**《网络工程与组网技术》**

**课程实验报告**

（2021学年）

实验名称 综合实验

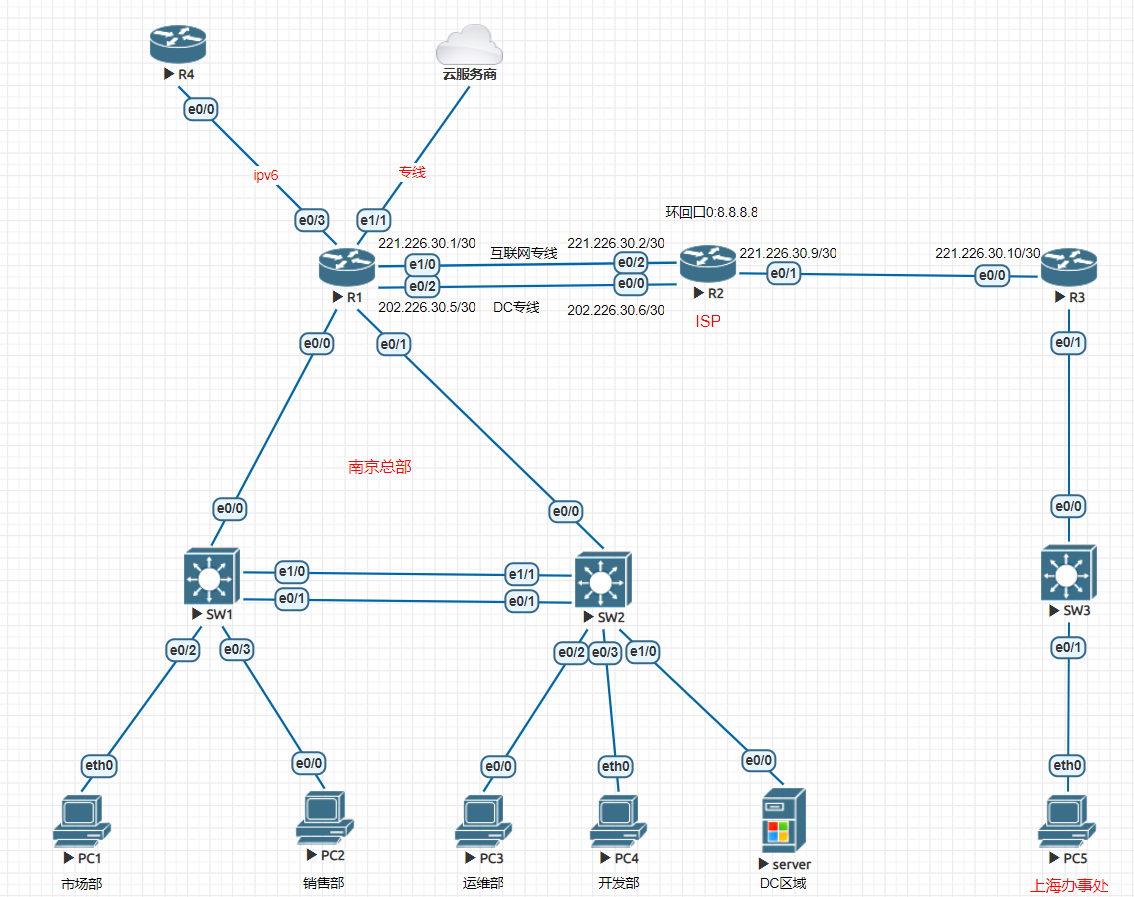
学 院 网络空间安全学院

专业班级 571191

学号姓名 57119101王晨阳

2021年 7月27日

1. 实验说明
2. 网络拓扑



二、实验任务

**1**、**IP**及**VLAN**规划

南京总部: 市场部（30人）销售部（13人）运维部（3人）开发部（40人），上海办事处共20人。其中：

⚫南京总部可用地址段:192.168.10.0/24

⚫上海办事处可用地址段:192.168.20.0/24

⚫互联地址段:192.168.255.0/24

⚫DC区域使用:210.28.91.0/24网段（该区域网段不需进行子网划分）

⚫IPV6地址段:2001:250:A160::/48

1.1 地址规划原则：请在尽量节省IP资源的前提下划分IP地址，IPV6每个部门和互联均分配/64前缀的地址。

1.2 vlan规划：为了隔离各部门间的广播流量，请合理划分vlan。

**2**、**DHCP**配置

市场部门使用DHCP来为用户下发V4地址，请在接入设备上配置DHCP服务，dns为114.114.114.114，地址租期为24小时，地址池中排除网关地址。

**3**、远程配置管理

为了管理方便，总部SW1、SW2、R1上配置TELNET服务，只允许运维部门访问登陆，用户名为se，密码为lab@seu，并请加密登录密码。

**4**、防止环路

为了防止环路产生，将总部SW1和SW2之间两条线路做成聚合链路。

**5**、路由配置。

5.1南京总部SW1、SW2、R1之间运行OSPF协议。

5.2南京总部R1和ISP的R2之间运行EBGP协议，总部AS为65511，ISP的AS为65512，在BGP中重分发OSPF路由。

5.3上海分部内使用静态路由协议。

5.4IPV6网络均通过静态路由实现互通。

**6**、隧道配置

南京总部出口接入了IPV6网络(R1-R4之间连接)，并分配一段V6地址给到上海办事处，但由于中间是ISP网络，无法直接实现V6网路互通,请在R1-R3之间建立6 TO 4隧道实现总部与办事处V6网络互通。

