interface Vlan60
 ip address 10.1.10.253 255.255.255.0
!
interface Vlan70
 ip address 10.1.20.254 255.255.255.0
!
router rip
 network 10.1.1.0/24
 network 10.1.10.0/24
 network 10.1.20.0/24
!
ip route 0.0.0.0/0 10.1.1.254
!
no login
!
end

SWB#
```

防火墙：

```
SHO CONF

Building configuration..
Running configuration:
!
```

```
Version 2.0

aaa-server "local" type local
exit

admin user "admin"
   password ZgVGVdJYHH9wGebU+a+eXalQwc
   privilege RXW
   access console
   access telnet
   access ssh
   access http
   access https
exit

hostname "DCFW-1800"
admin host any telnet
admin host any ssh
admin host any http
admin host any https
ip vrouter trust-vr
exit

vswitch "vswitch1"
exit

zone "trust"
exit

zone "untrust"
   ad tear-drop
   ad ip-spoofing
   ad land-attack
   ad ip-option
   ad ip-option action alarm
   ad ip-fragment
   ad winnuke
   ad port-scan
   ad syn-flood
   ad icmp-flood
   ad ip-sweep
   ad ping-of-death
   ad udp-flood
```

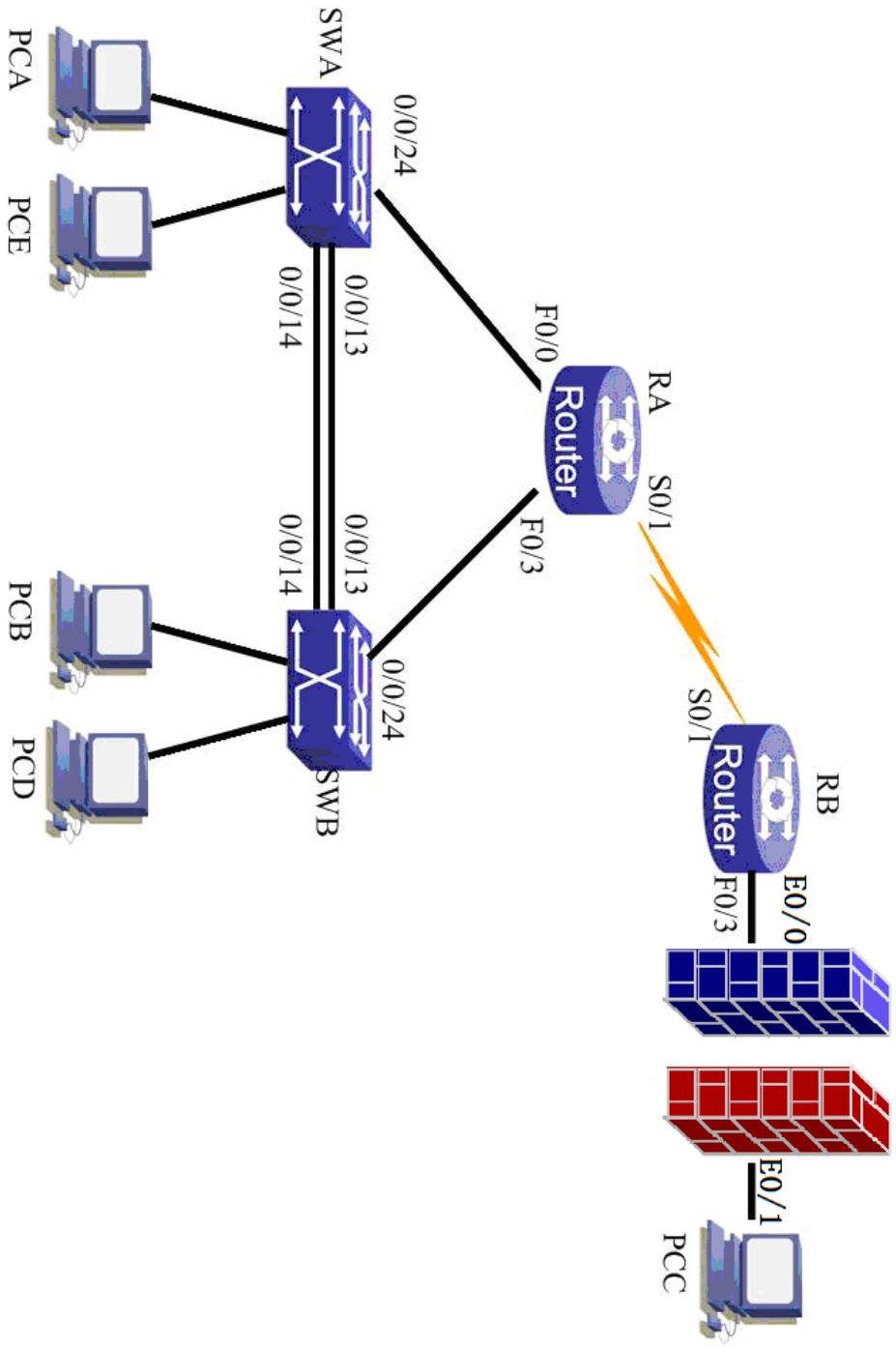
```
   ad ip-directed-broadcast
exit

zone "dmz"
exit

zone "l2-trust" l2
exit

zone "l2-untrust" l2
exit

zone "l2-dmz" l2
exit

zone "VPNHub"
exit

zone "HA"
exit

interface vswitchif1
exit

interface ethernet0/0
exit

interface ethernet0/1
exit

interface ethernet0/2
exit

interface ethernet0/3
exit

interface ethernet0/4
exit

pki trust-domain "trust_domain_default"
   keypair "Default-Key"
   enrollment self
   subject commonName "DCFW-1800"
```

```
   subject organization "DigitalChina Networks Limited"
exit

interface ethernet0/0
   zone   "trust"
   ip address 192.168.30.253 255.255.255.0
   manage ssh
   manage telnet
   manage ping
   manage snmp
   manage http
   manage https
exit

interface ethernet0/1
   zone   "untrust"
   ip address 202.106.1.1 255.255.255.240
   manage telnet
   manage ssh
   manage ping
   manage http
   manage https
   manage snmp
exit

interface ethernet0/3
   zone   "trust"
   ip address 10.1.1.1 255.255.255.0
   manage ip 10.1.1.2
   manage telnet
   manage ssh
   manage ping
   manage http
   manage https
   manage snmp
exit

ip vrouter trust-vr
   ip route 192.168.10.0/24 192.168.30.254
   ip route 192.168.20.0/24 192.168.30.254
   ip route 0.0.0.0/0 202.106.1.2
exit
```

```
policy from "trust" to "untrust"
  rule id 1
    action permit
    src-addr "Any"
    dst-addr "Any"
    service "Any"
  exit

exit

no tcp-syn-check
l2-nonip-action drop
nat
snatrule id 1 from "Any" to "Any" trans-to eif-ip mode dynamicport
exit

ecmp-route-select by-src-and-dst
strict-tunnel-check

end
DCFW-1800#
```

12

一、 拓扑图


PCA
PCE
SWA
0/0/24
0/0/13
0/0/14
F0/0
RA
Router
S0/1
F0/3
PCB
PCD
SWB
0/0/14
0/0/13
0/0/24
S0/1
RB
Router
F0/3
E0/0
E0/1
PCC

二、 环境准备

1. 设备要求

2 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

1 台防火墙 DCFWS-1800v2

4 台 PC 电脑

2. IP 地址规划

RB		
S0/1	202.106.10.2/27	
F0/3	10.1.100.1/24	
RA		
S0/1	202.106.10.1/27	
F0/0	172.16.1.2/30	
F0/3	172.15.1.2/30	
SWA		
VLAN10	0/0/1-5	192.168.10.254//28
VLAN100	0/0/24	172.16.1.1//30
VLAN40	0/0/6-10	192.168.40.254//28
SWB		
VLAN100	0/0/24	172.15.1.1/30
VLAN20	0/0/1-5	192.168.20.254/28
VLAN30	0/0/6-10	192.168.30.254/28
FW		
0/0	10.1.100.2/24	
0/1	10.1.10.254/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 在 SWA、SWB、RA 之间采用 RIPv2 动态路由协议。

2. 在 SWA 与 SWB 之间配置 MSTP 生成树算法：

A. 设置两个实例，分别为实例一与实例二；

B. VLAN10 与 VLAN40 属于实例一；

C. VLAN20 与 VLAN30 属于实例二；

D. 在实例一中，SWA 的桥优先级为 4096；

E. 在实例二中，SWB 的桥优先级为 0.

3. 在 RA 与 RB 之间配置 PPP 链路封装协议：

A. 采用 CHAP 认证封装；

B. 设置 RA 为 DCE 端，时钟频率为 9600；

C. 用户名：digitalchina ，密码：123456；

D. 设置为单向认证。

4. 在 RA 路由器上配置网络地址转换：

将内网的计算机（PCB、PCD、PCE）转换为 RA 路由器的 S0/1 接口的 IP 地址。

5. 在 RB 路由器上配置网络地址转换：

将内网计算机（PCC）转换为 RB 路由器的 S0/1 接口的 IP 地址。

6. 将防火墙设置为路由模式：

采用默认路由

7. PCA 是一台 Web 服务器，将 PCA 发布到公网：

发布地址为：202.106.10.1/27，80 端口

8. 在 RA 上配置 QoS：

使 80 服务更加优先，使用优先级列表实现。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。

Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

3. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 rip 路由协议状态，能够看到所使用的版本等信息
Show ip rip protocol
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

4. 验证策略路由

可使用 show running-config 进行配置查看，也可使用 taceroute 命令在 PC 机上进行验证，若正确会遵循题目要求中的线路进行路由，若不正确则会走另外一条线路。（必须在全网互通的前提下）
在网络设备上可以使用 tracert 命令进行数据路由的查看。

5. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需流量触发）
show ip nat translations

6. 验证服务质量

查看 QoS 端口信息
Show mls qos interface
也可以设置一个 FTP 服务器，在 FTP server 端放置文件大小约为 14M 的测试文件，在端口应用 QOS 策略前后观察客户端下载同一文件所用时间，直观观察速率变化

7. 验证生成树协议

查看生成树状态，可以看到本网桥在每一个实例中状态，包括 STP 版本，该实例对应的本网桥优先级及 MAC，该实例对应的根网桥优先级及 MAC，网桥到整个网络根桥 的路径代价，网桥上该实例的根端口，该实例对应的端口状态，该实例对应的端口角色等
show spanning-tree

五、 注意事项

1. 配置 RIP 协议注意版本信息与端口的网段及宣告的网段。
2. MSTP 注意实例的配置以及实例的优先级配置模式。
3. PPP 协议注意 AAA 验证的用户库以及主验证方和验证方。
4. 注意内网地址转换发生在 NAT 的 inside 端？

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp lin local
!
username digitalchina password 0 123456
!
!
interface FastEthernet0/0
 ip address 172.16.1.2 255.255.255.252
 no ip directed-broadcast
 priority-group 1
 ip nat inside
!
interface FastEthernet0/3
 ip address 172.15.1.2 255.255.255.252
 no ip directed-broadcast
```

```
 ip nat inside
!
interface Serial0/1
 ip address 202.106.10.1 255.255.255.224
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap lin
 ppp chap hostname digitalchina
 ppp chap password 0 123456
 physical-layer speed 9600
 ip nat outside
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router rip
 version 2
 no auto-summary
 network 172.16.1.0 255.255.255.252
 network 172.15.1.0 255.255.255.252
!
!
ip route default Serial0/1
!
!
priority-list 1 protocol ip high tcp www
!
ip access-list standard lin
 permit any
!
!
ip nat inside source static tcp 192.168.10.241 80 202.106.10.1 80
ip nat inside source list lin interface Serial0/1
!
!
RA#
```

RB 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp default local
!
username digitalchina password 0 123456
!
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 10.1.100.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0/1
 ip address 202.106.10.2 255.255.255.224
 no ip directed-broadcast
 encapsulation ppp
 ppp chap hostname digitalchina
 ppp chap password 0 123456
 ip nat outside
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
```

```
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
ip route default Serial0/1
ip route 10.1.10.0 255.255.255.0 10.1.100.2
!
!
ip access-list standard lin
 permit any
!
!
ip nat inside source list lin interface Serial0/1
!
!
RB#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
spanning-tree mst configuration
instance 0 vlan 1-9;11-39;41-4094
instance 1 vlan 10;40
exit
!
spanning-tree
spanning-tree mst 0 priority 0
spanning-tree mst 1 priority 4096
!
vlan 1
!
vlan 10
!
vlan 40
!
vlan 100
!
```

```
Interface Ethernet0/0/1
switchport access vlan 10
!
Interface Ethernet0/0/2
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 40
!
Interface Ethernet0/0/7
 switchport access vlan 40
!
Interface Ethernet0/0/8
 switchport access vlan 40
!
Interface Ethernet0/0/9
switchport access vlan 40
!
Interface Ethernet0/0/10
 switchport access vlan 40
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
```

```
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.240
!
interface Vlan40
 ip address 192.168.40.254 255.255.255.240
!
interface Vlan100
 ip address 172.16.1.1 255.255.255.252
!
router rip
 network 172.16.1.0/30
 network 192.168.10.240/28
 network 192.168.40.240/28
!
ip route 0.0.0.0/0 172.16.1.2
!
no login
!
end
```

SWA#

SWB 路由器：

```
sho run
!
no service password-encryption
!
hostname SWB
!
spanning-tree mst configuration
 instance 0 vlan 1-19;21-29;31-4094
 instance 2 vlan 20;30
 exit
!
spanning-tree
spanning-tree mst 2 priority 0
!
vlan 1
!
vlan 20
!
vlan 30
!
vlan 100
!
Interface Ethernet0/0/1
 switchport access vlan 20
!
Interface Ethernet0/0/2
 switchport access vlan 20
!
Interface Ethernet0/0/3
 switchport access vlan 20
!
Interface Ethernet0/0/4
 switchport access vlan 20
!
Interface Ethernet0/0/5
 switchport access vlan 20
!
Interface Ethernet0/0/6
 switchport access vlan 30
!
```

```
Interface Ethernet0/0/7
 switchport access vlan 30
!
Interface Ethernet0/0/8
 switchport access vlan 30
!
Interface Ethernet0/0/9
 switchport access vlan 30
!
Interface Ethernet0/0/10
 switchport access vlan 30
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
```

```
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.240
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.240
!
interface Vlan100
 ip address 172.15.1.1 255.255.255.252
!
router rip
 network 172.15.1.0/30
 network 192.168.20.240/28
 network 192.168.30.240/28
!
ip route 0.0.0.0/0 172.15.1.2
!
no login
!
end
SWB#
```

防火墙：

```
DCFW-1800# sho configuration
Building configuration..
Running configuration:
!
Version 2.0

aaa-server "local" type local
exit

admin user "admin"
   password iNykdNw4TYs1IaO2HtYMFgUwwI
   privilege RXW
   access console
   access telnet
   access ssh
```

```
   access http
   access https
exit

hostname "DCFW-1800"
admin host any telnet
admin host any ssh
admin host any http
admin host any https
admin host 10.1.1.3 255.255.255.0 http
ip vrouter trust-vr
exit

vswitch "vswitch1"
exit

zone "trust"
exit

zone "untrust"
   ad tear-drop
   ad ip-spoofing
   ad land-attack
   ad ip-option
   ad ip-option action alarm
   ad ip-fragment
   ad winnuke
   ad port-scan
   ad syn-flood
   ad icmp-flood
   ad ip-sweep
   ad ping-of-death
   ad udp-flood
   ad ip-directed-broadcast
exit

zone "dmz"
exit

zone "l2-trust" l2
exit

zone "l2-untrust" l2
```

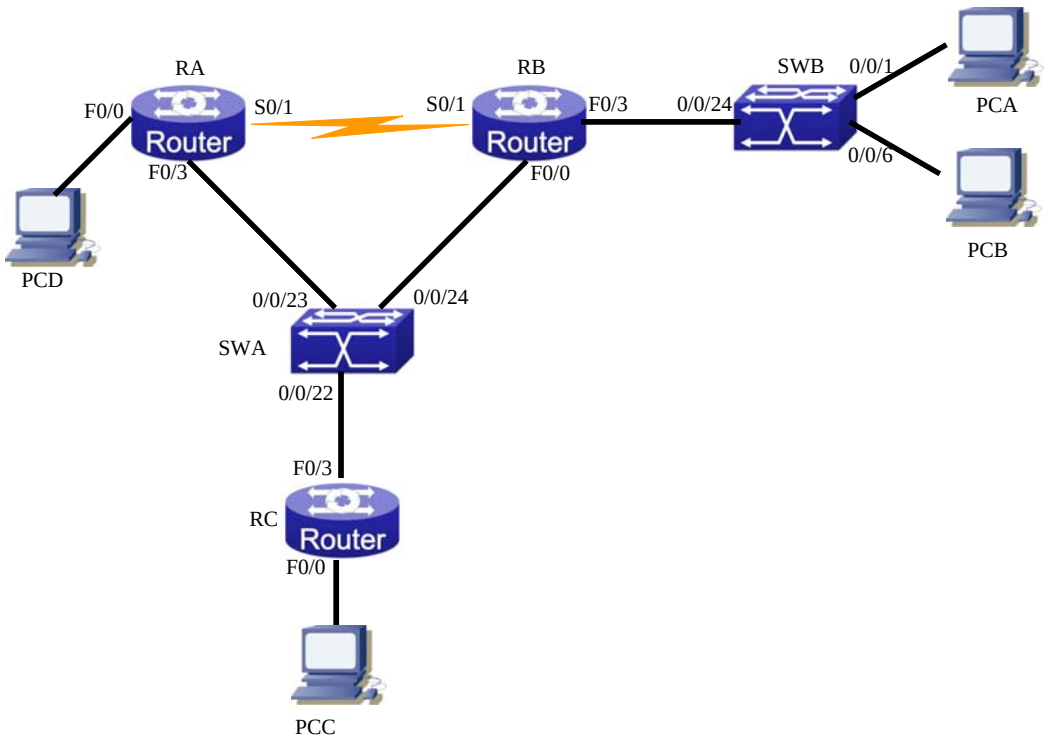
```
exit

zone "l2-dmz" l2
exit

zone "VPNHub"
exit

zone "HA"
exit

interface vswitchif1
exit

interface ethernet0/0
exit

interface ethernet0/1
exit

interface ethernet0/2
exit

interface ethernet0/3
exit

interface ethernet0/4
exit

pki trust-domain "trust_domain_default"
  keypair "Default-Key"
  enrollment self
  subject commonName "DCFW-1800"
  subject organization "DigitalChina Networks Limited"
exit

interface ethernet0/0
  zone   "trust"
  ip address 10.1.100.2 255.255.255.0
  manage ssh
  manage telnet
  manage ping
  manage snmp
```

```
   manage http
   manage https
exit

interface ethernet0/1
   zone    "trust"
   ip address 10.1.10.254 255.255.255.0
   manage telnet
   manage ssh
   manage ping
   manage http
   manage https
   manage snmp
exit

interface ethernet0/3
   zone    "trust"
   ip address 10.1.1.1 255.255.255.0
   manage ip 10.1.1.2
   manage telnet
   manage ping
   manage http
   manage https
exit

ip vrouter trust-vr
   ip route 0.0.0.0/0 10.1.100.1
exit

policy from "trust" to "trust"
   default-action permit
   rule id 4
      action permit
      src-addr "Any"
      dst-addr "Any"
      service "Any"
   exit

exit

no tcp-syn-check
l2-nonip-action drop
ecmp-route-select by-src-and-dst
```

```
strict-tunnel-check

end
DCFW-1800#
```

13

一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC	
F0/0	10.1.4.2/24
F0/3	202.106.2.254/24
RB	
S0/1	10.1.1.2/24
F0/0	10.1.3.2/24
F0/3.1	192.168.10.254/24
F0/3.2	192.168.20.254/24
RA	
S0/1	10.1.1.1/24
F0/0	10.1.2.1/24

F0/3	202.106.1.254/24	
SWA		
VLAN11	0/0/23	10.1.2.2/24
VLAN12	0/0/24	10.1.3.1/24
VLAN13	0/0/22	10.1.4.1/24
SWB		
VLAN10	0/0/1-5	
VLAN20	0/0/6-10	
PC		
PCA	192.168.10.1/24	
PCB	192.168.20.1/24	
PCC	202.106.2.1/24	
PCD	202.106.1.1/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 路由器 RA 与 RB 之间配置 PPP 链路封装协议：

A. 采用 chap 认证；

B. 设置为单向认证；

C. RA 为主验证方；

D. 时钟速率设置为 2048000;

2. 在 RA、RB、RC、SWA、SWB 之间采用 ospf 单区域动态路由协议；

3. 在 RA 与 RC 上配置网络地址转换：

A. 将 RA 的内网地址全部转换成 f0/3 的 IP 地址；

B. 将 RC 的内网地址全部转换成 F0/3 的 IP 地址。

4. 在 RB 上配置单臂路由；

5. 在 RC 与 SWA 上开启 telnet 服务：

用户名：admin 密码：admin

6. 将服务器 PCA 发布到互联网之上：

发布 ip：202.106.1.10/24

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

4. 验证 telnet 服务

可使用 ping 命令测试主机与网络中各个设备的连通情况，如果连通使用 telnet 命令进行验证，也可使用 show running-config 命令验证。

5. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需流量触发）
show ip nat translations

五、 注意事项

1. OSPF 区域宣告时注意掩码的写法,并保证直连网段能 ping 通。
2. 注意网络地址转换时内、外网接口的指定与缺省路由的配置。
3. 注意不要忘记交换机上端口要配置 trunk，路由器上接口要划分子接口，并设置 802.1Q 协议
4. 在配置 telnet 服务的路由器上，注意开启 AAA 认证。
5. 做端口映射的时候注意用的是 inside source，把内网的源地址映射到外网。

六、 配置参考

RA 路由器：

