# 网络划分

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | / |

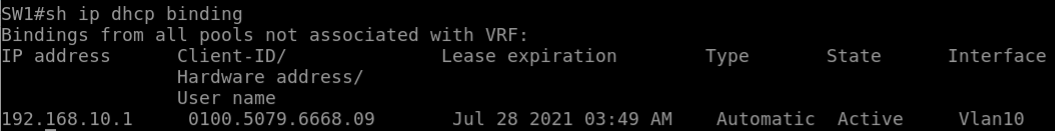
# IP 及 VLAN 规划

#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

SW1

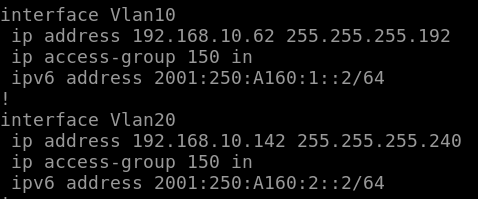


# 远程配置管理

#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

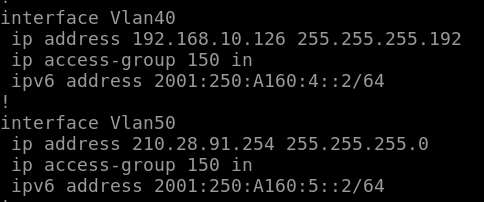
SW1



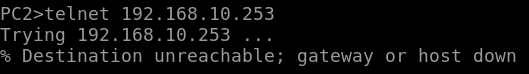


SW2

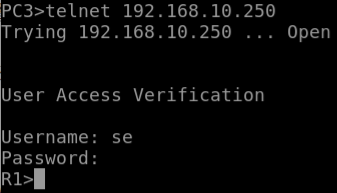




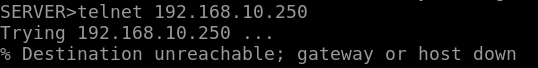
PC1



PC3



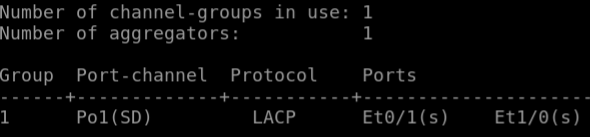
SERVER



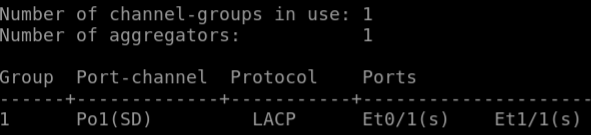
# 防止环路

#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

SW1



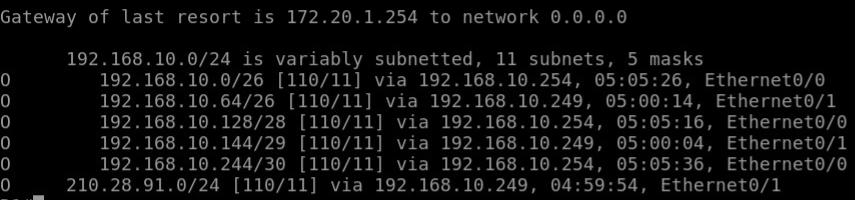
SW2



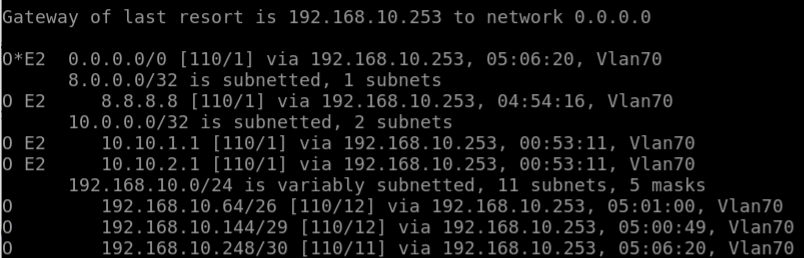