**7**、策略配置

7.1 安全监管：南京总部内配置了OSPF路由协议，正常情况下SW1与SW2之间的网络互通优先走SW1-SW2之间链路，假设总部为了加强上网行为监管，要求跨交换机部门之间的互访均优先通过交换机与R1之间链路进行通信，SW1与SW2之间链路只作为备份链路。

7.2 带宽优化：由于DC区域出外网流量较大，为了保障公司内部员工访问互联网的带宽，需请实现DC区域与8.8.8.8之间来往流量优先走DC专线，其它区域与8.8.8.8之间的流量优先走互联网专线，二者相互备份。

**8**、安全机制

8.1 请在开发部接入交换机已接入的终端接口上配置MAC地址绑定，防止员工私自接入其它终端设备。

8.2 禁止总部内销售部和市场部包含ICMP的流量访问DC区域。

8.3 考虑到上海办事处经常需要访问总部DC区域的服务器进行上传和下载资料，为了保障流量的安全性，请在R1和R3之间原有的6 TO 4隧道上添加V4互联，使得办事处与总部DC区域之间的流量通过隧道直接传递，并通过IPSEC来对隧道流量进行加密。

**9**、**NAT**配置。

公司在某云服务商租用了一批云主机来建立公司网站等应用，总部与云服务商之间通过光纤线路发送公司内部与云主机之间的流量。总部R1通过此线路与云服务商建立EBGP邻居关系，云服务商的AS为65513。请配置BGP与云服务商建立邻居关系，使得R1能够学到云主机的明细路由。另外配置NAT使公司内部访问云主机的时候地址都转换为R1与云服务商相连接的接口地址。（具体的互联地址分配在云服务商互联IP分配表中查找）

**10**、拓扑发现

分析云服务商内部的拓扑结构，画出拓扑图。

三、网络节点配置

IP 及 VLAN 规划

#PC1   
ip 2001:250:a160:1::1/64   
   
#PC2   
int e0/0   
no shutdown   
ip address 192.168.10.129 255.255.255.240   
ipv6 address 2001:250:a160:2::1/64   
ip route 0.0.0.0 0.0.0.0 192.168.10.142   
   
#PC3   
int e0/0   
no shutdown   
ip address 192.168.10.145 255.255.255.248   
ipv6 address 2001:250:a160:3::1/64   
ip route 0.0.0.0 0.0.0.0 192.168.10.150   
   
#PC4   
ip 192.168.10.65/26 192.168.10.126   
ip 2001:250:a160:4::1/64   
   
#PC5   
ip 192.168.20.1/27 192.168.20.30   
ip 2001:250:a160:6::1/64   
   
#SERVER   
int e0/0   
no shutdown   
ip address 210.28.91.1 255.255.255.0   
ipv6 address 2001:250:a160:5::1/64   
ip route 0.0.0.0 0.0.0.0 210.28.91.254   
   
#SW1   
vlan 10 # SW1-PC1   
int vlan 10   
no shutdown   
ip address 192.168.10.62 255.255.255.192   
ipv6 address 2001:250:a160:1::2/64   
int e0/2   
no shutdown   
sw ac vlan 10   
vlan 20 # SW1-PC2   
int vlan 20   
no shutdown   
ip address 192.168.10.142 255.255.255.240   
ipv6 address 2001:250:a160:2::2/64   
int e0/3   
no shutdown   
sw ac vlan 20   
vlan 70 # SW1-R1   
int vlan 70   
no shutdown   
ip address 192.168.10.254 255.255.255.252   
ipv6 address 2001:250:a160:7::2/64   
int e0/0   
no shutdown   
sw ac vlan 70   
   
#SW2   
vlan 30 # SW2-PC3   
int vlan 30   
no shutdown   
ip address 192.168.10.150 255.255.255.248   
ipv6 address 2001:250:a160:3::2/64   
int e0/2   
no shutdown   
sw ac vlan 30   
vlan 40 # SW2-PC4   
int vlan 40   
int vlan 40   
no shutdown   
ip address 192.168.10.126 255.255.255.192   
ipv6 address 2001:250:a160:4::2/64   
int e0/3   
no shutdown   
sw ac vlan 40   
vlan 50 # SW2-SERVER   
int vlan 50   
no shutdown   
ip address 210.28.91.254 255.255.255.0   
ipv6 address 2001:250:a160:5::2/64   
int e1/0   
no shutdown   
sw ac vlan 50   
vlan 80 # SW2-R1   
int vlan 80   
no shutdown   
ip address 192.168.10.249 255.255.255.252   
ipv6 address 2001:250:a160:8::2/64   
int e0/0   
no shutdown   
sw ac vlan 80   
   
#SW3   
vlan 60 # SW3-PC5   
int vlan 60   
no shutdown   
ip address 192.168.20.30 255.255.255.224   
ipv6 address 2001:250:a160:6::2/64   
int e0/1   
no shutdown   
sw ac vlan 60   
vlan 90 # SW3-R3   
int vlan 90   
no shutdown   
ip address 192.168.20.254 255.255.255.252   
ipv6 address 2001:250:a160:9::2/64   
int e0/0   
no shutdown   
sw ac vlan 90   
   