```
RA#sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp lin local
!
username RB password 0 123456
!
!
interface FastEthernet0/0
 ip address 10.1.2.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
```

```
interface FastEthernet0/3
 ip address 202.106.1.254 255.255.255.0
 no ip directed-broadcast
 ip nat outside
!
interface Serial0/1
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap lin
 ppp chap hostname RA
 ppp chap password 0 123456
 ip nat inside
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
!
!
ip route default FastEthernet0/3
!
!
ip access-list standard lin
 permit 192.168.10.0 255.255.255.0
 permit 192.168.20.0 255.255.255.0
!
!
ip nat inside source static 192.168.10.1 202.106.1.254
ip nat inside source list lin interface FastEthernet0/3
!
!
RA#
```

RB 路由器：

```
sho run
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp default local
!
username RA password 0 123456
!
!
interface FastEthernet0/0
 ip address 10.1.3.2 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3.1
 ip address 192.168.10.254 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 10
 bandwidth 100000
 delay 1
!
interface FastEthernet0/3.2
 ip address 192.168.20.254 255.255.255.0
 no ip directed-broadcast
 encapsulation dot1Q 20
 bandwidth 100000
 delay 1
!
```

```
interface Serial0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp chap hostname RB
 ppp chap password 0 123456
 physical-layer speed 2048000
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.3.0 255.255.255.0 area 0
 network 192.168.10.0 255.255.255.0 area 0
 network 192.168.20.0 255.255.255.0 area 0
!
!
ip route default 10.1.1.1
ip route default 10.1.3.1
!
!
RB#
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
```

```
!
gbsc group default
!
!
aaa authentication login default local
aaa authentication enable default enable
!
username admin password 0 admin
enable password 0 123456 level 15
!
!
interface FastEthernet0/0
 ip address 10.1.4.2 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface FastEthernet0/3
 ip address 202.106.2.254 255.255.255.0
 no ip directed-broadcast
 ip nat outside
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 10.1.4.0 255.255.255.0 area 0
!
!
ip route default FastEthernet0/3
!
!
ip access-list standard lin
 permit 192.168.10.0 255.255.255.0
```

```
 permit 192.168.20.0 255.255.255.0
!
!
ip nat inside source list lin interface FastEthernet0/3
!
!
RC#    RC#
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
enable password 123456
!
!
telnet-user admin password 0 admin
!
vlan 1
!
vlan 11
!
vlan 12
!
vlan 13
!
Interface Ethernet0/0/1
!
Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
```

```
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
 switchport access vlan 13
!
Interface Ethernet0/0/23
 switchport access vlan 11
!
Interface Ethernet0/0/24
 switchport access vlan 12
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
```

```
Interface Ethernet0/0/28
!
interface Vlan11
 ip address 10.1.2.2 255.255.255.0
!
interface Vlan12
 ip address 10.1.3.1 255.255.255.0
!
interface Vlan13
 ip address 10.1.4.1 255.255.255.0
!
router ospf 1
 network 10.1.2.0 0.0.0.255 area 0
 network 10.1.3.0 0.0.0.255 area 0
 network 10.1.4.0 0.0.0.255 area 0
!
ip route 0.0.0.0/0 10.1.2.1
ip route 0.0.0.0/0 10.1.4.2
!
no login
!
end

SWA#
```

SWB 交换机：

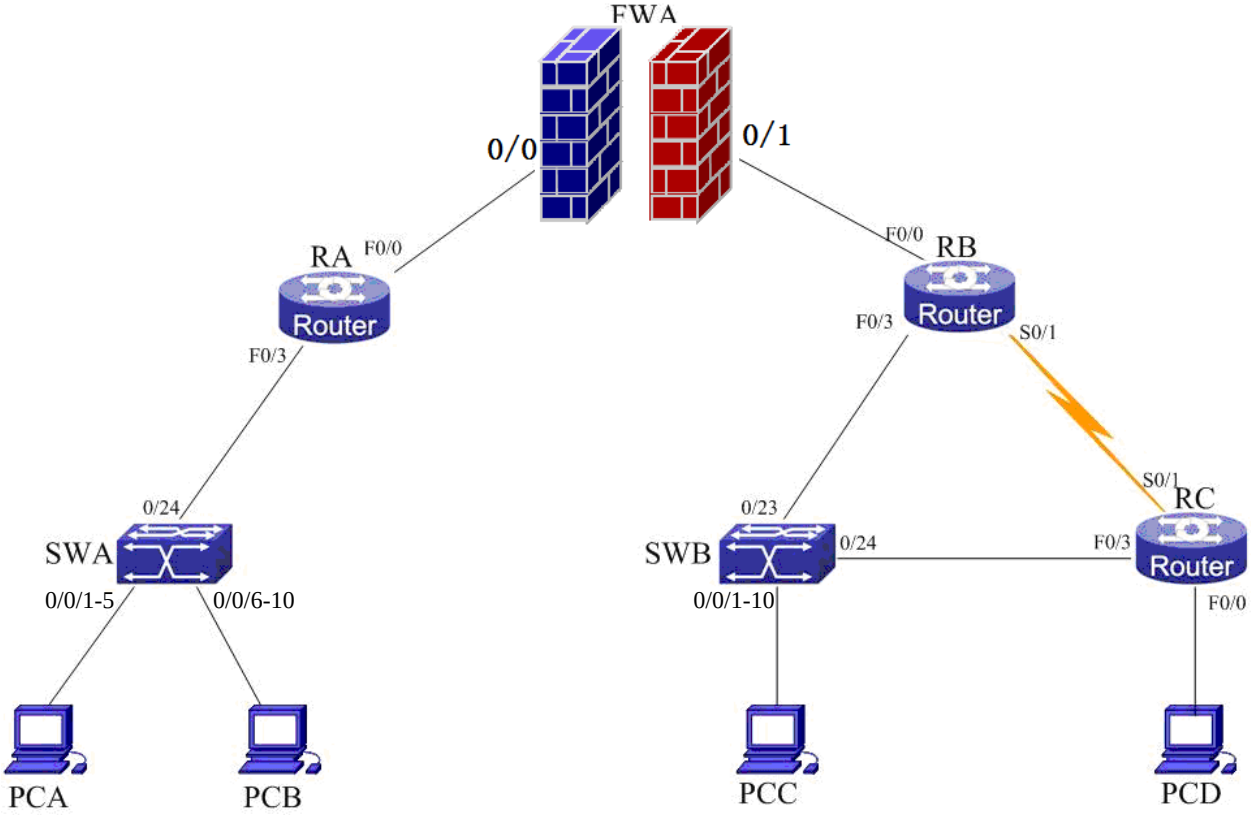
```
sho run
!
no service password-encryption
!
hostname SWB
!
vlan 1
!
vlan 10
!
vlan 20
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
Interface Ethernet0/0/2
 switchport access vlan 10
```

```
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 20
!
Interface Ethernet0/0/7
 switchport access vlan 20
!
Interface Ethernet0/0/8
 switchport access vlan 20
!
Interface Ethernet0/0/9
 switchport access vlan 20
!
Interface Ethernet0/0/10
 switchport access vlan 20
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
```

```
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
  switchport mode trunk
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
no login
!
end
SWB#
```

14

一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

1 台防火墙 DCFW-1800S-V2

4 台 PC 电脑

2. IP 地址规划

RC	
S0/1	211.11.10.2/28
F0/0	10.1.20.254/24
F0/3	211.13.10.2/28
RB	
S0/1	211.11.10.1/28

F0/0	202.106.1.2/28	
F0/3	211.12.10.1/28	
RA		
F0/3	172.16.2.1/27	
F0/0	202.106.1.1/28	
SWA		
VLAN10	0/0/1-5	172.16.10.254/24
VLAN20	0/0/6-10	172.16.20.254/24
VLAN100	0/0/24	172.16.2.2/27
SWB		
VLAN200	0/0/24	211.13.10.1/28
VLAN100	0/0/23	211.12.10.2/28
VLAN30	0/0/1-10	10.1.10.254/24

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 网络采用 OSPF 动态路由协议：

A. SWA 与 RA 属于 area1；

B. RA、FWA 与 RB 属于 area0；

C. RB、SWB、RC 属于 area 2;

D. Area1 中采用 MD5 认证，用户名：root123 ，密码为：digitalchina。

2. 在 RC 与 RB 之间运行 PPP 链路封装协议：

A. 采用 CHAP 认证，RC 的用户名：RC，密码为：digitalchina，RB 的用户名：RB ，密码为：digitalchina ；

B. 在 DCE 端设置时钟频率：64000bps。

3. FWA 采用透明模式传输，开启 URL 防病毒功能。

4. 在 SWA 上过滤 PCB 的 MAC 地址：

使用 MAC 地址表的方法。

5. 在 SWB 上配置端口镜像：

要求在 E0/0/1 接口上可以监听 E0/0/23 和 E0/0/24 口的全部数据。

6. 在 SWA 上开启 MAC 地址绑定：

A. 将 PCA 的 mac 地址进行绑定；

B. 如果违反匹配规则，则端口关闭掉。

7. 在 SWA 与 RA 上开启 telnet 服务

帐号： admin ，密码为：admin

8. 在 RB 与 RC 之间配置 IPSCE VPN：

A. RC 与 RB 之间 IKE 方式协商安全联盟主动模式；

B. IKE 策略采用 md5 hash 算法；

C. transform-set（协议变换集）名称为 lin，加密验证方式为：ah-sha-hmac、esp-des，共享密钥为：lin

D. 加密映射表进行协商的安全联盟的生命周期为 86400 秒

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由

Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证端口绑定

可使用 show running-config 进行配置查看，也可将 PC 从当前交换机端口换至其他端口验证，如果换至其他端口无法通信，说明配置成功。

6. 验证 telnet 服务

可使用 ping 命令测试主机与网络中各个设备的连通情况，如果连通使用 telnet 命令进行验证，也可使用 show running-cnfig 命令验证。

五、 注意事项

1. IPSCE VPN 推荐配置顺序：
   A. RB 上开启访问控制列表；
   B. 配置变换集；
   C. 创建策略表；
   D. 配置加密映射表，将刚才配置的访问列表，变换集，策略表进行引用；
   E. 最后绑定到端口上。RA 的配置方法与 RB 上一致。
2. IPSEC IKE 主动模式默认开启
3. crypto map 的名字必须与接口上应用的名字一致
4. 配置动态路由协议时，先 ping 通直连路由器的接口，再配置动态路由。防止因为物理连线路由信息不能相互学习到路由。
5. 配置加密认证时，要确保两端加密方式一样、两端密码一致。
6. 防火墙注意开通明模式，将两个接口放入 l2-trust 区域内，并配置 l2-trust 到 l2-trunk 的安全策略。
7. 开启端口安全时注意 show ip mac-address-table，查看交换机内学到的 mac 地址，学到后才能开始绑定。

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
interface FastEthernet0/0
 ip address 202.106.1.1 255.255.255.240
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 172.16.2.1 255.255.255.224
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 172.16.2.0 255.255.255.224 area 1
```

```
 network 202.106.1.0 255.255.255.240 area 0
!
!
```

RB 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp lin local
!
username RC password 0 digitalchina
!
crypto isakmp key lin 211.11.10.2 255.255.255.255
!
!
crypto isakmp policy 10
 hash md5
!
crypto ipsec transform-set lin
 transform-type ah-sha-hmac esp-des
!
crypto map lin 10 ipsec-isakmp
 set peer 211.11.10.2
 set pfs group1
 set security-association lifetime seconds 86400
 set transform-set lin
 match address lin-acl
!
!
interface FastEthernet0/0
```

```
 ip address 202.106.1.2 255.255.255.240
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 211.12.10.1 255.255.255.240
 no ip directed-broadcast
!
interface Serial0/1
 ip address 211.11.10.1 255.255.255.240
 no ip directed-broadcast
 crypto map lin
 encapsulation ppp
 ppp authentication chap lin
 ppp chap hostname RB
 ppp chap password 0 digitalchina
 physical-layer speed 64000
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 202.106.1.0 255.255.255.240 area 0
 network 211.11.10.0 255.255.255.240 area 2
 network 211.12.10.0 255.255.255.240 area 2
!
!
ip access-list extended lin-acl
 permit ip any any
!
!
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
```

```
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication ppp default local
!
username RB password 0 digitalchina
!
crypto isakmp key lin 211.11.10.1 255.255.255.255
!
!
crypto isakmp policy 10
 hash md5
!
crypto ipsec transform-set lin
 transform-type ah-sha-hmac esp-des
!
crypto map lin 10 ipsec-isakmp
 set peer 211.11.10.1
 set pfs group1
 set security-association lifetime seconds 86400
 set transform-set lin
 match address lin-acl
!
!
interface FastEthernet0/0
 ip address 10.1.20.254 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 211.13.10.2 255.255.255.240
 no ip directed-broadcast
!
interface Serial0/1
 ip address 211.11.10.2 255.255.255.240
 no ip directed-broadcast
```

```
 crypto map lin
 encapsulation ppp
 ppp chap hostname RC
 ppp chap password 0 digitalchina
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 10.1.20.0 255.255.255.0 area 2
 network 211.13.10.0 255.255.255.240 area 2
 network 211.11.10.0 255.255.255.240 area 2
!
!
ip access-list extended lin-acl
 permit ip any any
!
!
```

SWA 交换机：

```
sho run
!
no service password-encryption
!
hostname SWA
!
enable password admin
!
!
telnet-user admin password 0 admin
!
vlan 1
!
vlan 10
!
vlan 20
!
```

```
vlan 100
!
Interface Ethernet0/0/1
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address aa-aa-aa-aa-aa-aa
 switchport port-security violation shutdown
!
Interface Ethernet0/0/2
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 20
!
Interface Ethernet0/0/7
 switchport access vlan 20
!
Interface Ethernet0/0/8
 switchport access vlan 20
!
Interface Ethernet0/0/9
 switchport access vlan 20
!
Interface Ethernet0/0/10
 switchport access vlan 20
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
```

```
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 100
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan10
 ip address 172.16.10.254 255.255.255.0
!
interface Vlan20
 ip address 172.16.20.254 255.255.255.0
!
interface Vlan100
ip address 172.16.2.2 255.255.255.224
!
mac-address-table blackhole address aa-bb-cc-dd-ee-ff vlan 20
!
router ospf 1
 network 172.16.2.0 0.0.0.31 area 1
 network 172.16.10.0 0.0.0.255 area 1
```

```
 network 172.16.20.0 0.0.0.255 area 1
!
no login
!
end
```

SWB 交换机：

```
sho run
!
no service password-encryption
!
hostname SWB
!
monitor session 1 source interface Ethernet0/0/24;23 rx
monitor session 1 source interface Ethernet0/0/24;23 tx
monitor session 1 destination interface Ethernet0/0/1
!
vlan 1
!
vlan 30
!
vlan 100
!
vlan 200
!
Interface Ethernet0/0/1
 switchport access vlan 30
!
Interface Ethernet0/0/2
 switchport access vlan 30
!
Interface Ethernet0/0/3
 switchport access vlan 30
!
Interface Ethernet0/0/4
 switchport access vlan 30
!
Interface Ethernet0/0/5
 switchport access vlan 30
!
Interface Ethernet0/0/6
 switchport access vlan 30
!
```

```
Interface Ethernet0/0/7
 switchport access vlan 30
!
Interface Ethernet0/0/8
 switchport access vlan 30
!
Interface Ethernet0/0/9
 switchport access vlan 30
!
Interface Ethernet0/0/10
 switchport access vlan 30
!
Interface Ethernet0/0/11
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
 switchport access vlan 100
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
```

```
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan30
 ip address 10.1.10.254 255.255.255.0
!
interface Vlan100
 ip address 211.12.10.2 255.255.255.240
!
interface Vlan200
 ip address 211.13.10.1 255.255.255.240
!
router ospf 1
 network 10.1.10.0 0.0.0.255 area 2
 network 211.12.10.0 0.0.0.15 area 2
 network 211.13.10.0 0.0.0.15 area 2
!
no login
!
end
```

防火墙：

```
sho conf

Building configuration..
Running configuration:
!
Version 2.0

aaa-server "local" type local
exit

admin user "admin"
   password iNykdNw4TYs1IaO2HtYMFgUwwI
   privilege RXW
   access console
   access telnet
   access ssh
   access http
```

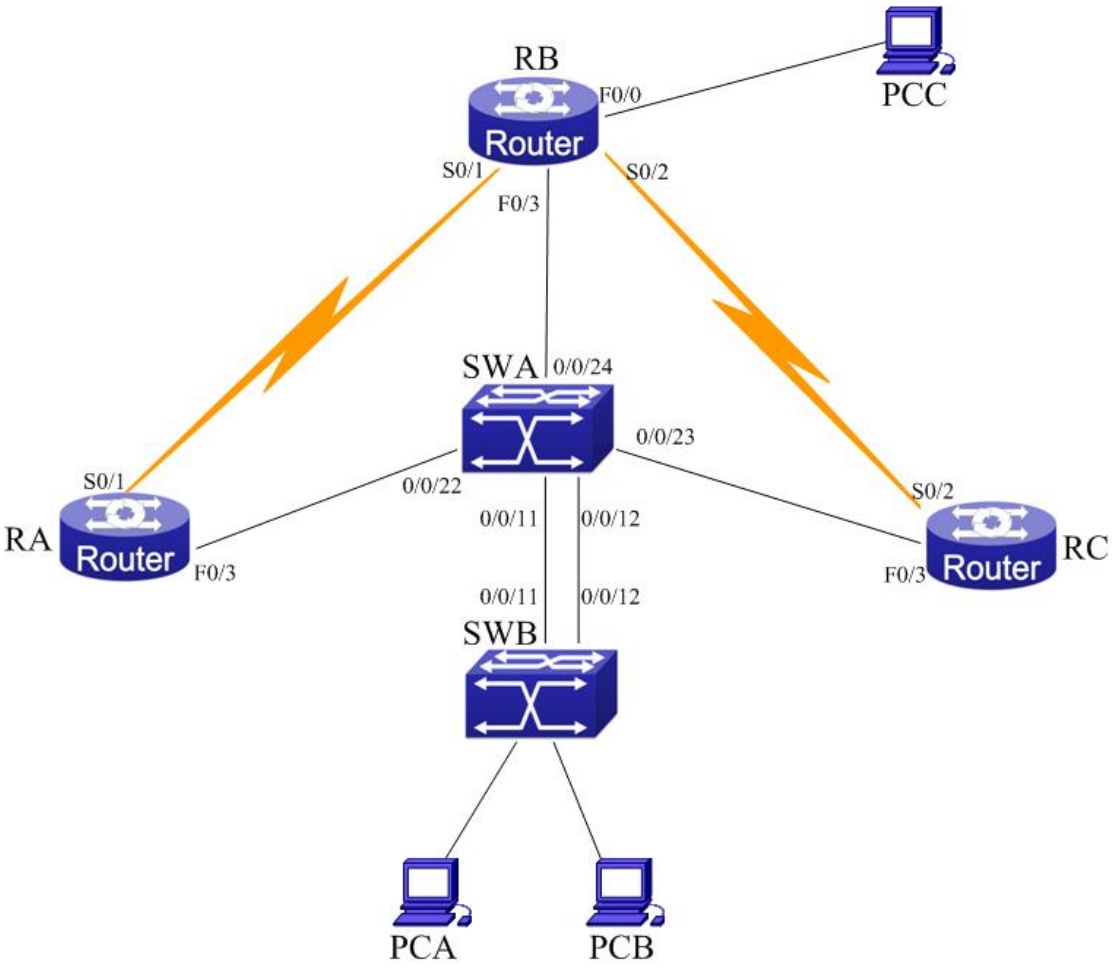
```
   access https
exit

hostname "DCFW-1800"
admin host any telnet
admin host any ssh
admin host any http
admin host any https
admin host 10.1.1.3 255.255.255.0 http
ip vrouter trust-vr
exit

vswitch "vswitch1"
exit

zone "trust"
exit

zone "untrust"
   ad tear-drop
   ad ip-spoofing
   ad land-attack
   ad ip-option
   ad ip-option action alarm
   ad ip-fragment
   ad winnuke
   ad port-scan
   ad syn-flood
   ad icmp-flood
   ad ip-sweep
   ad ping-of-death
   ad udp-flood
   ad ip-directed-broadcast
exit

zone "dmz"
exit

zone "l2-trust" l2
exit

zone "l2-untrust" l2
exit
```

```
zone "l2-dmz" l2
exit

zone "VPNHub"
exit

zone "HA"
exit

interface vswitchif1
exit

interface ethernet0/0
exit

interface ethernet0/1
exit

interface ethernet0/2
exit

interface ethernet0/3
exit

interface ethernet0/4
exit

pki trust-domain "trust_domain_default"
  keypair "Default-Key"
  enrollment self
  subject commonName "DCFW-1800"
  subject organization "DigitalChina Networks Limited"
exit

interface ethernet0/0
  zone   "l2-trust"
  manage ssh
  manage telnet
  manage ping
  manage snmp
  manage http
  manage https
```