# 路由配置

#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

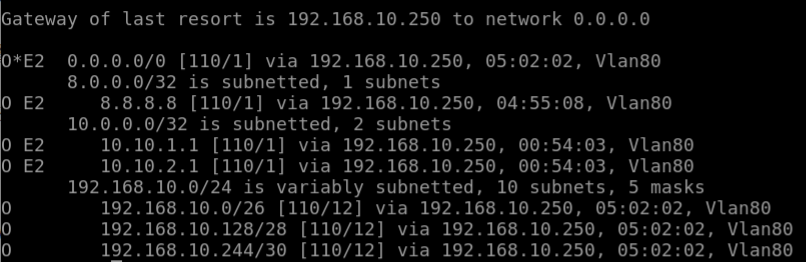
R1



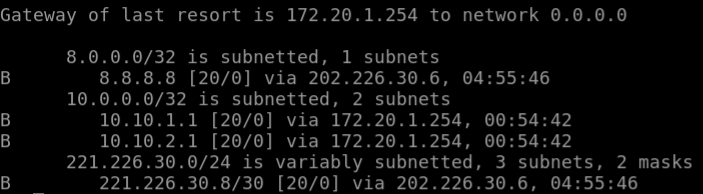
SW1



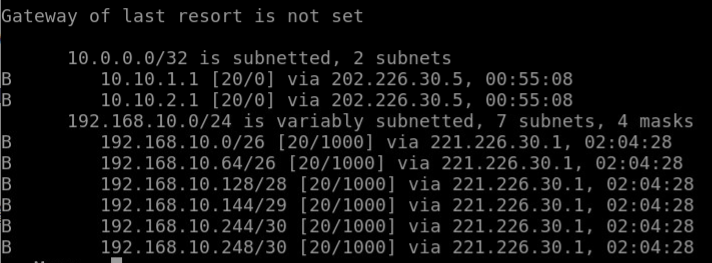
SW2



R1

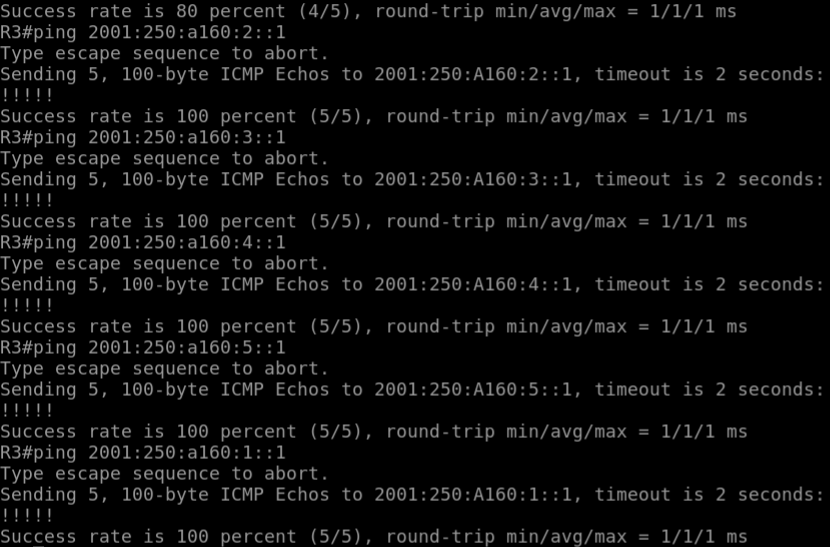


R2



# 隧道配置

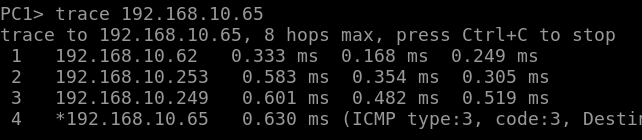
#R1
  
int tunnel1
  
no shutdown
  
ipv6 enable
  
ipv6 address 2001:250:a160:10::1/64
  
tunnel source 221.226.30.1
  
tunnel destination 221.226.30.10
  
tunnel mode ipv6ip
  
  
#R3
  
int tunnel1
  
no shutdown
  
ipv6 enable
  
ipv6 address 2001:250:a160:10::2/64
  
tunnel source 221.226.30.10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



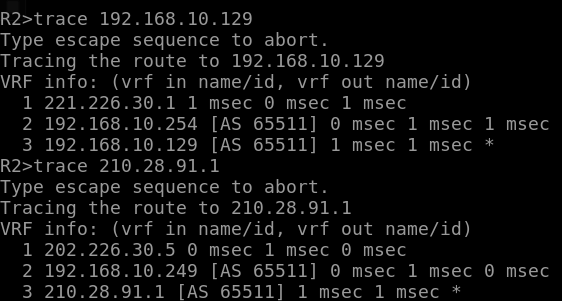
# 策略配置

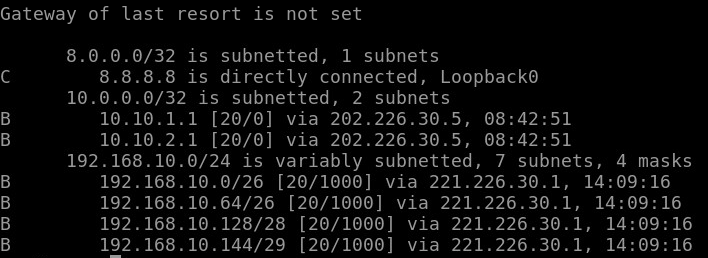
#SW1
  