#R1   
int e0/0 # R1-SW1   
no shutdown   
ip address 192.168.10.253 255.255.255.252   
ipv6 address 2001:250:a160:7::1/64   
int e0/1 # R1-SW2   
no shutdown   
ip address 192.168.10.250 255.255.255.252   
ipv6 address 2001:250:a160:8::1/64   
int e0/2 # R1-R2   
no shutdown   
ip address 202.226.30.5 255.255.255.252   
int e1/0 # R1-R2   
no shutdown   
ip address 221.226.30.1 255.255.255.252   
int e0/3 # R1-R4   
no shutdown   
ipv6 address 2001:250:a160::2/64   
   
#R2   
int loopback0 # R2-lo0   
no shutdown   
ip address 8.8.8.8 255.255.255.255   
int e0/0 # R2-R1   
no shutdown   
ip address 202.226.30.6 255.255.255.252   
int e0/1 # R2-R3   
no shutdown   
ip address 221.226.30.9 255.255.255.252   
int e0/2 # R2-R1   
no shutdown   
ip address 221.226.30.2 255.255.255.252   
   
#R3   
int e0/0 # R3-R2   
no shutdown   
ip address 221.226.30.10 255.255.255.252   
int e0/1 # R3-SW3   
no shutdown   
ip address 192.168.20.253 255.255.255.252   
ipv6 address 2001:250:a160:9::1/64   
   
#R4   
int e0/0 # R4-R1   
no shutdown   
ipv6 address 2001:250:a160::1/64

DHCP 配置

#SW1   
service dhcp   
ip dhcp excluded-address 192.168.10.62   
ip dhcp pool dhcp-pool1   
network 192.168.10.0 255.255.255.192   
dns-server 114.114.114.114   
default-router 192.168.10.62   
lease 1   
   
#PC1   
ip dhcp

远程配置管理

#R1   
username se secret lab@seu   
line vty 0 4   
login local   
transport input telnet   
   
#SW1   
username se secret lab@seu   
line vty 0 4   
login local   
transport input telnet   
access-list 150 deny ip 0.0.0.0 255.255.255.255 192.168.10.0 0.0.0.255 sq telnet   
access-list 150 permit ip any any   
int vlan 10   
ip access-group 150 in   
int vlan 20   
ip access-group 150 in   
   
#SW2   
username se secret lab@seu   
line vty 0 4   
login local   
transport input telnet   
access-list 150 deny ip 0.0.0.0 255.255.255.255 192.168.10.0 0.0.0.255 sq telnet   
access-list 150 permit ip any any   
int vlan 40   
ip access-group 150 in   
int vlan 50   
ip access-group 150 in

防止环路

#SW1   
int range e0/1-1,e1/0-0   
channel-group 1 mode active   
vlan 100   
int vlan 100   
no shutdown   
ip address 192.168.10.246 255.255.255.252   
int range e0/1-1,e1/0-0   
sw ac vlan 100   
   
#SW2   
int range e1/1-1,e0/1-1   
channel-group 1 mode passive   
vlan 100   
int vlan 100   
no shutdown   
ip address 192.168.10.245 255.255.255.252   
int range e1/1-1,e0/1-1   
sw ac vlan 100

路由配置

#R1   
router ospf 100   
router-id 1.1.1.1   
redistribute bgp 65511 subnets   
network 192.168.10.252 0.0.0.3 area 0   
network 192.168.10.248 0.0.0.3 area 0   
default-information originate always   
router bgp 65511   
no bgp log-neighbor-changes   
neighbor 221.226.30.2 remote-as 65512   
neighbor 202.226.30.6 remote-as 65512   
router bgp 65511   
redistribute ospf 100   
ipv6 route 2001:250:a160:1::/64 2001:250:a160:7::2   
ipv6 route 2001:250:a160:2::/64 2001:250:a160:7::2   
ipv6 route 2001:250:a160:3::/64 2001:250:a160:8::2   
ipv6 route 2001:250:a160:4::/64 2001:250:a160:8::2   
ipv6 route 2001:250:a160:5::/64 2001:250:a160:8::2   
ipv6 route ::/0 2001:250:a160:10::2   
ipv6 unicast-routing   
   
#R2   
router bgp 65512   
no bgp log-neighbor-changes   
neighbor 221.226.30.1 remote-as 65511   
neighbor 202.226.30.5 remote-as 65511   
neighbor 221.226.30.10 remote-as 65512   
neighbor 221.226.30.10 next-hop-self   
router bgp 65512   
redistribute connected   
redistribute static   
ip route 192.168.20.0 255.255.255.0 221.226.30.10   
   
#R3   
ip route 192.168.10.0 255.255.255.0 221.226.30.9   
ip route 192.168.30.0 255.255.255.0 192.168.30.254   
ip route 0.0.0.0 0.0.0.0 221.226.30.9   
ipv6 route ::/0 2001:250:a160:10::1   
ipv6 route 2001:250:a160:6::/0 2001:250:a160:9::2   
ipv6 unicast-routing   
   
