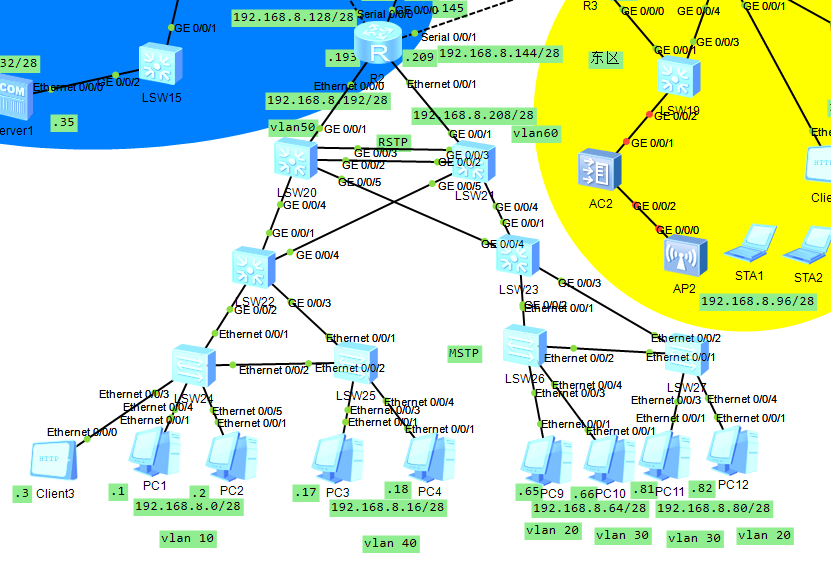
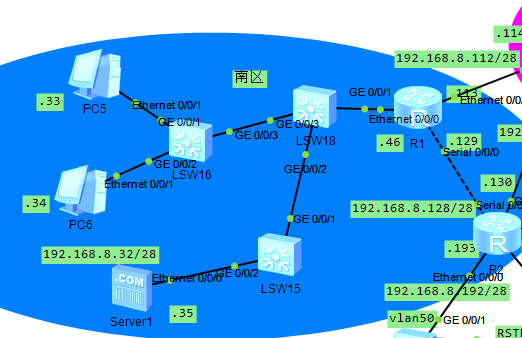
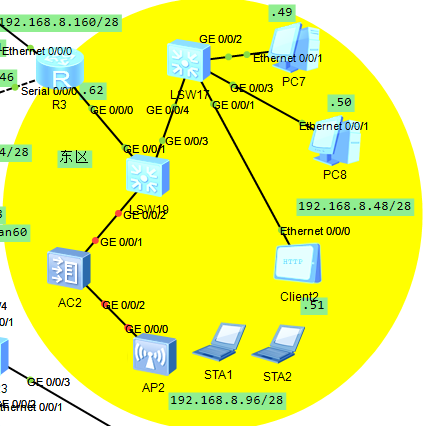
一、方案设计

（1）北区：

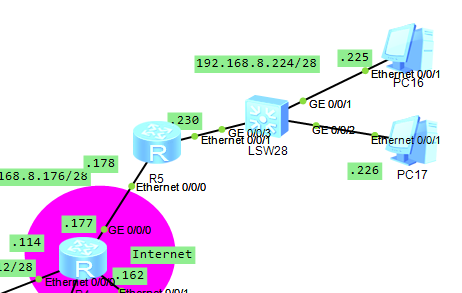


（2）南区：  


（3）东区：



（4）外网（搭建VPN）



二、设置过程

（1）网段访问控制：

R1

acl number 2019

rule 5 permit source 192.168.8.32 0.0.0.15

#

acl number 3001

rule 10 deny tcp source 192.168.8.48 0.0.0.15 destination 192.168.8.35 0 destin

ation-port eq ftp

#

acl number 3010

rule 5 permit ip source 192.168.8.32 0.0.0.15 destination 192.168.8.224 0.0.0.1

5

rule 10 deny ip

（2）nat地址转换：

R1

nat address-group 1 192.168.8.115 192.168.8.116

nat address-group 2 192.168.8.117 192.168.8.120

（3）IPsec VPN设置：

R1

ipsec proposal prop10

esp authentication-algorithm sha2-256

esp encryption-algorithm aes-128

#

ike proposal 10

encryption-algorithm aes-cbc-128

#

ike peer ike10 v1

pre-shared-key cipher WL,HSrw:,#mVJbFY|9$Q~.2#

ike-proposal 10

remote-address 192.168.8.178

#

ipsec policy po10 10 isakmp

security acl 3010

ike-peer ike10

proposal prop10

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password cipher BJB3#A}[;JbL^B&WSBiQTnp#

local-user admin service-type http

#

firewall zone Local

priority 16

#

interface Ethernet0/0/0

ip address 192.168.8.46 255.255.255.240

dhcp select global

#

interface Ethernet0/0/1

ip address 192.168.8.113 255.255.255.240

ipsec policy po10

nat outbound 2019 address-group 2

#

interface Serial0/0/0

link-protocol ppp

ip address 192.168.8.129 255.255.255.240

#

ip route-static 192.168.8.176 255.255.255.240 192.168.8.114

ip route-static 192.168.8.224 255.255.255.240 192.168.8.114

（4）dhcp地址池：

R1

ip pool \_R1

gateway-list 192.168.8.46

network 192.168.8.32 mask 255.255.255.240

static-bind ip-address 192.168.8.33 mac-address 5489-98aa-7bad

excluded-ip-address 192.168.8.40 192.168.8.45

lease day 30 hour 0 minute 0

（5）单区域ospf设置：

R1

ospf 100

area 0.0.0.0

network 192.168.8.46 0.0.0.0

network 192.168.8.113 0.0.0.0

network 192.168.8.129 0.0.0.0

（6）南区和东区PC端Ping通：  
