**上海市“星光计划”**

**第十届职业院校职业技能大赛**

“网络搭建与应用”项目样题

竞赛时长 3小时

上海市星光计划组委会竞赛办公室

竞赛说明：

1.禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

2.请根据大赛所提供的比赛环境，检查所列的硬件设备、软件及文档清单、材料清单是否齐全，计算机设备是否能正常使用。

3.请参赛选手仔细阅读赛卷，按照要求完成各项操作。

4.操作过程中，需要及时保存配置。

5.比赛结束后，所有设备保持运行状态，评判以最后的硬件连接和提交文档为最终结果。禁止将比赛所用的所有物品（包括赛卷）带离赛场。

6.禁止在纸质资料、比赛设备和电脑桌上作任何与竞赛无关的标记，如违反规定，可视为0分。

7.与比赛相关的软件和文档存放在物理机的D:\soft文件夹中。

8.请在物理机PC1桌面上新建“XXX”文件夹作为“选手目录”（XXX为赛位号。举例：1号赛位，文件夹名称为“001”），按照“网络搭建及安全部署竞赛结果提交指南.txt”保存要求生成的全部结果文档，将生成的文档复制到

“选手目录”。

项目简介:

某集团公司原在北京建立了总公司，后在成都建立了分公司，又在广东设立了办事处。集团设有产品、营销、法务、财务、人力5个部门，统一进行IP及业务资源的规划和分配，全网采用OSPF、RIP、ISIS、BGP路由协议进行互联互通。

2022 年在党的坚强领导下，全年公司规模保持快速增长，业务数据量和公司访问量增长巨大，不断开创新局面，向着全面建成社会主义现代化强国的第二个百年奋斗目标迈进。为了更好管理数据，提供服务，集团决定在北京建立两个数据中心，在贵州建立异地灾备数据中心，以达到快速、可靠交换数据，增强业务部署弹性的目的，完成向两地三中心整体战略架构演进，更好的服务于公司客户。

集团、分公司及办事处的网络结构详见拓扑图。编号为SW1的设备作为集团北京1#DC核心交换机，编号为SW2的设备作为集团北京2#DC核心交换机；编号为SW3的设备作为贵州DC核心交换机；编号FW1的设备作为集团互联网出口防火墙；编号为FW2的设备作为办事处防火墙；编号为RT1的设备作为集团核心路由器；编号为RT2的设备作为分公司路由器；编号为AC1的设备作为分公司的有线无线智能一体化控制器，通过与AP1配合实现分公司无线覆盖。

注意：在此典型互联网应用网络架构中，作为IT网络运维人员，请根据拓扑构建完整的系统环境，使整体网络架构具有良好的稳定性、安全性、可扩展性。

请完成所有服务配置后，从客户端进行测试，确保能正常访问到相应应用。网络拓扑:

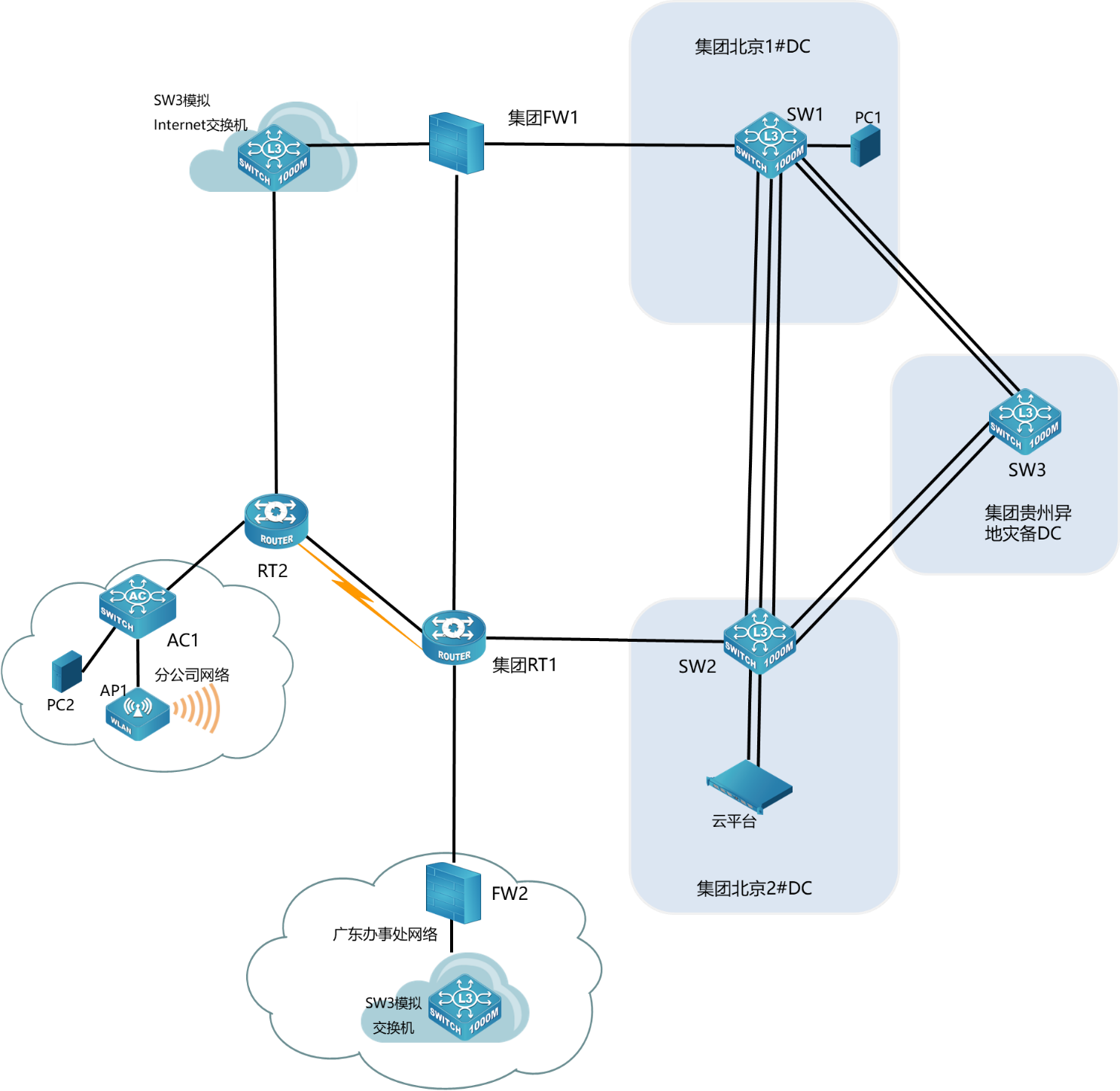


表1-网络设备连接表

|  |  |  |  |
| --- | --- | --- | --- |
| A设备连接至B设备 | | | |
| 设备名称 | 接口 | 设备名称 | 接口 |
| SW1 | E1/0/21 | FW1 | E0/1 |
| SW1 | E1/0/22 | SW3 | E1/0/21 |
| SW1 | E1/0/23 二层 | SW3 | E1/0/23 二层 |
| SW1 | E1/0/26 三层 | SW2 | E1/0/26 三层 |
| SW1 | E1/0/27 VPN | SW2 | E1/0/27 VPN |
| SW1 | E1/0/28 二层 | SW2 | E1/0/28 二层 |
| SW1 | E1/0/1 | PC1 | NIC |
| SW2 | E1/0/21 | RT1 | G0/1 |
| SW2 | E1/0/22 | SW3 | E1/0/22 |
| SW2 | E1/0/23 二层 | SW3 | E1/0/24 二层 |
| SW3模拟办事处 | E1/0/11 | 模拟产品PC |  |
| SW3模拟办事处 | E1/0/12 | 模拟营销PC |  |
| SW3模拟办事处 | E1/0/15 | FW2 | E0/1 |
| SW3模拟Internet | E1/0/17 | FW1 | E0/3 |
| SW3模拟Internet | E1/0/18 | RT2 | G0/3 |
| RT1 | G0/0 | RT2 | G0/0 |
| RT1 | S1/0 | RT2 | S1/1 |
| RT1 | S1/1 | RT2 | S1/0 |
| RT1 | G0/2 | FW1 | E0/2 |
| RT1 | G0/3 | FW2 | E0/2 |
| RT2 | G0/1 | AC1 | E1/0/1 |
| AC1 | E1/0/3 | AP1 | ETH |
| AC1 | E1/0/4 vlan110 | PC2 | NIC |
| SW2 | E1/0/11 | 云平台 | Eth1 |
| SW2 | E1/0/12 | 云平台 | Eth2 |