#R4   
ipv6 route ::/0 2001:250:a160::2   
   
#SW1   
router ospf 100   
router-id 2.2.2.2   
network 192.168.10.244 0.0.0.3 area 0   
network 192.168.10.252 0.0.0.3 area 0   
network 192.168.10.0 0.0.0.63 area 0   
network 192.168.10.128 0.0.0.15 area 0   
int vlan 70   
ip ospf priority 0   
int vlan 100   
ip ospf priority 0   
ipv6 route ::/0 2001:250:a160:7::1   
ipv6 unicast-routing   
   
#SW2   
router ospf 100   
router-id 3.3.3.3   
network 192.168.10.244 0.0.0.3 area 0   
network 192.168.10.248 0.0.0.3 area 0   
network 192.168.10.64 0.0.0.63 area 0   
network 192.168.10.144 0.0.0.63 area 0   
network 210.28.91.0 0.0.0.255 area 0   
int vlan 80   
ip ospf priority 0   
int vlan 100   
ip ospf priority 0   
ipv6 route ::/0 2001:250:a160:8::1   
ipv6 unicast-routing   
   
#SW3   
ip route 0.0.0.0 0.0.0.0 192.168.20.253   
ipv6 route ::/0 2001:250:a160:9::1   
ipv6 unicast-routing

隧道配置

#R1   
int tunnel1   
no shutdown   
ipv6 enable   
ipv6 address 2001:250:a160:10::1/64   
tunnel source 221.226.30.1   
tunnel destination 221.226.30.10   
tunnel mode ipv6ip   
   
#R3   
int tunnel1   
no shutdown   
ipv6 enable   
ipv6 address 2001:250:a160:10::2/64   
tunnel source 221.226.30.10   
tunnel destination 221.226.30.1   
tunnel mode ipv6ip

策略配置

#SW1   
access-list 100 permit ip 192.168.10.0 0.0.0.63 192.168.10.144 0.0.0.7   
access-list 100 permit ip 192.168.10.0 0.0.0.63 192.168.10.64 0.0.0.63   
access-list 100 permit ip 192.168.10.128 0.0.0.15 192.168.10.144 0.0.0.7   
access-list 100 permit ip 192.168.10.128 0.0.0.15 192.168.10.64 0.0.0.63   
route-map out permit 10   
match ip address 100   
set ip next-hop 192.168.10.253   
ip local policy route-map out   
   
#SW2   
access-list 100 permit ip 192.168.10.144 0.0.0.7 192.168.10.0 0.0.0.63   
access-list 100 permit ip 192.168.10.144 0.0.0.7 192.168.10.128 0.0.0.15   
access-list 100 permit ip 192.168.10.64 0.0.0.63 192.168.10.0 0.0.0.63   
access-list 100 permit ip 192.168.10.64 0.0.0.63 192.168.10.128 0.0.0.15   
route-map out permit 10   
match ip address 100   
set ip next-hop 192.168.10.250   
ip local policy route-map out   
   
#R1   
access-list 1 permit 192.168.10.0 0.0.0.255   
access-list 2 permit 210.28.91.0 0.0.0.255   
access-list 99 permit any   
route-map bgp1 permit 10 #互联专线   
match ip address 1   
set metric 1000   
route-map bgp1 permit 20   
match ip address 2   
set metric 2000   
route-map bgp1 permit 30   
match ip address 99   
router bgp 65511   
neighbor 221.226.30.2 route-map bgp1 out   
route-map bgp2 permit 10 #DC专线   
match ip address 1   
set metric 2000   
route-map bgp2 permit 20   
match ip address 2   
set metric 1000   
match ip address 99   
router bgp 65511   
neighbor 202.226.30.6 route-map bgp2 out   
   
#R2   
access-list 110 permit ip 192.168.10.0 0.0.0.255 8.8.8.8 0.0.0.0   
access-list 120 permit ip 210.28.91.0 0.0.0.255 8.8.8.8 0.0.0.0   
access-list 99 permit any   
route-map bgp1 permit 10 #互联专线   
match ip address 110   
set metric 1000   
route-map bgp1 permit 20   
match ip address 120   
set metric 2000   
route-map bgp1 permit 30   
match ip address 99   
router bgp 65512   
neighbor 221.226.30.1 route-map bgp1 out   
route-map bgp2 permit 10 #DC专线   
match ip address 110   
set metric 2000   
route-map bgp2 permit 20   
match ip address 120   
set metric 1000   
route-map bgp2 permit 30   
match ip address 99   
router bgp 65512   
neighbor 202.226.30.5 route-map bgp2 out

安全机制

#SW2   
int e0/3   
sw port-security mac-address 0050.7966.680c   
sw port-security maximum 1   
sw port-security violation shutdown   
sw mode access   
sw port-security   
   
#R1   
access-list 101 deny icmp 192.168.10.0 0.0.0.63 210.28.91.0 0.0.0.255   
access-list 101 deny icmp 192.168.10.128 0.0.0.15 210.28.91.0 0.0.0.255   
access-list 101 permit ip any any   
int e0/0   
ip access-group 101 in   
   