```
exit

interface ethernet0/1
   zone    "l2-trust"
   manage telnet
   manage ssh
   manage ping
   manage http
   manage https
   manage snmp
exit

interface ethernet0/3
   zone    "trust"
   ip address 10.1.1.1 255.255.255.0
   manage ip 10.1.1.2
   manage telnet
   manage ping
   manage http
   manage https
exit

policy from "l2-trust" to "l2-trust"
   rule id 1
      action permit
      src-addr "Any"
      dst-addr "Any"
      service "Any"
   exit

exit

no tcp-syn-check
l2-nonip-action drop
ecmp-route-select by-src-and-dst
strict-tunnel-check

end
```

15

一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

3 台 PC 电脑

2. IP 地址规划

RC		
S0/2	210.216.1.2/24	T2:2.2.2.2/24
F0/3	192.168.2.1/24	
RB		
S0/2	210.216.1.1/24	T1:2.2.2.1/24
S0/1	202.106.1.2/24	T2:1.1.1.2/24
F0/0	172.16.1.1/24	
F0/3	192.168.3.1/24	

RA		
S0/1	202.106.1.1/24	T1:1.1.1.1/24
F0/3	192.168.1.1/24	
SWA		
VLAN10	0/0/22	192.168.1.2/24
VLAN20	0/0/23	192.168.3.2/24
VLAN30	0/0/24	192.168.2.2/24
VLAN40	0/0/1-5	192.168.10.254/24
VLAN50	0/0/6-10	192.168.20.254/24
SWB		
VLAN40	0/0/1-5	
VLAN50	0/0/6-10	
PCA	192.168.10.1/24	
PCB	192.168.20.1/24	
PCC	172.16.1.2/24	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 网络配置多区域 OSPF 动态路由协议：

A. RA、RB、RC 在区域 0 中；

B. RA、RC 与 SWA 在区域 2 中；

C. RB 与 SWA 在区域 1 中；

2. 路由器之间配置 GRE：

路由采用隧道模式，路由器不能用实际接口的 IP 做 OSPF 路由，必须使用虚拟隧道 Tunnel 的 IP 进行路由。

3. RA 与 RB 之间配置 PPP 链路封装协议：

A. 采用 CHAP 认证；

B. RA 用户名：ra_route,RB 用户名:rb_route 密码为：digitalchina；

C. RB 为 DCE 端，时钟频率为 9600bps。

4. SWA 与 SWB 开启快速生成树协议：

将 SWA 设置为根交换机。

5. RB 开启 L2TP VPN：

A. 使 PCA 与 PCB 可以拨入到 RB 路由器上；

B. 用户名为：admin 密码为：123456

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证 VPN 连接

查看第一阶段连接后情况，如果正确，则会出现已连接好信息，若不正确，则空白
sh crypto isakmp sa
查看第二阶段连接后情况，如果正确，则会出现已连接好信息，并将加密信息与认证信息一 一呈现，若不正确，则空白
sh crypto ipsec sa
查看第一阶段连接过程
debug crypto isakmp
查看第二阶段连接过程
debug crypto ipsec

3. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

4. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database

查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

5. 验证生成树协议

查看生成树状态，可以看到本网桥在每一个实例中状态，包括 STP 版本，该实例对应的本网桥优先级及 MAC，该实例对应的根网桥优先级及 MAC，网桥到整个网络总根的路径代价，网桥上该实例的根端口，该实例对应的端口状态，该实例对应的端口角色等
show spanning-tree

五、 注意事项

1. 配置 ospf 时，需要注意先要配置 GRE 隧道绑定源和目的端口 IP，通过隧道的 IP 网段宣告到 OSPF 里的直连网段。
2. 配置 L2TP 时候注意开启 AAA 认证，创建本地地址池，创建虚拟模板调用地址池，最后创建 VPDN。

六、 配置参考

RA 路由器：

```
RA_config#show running-config
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication login default local
aaa authentication ppp default local
```

```
!
username ra_route password 0 digitalchina
!
!
interface Tunnel1
 mtu 1476
 ip address 1.1.1.1 255.255.255.0
 no ip directed-broadcast
 tunnel source 202.106.1.1
 tunnel destination 202.106.1.2
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 ip address 202.106.1.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname rb_route
 ppp chap password 0 digitalchina
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 1.1.1.0 255.255.255.0 area 0
 network 192.168.1.0 255.255.255.0 area 2
!
!
RA_config#
RA_config#
```

RB 路由器：

```
RB_config#show running-config
正在收集配置...

当前配置:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
ip local pool l2tp_pool 192.168.100.1 10
!
aaa authentication login default local
aaa authentication ppp default local
!
username rb_route password 0 digitalchina
username admin password 0 123456
!
!
interface Tunnel1
 mtu 1476
 ip address 1.1.1.2 255.255.255.0
 no ip directed-broadcast
 tunnel source 202.106.1.2
 tunnel destination 202.106.1.1
!
interface Tunnel3
 mtu 1476
 ip address 2.2.2.1 255.255.255.0
 no ip directed-broadcast
 tunnel source 210.216.1.1
 tunnel destination 210.216.1.2
!
interface Virtual-template0
 ip address 192.168.100.254 255.255.255.0
```

```
 no ip directed-broadcast
 peer default ip address pool l2tp_pool
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 192.168.3.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 ip address 202.106.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ra_route
 ppp chap password 0 digitalchina
 physical-layer speed 9600
!
interface Serial0/2
 ip address 210.216.1.1 255.255.255.0
 no ip directed-broadcast
 physical-layer speed 9600
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 2.2.2.0 255.255.255.0 area 0
 network 1.1.1.0 255.255.255.0 area 0
 network 172.16.1.0 255.255.255.0 area 0
 network 192.168.3.0 255.255.255.0 area 1
!
!
vpdn enable
!
vpdn-group 0
 accept-dialin
 port Virtual-template0
 protocol l2tp
```

```
 lcp-renegotiation
!
!
RB_config#
```

RC 路由器：

```
RC#show running-config
Building configuration...

Current configuration:
!
!version 1.3.3G
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
interface Tunnel2
 mtu 1476
 ip address 2.2.2.2 255.255.255.0
 no ip directed-broadcast
 tunnel source 210.216.1.2
 tunnel destination 210.216.1.1
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/3
 ip address 192.168.2.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
```

```
 ip address 210.216.1.2 255.255.255.0
 no ip directed-broadcast
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 2.2.2.0 255.255.255.0 area 0
 network 192.168.2.0 255.255.255.0 area 2
!
RC#
```

SWA 交换机：

```
SWA#show running-config
!
no service password-encryption
!
hostname SWA
!
spanning-tree
spanning-tree mst 0 priority 0
!
ipv6 enable
!
vlan 1
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
vlan 50
!
Interface Ethernet0/0/1
!
Interface Ethernet0/0/2
!
```

```
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
!
Interface Ethernet0/0/11
 switchport mode trunk
!
Interface Ethernet0/0/12
 switchport mode trunk
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
 switchport access vlan 10
!
```

```
Interface Ethernet0/0/23
 switchport access vlan 20
!
Interface Ethernet0/0/24
 switchport access vlan 30
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
interface Vlan1
!
interface Vlan10
 ip address 192.168.1.2 255.255.255.0
!
interface Vlan20
 ip address 192.168.3.2 255.255.255.0
!
interface Vlan30
 ip address 192.168.2.2 255.255.255.0
!
interface Vlan40
 ip address 192.168.10.254 255.255.255.0
!
interface Vlan50
 ip address 192.168.20.254 255.255.255.0
!
router ospf 1
 network 192.168.1.0 0.0.0.255 area 2
 network 192.168.2.0 0.0.0.255 area 2
 network 192.168.3.0 0.0.0.255 area 1
 network 192.168.10.0 0.0.0.255 area 2
 network 192.168.20.0 0.0.0.255 area 2
!
no login
!
End
```

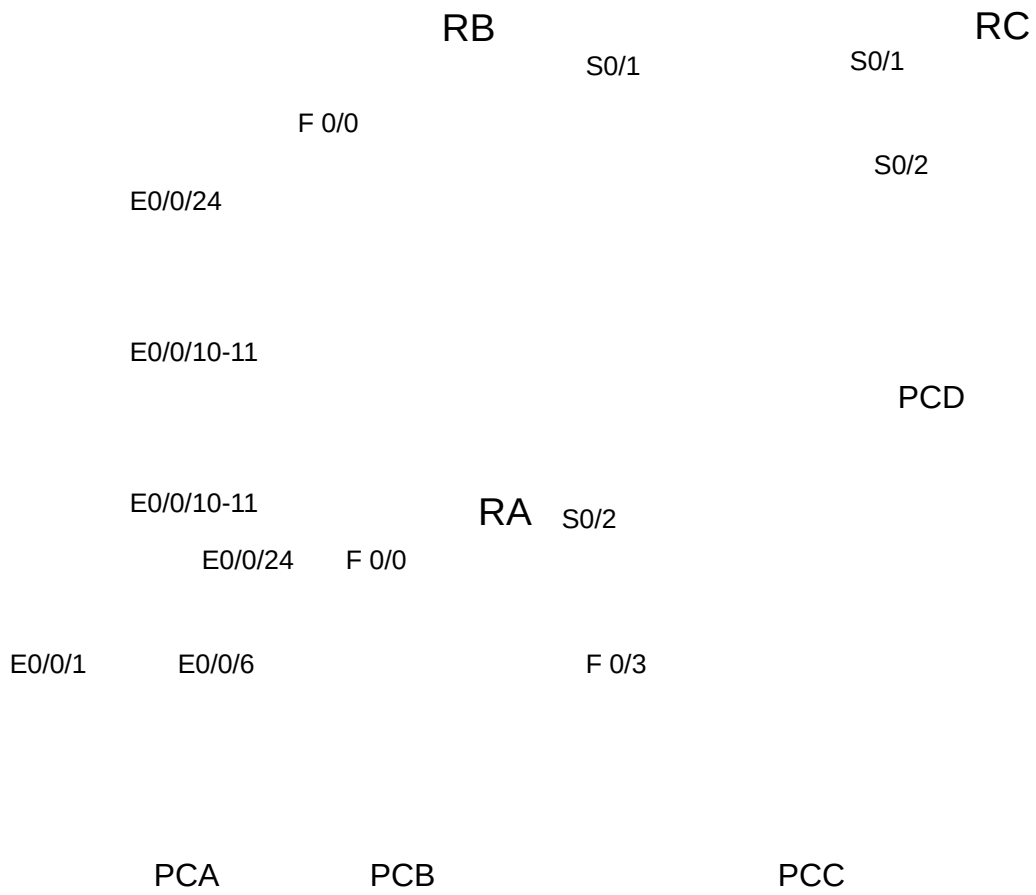
SWB 交换机：

```
SWB#show run
SWB#show running-config
!
no service password-encryption
!
hostname SWB
!
spanning-tree
!
vlan 1
!
vlan 40
!
vlan 50
!
Interface Ethernet0/0/1
 switchport access vlan 40
!
Interface Ethernet0/0/2
 switchport access vlan 40
!
Interface Ethernet0/0/3
 switchport access vlan 40
!
Interface Ethernet0/0/4
 switchport access vlan 40
!
Interface Ethernet0/0/5
 switchport access vlan 40
!
Interface Ethernet0/0/6
 switchport access vlan 50
!
Interface Ethernet0/0/7
 switchport access vlan 50
!
Interface Ethernet0/0/8
 switchport access vlan 50
!
Interface Ethernet0/0/9
 switchport access vlan 50
!
Interface Ethernet0/0/10
```

```
 switchport access vlan 50
!
Interface Ethernet0/0/11
 switchport mode trunk
!
Interface Ethernet0/0/12
 switchport mode trunk
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
no login
!
end
```

16

一、 拓扑图



二、 环境准备

1. 设备要求

3 台路由器 DCR-2626

2 台交换机 DCRS-5650-28

4 台 PC 电脑

2. IP 地址规划

RC	
S0/1	202.106.0.2/24
S0/2	202.106.1.2/24
F0/0	192.168.40.1/24
RB	
S0/1	202.106.0.1/24

F0/0	100.1.3.2/24	
RA		
S0/2	202.106.1.1/24	
F0/0	100.1.2.2/24	
F0/3	192.168.30.1/24	
SWA		
VLAN10	E0/0/1-5	192.168.10.1/24
VLAN20	E0/0/6-9	192.168.20.1/24
VLAN100	Group1	100.1.1.1/24
VLAN200	E0/0/24	100.1.2.1/24
SWB		
VLAN100	Group1	100.1.1.2/24
VLAN200	E0/0/24	100.1.3.1/24
PCA	192.168.10.10	
PCB	192.168.20.10	
PCC	192.168.30.10	
PCD	192.168.40.10	

3. 配置准备

A. 按照题目 VLAN 表正确配置 VLAN 以及端口划分。

B. 按照实验拓扑正确连接各个设备。

C. 按照 IP 表正确配置路由交换之间的 IP。

D. 按照题目要求配置设备

三、 方案要求

1. 在 RA 上配置网络地址转换：

A. FA0/3 所连接网络为外网；

B. PCA 为 web 服务器，将服务器 80 端口镜像到 FA0/3 端口。

2. 全网络运行 ospf 动态路由选择协议：

全网进行区域加密，采用密文方式，密码为：lin。

3. 在 SWA 与 SWB 之间配置链路聚合。

4. 使 SWA 的 PCA 端口可以监听 PCB 端口的所有入数据。

5. RA 与 RC 配置 PPP 链路封装协议：

使用 PAP 单向认证

6. RB 与 RC 配置 PPP 链路封装协议：

使用 CHAP 双向认证。

四、 验证思路

1. 查看配置文件

Show running-config 确保配置是否正确

2. 验证网络地址转换

查看协议状态
Show ip nat statistics
查看转换后的 ip 信息，如果配置正确，则会出现 nat 转换表（注：在查看之前请先让内网用户与外网进行通信，以保证有数据通过而进行转换，静态 NAT 不需流量触发）
show ip nat translations

3. 查看全网互通

查看路由表，是否学到全网路由
Show ip route
查看 OSPF 路由协议状态，可以看到 OSPF 进程号、router id、管理距离等信息
Show ip ospf
查看路由表，可以看到路由器学到的各个路由条目，同区域内以“O”开头，不同区域以“OIA”开头
Show ip route
查看链路状态数据库，可以看到整个网络内所有的链路状态信息
Show ip ospf database
查看设备的 OSPF 邻居信息，可以看到所相邻的 OSPF 设备
Show ip ospf neighbor
也可在 PC 上使用 Ping 命令进行链路连通性的测试。

4. 验证 PPP 连接

查看 PPP 连接状态，若已连接，会出现连接后的状况，并显示对端路由器信息及认证信息。
Show ppp status
查看 PPP 的认证过程，会出现相互验证过程，如果成功会停止认证并显示已建立连接，否则则不停认证。
Debug ppp authentication

5. 验证端口镜像

在目的端口上的 PC 上开启抓包软件，检查是否能抓获到监控端口的数据包。

五、 注意事项

1. 在 RA 上配置网络地址转换时注意方向。
2. 做端口映射的时候注意用的是 inside source，把内网的源地址映射到外网。
3. 配置链路聚合时要注意先配置，后连线。

六、 配置参考

RA 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RA
!
!
gbsc group default
!
!
aaa authentication ppp lin local
!
username RC password 0 123456
!
!
interface FastEthernet0/0
 ip address 100.1.2.2 255.255.255.0
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip nat inside
!
interface FastEthernet0/3
 ip address 192.168.30.1 255.255.255.0
 no ip directed-broadcast
 ip nat outside
!
```

```
interface Serial0/1
 no ip address
 no ip directed-broadcast
!
interface Serial0/2
 ip address 202.106.1.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication pap lin
 ppp pap sent-username RA password 0 123456
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip nat inside
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 202.106.1.0 255.255.255.0 area 0
 network 100.1.2.0 255.255.255.0 area 0
 area 0 authentication message-digest
!
!
ip route default FastEthernet0/3
!
!
ip access-list standard lin
 permit any
!
!
ip nat inside source static tcp 192.168.10.10 80 192.168.30.1 80
ip nat inside source list lin interface FastEthernet0/3
!
!
```

RB 路由器：

```
RB#sho run
Building configuration...
```

```
Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RB
!
!
gbsc group default
!
!
aaa authentication ppp lin-chap local
!
username RC password 0 123456
!
!
interface FastEthernet0/0
 ip address 100.1.3.2 255.255.255.0
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
!
interface FastEthernet0/3
 no ip address
 no ip directed-broadcast
!
interface Serial0/1
 ip address 202.106.0.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap lin-chap
 ppp chap hostname RB
 ppp chap password 0 123456
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
!
interface Async0/0
```

```
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 100.1.3.0 255.255.255.0 area 0
 network 202.106.0.0 255.255.255.0 area 0
 area 0 authentication message-digest
!
!
!
```

RC 路由器：

```
sho run
Building configuration...

Current configuration:
!
!version 1.3.3F
service timestamps log date
service timestamps debug date
no service password-encryption
!
hostname RC
!
!
gbsc group default
!
!
aaa authentication ppp default local
aaa authentication ppp lin-chap local
!
username RA password 0 123456
username RB password 0 123456
!
!
interface FastEthernet0/0
 ip address 192.168.40.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/3
 no ip address
```

```
 no ip directed-broadcast
!
interface Serial0/1
 ip address 202.106.0.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp authentication chap lin-chap
 ppp chap hostname RC
 ppp chap password 0 123456
 physical-layer speed 64000
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
!
interface Serial0/2
 ip address 202.106.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp pap sent-username RC password 0 123456
 physical-layer speed 64000
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
!
interface Async0/0
 no ip address
 no ip directed-broadcast
!
!
router ospf 1
 network 202.106.0.0 255.255.255.0 area 0
 network 202.106.1.0 255.255.255.0 area 0
 network 192.168.40.0 255.255.255.0 area 0
 area 0 authentication message-digest
!
!
ip route default 202.106.1.1
!
!
```

SWA 交换机：

```
sho run
!
```

```
no service password-encryption
!
hostname SWA
!
vlan 1
!
vlan 10
!
vlan 20
!
vlan 100
!
vlan 200
!
port-group 1 load-balance src-mac
!
Interface Ethernet0/0/1
 switchport access vlan 10
!
Interface Ethernet0/0/2
 switchport access vlan 10
!
Interface Ethernet0/0/3
 switchport access vlan 10
!
Interface Ethernet0/0/4
 switchport access vlan 10
!
Interface Ethernet0/0/5
 switchport access vlan 10
!
Interface Ethernet0/0/6
 switchport access vlan 20
!
Interface Ethernet0/0/7
 switchport access vlan 20
!
Interface Ethernet0/0/8
 switchport access vlan 20
!
Interface Ethernet0/0/9
 switchport access vlan 20
!
```

```
Interface Ethernet0/0/10
 switchport access vlan 100
 port-group 1 mode on
!
Interface Ethernet0/0/11
 switchport access vlan 100
 port-group 1 mode on
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
```

```
Interface Port-Channel1
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan100
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip address 100.1.1.1 255.255.255.0
!
interface Vlan200
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip address 100.1.2.1 255.255.255.0
!
router ospf 1
 area 0 authentication message-digest
 network 100.1.1.0 0.0.0.255 area 0
 network 100.1.2.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
ip route 0.0.0.0/0 100.1.2.2
!
no login
!
end
```

SWB 交换机：

```
sho run
!
no service password-encryption
!
hostname SWB
!
vlan 1
!
vlan 100
!
```

```
vlan 200
!
port-group 1 load-balance src-mac
!
Interface Ethernet0/0/1
!
Interface Ethernet0/0/2
!
Interface Ethernet0/0/3
!
Interface Ethernet0/0/4
!
Interface Ethernet0/0/5
!
Interface Ethernet0/0/6
!
Interface Ethernet0/0/7
!
Interface Ethernet0/0/8
!
Interface Ethernet0/0/9
!
Interface Ethernet0/0/10
 switchport access vlan 100
 port-group 1 mode on
!
Interface Ethernet0/0/11
 switchport access vlan 100
 port-group 1 mode on
!
Interface Ethernet0/0/12
!
Interface Ethernet0/0/13
!
Interface Ethernet0/0/14
!
Interface Ethernet0/0/15
!
Interface Ethernet0/0/16
!
Interface Ethernet0/0/17
!
Interface Ethernet0/0/18
```

```
!
Interface Ethernet0/0/19
!
Interface Ethernet0/0/20
!
Interface Ethernet0/0/21
!
Interface Ethernet0/0/22
!
Interface Ethernet0/0/23
!
Interface Ethernet0/0/24
 switchport access vlan 200
!
Interface Ethernet0/0/25
!
Interface Ethernet0/0/26
!
Interface Ethernet0/0/27
!
Interface Ethernet0/0/28
!
Interface Port-Channel1
!
interface Vlan100
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip address 100.1.1.2 255.255.255.0
!
interface Vlan200
 ip ospf authentication message-digest
 ip ospf message-digest-key 10 md5 lin
 ip address 100.1.3.1 255.255.255.0
!
router ospf 1
 area 0 authentication message-digest
 network 100.1.1.0 0.0.0.255 area 0
 network 100.1.3.0 0.0.0.255 area 0
!
no login
!
end
```