表2-网络设备IP地址分配表

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备接口 | IP地址 |
| SW1 | loopback1 ospfv2 ospfv3 bgp | 10.10.1.1/32  2001:10:10:1::1/128 |
| loopback2 | 10.10.1.2/32  2001:10:10:1::2/128 |
| vlan10 | 10.10.11.1/24  2001:10:10:11::1/64 |
| vlan20 | 10.10.12.1/24  2001:10:10:12::1/64 |
| vlan30 | 10.10.13.1/24  2001:10:10:13::1/64 |
| vlan40 | 10.10.14.1/24  2001:10:10:14::1/64 |
| vlan50 | 10.10.15.1/24  2001:10:10:15::1/64 |
| vlan60 | 10.10.60.1/24  2001:10:10:60::1/64 |
| vlan70 | 10.10.70.1/24  2001:10:10:70::1/64 |
| vlan80 | 10.10.80.1/24  2001:10:10:80::1/64 |
| vlan90 | 10.10.90.1/24  2001:10:10:90::1/64 |
| vlan1021 | 10.10.255.14/30 |
| vlan1022 | 10.10.255.5/30 |
| vlan1026 | 10.10.255.1/30 |
| vlan1027 vpn | 10.10.255.1/30 |
| SW2 | loopback1 ospfv2 ospfv3 bgp | 10.10.2.1/32  2001:10:10:2::1/128 |
| loopback2 | 10.10.2.2/32  2001:10:10:2::2/128 |
| vlan10 | 10.10.21.1/24  2001:10:10:21::1/64 |
| vlan20 | 10.10.22.1/24  2001:10:10:22::1/64 |

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备接口 | IP地址 |
|  | vlan30 | 10.10.23.1/24  2001:10:10:23::1/64 |
| vlan40 | 10.10.24.1/24  2001:10:10:24::1/64 |
| vlan50 | 10.10.25.1/24  2001:10:10:25::1/64 |
| vlan60 | 10.10.60.2/24  2001:10:10:60::2/64 |
| vlan70 | 10.10.70.2/24  2001:10:10:70::2/64 |
| vlan80 | 10.10.80.2/24  2001:10:10:80::2/64 |
| vlan90 | 10.10.90.2/24  2001:10:10:90::2/64 |
| vlan1021 | 10.10.255.22/30 |
| vlan1022 | 10.10.255.9/30 |
| vlan1026 | 10.10.255.2/30 |
| vlan1027 vpn | 10.10.255.2/30 |
| SW3 | loopback1 ospfv2 ospfv3 bgp | 10.10.3.1/32  2001:10:10:3::1/128 |
| vlan10 | 10.10.31.1/24  2001:10:10:31::1/64 |
| vlan20 | 10.10.32.1/24  2001:10:10:32::1/64 |
| vlan30 | 10.10.33.1/24  2001:10:10:33::1/64 |
| vlan50 | 10.10.35.1/24  2001:10:10:35::1/64 |
| vlan60 | 10.10.60.3/24  2001:10:10:60::3/64 |
| vlan70 | 10.10.70.3/24  2001:10:10:70::3/64 |
| vlan80 | 10.10.80.3/24  2001:10:10:80::3/64 |
| vlan90 | 10.10.90.3/24 |

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备接口 | IP地址 |
|  |  | 2001:10:10:90::3/64 |
| vlan1021 | 10.10.255.6/30 |
| vlan1022 | 10.10.255.10/30 |
| SW3模拟办事处 | loopback2 | 10.10.3.2/32  2001:10:10:3::2/128 |
| vlan110 | 10.16.110.1/24  2001:10:16:110::1/64 |
| vlan120 | 10.16.120.1/24  2001:10:16:120::1/64 |
| vlan1015 | 10.10.255.46/30 |
| SW3模拟  Internet | loopback3 | 200.200.3.3/32  2001:200:200:3::3/128 |
| vlan1017 | 200.200.200.1/30 |
| vlan1018 | 200.200.200.5/30 |
| RT1 | loopback1 ospfv2 ospfv3 bgp mpls | 10.10.4.1/32  2001:10:10:4::1/128 |
| loopback2 rip ripng | 10.10.4.2/32  2001:10:10:4::2/128 |
| loopback3 isis | 10.10.4.3/32  2001:10:10:4::3/128 |
| loopback4 集团与办事处互联 | 10.10.4.4/32  2001:10:10:4::4/128 |
| loopback5 vpn财务 | 10.10.4.5/32  2001:10:10:4::5/128 |
| g0/0 | 10.10.255.29/30 |
| g0/1 | 10.10.255.21/30 |
| g0/2 | 10.10.255.18/30 |
| g0/3 | 10.10.255.25/30 |
| s1/0 | 10.10.255.33/30 |
| s1/1 | 10.10.255.37/30 |
| RT2 | loopback1 ospfv2 ospfv3 bgp mpls | 10.10.5.1/32  2001:10:10:5::1/128 |
| loopback2 rip ripng | 10.10.5.2/32  2001:10:10:5::2/128 |
| loopback3 isis | 10.10.5.3/32 |