#R1   
crypto isakmp policy 2   
hash md5   
authentication pre-share   
group 2   
crypto isakmp key lab@seu address 221.226.30.10   
crypto ipsec transform-set tor3 esp-des esp-md5-hmac   
mode transport   
crypto ipsec profile ipsec   
set transform-set tor3   
int tunnel0   
tunnel mode ipip   
ip address 192.168.10.242 255.255.255.252   
tunnel protection ipsec profile ipsec   
ip route 192.168.20.0 255.255.255.0 192.168.10.241   
   
#R3   
crypto isakmp policy 2   
hash md5   
authentication pre-share   
group 2   
crypto isakmp key lab6 address 221.226.30.1   
crypto ipsec transform-set tor1 esp-des esp-md5-hmac   
mode transport   
crypto ipsec profile ipsec   
set transform-set tor1   
int tunnel0   
tunnel mode ipip   
ip address 192.168.10.241 255.255.255.252   
tunnel protection ipsec profile ipsec   
ip route 210.28.91.0 255.255.255.0 192.168.10.242

NAT 配置

#R1   
int e1/1   
no shutdown   
ip address 172.20.1.3 255.255.255.0   
ip route 0.0.0.0 0.0.0.0 172.20.1.254   
router bgp 65511   
no bgp log-neighbor-changes   
neighbor 172.20.1.254 remote-as 65513   
access-list 5 permit 192.168.10.0 0.0.0.255   
access-list 5 permit 192.168.20.0 0.0.0.255   
ip nat inside source list 5 int e1/1 overload   
int e0/0   
ip nat inside   
int e0/1   
ip nat inside   
int e0/2   
ip nat inside   
int e1/0   
ip nat inside   
int e1/1   
ip nat outside

四、功能测试

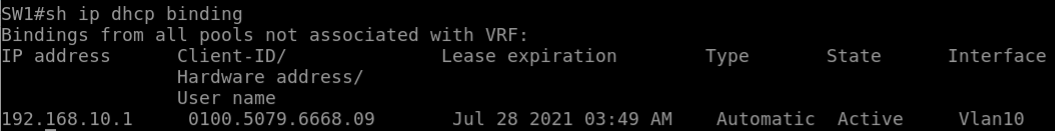
1. 将IP地址规划与VLAN规划以表格形式列出。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 部门 | 人数 | ipv4 | vlan | ipv4 网关 | ipv6 | ipv6 网关 |
| 市场 | 30 | 192.168.10.1/26 | 10 | 192.168.10.62 | 2001:250:a160:1::1/64 | 2001:250:a160:1::2 |
| 销售 | 13 | 192.168.10.129/28 | 20 | 192.168.10.142 | 2001:250:a160:2::1/64 | 2001:250:a160:2::2 |
| 运维 | 3 | 192.168.10.145/29 | 30 | 192.168.10.150 | 2001:250:a160:3::1/64 | 2001:250:a160:3::2 |
| 开发 | 40 | 192.168.10.65/26 | 40 | 192.168.10.126 | 2001:250:a160:4::1/64 | 2001:250:a160:4::2 |
| DC | / | 210.28.91.1/24 | 50 | 210.28.91.254 | 2001:250:a160:5::1/64 | 2001:250:a160:5::2 |
| 上海 | 20 | 192.168.20.1/27 | 60 | 192.168.20.30 | 2001:250:a160:6::1/64 | 2001:250:a160:6::2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | ipv4 | ipv6 | vlan |
| SW1 | e0/0 | 192.168.10.254/30 | 2001:250:a160:7::2/24 | 70 |
| SW1 | e0/1 | 192.168.10.246/30 | / | 100 |
| SW1 | e0/2 | 192.168.10.62/26 | 2001:250:a160:1::2/24 | 10 |
| SW1 | e0/3 | 192.168.10.142/28 | 2001:250:a160:2::2/24 | 20 |
| SW1 | e1/0 | 192.168.10.246/30 | / | 100 |
| SW2 | e0/0 | 192.168.10.249/30 | 2001:250:a160:8::2/24 | 80 |
| SW2 | e0/1 | 192.168.10.245/30 | / | 100 |
| SW2 | e0/2 | 192.168.10.150/29 | 2001:250:a160:3::2/24 | 30 |
| SW2 | e0/3 | 192.168.10.126/26 | 2001:250:a160:4::2/24 | 40 |
| SW2 | e1/0 | 210.28.91.254/24 | 2001:250:a160:5::2/24 | 50 |
| SW2 | e1/1 | 192.168.10.245/30 | / | 100 |
| SW3 | e0/0 | 192.168.20.254/30 | 2001:250:a160:9::2/24 | 90 |
| SW3 | e0/1 | 192.168.20.30/27 | 2001:250:a160:6::2/24 | 60 |
| R1 | e0/0 | 192.168.10.253/30 | 2001:250:a160:7::1/24 | / |
| R1 | e0/1 | 192.168.10.250/30 | 2001:250:a160:8::1/24 | / |
| R1 | e0/2 | 202.226.30.5/30 | / | / |
| R1 | e0/3 | / | 2001:250:a160::2/24 | / |
| R1 | e1/0 | 221.226.30.1/30 | / | / |
| R1 | e1/1 | 172.20.1.3 | / | / |
| R1 | 隧道 | 192.168.10.242/30 | 2001:250:a160:10::1/24 | / |
| R2 | e0/0 | 202.226.30.6/30 | / | / |
| R2 | e0/1 | 221.226.30.9/30 | / | / |
| R2 | e0/2 | 221.226.30.2/30 | / | / |
| R3 | e0/0 | 221.226.30.10/30 | / | / |
| R3 | e0/1 | 192.168.20.253/30 | 2001:250:a160:9::1/24 | / |
| R3 | 隧道 | 192.168.10.241/30 | 2001:250:a160:10::2/24 | / |
| R4 | e0/0 | / | 2001:250:a160::1/24 | / |