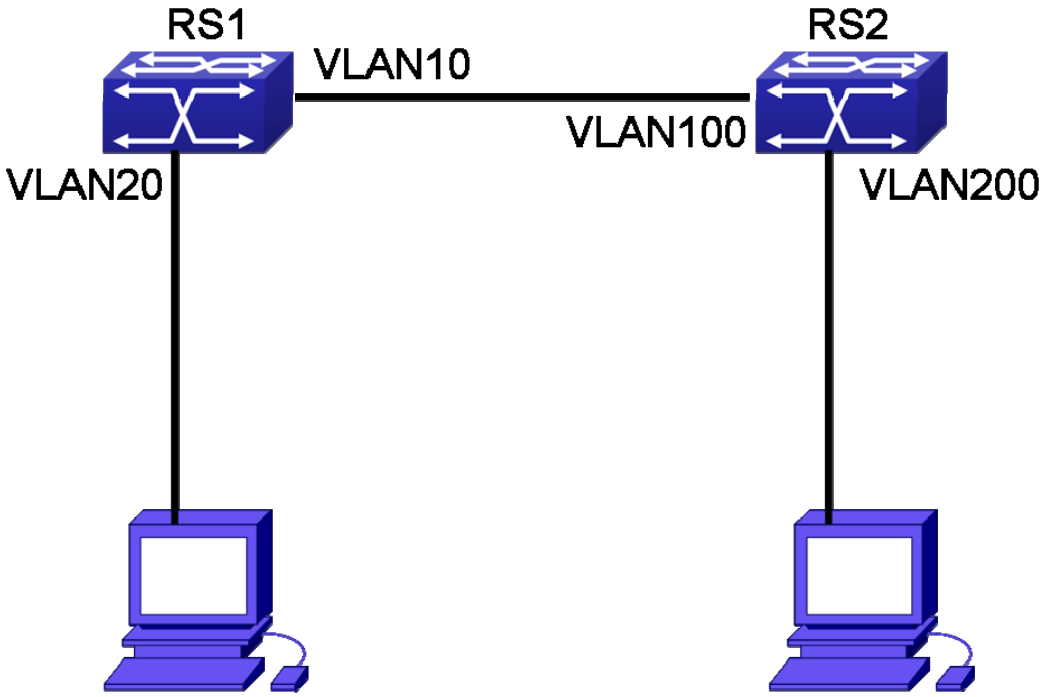
附录一：

交换机组播三层对接实训 一

一、 实训设备

1、 DCRS-5650 交换机 2 台（SoftWare version is DCRS-5650-28_5.2.1.0）
2、 PC 机 2-4 台
3、 Console 线 1-2 根
4、 直通网线 2-8 根

二、 实训拓扑



三、 实训要求

1、在交换机上划分基于端口的 VLAN：

交换机	VLAN	端口成员	IP	连接
交换机 A	10	E0/0/11	10.0.0.1/24	交换机 B e0/0/24
交换机 A	20	E0/0/1	20.0.0.1/24	20.0.0.2/24
交换机 B	100	E0/0/11	10.0.0.2/24	交换机 A e0/0/11
交换机 B	200	E0/0/1	30.0.0.1/24	30.0.0.2/24

2、所有左 PC 是组播服务器，右 PC 是客户端，在组播服务器上运行服务器软件 Wsend.exe，在 PC 客户端软件 MCastTest20，查看组播状态。

四、 实训步骤

第一步：交换机全部恢复出厂设置，配置交换机的VLAN信息

交换机A：

```
DCRS-5650-A(Config)#vlan 10
DCRS-5650-A(Config-Vlan10)#switchport interface ethernet 0/0/11
DCRS-5650-A(Config-Vlan10)#exit
DCRS-5650-A(Config)#int vlan 10
DCRS-5650-A(Config-If-Vlan10)#ip add 10.0.0.1 255.255.255.0
DCRS-5650-A(Config-If-Vlan10)#exit
DCRS-5650-A(Config)#vlan 20
DCRS-5650-A(Config-Vlan20)#switchport interface ethernet 0/0/1
DCRS-5650-A(Config-Vlan10)#exit
DCRS-5650-A(Config)#int vlan 20
DCRS-5650-A(Config-If-Vlan20)#ip add 20.0.0.1 255.255.255.0
DCRS-5650-A(Config-If-Vlan20)#exit
DCRS-5650-A(Config)#
```

交换机B：

```
DCRS-5650-B(Config)#vlan 100
DCRS-5650-B(Config-Vlan100)#switchport interface ethernet 0/0/11
DCRS-5650-B(Config-Vlan100)#exit
DCRS-5650-B(Config)#int vlan 100
DCRS-5650-B(Config-If-Vlan100)#ip add 10.0.0.2 255.255.255.0
DCRS-5650-B(Config-If-Vlan100)#exit
DCRS-5650-B(Config)#vlan 200
DCRS-5650-B(Config-Vlan200)#switchport interface ethernet 0/0/1
DCRS-5650-B(Config-Vlan200)#exit
DCRS-5650-B(Config)#int vlan 200
DCRS-5650-B(Config-If-Vlan200)#ip add 30.0.0.1 255.255.255.0
DCRS-5650-B(Config-If-Vlan200)#exit
DCRS-5650-B(Config)#
```

验证配置

由左PC ping 右PC，不能够通信。

第二步：启动DVMRP协议

交换机A：

```
DCRS-5650-A(Config)ip dvmrp multicast-routing    ！开启组播协议
DCRS-5650-A(Config)#int vlan 10
DCRS-5650-A(Config-If-Vlan1)#ip dvmrp enable        ！在vlan接口上开启dvmrp
```

协议

DCRS-5650-A(Config-If-Vlan1)#exit

DCRS-5650-A(Config)#int vlan 20

DCRS-5650-A(Config-If-Vlan20)#ip dvmrp enable

DCRS-5650-A(Config-If-Vlan20)#

DCRS-5650-A(Config-If-Vlan20)#exit

DCRS-5650-A(Config)#

交换机B：

DCRS-5650-B(Config)ip dvmrp multicast-routing

DCRS-5650-B(Config)#int vlan 100

DCRS-5650-B(Config-If-Vlan100)#ip dvmrp enable

DCRS-5650-B(Config-If-Vlan100)#exit

DCRS-5650-B(Config)#int vlan 200

DCRS-5650-B(Config-If-Vlan200)#ip dvmrp enable

DCRS-5650-B(Config-If-Vlan200)#exit

DCRS-5650-B(Config)#

验证配置

RSB#show ip dvmrp route

Flags: N = New, D = DirectlyConnected, H = Holddown

Network Flags Nexthop Nexthop Metric Uptime Exptime

Xface Neighbor

10.0.0.0/8 .D. Vlan100 Directly Connected 1 00:00:53 00:00:00

30.0.0.0/8 .D. Vlan200 Directly Connected 1 00:00:32 00:00:00

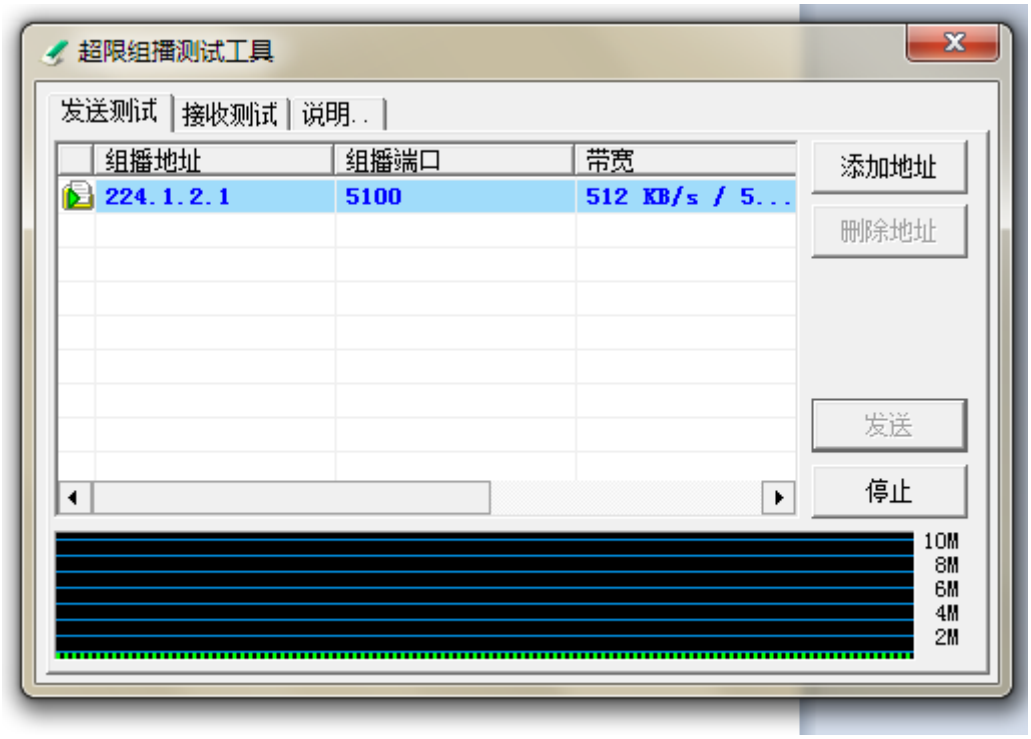
RSA#show ip dvmrp neighbor

Neighbor Address Interface Uptime/Expires Maj Ver Min Ver Cap Flg

10.0.0.2 Vlan10 00:02:00/00:00:25 3 255 2e

RSA#

组播服务器发送广播包：



组播客户端成功接收：

由左PC做组播服务器，向右PC发送组播报，右PC做组播客户端，可以接收由左PC发出的组播报，证明成功。

由此证明即使在单播不能够进行通信的情况下，dvmrp组播协议也能通信，DVMRP组播协议带有有最优路由选择功能。

五、 注意事项和排错

DVMRP 的一些重要特性是：

1.用于决定反向路径检查信息的路由交换以距离向量为基础（方式与 RIP 相似）

2. 路由交换更新周期性的发生（缺省为 60 秒）

3. TTL 上限 = 32 跳（而 RIP 是 16）

4.路由更新包括掩码，支持 CIDR

交换机组播三层对接实训 二

一、 实训设备

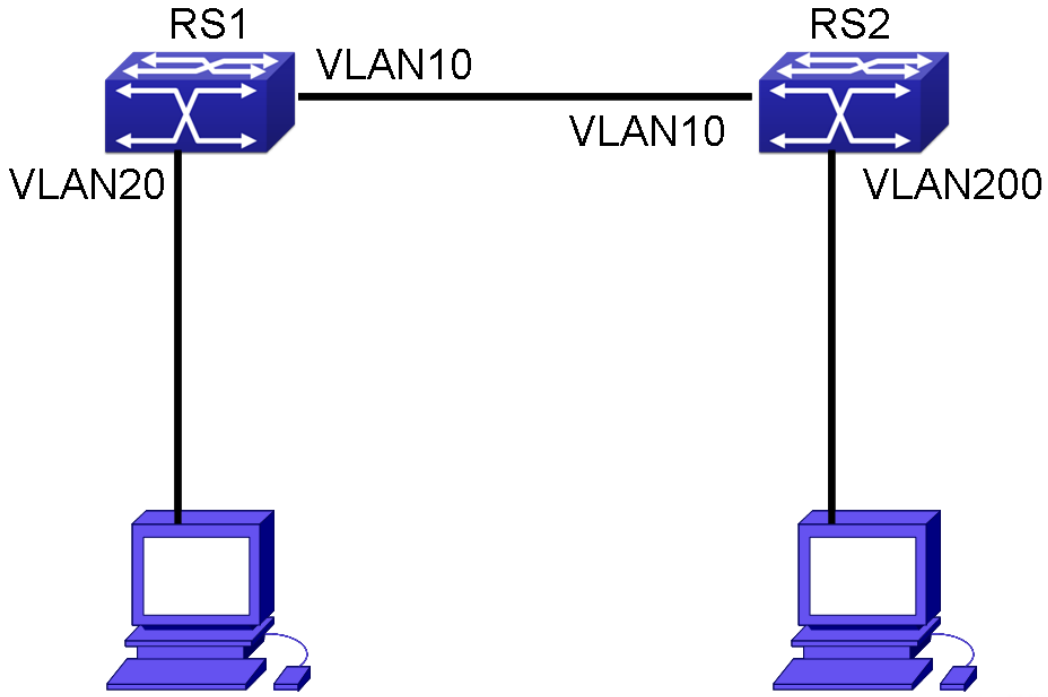
1、 DCRS-5650 交换机 2 台（SoftWare version is DCRS-5650-28_5.2.1.0）

2、 PC 机 2-4 台

3、 Console 线 1-2 根

4、 直通网线 2-8 根

二、 实训拓扑



三、 实训要求

1、 在交换机上划分基于端口的 VLAN：

交换机	VLAN	端口成员	IP	连接
交换机 A	10	E0/0/11	10.0.0.1/24	交换机 B e0/0/24
交换机 A	20	E0/0/1	20.0.0.1/24	20.0.0.2/24
交换机 B	10	E0/0/11	10.0.0.2/24	交换机 A e0/0/11

交换机 B	200	E0/0/1	30.0.0.1/24	30.0.0.2/24

2、所有左 PC 是组播服务器，右 PC 是客户端，在组播服务器上运行服务器软件 Wsend.exe，在 PC 客户端软件 MCastTest20，查看组播状态。

四、 实训步骤

第一步：交换机全部恢复出厂设置，配置交换机的VLAN信息

交换机A：

```
DCRS-5650-A(Config)#vlan 10
DCRS-5650-A(Config-Vlan10)#switchport interface ethernet 0/0/11
DCRS-5650-A(Config-Vlan10)#exit
DCRS-5650-A(Config)#int vlan 10
DCRS-5650-A(Config-If-Vlan10)#ip add 10.0.0.1 255.255.255.0
DCRS-5650-A(Config-If-Vlan10)#exit
DCRS-5650-A(Config)#vlan 20
DCRS-5650-A(Config-Vlan20)#switchport interface ethernet 0/0/1
DCRS-5650-A(Config-Vlan10)#exit
DCRS-5650-A(Config)#int vlan 20
DCRS-5650-A(Config-If-Vlan20)#ip add 20.0.0.1 255.255.255.0
DCRS-5650-A(Config-If-Vlan20)#exit
DCRS-5650-A(Config)#
```

交换机B：

```
DCRS-5650-B(Config)#vlan 10
DCRS-5650-B(Config-Vlan10)#switchport interface ethernet 0/0/11
DCRS-5650-B(Config-Vlan10)#exit
DCRS-5650-B(Config)#int vlan 10
DCRS-5650-B(Config-If-Vlan10)#ip add 10.0.0.2 255.255.255.0
DCRS-5650-B(Config-If-Vlan10)#exit
DCRS-5650-B(Config)#vlan 200
DCRS-5650-B(Config-Vlan200)#switchport interface ethernet 0/0/1
DCRS-5650-B(Config-Vlan200)#exit
DCRS-5650-B(Config)#int vlan 200
DCRS-5650-B(Config-If-Vlan200)#ip add 30.0.0.1 255.255.255.0
DCRS-5650-B(Config-If-Vlan200)#exit
DCRS-5650-B(Config)#
```

验证配置

由左PC ping 右PC，不能够通信。

第二步：启动DVMRP协议

交换机A：

DCRS-5650-A(Config)ip pim multicast-routing ！开启组播协议

DCRS-5650-A(Config)#int vlan 10

DCRS-5650-A(Config-If-Vlan1)#ip pim dense-mode !在vlan接口上开启pim协议

DCRS-5650-A(Config-If-Vlan1)#exit

DCRS-5650-A(Config)#int vlan 20

DCRS-5650-A(Config-If-Vlan20)#ip pim dense-mode

DCRS-5650-A(Config-If-Vlan20)#

DCRS-5650-A(Config-If-Vlan20)#exit

DCRS-5650-A(Config)#

交换机B：

DCRS-5650-B(Config)ip pim multicast-routing

DCRS-5650-B(Config)#int vlan 10

DCRS-5650-B(Config-If-Vlan10)#ip pim dense-mode

DCRS-5650-B(Config-If-Vlan10)#exit

DCRS-5650-B(Config)#int vlan 200

DCRS-5650-B(Config-If-Vlan200)#ip pim dense-mode

DCRS-5650-B(Config-If-Vlan200)#exit

DCRS-5650-B(Config)#

验证配置

RSB#show ip pim nei

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.0.0.1	Vlan10	00:00:19/00:01:43	v2	1 /

RSB#show ip pim interface detail

Vlan10 (vif 0):

Address 10.0.0.2, DR 10.0.0.2

Hello period 30 seconds, Next Hello in 0 seconds

Triggered Hello period 5 seconds

Neighbors:

10.0.0.1

Vlan200 (vif 1):

Address 30.0.0.1, DR 30.0.0.1

Hello period 30 seconds, Next Hello in 12 seconds

Triggered Hello period 5 seconds

Neighbors:

由左PC做组播服务器，向右PC发送组播报，右PC做组播客户端，不可以接收由左PC发出的组播报。

由此证明在单播不能够进行通信的情况下，pim组播协议也不能通信，pim组播协议不带有路由选择功能。

第三步：配置路由协议

DCRS-5650-A(Config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2

DCRS-5650-A(Config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1

验证配置

由左PC ping 右PC，可以通信。

由左PC做组播服务器，向右PC发送组播报，右PC做组播客户端，可以接收由左PC发出的组播报。

由此证明pim组播协议本身不带有最优路径的算法，要依靠单薄协议或静态路由完成最优路径的选择，但是并不管是什么协议。

五、 注意事项和排错

DVMRP 的一些重要特性是：

1.用于决定反向路径检查信息的路由交换以距离向量为基础（方式与 RIP 相似）

2. 路由交换更新周期性的发生（缺省为 60 秒）

3. TTL 上限 = 32 跳（而 RIP 是 16）

4.路由更新包括掩码，支持 CIDR

交换机组播二层对接

一、 实训设备

1、 DCRS-5650 交换机 1 台（SoftWare version is DCRS-5650-28_5.2.1.0）

2、 DCS-3926S 交换机 1 台

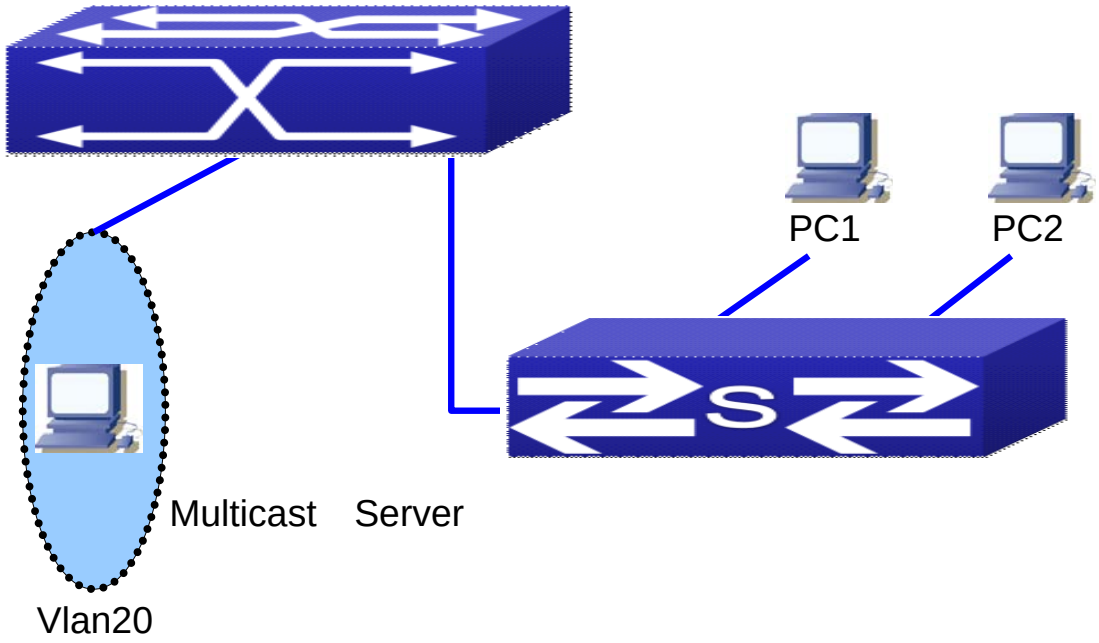
3、 PC 机 2-4 台

4、 Console 线 1-2 根

5、 直通网线 2-8 根

6、 组播测试软件：发送端、接收端

二、 实训拓扑



三、 实训要求

1、在交换机 C 上划分基于端口的 VLAN：

VLAN	端口成员	IP	连接
1	e0/0/24	192.168.10.0/0/24	交换机 e0/0/24
20	e0/0/9	192.168.20.0/0/24	组播服务器

2、所有 PC 的都是组播客户端，在组播服务器上运行服务器软件 Wsend.exe，在 PC 客户端软件 Wsend.exe，查看组播状态。

四、 实训步骤

第一步：在三层交换机上恢复出厂设置，配置交换机的VLAN信息

DCRS-5650(Config)#vlan 20
DCRS-5650(Config-Vlan20)#switchport interface ethernet 0/0/9
Set the port Ethernet0/0/9 access vlan 20 successfully
DCRS-5650(Config-Vlan20)#exit
DCRS-5650(Config)#
DCRS-5650(Config)#interface vlan 1
DCRS-5650(Config-If-Vlan1)#ip address 192.168.10.1 255.255.255.0
DCRS-5650(Config-If-Vlan1)#exit

