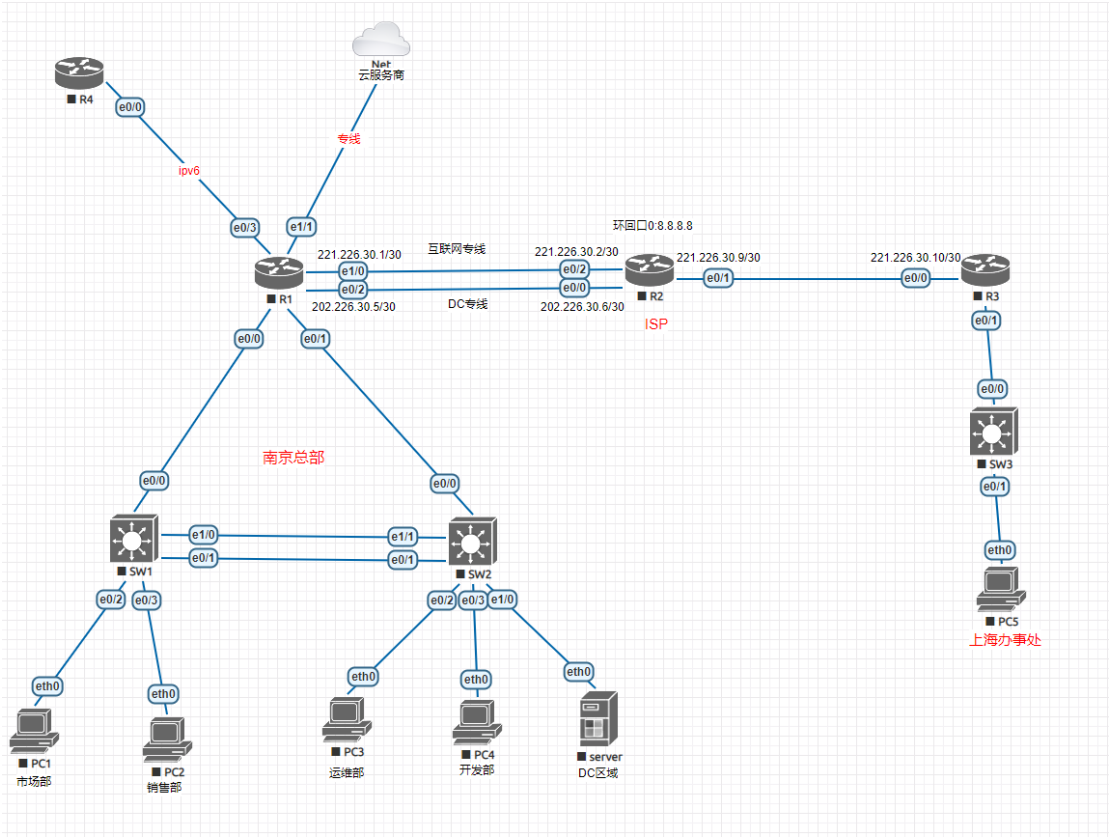


# 一. 网络拓扑



## 二. 功能需求

### 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。

5.4 IPV6 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、实验报告

根据要求给出实验配置与效果验证(截图)，统一保存到 word 文档中，文档以姓名+学号命名，注意每题截图请标注题目序号和每个截图的设备名称。

- 1、将 IP 地址规划与 VLAN 规划以表格形式列出。
- 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。
- 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。
- 4、输入 `show etherchannel summary` 截图 SW1 与 SW2 上的聚合接口信息。
- 5.1、输入 `sh ip 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
- 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
- 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。
- 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。
- 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。