2. 在交换机上使用命令sh ip dhcp binding查看地址下发情况，并截图。

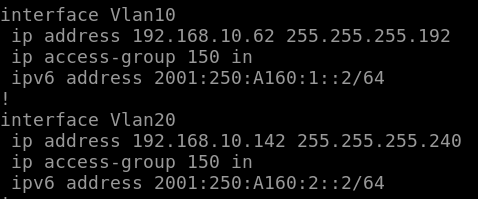
SW1



3. 请将总部 SW1,SW2,R1 的相关配置截图列出，并通过总部运维部的主机上分别 telnet R1 设备将结果截图保存。

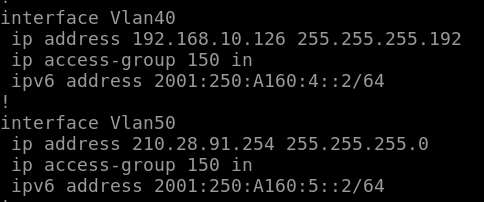
SW1



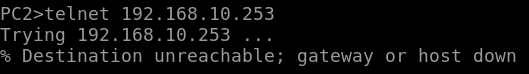


SW2

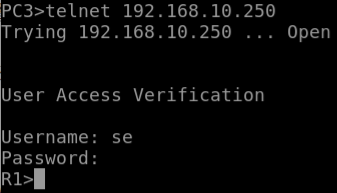




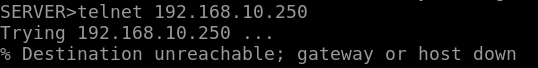
PC1



PC3

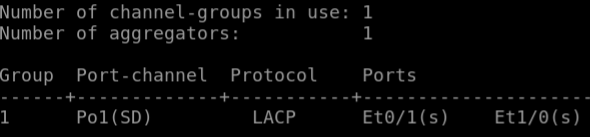


SERVER

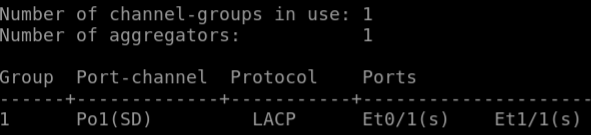


4. 输入show etherchannel summary截图SW1与SW2上的聚合接口信息。

SW1

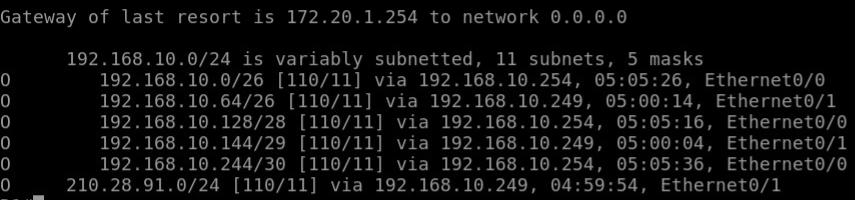


SW2

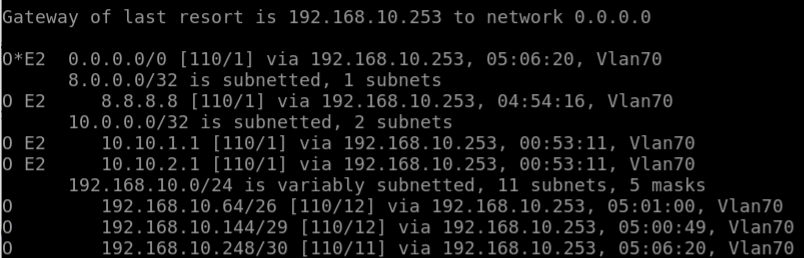