DCRS-5650(Config)#interface vlan 20

DCRS-5650(Config-If-Vlan20)#ip address 192.168.20.1 255.255.255.0

DCRS-5650(Config-If-Vlan20)#exit

第二步：三层交换机启动PIM-DM协议

DCRS-5650 (Config)#ip pim multicast-routing ！使能组播协议

DCRS-5650(Config)#int vlan 1

DCRS-5650(Config-If-Vlan1)#ip pim dense-mode !启动本接口PIM-DM协议

DCRS-5650(Config-If-Vlan1)#exit

DCRS-5650(Config)#int vlan 20

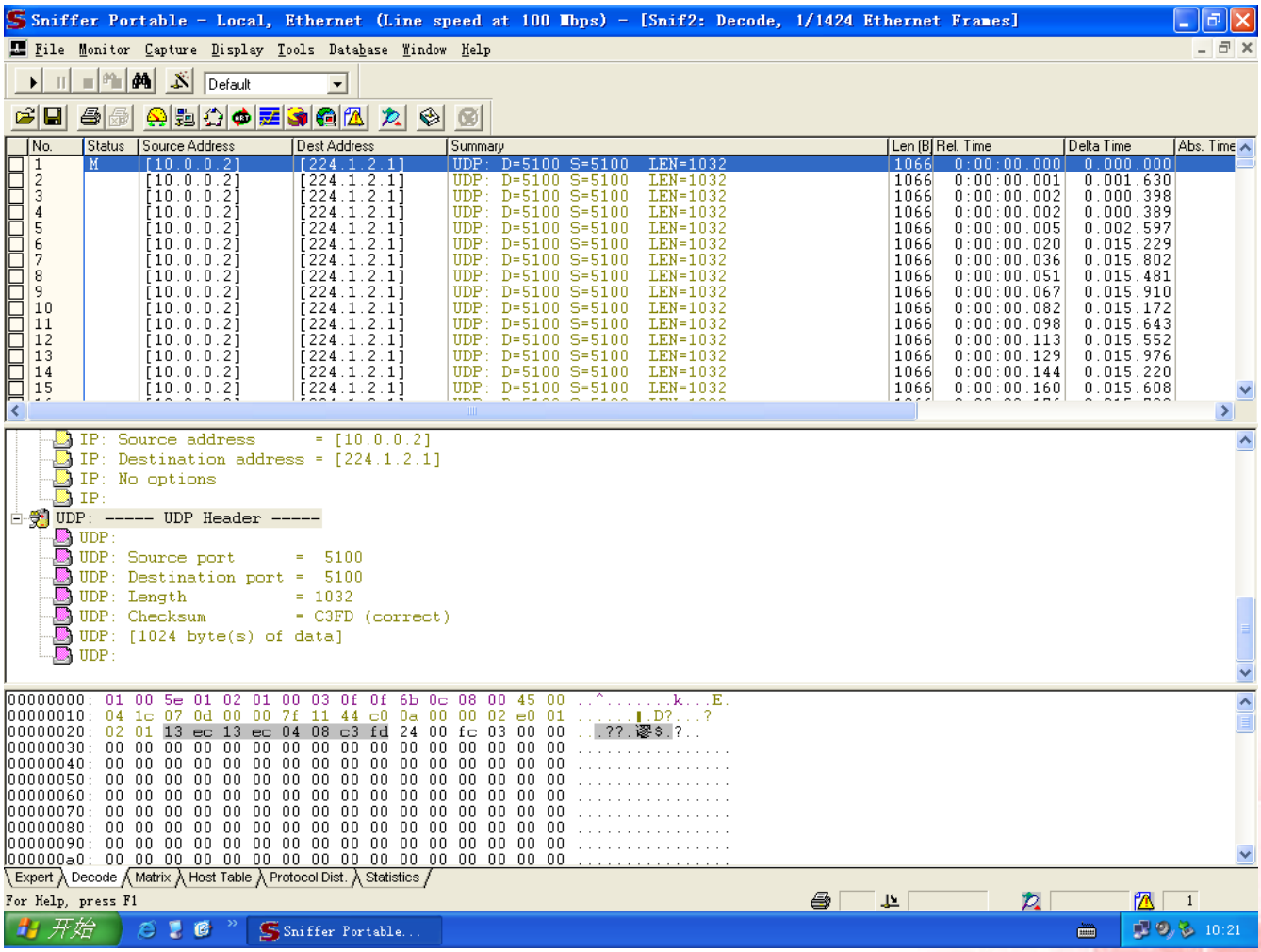
DCRS-5650(Config-If-Vlan20)#ip pim dense-mode

DCRS-5650(Config-If-Vlan20)#exit

DCRS-5650(Config)#

验证配置：

在组播服务器发生那个组播数据包，组播客户端可以接收，同时用另外一台计算机开启sniffer进行抓包，可以抓到网络中的组播数据：



第三步：二层交换机启动IGMP侦听

在二层交换机启动指定vlan的IGMP Snooping功能，二层交换机默认接受组播数据，可以不做配置，这样组播数据会按照广播的形式传送。以下以 vlan1 为例。

其他二层功能参考前面实验，先配置vlan信息，trunk端口等，与三层交换机连通，再进行如下配置：

```
switch(Config)#ip igmp snooping                    ! 启动 IGMP Snooping功能
switch(Config)#ip igmp snooping vlan 1             ! 指定vlan的IGMP Snooping
IGMP snooping is started on Vlan 1
switch(Config)#ip igmp snooping vlan 1 mroute interface ethernet0/0/2
switch(config)#
```

验证配置

```
switch#show ip igmp snooping
igmp snooping status                :  Enabled
IGMP information for VLAN 20:

igmp snooping vlan status          :Disabled
igmp snooping vlan query           :Disabled
igmp snooping vlan mrouter port :
-------------------------------

IGMP information for VLAN 1:

igmp snooping vlan status          :Enabled
igmp snooping vlan query           :Disabled
igmp snooping vlan mrouter port :
            Ethernet0/0/2;state :UP
```

```
switch#show mac
Read mac address table....
Vlan Mac Address                    Type      Creator     Ports
------------------------------------------------------------------------
1      00-03-0f-0f-6b-0c            DYNAMIC Hardware Ethernet0/0/2
1      00-03-0f-0f-6b-0d            DYNAMIC Hardware Ethernet0/0/2
1      00-26-9e-52-4a-05             DYNAMIC Hardware Ethernet0/0/2
10     00-03-0f-00-a9-59             STATIC   System     CPU
10     00-03-0f-0f-6b-0c            DYNAMIC Hardware Ethernet0/0/2
10     00-0b-cd-4a-97-2e             DYNAMIC Hardware Ethernet0/0/18
10     00-22-64-c0-80-94             DYNAMIC Hardware Ethernet0/0/16
switch#

switch#show mac multicast
Vlan Mac Address                    Type      Creator     Ports
------------------------------------------------------------------------
1      01-00-5e-00-00-fc            MULTI     IGMP        Ethernet0/0/2
switch#show mac multicast
Vlan Mac Address                    Type      Creator     Ports
----------------------------------- ----------------------------------
1      01-00-5e-00-00-fc            MULTI     IGMP        Ethernet0/0/2
1      01-00-5e-01-02-01             MULTI     IGMP        Ethernet0/0/2
switch#
```

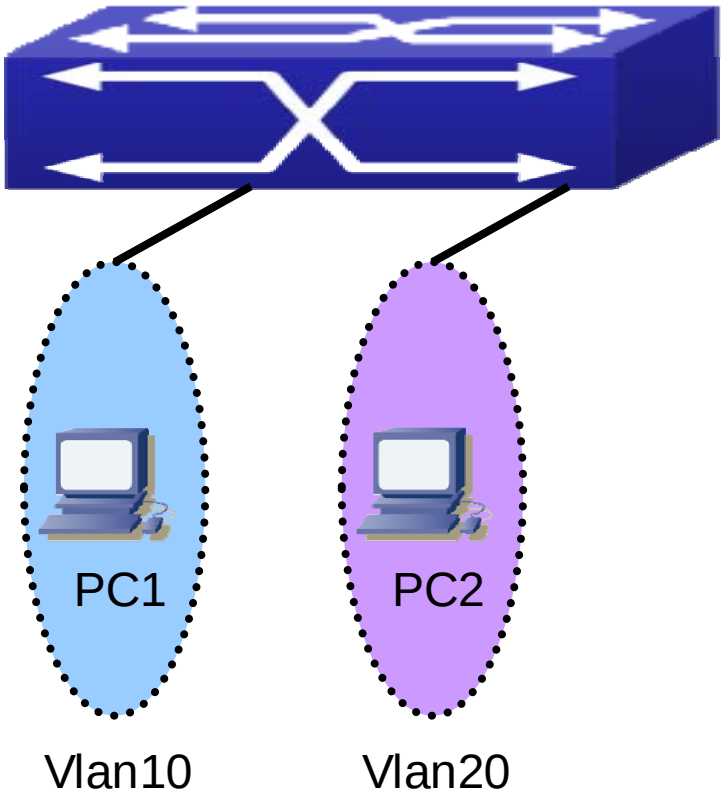
在二层交换上启动snoop侦听后，在非组播客户端上无法捕获组播客户端上的组播数据，说明组播已经不在以广播的形式发包。

多层交换机 QoS

一、 实训设备

1. DCRS-5650 交换机 1 台（SoftWare version is DCRS-5650-28_5.2.1.0）
2. PC 机 2-4 台
3. Console 线 1 根
4. 直通网线若干

二、 实训拓扑



三、 实训要求

在交换机上划分两个基于端口的 VLAN：VLAN10，VLAN20

VLAN	端口成员	IP 地址
10	0/0/1-8	192.168.10.1/24
20	0/0/9-16	192.168.20.1/24

PC 的网络设置为：

设备	IP	网关 2
PC1	192.168.10.2/24	192.168.10.1
PC2	192.168.20.2/24	192.168.20.1

实施 QoS 策略，使来自 192.168.10.2/24 的 FTP 报文带宽限制为 1M 比特/秒，突发值设为 1M 字节，超过带宽的该网段内的报文一律丢弃。

四、 实训步骤

第一步：交换机全部恢复出厂设置，创建 vlan 并添加端口。

DCRS-5650(Config)#vlan 10

DCRS-5650(Config-Vlan10)#DCRS-5650port interface e 0/0/1-8

DCRS-5650(Config-Vlan10)#exit
DCRS-5650(Config)#vlan 20
DCRS-5650(Config-Vlan20)#DCRS-5650port interface ethernet 0/0/9-16
DCRS-5650(Config-Vlan20)#exit
DCRS-5650(Config)#

第二步：添加 vlan 地址。

DCRS-5650(Config)#int vlan 10
DCRS-5650(Config-If-Vlan10)#ip address 192.168.10.1 255.255.255.0
DCRS-5650(Config-If-Vlan10)#no shut
DCRS-5650(Config-If-Vlan10)#exit
DCRS-5650(Config)#int vlan 20
DCRS-5650(Config-If-Vlan20)#ip address 192.168.20.1 255.255.255.0
DCRS-5650(Config-If-Vlan20)#exit
DCRS-5650(Config)#

第三步：配置 QoS

1、启动 QoS 功能：在全局下启动和关闭 QoS 功能。必须在全局下启动 QoS 功能后才能配置其它的 QoS 命令。

DCRS-5650(Config)#mls qos
DCRS-5650(Config)#

2、本实训中，因为要针对特定协议做 QOS，所以首先配置一个名字为 ftp_acl 的 ACL。

DCRS-5650(Config)# firewall enable
DCRS-5650(Config)# ip access-list extended ftp_acl
DCRS-5650(Config-IP-Ext-Nacl-ftp_acl)# permit tcp any-source any-destination d-port 21
DCRS-5650(Config-IP-Ext-Nacl-ftp_acl)# deny ip any-source any-destination
DCRS-5650(Config-IP-Ext-Nacl-ftp_acl)# exit
DCRS-5650(Config)#

3、置分类表(classmap):建立一个分类规则,可以按照 ACL,VLAN ID,IP Precedent，DSCP 来分类，本实训中使用刚建好的 ACL 来分类。

DCRS-5650(Config)#class-map ftp_class
DCRS-5650(Config-ClassMap)#match access-group ftp_acl
DCRS-5650(Config-ClassMap)#exit

DCRS-5650(Config)#

4、配置策略表（policymap）：建立一个策略表，可以对相应的分类规则进行带宽限制，优先级降低等操作。

DCRS-5650(Config)#policy-map qos_ftp
DCRS-5650(Config-PolicyMap)#class ftp_class
DCRS-5650(Config-Policy-Class)# police 1000 1000 exceed-action drop
DCRS-5650(Config-Policy-Class)#exit
DCRS-5650(Config-PolicyMap)#exit
DCRS-5650(Config)#

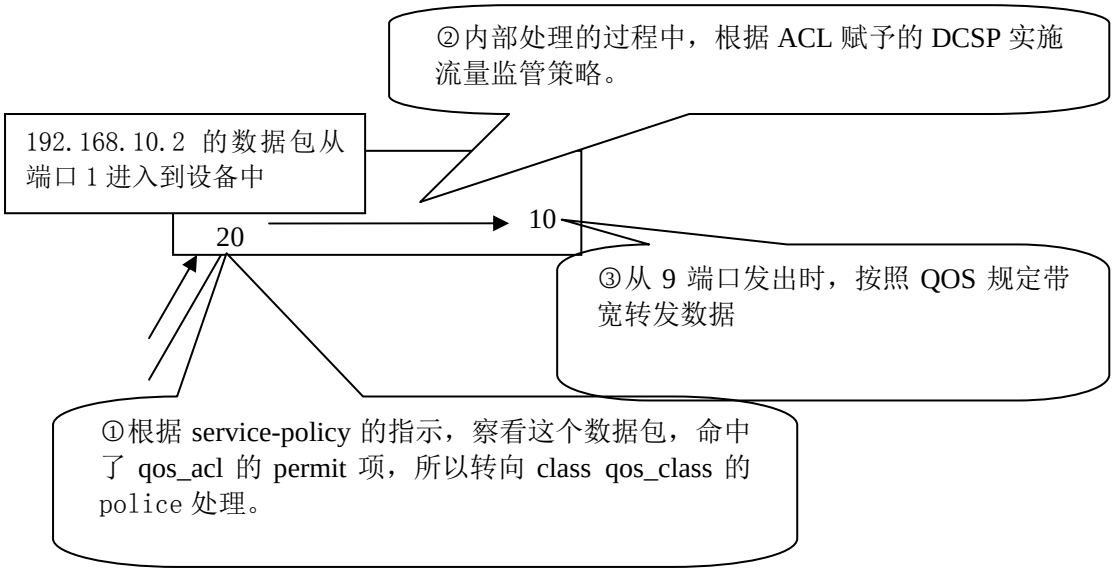
5、将 QoS 应用到端口：配置端口的信任模式，或者绑定策略。策略只有绑定到具体的端口，才在此端口生效。
DCRS-5650(Config)#interface ethernet 0/0/1
DCRS-5650(Config-Ethernet0/0/6)#service-policy input qos_ftp
DCRS-5650(Config-Ethernet0/0/6)#exit
DCRS-5650(Config)#

验证配置：
在 FTP server 端放置文件大小约为 14M 的测试文件，

在端口应用 QOS 策略前后观察客户端下载同一文件所用时间，直观观察速率变化

第四步：结论。

综合以上的分析，我们了解到本试验的数据将以如下图所示的方式进行处理：



五、 注意事项和排错

1、交换机端口缺省关闭 QoS，缺省设置 8 条发送队列，队列 1 转发普通的数据包，其它队列分别发送一些重要的控制报文（BPDU 等）。

2、在使能全局 QoS 后，所有交换机端口打开 QoS 功能，设置 8 条发送队列。端口的缺省 CoS 值为 0；端口为 not Trusted（不信任）状态；缺省优先级队列的 weights 值依次为 1，2，3，4，5，6，7，8，所有的 QoS Map 都采用缺省值。

3、CoS 值 7 默认映射到最高优先级队列 8，通常保留给某些协议报文使用，建议用户不要随意改变 COS 值 7 到队列 8 的映射关系，端口的缺省 CoS 值通常也不要设置为 7。

4、目前策略表只支持绑定到入口，对出口不支持。

附录二：

防火墙 SNAT 配置

一、实验设备

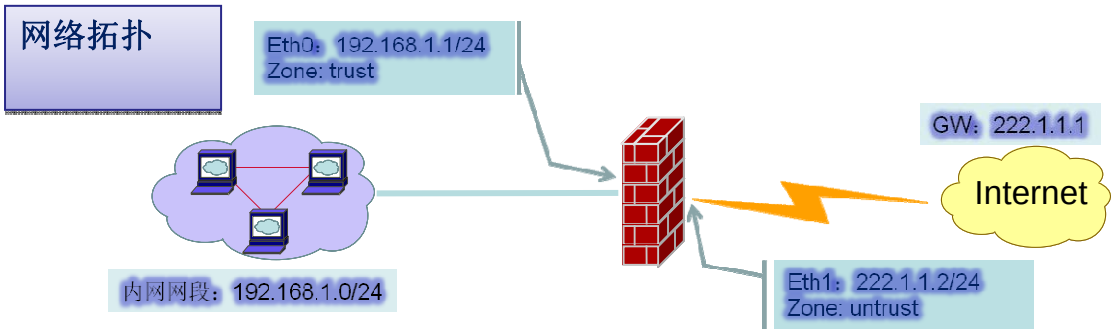
(1) 防火墙设备 1 台

(2) 局域网交换机 n 台

(3) 网络线 n 条

(4) PC 机 n 台

二、实验拓扑



三、实验要求

配置防火墙使内网 192.168.1.0/24 网段可以访问 internet

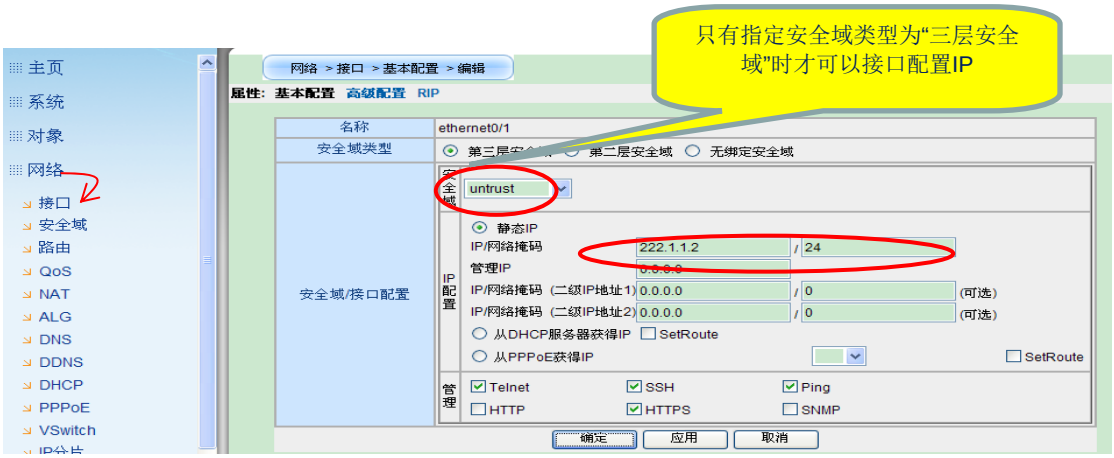
四、实验步骤

第一步：配置接口

首先通过防火墙默认 eth0 接口地址 192.168.1.1 登录到防火墙界面进行接口的配置

通过 Webui 登录防火墙界面

输入缺省用户名 admin，密码 admin 后点击登录，配置外网接口地址



内口网地址使用缺省 192.168.1.1

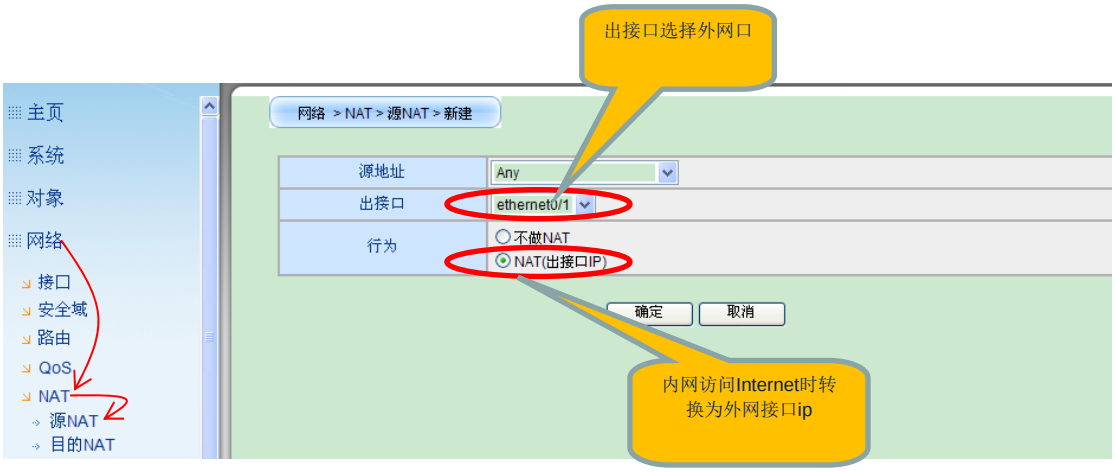
第二步：添加路由

添加到外网的缺省路由，在目的路由中新建路由条目

添加下一条地址

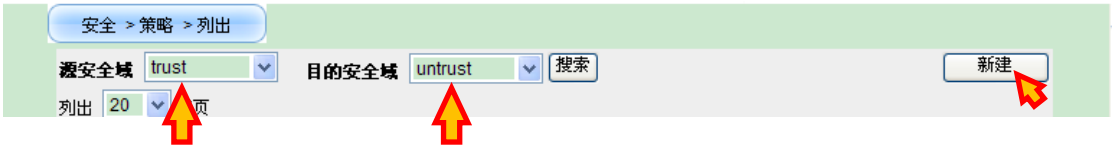
第三步：添加 SNAT 策略

在网络/NAT/SNAT 中添加源 NAT 策略



第四步：添加安全策略

在安全/策略中，选择好源安全域和目的安全域后，新建策略



关于 SNAT，我们只需要建立一条内网口安全域到外网口安全域放行的一条策略就可以保证内网能够访问到外网。

如果是需要对于策略中各个选项有更多的配置要求可以点击高级哦遏制进行编辑

防火墙 DNAT 配置

一、实验设备

(1) 防火墙设备 1 台

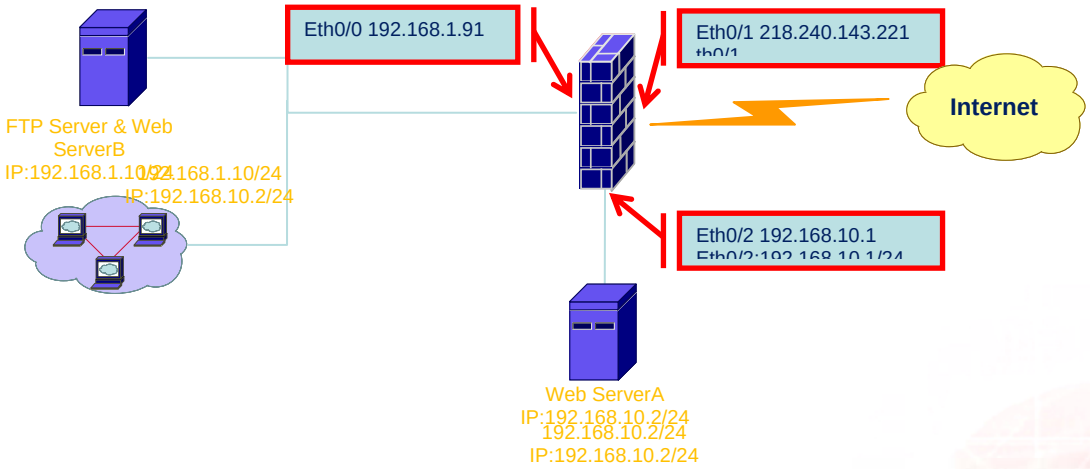
(2) Console 线 1 条

(3) 网络线 n 条

(4) 网络交换机 n 台

(5) PC 机 n 台，服务器器 n 台

二、实验拓扑



三、实验要求

1、使用外网口 IP 为内网 FTP Server 及 WEB ServerB 做端口映射，并允许外网用户访问该 Server 的 FTP 和 WEB 服务，其中 Web 服务对外映射的端口为 TCP8000。