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备接口 | IP地址 |
|  |  | 2001:10:10:5::3/128 |
| loopback4 ipsecvpn | 10.10.5.4/32  2001:10:10:5::4/128 |
| tunnel4 ipsecvpn | 10.10.255.50/30 |
| loopback5 vpn财务 | 10.10.5.5/32  2001:10:10:5::5/128 |
| g0/0 | 10.10.255.30/30 |
| g0/1 | 10.10.255.41/30 |
| g0/3 | 200.200.200.6/30 |
| s1/0 | 10.10.255.38/30 |
| s1/1 | 10.10.255.34/30 |
| FW1 | loopback1 ospfv2 ospfv3 trust | 10.10.6.1/32  2001:10:10:6::1/128 |
| loopback2 rip ripng trust | 10.10.6.2/32  2001:10:10:6::2/128 |
| loopback4 ipsecvpn trust | 10.10.6.4/32  2001:10:10:6::4/128 |
| tunnel4 ipsecvpn VPNHUB | 10.10.255.49/30 |
| tunnel8 sslvpn VPNHUB | 10.18.0.1/24 |
| e0/1 trust | 10.10.255.13/30 |
| e0/2 trust | 10.10.255.17/30 |
| e0/3 untrust | 200.200.200.2/30 |
| FW2 | loopback1 ospfv2 ospfv3 trust | 10.10.7.1/32  2001:10:10:7::1/128 |
| e0/1 trust | 10.10.255.45/30 |
| e0/2 dmz | 10.10.255.26/30 |
| tunnel9 l2tpvpn VPNHUB | 10.19.0.1/24 |
| AC1 | loopback1 ospfv2 ospfv3 | 10.10.8.1/32  2001:10:10:8::1/128 |
| loopback2 rip ripng | 10.10.8.2/32  2001:10:10:8::2/128 |
| loopback3 | 10.10.8.3/32  2001:10:10:8::3/128 |
| vlan100 无线管理 | 10.17.100.1/24  2001:10:17:100::1/64 |
| 设备名称 | 设备接口 | IP地址 |
|  | vlan110 无线2.4G 产品 | 10.17.110.1/24  2001:10:17:110::1/64 |
| vlan120 无线5G 营销 | 10.17.120.1/24  2001:10:17:120::1/64 |
| vlan1001 | 10.10.255.42/30 |