5.1. 输入ship route ospf命令查看总部SW1、SW2、R1设备通过OSPF学到的路由信息，并截图

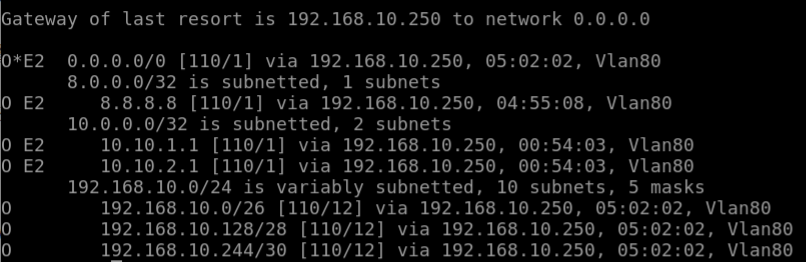
R1



SW1

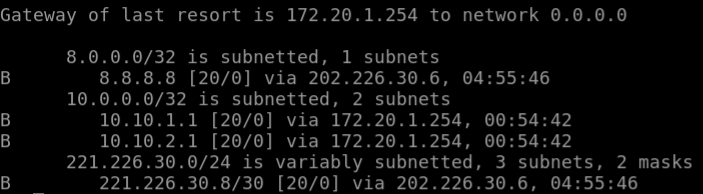


SW2

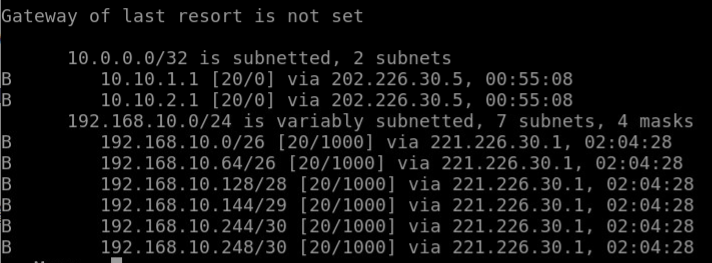


5.2. 输入sh ip route bgp查看R1与R2设备上通过BGP学习到的路由信息，并截图

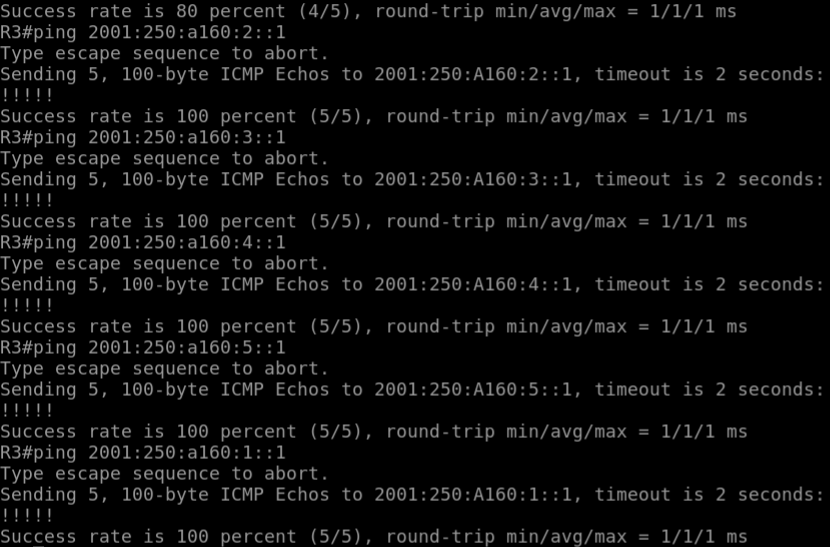
R1



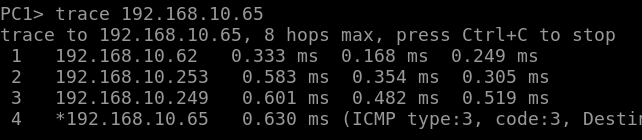
R2



6. 在R3上PING总部各部门主机IPV6地址，将结果截图保存

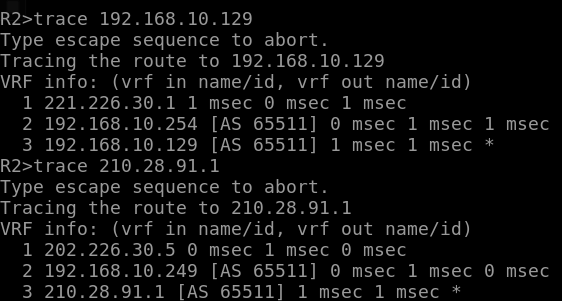


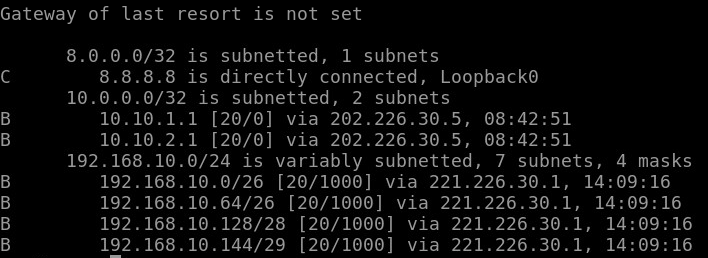
7.1。在市场部主机TRACERT开发部主机地址，将结果截图。



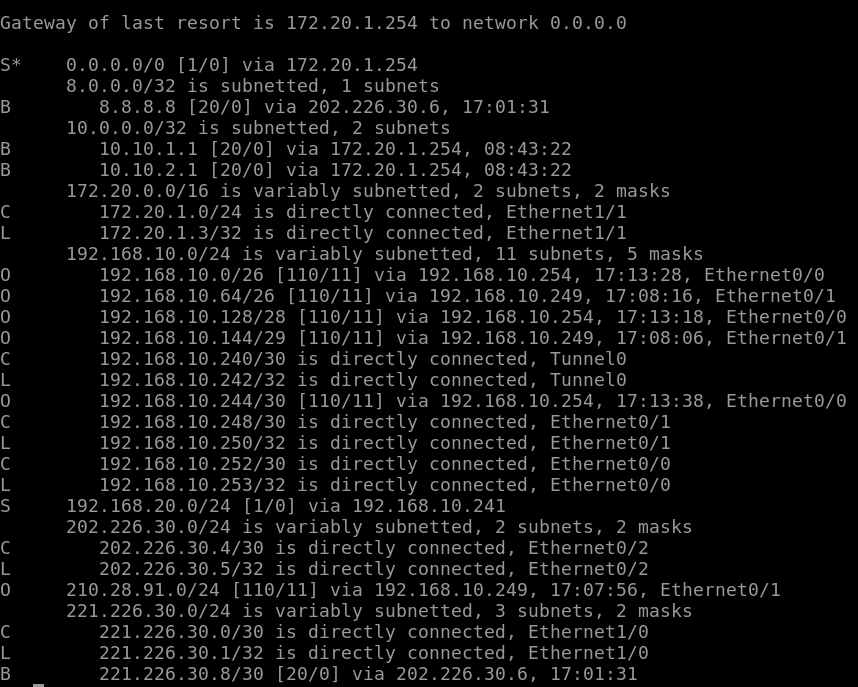