2、允许内网用户通过域名访问 WEB ServerB(即通过合法 IP 访问)。

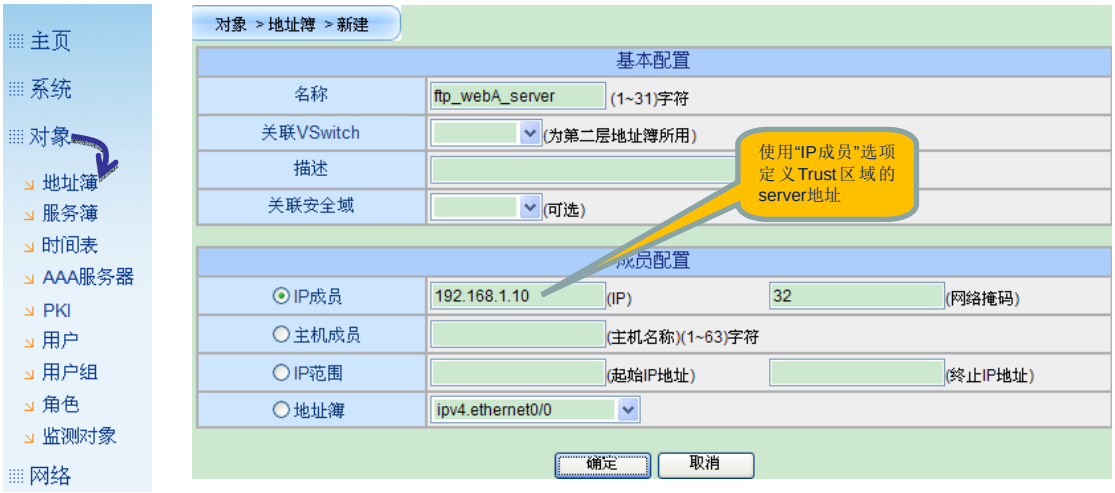
3、使用合法 IP 218.240.143.220 为 Web ServerA 做 IP 映射，允许内外网用户对该 Server 的 Web 访问。

四、实验步骤

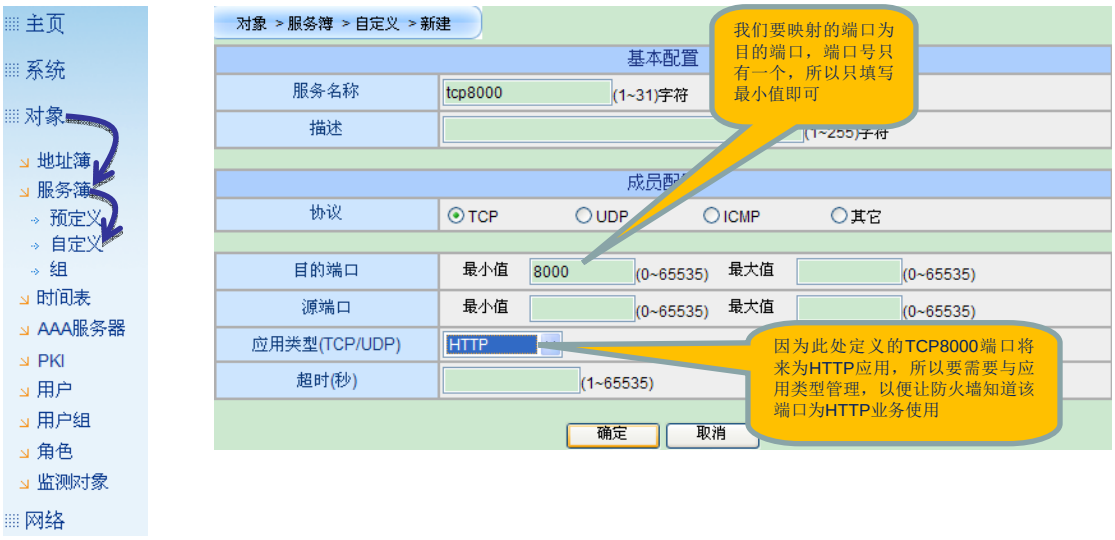
要求一：外网口 IP 为内网 FTP Server 及 WEB ServerB 做端口映射并允许外网用户访问该 Server 的 FTP 和 WEB 服务，其中 Web 服务对外映射的端口为 TCP8000。

第一步：配置准备工作

1、设置地址簿，在对象/地址簿中设置服务器地址

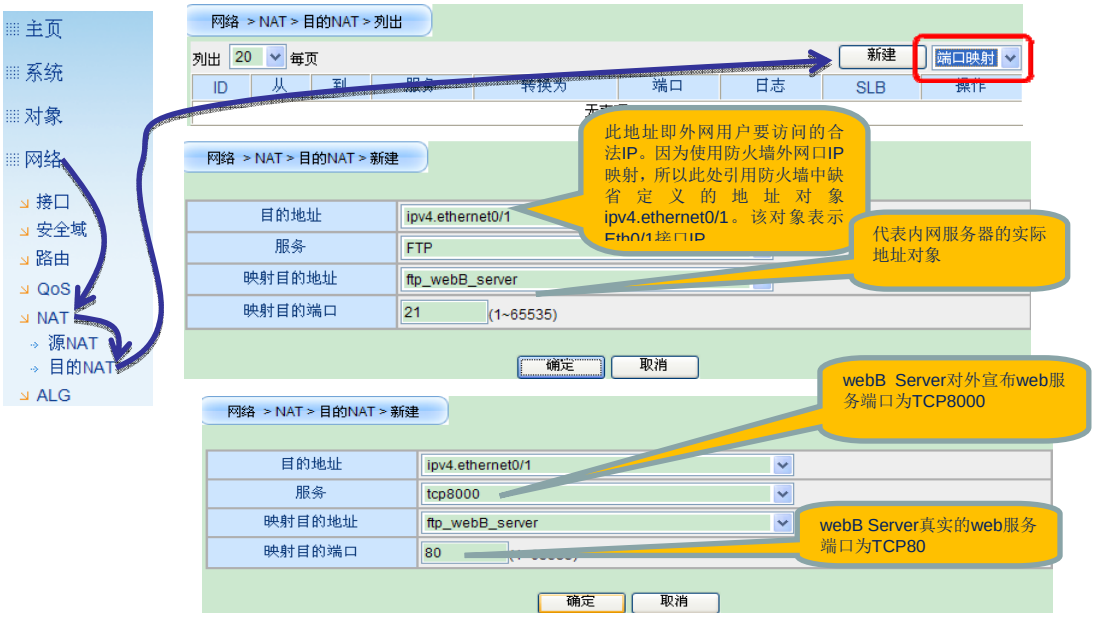


2、设置服务簿，防火墙出厂自带一些预定义服务，但是如果我们需要的服务在预定义中不包含时，需要在对象/服务簿中手工定义



第二步：创建目的 NAT

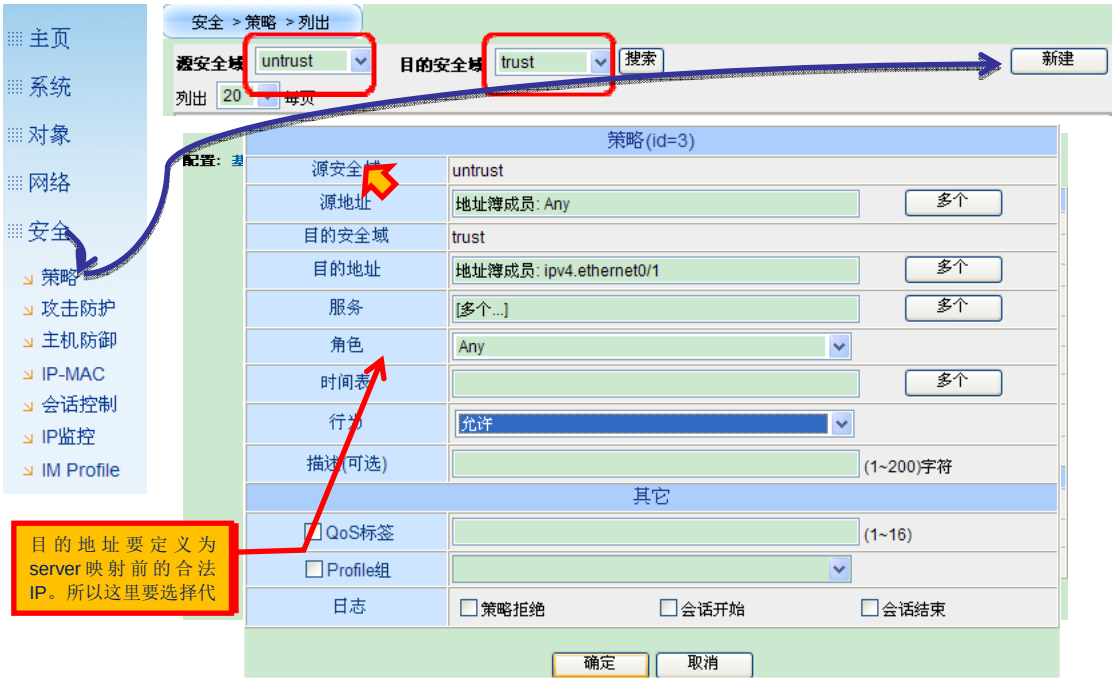
配置目的 NAT,为 trust 区域 server 映射 FTP(TCP21)和 HTTP(TCP80)端口



第三步：放行安全策略

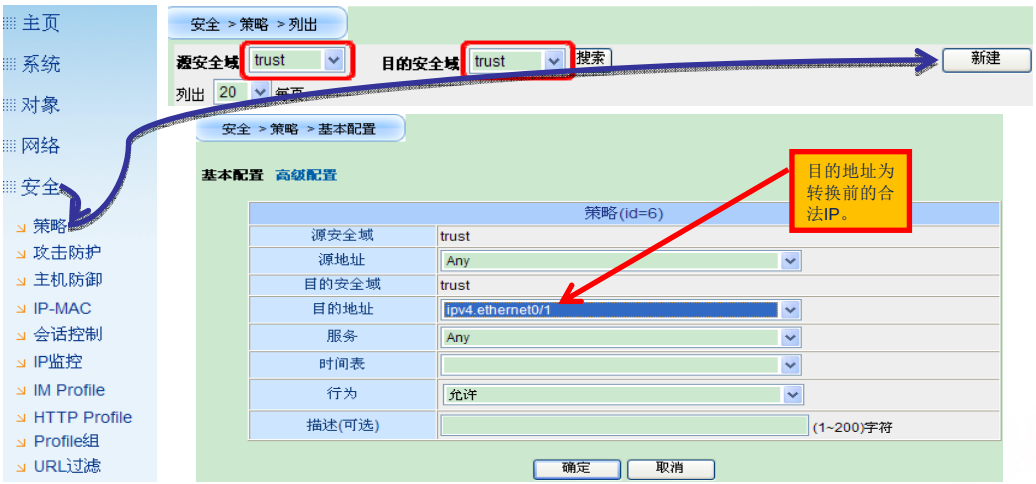
创建安全策略，允许 untrust 区域用户访问 trust 区域 server 的 FTP 和 web 应用

关于服务项中我们这里放行的是 FTP 服务和 TCP8000 服务



要求二：允许内网用户通过域名访问 WEB ServerB(即通过合法 IP 访问)。

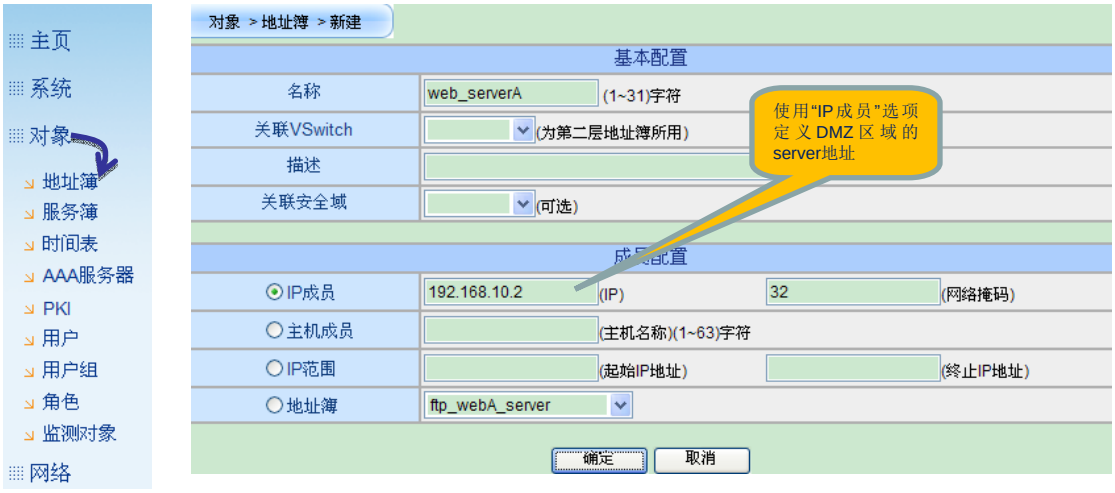
实现这一步所需要做的就是在之前的配置基础上，增加 Trust -> Trust 的安全策略



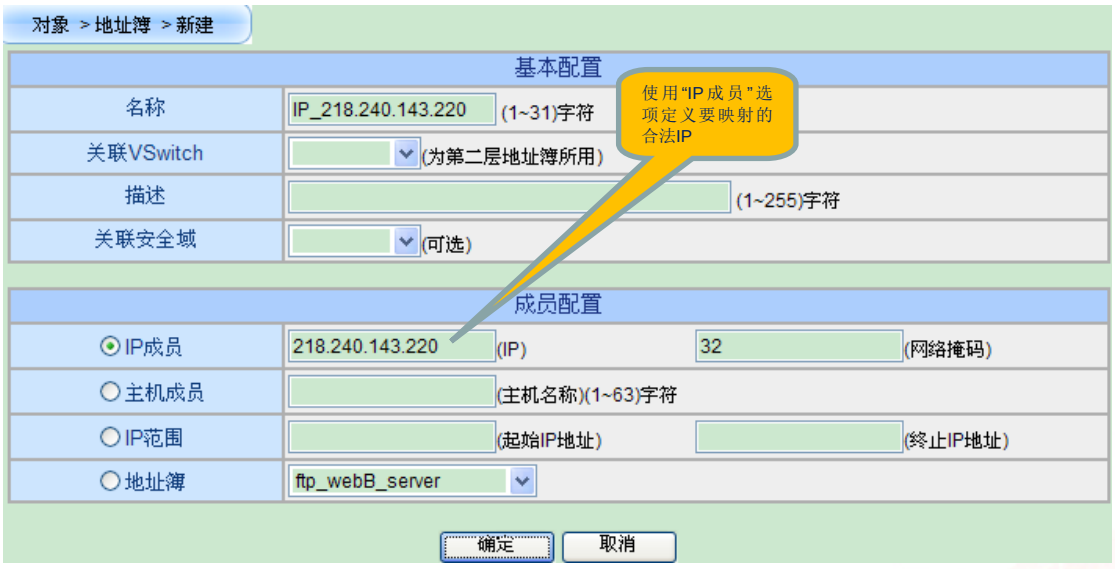
要求三：使用合法 IP　218.240.143.220 为 Web ServerA 做 IP 映射，允许内外网用户对该 Server 的 Web 访问。

第一步：配置准备工作

1、将服务器的实际地址使用 web_serverA 来表示

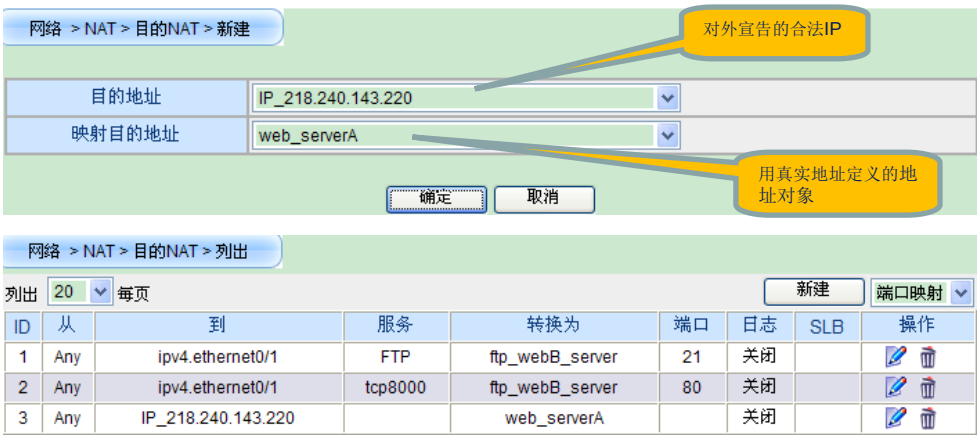


2、将服务器的公网地址使用 IP_218.240.143.220 来表示



第二步：配置目的 NAT

创建静态 NAT 条目，在新建处选择 IP 映射



第三步：放行安全策略

1、放行 untrust 区域到 dmz 区域的安全策略，使外网可以访问 dmz 区域服务器

2、放行 trust 区域到 dmz 区域的安全策略，使内网机器可以公网地址访问 dmz 区域内的服务器

防火墙透明模式配置

一、实验设备

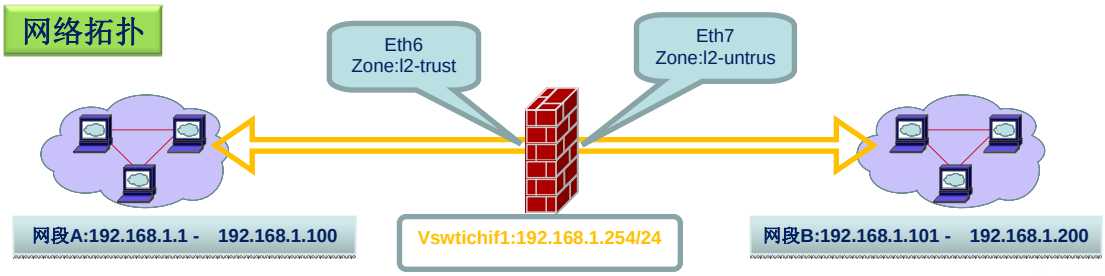
(1) 防火墙设备 1 台

(2) Console 线 1 条

(3) 网络线 2 条

(4) PC 机 1 台

二、实验拓扑



三、实验要求

1、防火墙 eth6 接口和 eth7 接口配置为透明模式

2、eth6 与 eth7 同属一个虚拟桥接组，eth6 属于 l2-trust 安全域，eth7 属于 l2-untrust 安全域。

3、为虚拟桥接组 Vswitch1 配置 ip 地址以便管理防火墙

4、允许网段 A ping 网段 B 及访问网段 B 的 WEB 服务

四、实验步骤

第一步：接口配置

将 eth6 接口加入二层安全域 l2-trust

- DCFW-1800(config)# interface ethernet0/6
- DCFW-1800(config-if-eth0/6)# zone l2-trust