1. 职业素养

1.整理赛位，工具、设备归位，保持赛后整洁有序。

2.无因选手原因导致设备损坏。

3.恢复调试现场，保证网络和系统安全运行。

二、理论测试

每组选手登录到指定的理论测试系统，进行答题。理论测试试题50道。答题时间为3小时。

三、交换配置

1.配置vlan，SW1、SW2、SW3、AC1的二层链路只允许相应vlan通过。

|  |  |  |  |
| --- | --- | --- | --- |
| 设备 | vlan编号 | 端口 | 说明 |
| SW1 | vlan10 | E1/0/1 | 产品1段 |
| vlan20 | E1/0/2 | 营销1段 |
| vlan30 | E1/0/3 | 法务1段 |
| vlan40 | E1/0/4 | 财务1段 |
| vlan50 | E1/0/5 | 人力1段 |
| vlan60 | E1/0/6 | 产品管理 |
| vlan70 | E1/0/7 | 产品研发 |
| vlan80 | E1/0/8 | 产品生产 |
| vlan90 | E1/0/9 | 产品支持 |
| SW2 | vlan10 | E1/0/1 | 产品2段 |
| vlan20 | E1/0/2 | 营销2段 |
| vlan30 | E1/0/3 | 法务2段 |
| vlan40 | E1/0/4 | 财务2段 |
| vlan50 | E1/0/5 | 人力2段 |
| vlan60 | E1/0/6 | 产品管理 |
| vlan70 | E1/0/7 | 产品研发 |
| vlan80 | E1/0/8 | 产品生产 |
| vlan90 | E1/0/9 | 产品支持 |
| SW3 | vlan10 | E1/0/1 | 产品3段 |
| vlan20 | E1/0/2 | 营销3段 |
| vlan30 | E1/0/3 | 法务3段 |
| vlan50 | E1/0/5 | 人力3段 |
| vlan60 | E1/0/6 | 产品管理 |
| vlan70 | E1/0/7 | 产品研发 |
| vlan80 | E1/0/8 | 产品生产 |
| vlan90 | E1/0/9 | 产品支持 |

2.SW1、SW2、SW3启用MSTP，实现网络二层负载均衡和冗余备份，创建实例 Instance10和Instance20，名称为SKILLS，修订版本为1，其中Instance10关联vlan60和vlan70，Instance20关联vlan80和vlan90。SW1为Instance0和 Instance10的根交换机，为Instance20备份根交换机；SW2为Instance20根交换机，为Instance0和Instance10的备份根交换机；根交换机STP优先级为0，备份根交换机STP优先级为4096。关闭交换机之间三层互联接口的STP。

3.SW1 和 SW2 之间利用三条裸光缆实现互通，其中一条裸光缆承载三层 IP 业务、一条裸光缆承载VPN业务、一条裸光缆承载二层业务。用相关技术分别实现财务1段、财务2段业务路由表与其它业务路由表隔离，财务业务VPN实例名称为CW。承载二层业务的只有一条裸光缆通道，配置相关技术，方便后续链路扩容与冗余备份，编号为1，用LACP协议，SW1为active，SW2为active；采用源、目的IP进行实现流量负载分担。

4.将 SW3 模拟为 Internet 交换机，实现与集团其它业务路由表隔离，Internet路由表VPN实例名称为Internet。将SW3模拟办事处交换机，实现与集团其它业务路由表隔离，办事处路由表VPN实例名称为Guangdong。

5.SW1法务物理接口限制收发数据占用的带宽均为1000Mbps，限制所有报文最大收包速率为1000packets/s，如果超过了配置交换机端口的报文最大收包速率则关闭此端口，1分钟后恢复此端口；启用端口安全功能，最大安全MAC地址数为20，当超过设定MAC地址数量的最大值，不学习新的MAC、丢弃数据包、发 snmp trap、同时在syslog日志中记录，端口的老化定时器到期后，在老化周期中没有流量的部分表项老化，有流量的部分依旧保留，恢复时间为10分钟；禁止采用访问控制列表，只允许IP主机位为20-50的数据包进行转发；禁止配置访问控制列表，实现端口间二层流量无法互通，组名称FW。

7.SW1 配置 SNMP，引擎 id 分别为 1；创建组 GROUP2022，采用最高安全级别，配置组的读、写视图分别为：SKILLS\_R、SKILLS\_W；创建认证用户为USER2022，采用aes算法进行加密，密钥为Pass-1234，哈希算法为sha，密钥为Pass-1234；当设备有异常时，需要用本地的环回地址loopback1发送v3 Trap消息至集团网管服务器10.10.11.99、2001:10:10:11::99，采用最高安全级别；当法务部门对应的用户接口发生UP DOWN事件时，禁止发送trap消息至上述集团网管服务器。

8.将W1与FW1互连流量镜像到SW1 E1/0/1，会话列表为1。

9.SW1和SW2 E1/0/21-28启用单向链路故障检测，当发生该故障时，端口标记为errdisable状态，自动关闭端口，经过1分钟后，端口自动重启；发送

Hello报文时间间隔为15s；

四、路由配置

3.配置所有设备接口ipv4地址和ipv6地址，互联接口ipv6地址用本地链路地址。

4.利用vrrpv2和vrrpv3技术实现vlan60、vlan70、vlan80、vlan90网关冗余备份，vrrp id与vlan id相同。vrrpv2 vip为10.10.vlanid.9（如vlan60 的vrrpv2 vip为10.10.60.9），vrrpv3 vip为FE80:vlanid::9（如vlan60的 vrrpv3 vip 为 FE80:60::9）。配置 SW1 为 vlan60、vlan70 的 Master，SW2 为 vlan80、vlan90的Master。要求vrrp组中高优先级为120，低优先级为默认值，抢占模式为默认值，vrrpv2和vrrpv3发送通告报文时间间隔为默认值。当SW1 或SW2上联链路发生故障，Master优先级降低50。