7.2. 、在R2上从8.8.8.8分别TRACE销售部和DC区域主机,将结果截图，并截图R1和R2上做完带宽优化题目后的路由表。

R2

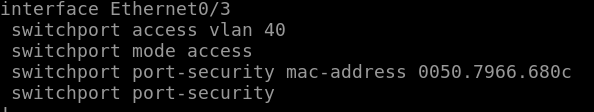




R1

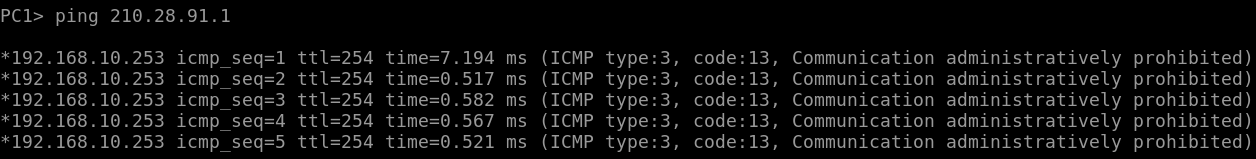


8.1. 截图SW1、SW2 MAC地址绑定相关配置。

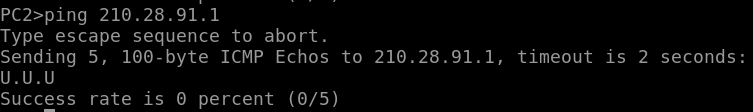


8.2. 在销售部和市场部主机上PING DC区域SERVER，将结果截图。

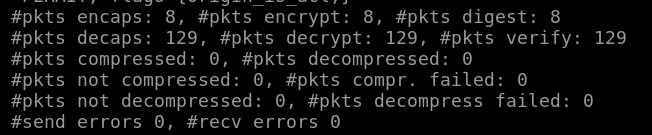
PC1

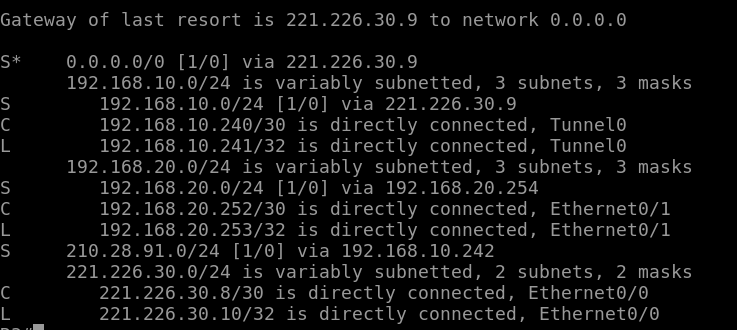


PC2

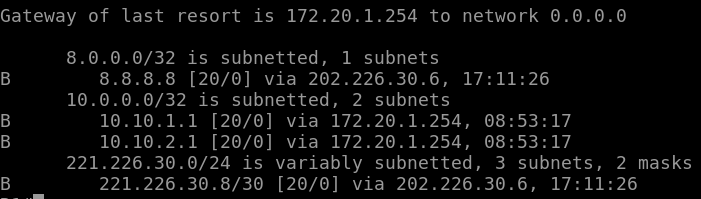


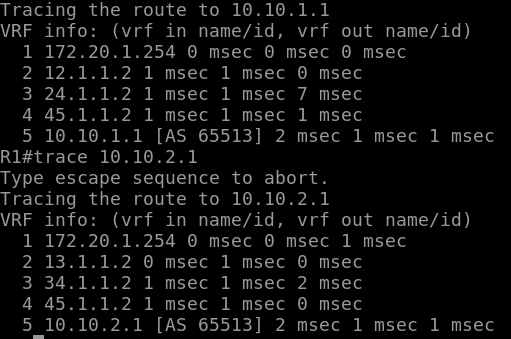
8.3. 在R3上查看通往DC区域的路由信息，并在R3上输入show crypto ipsec sa验证加解密后的数据包计数已增加，并截图。





9. 查看R1上通过与云服务资源商之间BGP学习到的路由信息，并测试与学习到的明细路由连通性，将结果截图。





10. 将分析后云服务商内部拓扑图画出。