将 eth7 接口设置成二层安全域 l2-untrust

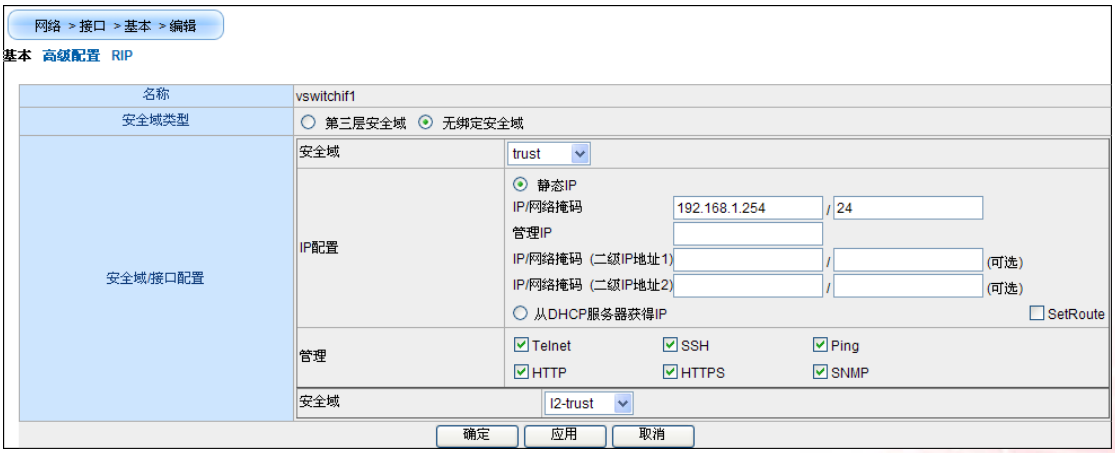
物理接口配置为二层安全域时无法配置 IP 地址

第二步：配置虚拟交换机（Vswitch）

如果没有单独接口做管理的话，可以先使用控制线通过控制口登陆下防火墙在命令下

- DCFW-1800(config)# interface vswitchif1
- DCFW-1800(config-if-vsw1)# zone trust
- DCFW-1800(config-if-vsw1)# ip address 192.168.1.254/24
- DCFW-1800(config-if-vsw1)# manage ping
- DCFW-1800(config-if-vsw1)# manage https

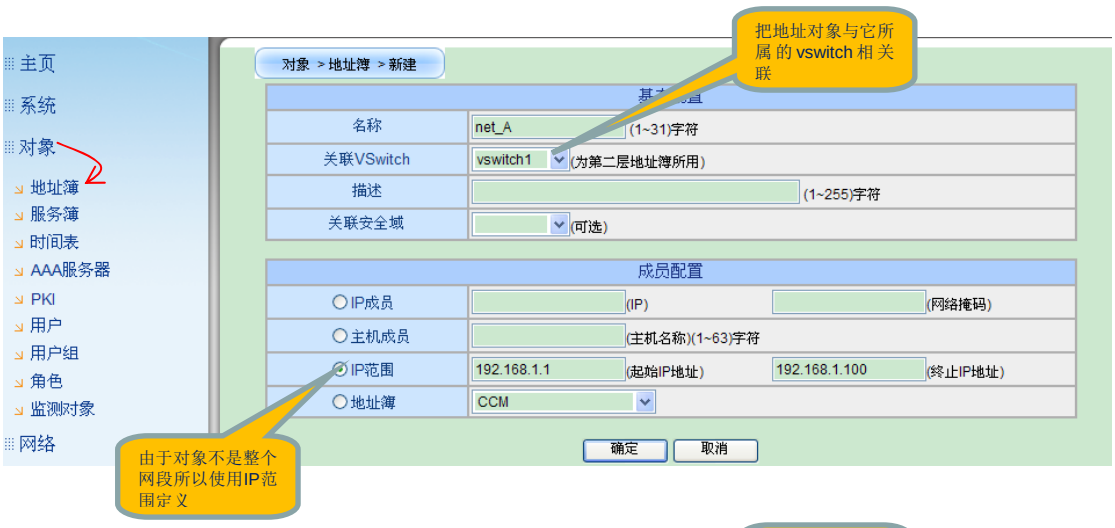
当然也可以在防火墙上单独使用一个接口做管理，通过该接口登陆到防火墙在 Web 下进行配置

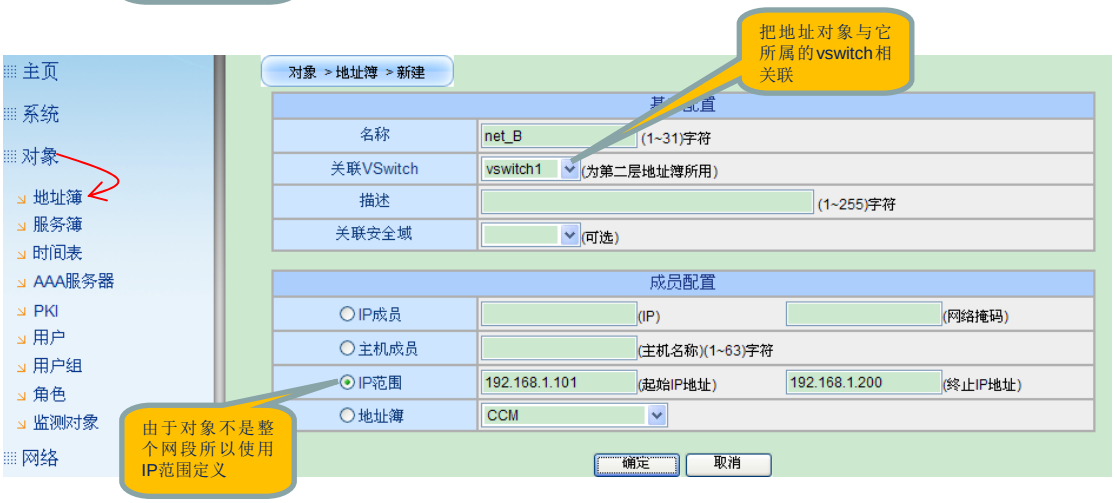


第三步：添加对象

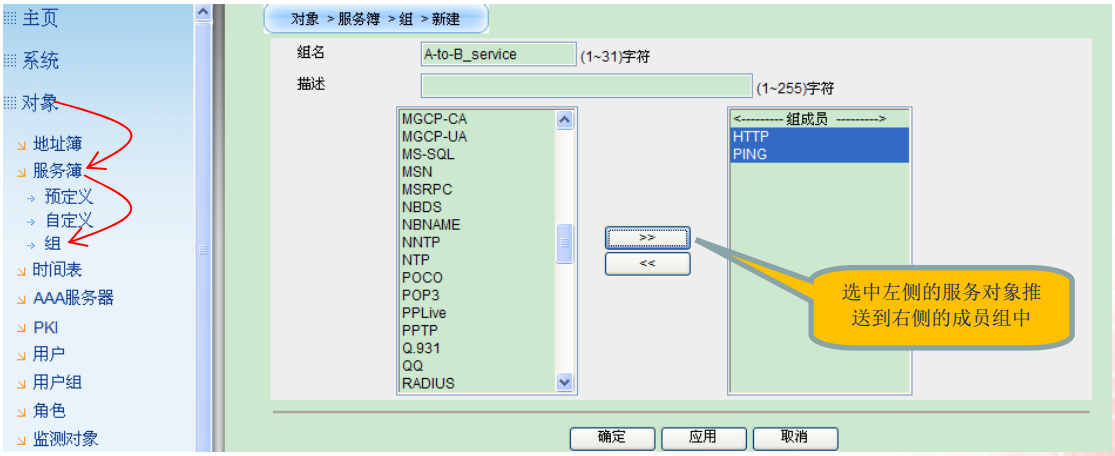
- 定义地址对象

- 定义网段 A (192.168.1.1 – 192.168.1.100)
- 定义网段 B (192.168.1.101 – 192.168.1.200)



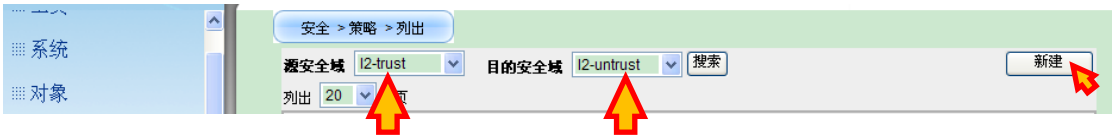


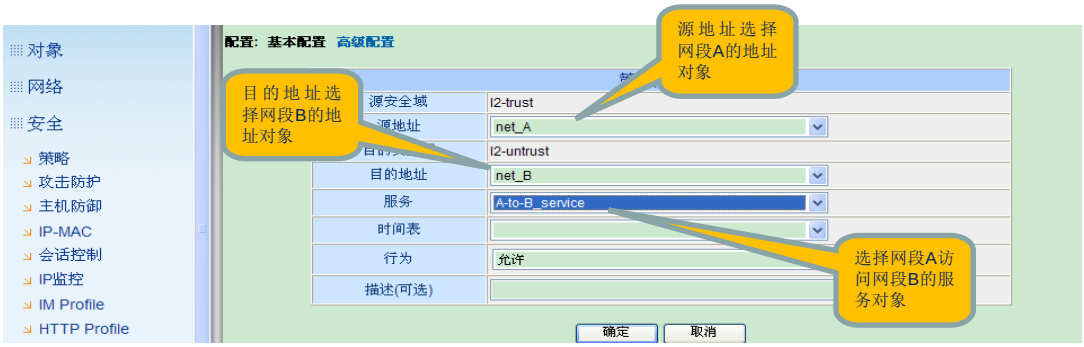
要求允许网段 A　ping　网段 B 及访问网段 B 的 WEB 服务，在这里我们将 ping 和 http 服务建立一个服务组



第四步：配置安全策略

在“安全”->“策略”中选择好“源安全域”和“目的安全域”后，新建策略





防火墙混合模式配置

一、实验设备

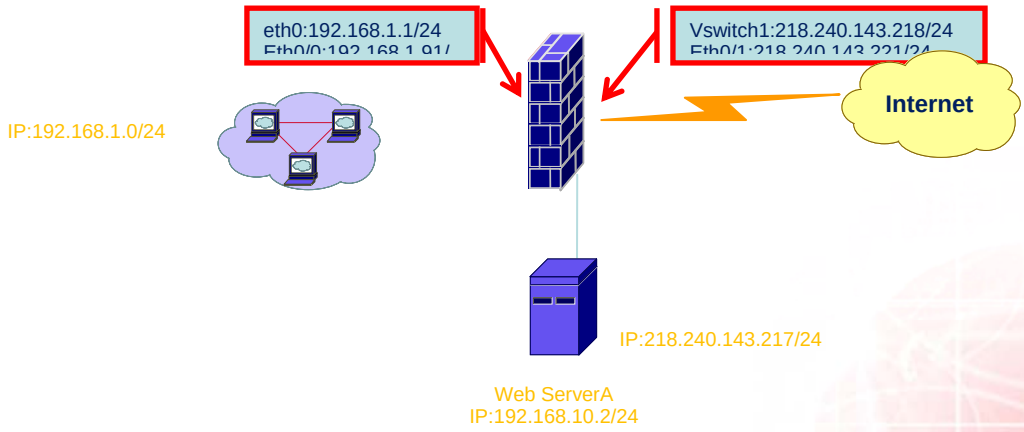
(1) 防火墙设备 1 台

(2) Console 线 1 条

(3) 网络线 2 条

(4) PC 机 1 台

二、实验拓扑



三、实验要求

1、将 eth0 口设置成路由接口，eth1 和 eth2 口设置成二层接口。并设置 Vswitch 接口；

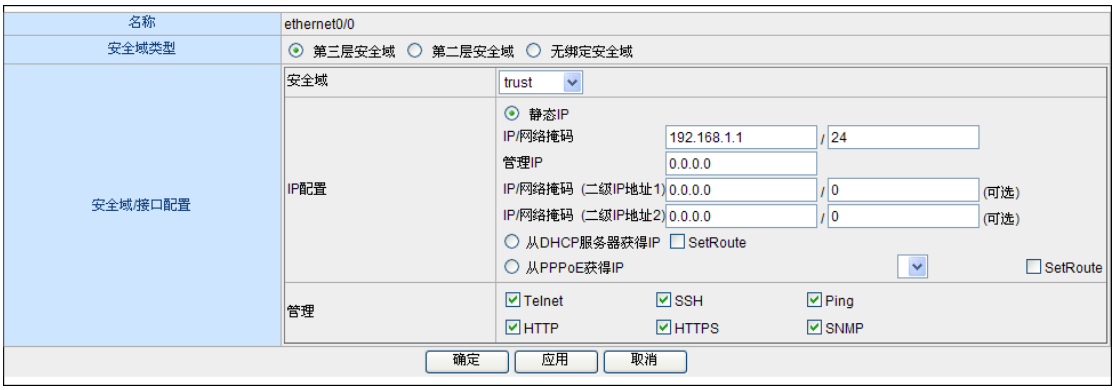
2、设置源 NAT 策略；

3、配置安全策略

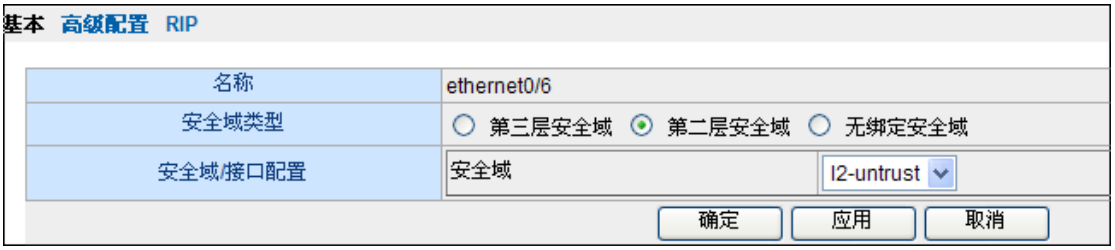
四、实验步骤

第一步：设置接口

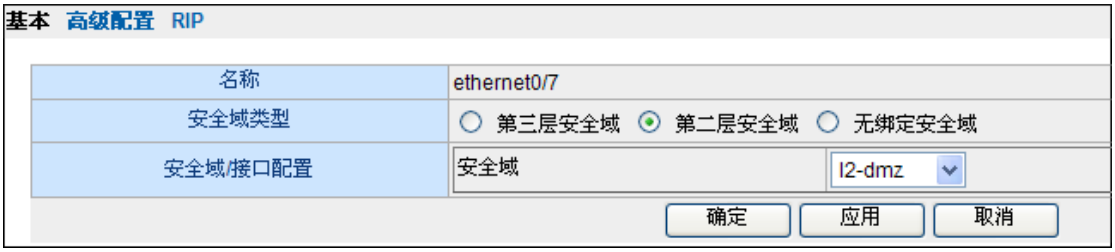
1、设置内网口地址，设置 eth0 口为内网口地址为 192.168.1.1/24



2、设置外网口，eth6 口连接外网，将 eth6 口设置成二层安全域 l2-untrust

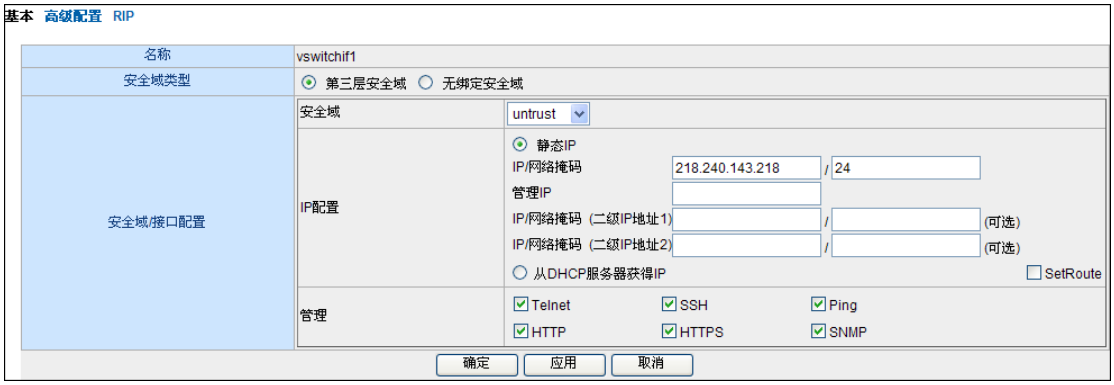


3、设置服务器接口，将 eth7 口设置成 l2-dmz 安全域，连接服务器。



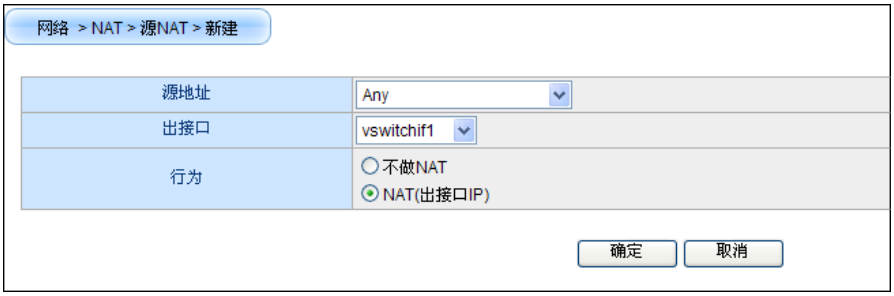
第二步：配置 Vswitch 接口

由于二层安全域接口不能设置地址，需要将地址设置在网桥接口上，该网桥接口即为 Vswitch



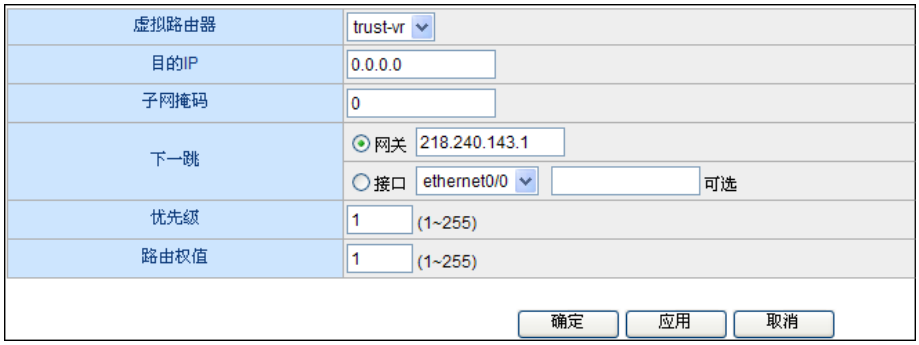
第三步：设置 SNAT 策略

针对内网所有地址我们在防火墙上设置源 NAT，内网 PC 在访问外网时，数据包凡是从 Vswitch 接口出去的数据包都做地址转换，转换地址为 Vswitch 接口地址



第四步：添加路由

要创建一条到外网的缺省路由，如果内网有三层交换机的话还需要创建到内网的回指路由。

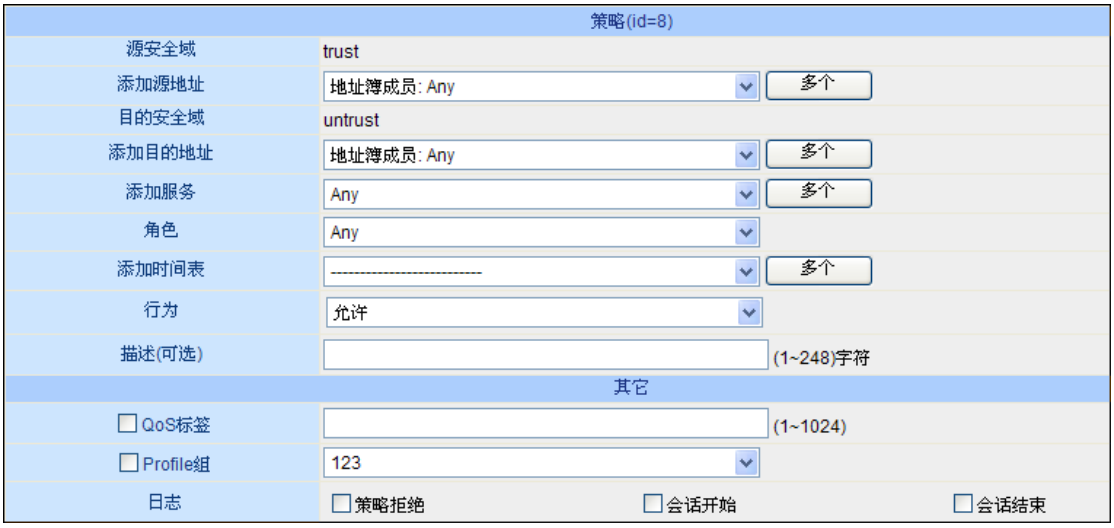


第五步：设置地址簿

在放行安全策略时，我们需要选择相应的地址和服务进行放行，所有这里首先要创建服务器的地址簿。在创建地址簿时，如果是创建的服务器属单个 ip，使用 IP 成员方式的话，那掩码一定要写 32 位