6.SW1、SW2、SW3、RT1以太链路、RT2以太链路、FW1、FW2、AC1之间运行 OSPFv2和OSPFv3协议（路由模式发布网络用接口地址，BGP协议除外）。

(1)SW1、SW2、SW3、RT1、RT2、FW1之间OSPFv2和OSPFv3协议，进程1，区域0，分别发布loopback1地址路由和产品路由，FW1通告type2默认路由。

(2)RT2与AC1之间运行OSPFv2协议，进程1，nssa no-summary区域1； AC1 发布 loopback1 地址路由、产品和营销路由，用 prefix-list 重发布 loopback3。

(4)SW3模拟办事处产品和营销接口配置为loopback，模拟接口up。SW3模拟办事处与 FW2 之间运行 OSPFv2 协议，进程 2，区域 2，SW3 模拟办事处发布 loopback2、产品和营销。SW3模拟办事处配置ipv6默认路由；FW2分别配置到 SW3模拟办事处loopback2、产品和营销的ipv6明细静态路由，FW2重发布静态路由到OSPFv3协议。

(5)RT1、FW2之间OSPFv2和OSPFv3协议，进程2，区域2；RT1发布loopback4 路由，向该区域通告type1默认路由；FW2发布loopback1路由，FW2禁止学习到集团和分公司的所有路由。RT1用prefix-list匹配FW2 loopback1路由、SW3 模拟办事处loopback2和产品路由、RT1与FW2直连ipv4路由，将这些路由重发布到区域0。

(6)修改ospf cost为100，实现SW1分别与RT2、FW2之间ipv4和ipv6互访流量优先通过SW1\_SW2\_RT1链路转发，SW2访问Internet ipv4和ipv6流量优先通过SW2\_SW1\_FW1链路转发。

7.RT1串行链路、RT2串行链路、FW1、AC1之间分别运行RIP和RIPng协议， FW1、RT1、RT2的RIP和RIPng发布loopback2地址路由，AC1 RIP发布loopback2 地址路由，AC1 RIPng采用route-map匹配prefix-list重发布loopback2地址路由。RT1配置offset值为3的路由策略，实现RT1-S1/0\_RT2-S1/1为主链路， RT1-S1/1\_RT2-S1/0为备份链路，ipv4的ACL名称为AclRIP，ipv6的ACL名称为AclRIPng。RT1的S1/0与RT2的S1/1之间采用chap双向认证，用户名为对端设备名称，密码为Pass-1234。

8.RT1 以太链路、RT2 以太链路之间运行 ISIS 协议，进程 1，分别实现 loopback3 之间 ipv4 互通和 ipv6 互通。RT1、RT2 的 NET 分别为

10.0000.0000.0001.00、10.0000.0000.0002.00，路由器类型是Level-2，接口网络类型为点到点。配置域md5认证和接口md5认证，密码均为Pass-1234。

10.SW1、SW2、SW3、RT1、RT2之间运行BGP协议，SW1、SW2、RT1 AS号65001、 RT2 AS号65002、SW3 AS号65003。

(1)SW1、SW2、SW3、RT1、RT2之间通过loopback1建立ipv4和ipv6 BGP邻居。SW1 和 SW2 之间财务通过 loopback2 建立 ipv4 BGP 邻居，SW1 和 SW2 的 loopback2互通采用静态路由。

(2)SW1、SW2、SW3、RT2分别只发布营销、法务、财务、人力等ipv4和ipv6 路由；RT1发布办事处营销ipv4和ipv6路由到BGP。

(3)SW3营销分别与SW1和SW2营销ipv4和ipv6互访优先在SW3\_SW1链路转发；SW3 法务及人力分别与 SW1 和 SW2法务及人力 ipv4 和ipv6 互访优先在 SW3\_SW2链路转发，主备链路相互备份；用prefix-list、route-map和BGP路径属性进行选路，新增AS 65000。

