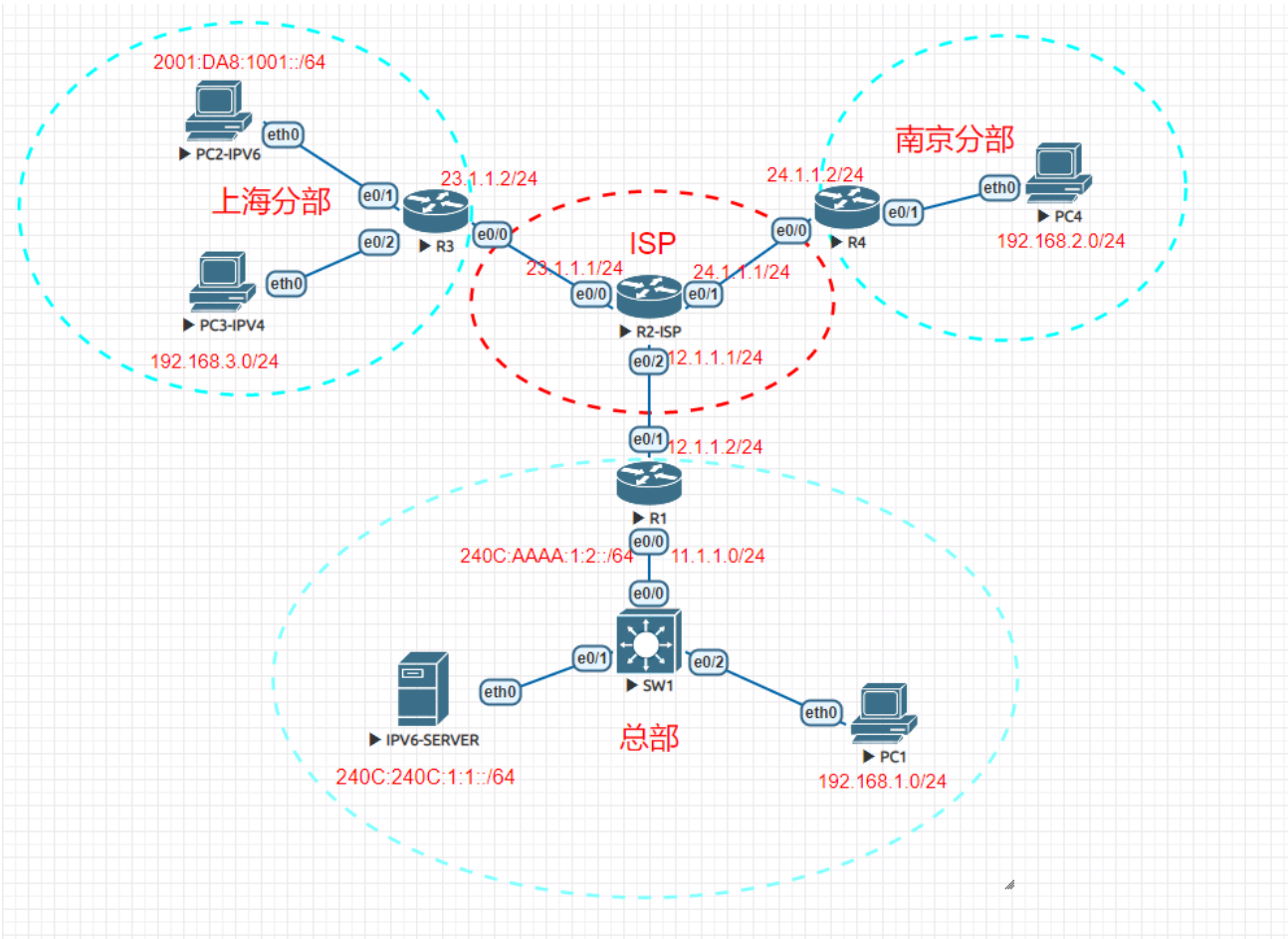


# 实验五

## 实验拓扑



## 实验需求

注:中间 R2 设备为模拟运营商设备,无法控制,本题目中 R2 已预配。(手动配置完 R2 的接口地址后,就不需要再配置其他的)

### 1、IP 配置

按照拓扑中 IP 标记配置 IP,主机网关自定义。

### 2、MAC 地址绑定

SW1 上与 IPV6 服务器和 PC1 所连接接口配置 MAC 地址绑定,只允许对应主机接入

### 3、6TO4 隧道配置

总部 R1 和上海分部之间建立 GRE(6to4)隧道,实现总部 IPV6-server 可以可上海分部 IPV6 网络互通,隧道所用 IPV6 地址段为:240C:6464:1:1::/64

### 4、IPSEC VPN

由于中间 R2 设备为运营商设备无法控制，总部想和南京分部之间建立一条 VPN 隧道传输内部数据，并且要保证数据安全，所以需要在总部和南京分部之间建立一条 IPSEC VPN，具体参数要求如下：隧道使用预共享密钥进行身份验证

- DES 加密方式
- HASH 算法为 MD5
- 预共享密钥为 lab5
- 密钥位数 group2

## 5、GRE OVER IPSEC

总部与上海分部之间也想建立一条 V4 的隧道来传递公司内部数据，同时要保证数据安全性，请在原有的 6TO4 隧道上增加 IPV4 互联:100.1.1.0/24,并通过 IPSEC 技术对隧道之间流量进行加密，IPSEC 参数配置同 4 题相同

## 功能测试

1、测试新建 VPC 接入 SW1 替换目前的 PC 是否能 ping 通 SW1 相对应 vlan 接口的 ip 地址。(请在所有实验完成后再进行此步骤)

2、测试总部与上海分部的 IPV6 网络是否可以 ping 通

3、测试总部与南京分部之间可以 ping 通，且如下图所示，ping 前和 ping 后在 R1 或 R4 上输入 show crypto ipsec sa 命令查看输出中的#pkts encrypt 和#pkts decrypt 值是否增加，如增加就表示已经成功加密了。

```
R4#sh cryp ipsec sa
interface: Ethernet0/0
  Crypto map tag: R4-map, local addr 24.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 12.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 572, #pkts encrypt: 572, #pkts digest: 572
  #pkts decaps: 575, #pkts decrypt: 575, #pkts verify: 575
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
```

4、测试总部与上海分部之间 IPV4 网络可以 ping 通，且如下图所示，ping 前和 ping 后在 R1 或 R3 上输入 show crypto ipsec sa interface tunnel 0 命令查看输出中的#pkts encrypt 和#pkts decrypt 值是否增加，如增加就表示已经成功加密了。

```
R1#sh crypto ipsec sa interface tunnel 0

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 12.1.1.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (12.1.1.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (23.1.1.2/255.255.255.255/47/0)
current_peer 23.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1496, #pkts encrypt: 1496, #pkts digest: 1496
    #pkts decaps: 1490, #pkts decrypt: 1490, #pkts verify: 1490
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```