access-list 100 permit ip 192.168.10.0 0.0.0.63 192.168.10.144 0.0.0.7
  
access-list 100 permit ip 192.168.10.0 0.0.0.63 192.168.10.64 0.0.0.63
  
access-list 100 permit ip 192.168.10.128 0.0.0.15 192.168.10.144 0.0.0.7
  
access-list 100 permit ip 192.168.10.128 0.0.0.15 192.168.10.64 0.0.0.63
  
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

PC1->PC4

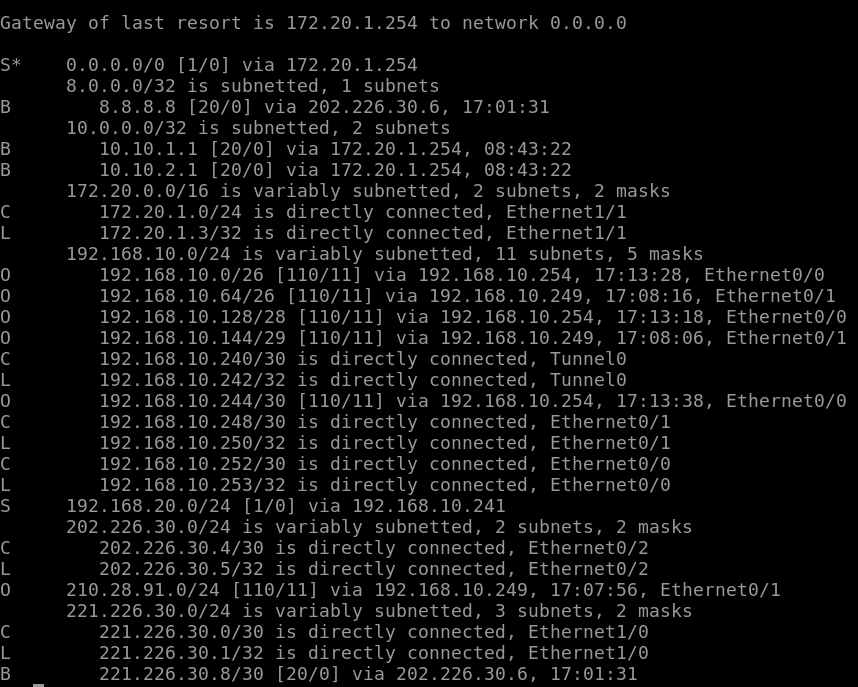


R2





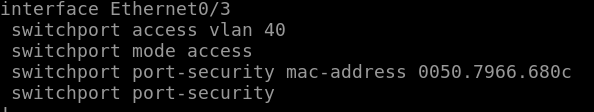
R1



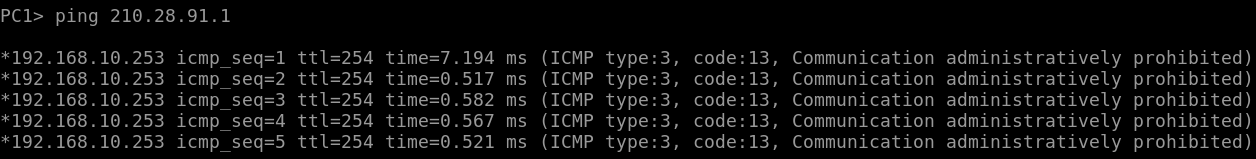
# 安全机制

#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

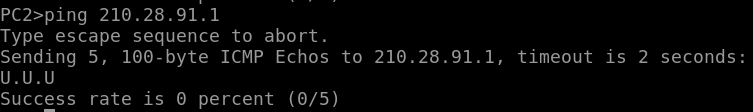
SW2



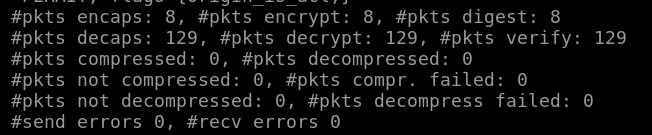
PC1

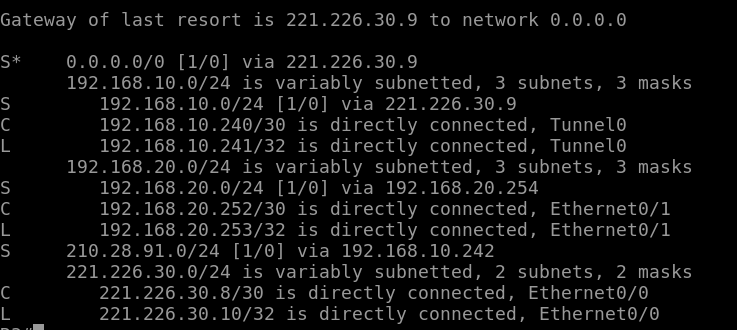


PC2



R3





# 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

R1