11.利用BGP MPLS VPN技术，RT1与RT2以太链路间运行多协议标签交换、标签分发协议。RT1与RT2间创建财务VPN实例，名称为CW，RT1的RD值为1:1， export rt值为1:2，import rt值为2:1；RT2的RD值为2:2。通过两端loopback1 建立VPN邻居，分别实现两端loopback5 ipv4互通和ipv6互通。

五、无线配置

1.AC1 loopback1 ipv4和ipv6地址分别作为AC1的ipv4和ipv6管理地址。AP二层自动注册，AP采用MAC地址认证。配置2个ssid，分别为SKILLS-

2.4G和SKILLS-5G。SKILLS-2.4G对应vlan110，用network 110和radio1（模式为 n-only-g）,用户接入无线网络时需要采用基于 WPA-personal 加密方式，密码为Pass-1234。SKILLS-5G对应vlan120，用network 120和radio2（模式为n-only-a），不需要认证，隐藏ssid，SKILLS-5G用倒数第一个可用VAP发送 5G信号。

5.AC1配置dhcpv4和dhcpv6，分别为SW1产品1段vlan10和分公司vlan100、 vlan110和vlan120分配地址；ipv4地址池名称分别为POOLv4-10、POOLv4-100、 POOLv4-110、POOLv4-120，ipv6 地址池名称分别为 POOLv6-10、POOLv6-100、

POOLv6-110、POOLv6-120；ipv6地址池用网络前缀表示；排除网关；DNS分别为 114.114.114.114 和 2400:3200::1；为 PC1 保留地址 10.10.11.9 和 2001:10:10:11::9，为AP1保留地址10.17.100.9和2001:10:17:100::9，为PC2 保留地址10.17.110.9和2001:10:17:110::9。SW1上中继地址为AC1 loopback1 地址。SW1启用dhcpv4和dhcpv6 snooping，如果E1/0/1连接dhcpv4服务器，则关闭该端口，恢复时间为1分钟。

4.防止多AP和AC相连时过多的安全认证连接而消耗CPU资源，检测到AP 与AC 10分钟内建立连接5次就不再允许继续连接，2小时后恢复正常。

5.配置vlan110无线接入用户上班时间（工作日09:00-17:00）访问Internet https上下行CIR为100Mbps，CBS为200Mbps，PBS为300Mbps，exceed-action 和violate-action均为drop。时间范围名称、控制列表名称、分类名称、策略名称均为SKILLS。

6.开启AP组播广播突发限制功能；AP收到错误帧时，将不再发送ACK帧； AP发送向无线终端表明AP存在的帧时间间隔为1秒。

7.AP发射功率为80%。

六、安全配置

说明：ip 地址按照题目给定的顺序用“ip/mask”表示，ipv4 any 地址用

0.0.0.0/0，ipv6 any地址用::/0，禁止用地址条目，否则按零分处理。

1.FW1配置ipv4 nat，实现集团产品1段ipv4访问Internet ipv4，转换 ip/mask为200.200.200.160/28，保证每一个源ip产生的所有会话将被映射到同一个固定的IP地址；当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至10.10.11.99的 UDP 514端口，记录主机名，用明文轮询方式分发日志；开启相关特性，实现扩展nat转换后的网络地址端口资源。

2.FW1配置nat64，实现集团产品1段ipv6访问Internet ipv4，转换为出接口IP，ipv4转ipv6地址前缀为64:ff9b::/96。

3.FW1和FW2策略默认动作为拒绝，FW1允许集团产品1段ipv4和ipv6访问Internet任意服务。

4.FW2允许办事处产品ipv4访问集团产品1段https服务，允许集团产品 1段和分公司产品访问办事处产品ipv4、FW2 loopback1 ipv4、SW3模拟办事处 loopback2 ipv4。

5.FW1与RT2之间用Internet互联地址建立GRE Over IPSec VPN，实现 loopback4之间的加密访问。

6.FW1配置SSL VPN，名称为VPNSSL，ssl协议为1.2版本，Internet用户通过端口 8888 连接，本地认证账号 UserSSL,密码 Pass-1234，地址池名称为