第六步：放行策略

放行策略时，首先要保证内网能够访问到外网。应该放行内网口所属安全域到 Vswitch 接口所属安全域的安全策略，应该是从 trust 到 untrust



另外还要保证外网能够访问 Web_server，该服务器的网关地址设置为 ISP 网关 218.240.143.1

那需要放行二层安全之前的安全策略，应该是放行 l2-untrust 到 l2-dmz 策略

防火墙 DHCP 配置

一、实验设备

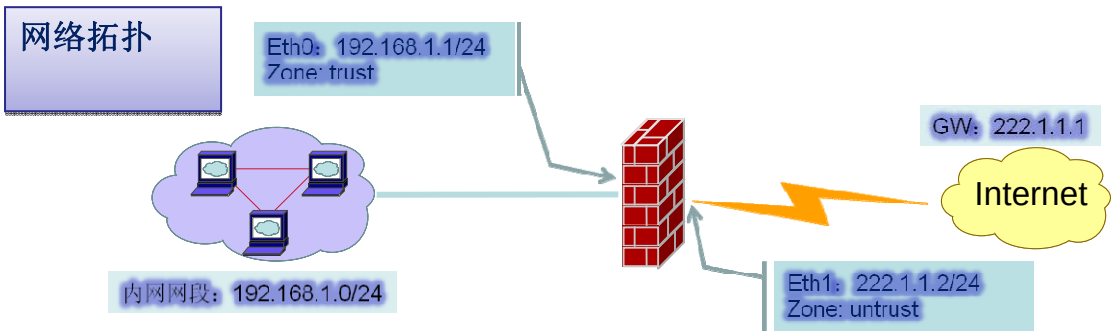
(1) 防火墙设备 1 台

(2) Console 线 1 条

(3) 网络线 2 条

(4) PC 机 1 台

二、实验拓扑



三、实验要求

1、要求内网用户能够自动获取到 IP 地址以及 DNS；

2、要求内网用户获取到 IP 地址后能直接访问外网

四、实验步骤

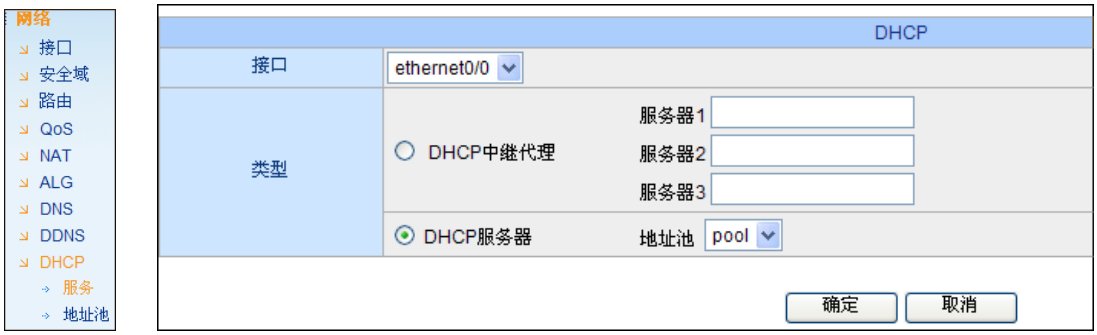
第一步：设置 DHCP 地址池

首先在创建 DHCP 前先要创建一个地址池，目的是 PC 获取地址时从该网段中来获取 IP。如下图设置好池名称、地址范围、网关、掩码和租约时间后点击确定即可。

另外如果需要内网 PC 自动获取 DNS 地址的话，需要在编辑下该地址池，在高级设置中填写 DNS 地址

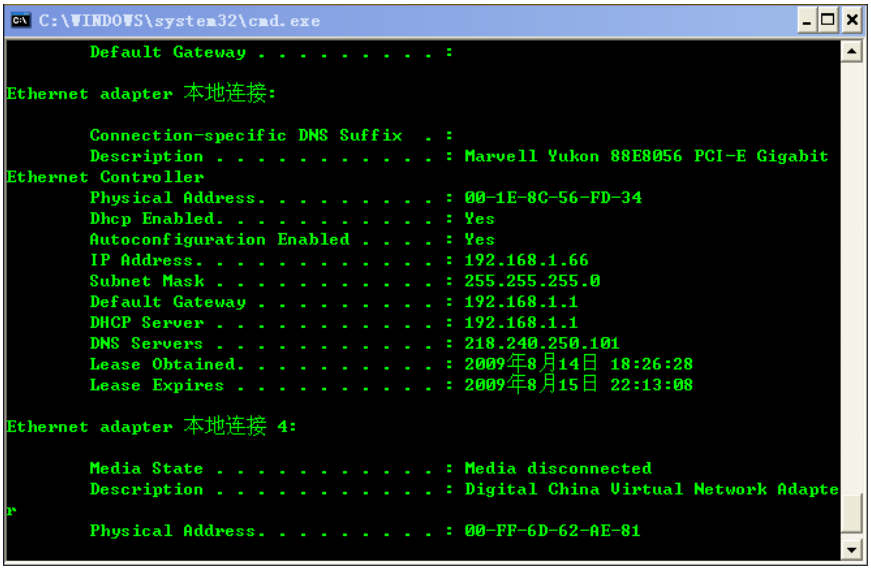
第二步：设置 DHCP 服务

在网络/DHCP/服务中 选择启用 DHCP 的服务接口。选择创建的 DHCP 服务器地址池即可



第三步：验证

内网 PC 使用自动获取 IP 地址的方式来获取 IP 地址 ,可以看到 PC 已经获取到 192.168.1.66 的 ip 地址网关为 192.168.1.1，DNS 地址是 218.240.250.101



防火墙 URL 过滤配置

一、实验设备

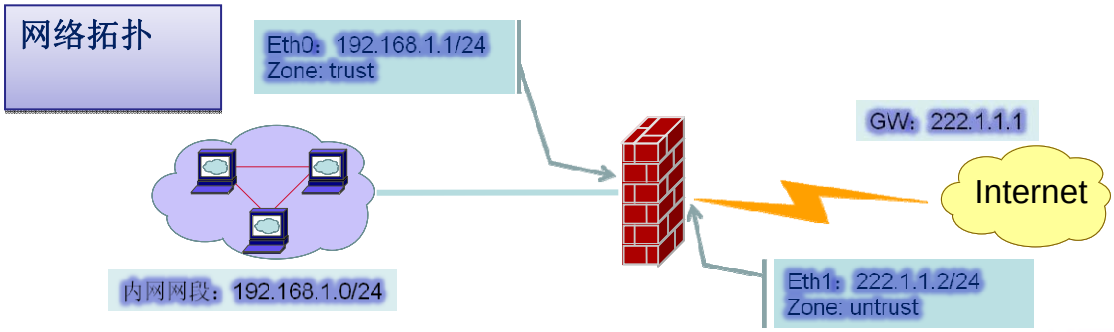
(1) 防火墙设备 1 台

(2) 局域网交换机 n 台

(3) 网络线 n 条

(4) PC 机 n 台

二、实验拓扑



三、实验要求

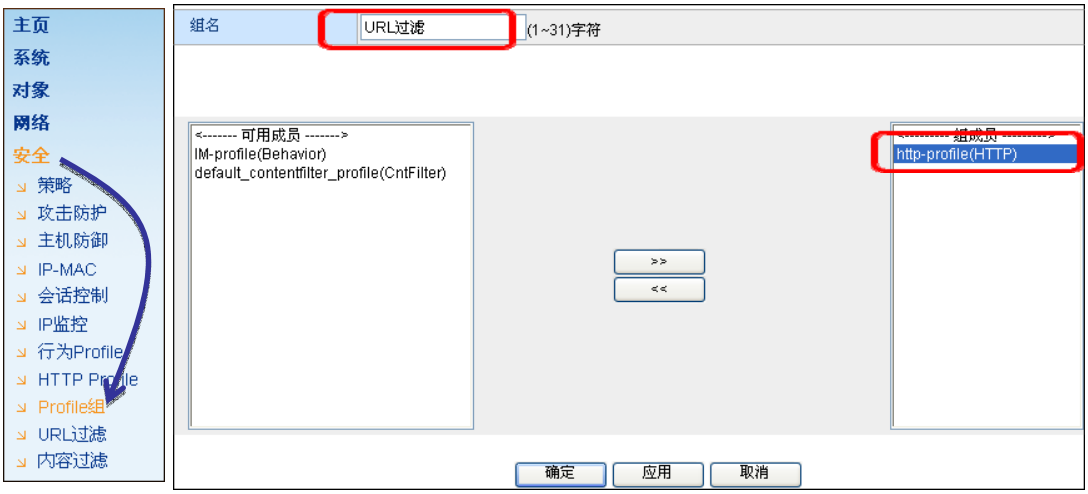
1、限制内网用户访问 baidu 首页

四、实验步骤

第一步：创建 http profile，启用 URL 过滤功能

在安全/HTTP Profile 中新建一个 http profile，名称为 http-profile，将 URL 过滤设置成启用状态点击确定即可。

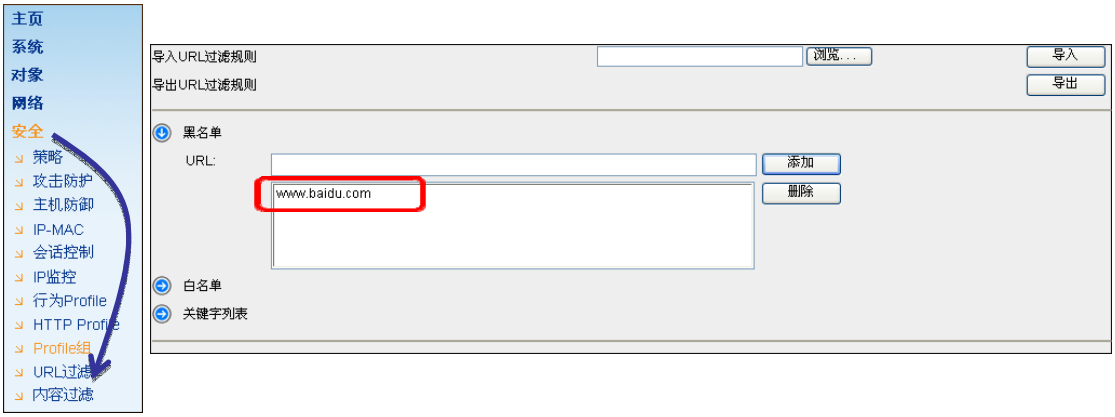
第二步：创建 profile 组，添加 http-profile



在安全/Profile 组中新建一个名为“URL 过滤”的 profile 组 ,并将之前创建好的 http profile 加入到该 profile 组中点击确定

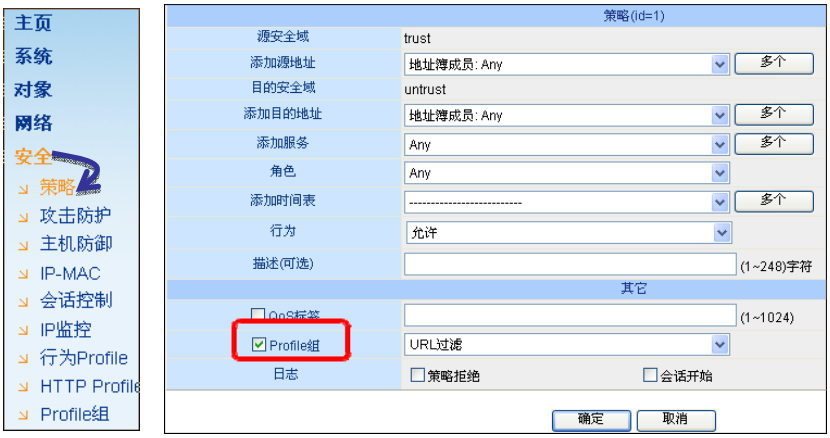
第三步：设置 URL 过滤规则

在安全/URL 过滤中，设置 URL 过滤规则，实验中要求我们只是限制访问 baidu 首页，我们在黑名单 URL 中输入 www.baidu.com 点击添加将其添加到了黑名单列表中。点击确定即可

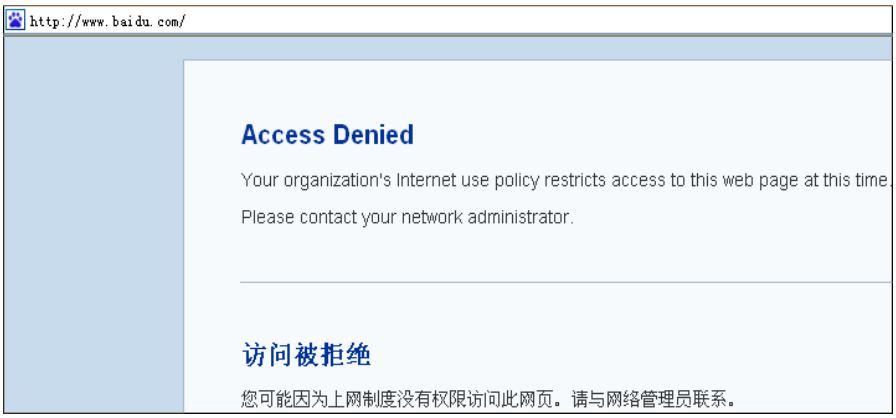


第四步：在安全策略中引用 profile 组

在安全/策略中 针对内网到外网的安全策略 引用 URL 过滤的 profile 组



第五步：测试验证



如上图内网用户在访问 baidu 首页时便会提示访问被拒绝。

防火墙网页内容过滤配置

一、实验设备

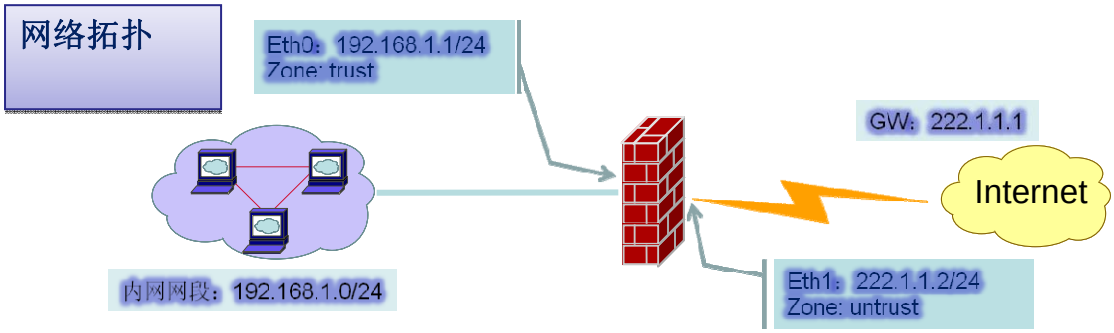
(1) 防火墙设备 1 台

(2) 局域网交换机 n 台

(3) 网络线 n 条

(4) PC 机 n 台

二、实验拓扑



三、实验要求

1、针对要访问的网页，如果包含一次或一次以上的黄秋生字样，则将该网页过滤掉。不允许用户访问

四、实验步骤

第一步：在内容过滤中创建类别

在安全/内容过滤/类别中 创建一个名为 test 的类别点击添加即可

第二步：指定要过滤的关键字并设置属性

在安全/内容过滤/关键字中，设置要过滤的关键字为“黄秋生”，设置该关键字类别为之前创建的 test 类型，并设置相应的信任值，我们使用默认的 100

第三步：创建类别组，添加类别成员并设置警戒值

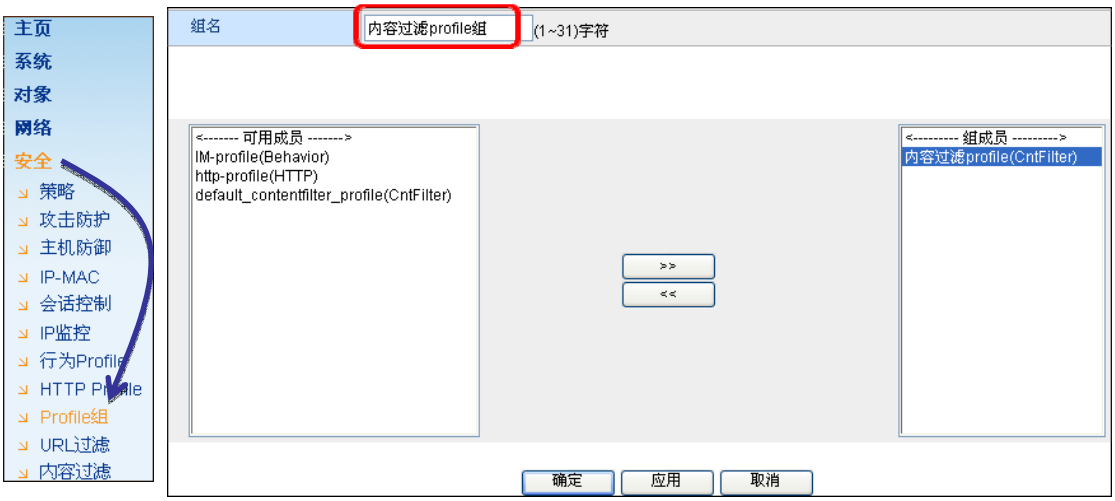
在安全/内容过滤/类别组中，创建一个类别组名为“test 类别组”，将之前创建好的 test 类别添加到该组中，并设置相应的警戒值，实验中我们要求只要包含一次黄秋生的关键字就进行过滤，因此此处我们设置的警戒值要小于等于信任值*1，实验中我们可以使用默认的 100

第四步：创建内容过滤 Profile，并添加类别组

在安全/内容过滤/Profile 中，创建一个名为“内容过滤 profole”的 profile，选择类别组为“test 类别组”点击添加，可以看到“test 类别组”已经添加到该 profile 中。

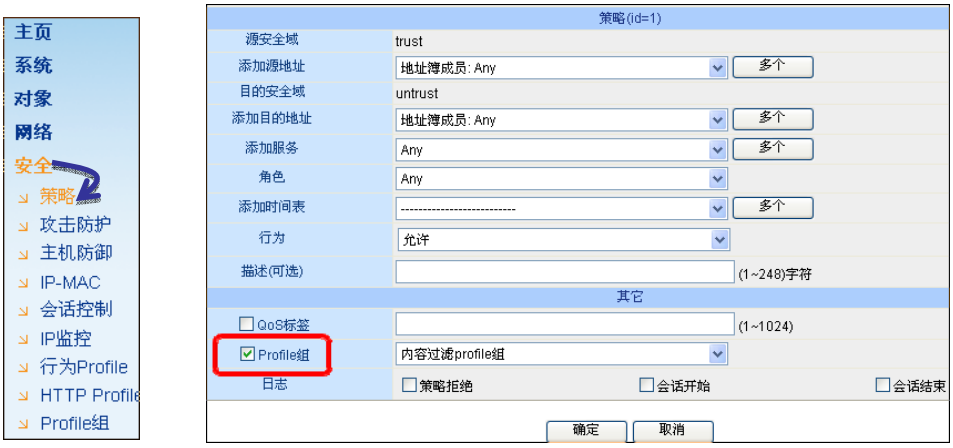
第五步 :创建一个 profile 组 ,将内容过滤 profile 加入到该 profile

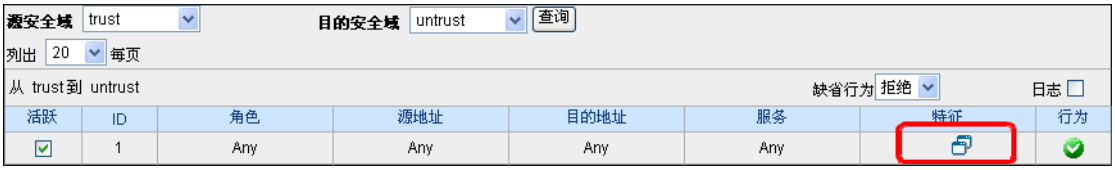
在安全/Profile 组中 创建一个 profile 组名为 “内容过滤 profile 组” ,并将内容过滤 profile 加如到该组中点击确定即可。



第六步：在策略中引用 profile 组

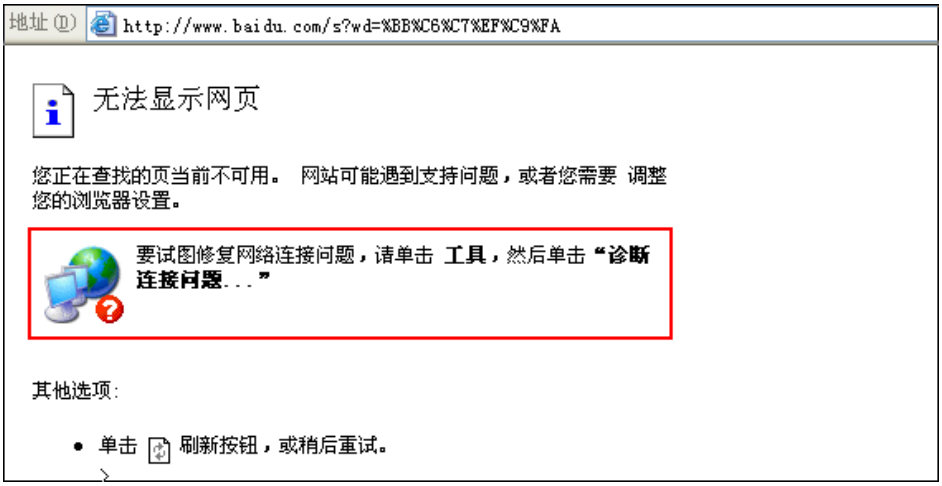
在安全/策略中 ,针对内网到外网的安全策略我们引用创建的内容过滤 profile 组 ,点击确定即可。





第七步：验证测试

在 www.baidu.com 搜索栏中输入黄秋生点击百度后提示一下界面 ,因为我们要访问的网页包含了一次或一次以上的黄秋生字样，所以不能访问到该网页。



一分学习，两分训练，三分优化，

冗余做创新，技能成就人生！