POOLSSL，地址池范围为10.18.0.100/24-10.18.0.199/24。保持PC1位置不变，用PC1测试。

9.FW1通过ping监控外网网关地址，监控对象名称为TRACK1，每隔5S发送探测报文，连续10次收不到监测报文，就认为线路故障，关闭外网接口。

云平台配置

云平台网络连接

**任务描述：**请使用超五类非屏蔽双绞线连接网络并设置云平台，保证网络10.10.110.0/24，10.10.120.0/24，192.168.100.100能够相互通信。（提示：关闭交换机与云平台业务相连端口的 STP）

1.网络信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络名称 | VLAN | 子网名称 | 网关 | ipv4地址池 |
| network110 | 110 | subnet110 | 10.10.110.1/24 | 10.10.110.100-10.10.110.199 |
| network120 | 120 | subnet120 | 10.10.110.1/24 | 10.10.110.100-10.10.110.199 |

2.实例类型信息表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 名称 | id | vcpu | 内存 | 磁盘 | 实例 | 模板 |
| windows | 1 | 4 | 4G | 40G | windows1-windows7 | windows2022 |
| linux | 2 | 4 | 4G | 40G | linux1-linux7 | rocky8.6 |
| openstack | 3 | 2 | 2G | 40G | openstack | dcnclient-cli |

3.卷信息

|  |  |  |
| --- | --- | --- |
| 卷名称 | 大小 | 连接的实例 |
| d1-d4 | 5G | windows3 |
| d5-d8 | 5G | linux3 |

4.实例信息表

|  |  |  |
| --- | --- | --- |
| 实例名称 | ipv4地址 | FQDN |
| windows1 | 10.10.110.101 | windows1.skills.com |
| windows2 | 10.10.110.102 | windows2.skills.com |
| windows3 | 10.10.110.103 | windows3.skills.com |
| windows4 | 10.10.110.104 | windows4.skills.com |
| windows5 | 10.10.110.105 | windows5.skills.com |
| windows6 | 10.10.110.106 | windows6.cnskills.com |
| windows7 | 10.10.110.107 | windows7.bj.skills.com |
| linux1 | 10.10.120.101 | linux1.skills.com |
| linux2 | 10.10.120.102 | linux2.skills.com |
| linux3 | 10.10.120.103 | linux3.skills.com |
| linux4 | 10.10.120.104 | linux4.skills.com |
| linux5 | 10.10.120.105 | linux5.skills.com |
| openstack | 10.10.120.111 |  |

Windows系统服务配置

# 域服务

**任务描述：**请采用域环境，管理企业网络资源。

**任务要求：**

1.配置windows2为skills.com域控制器；安装dns服务，dns正反向区域在activedirectory中存储，负责该域的正反向域名解析。

2.把skills.com域服务迁移到windows1；安装dns服务，dns正反向区域在activedirectory中存储，负责该域的正反向域名解析。

3.配置windows6为skills.com林中的cnskills.com域控制器；安装dns服务，负责该域的正反向域名解析。

4.配置windows7为bj.cnskills.com域控制器；安装dns服务，负责该域的正反向域名解析。

5.把其他windows主机加入到skills.com域。所有windows主机（含域控制器）用skills\Administrator身份登陆。

6.在windows1上安装证书服务，为windows主机颁发证书，证书颁发机构有效期为10年，证书颁发机构的公用名为windows1.skills.com。复制“计算机”证书模板，名称为“计算机副本”，申请并颁发一张供windows服务器使用的证书，证书友好名称为pc，（将证书导入到需要证书的windows服务器），证书信息：证书有效期=5年，公用名=skills.com，国家=CN，省=Beijing，城市=Beijing，组织=skills，组织单位=system，使用者可选名称=\*.skills.com和skills.com。浏览器访问https网站时，不出现证书警告信息。

7.在windows2上安装从属证书服务，证书颁发机构的公用名为windows2.skills.com。

8.在windows1上新建名称为manager、dev、sale的3个组织单元；每个组织单元内新建与组织单元同名的全局安全组；每个组内新建20个用户：行政部manager00-manager19、开发部dev00-dev19、营销部sale00-sale19，所有用户只能每天8:00-18:00可以登录，不能修改其口令，密码永不过期。manager00拥有域管理员权限。

# 文件共享

**任务描述：**请采用文件共享，实现共享资源的安全访问。

**任务要求：**

1.在windows1的C分区划分2GB的空间，创建NTFS主分区，驱动器号为D。创建用户主目录共享文件夹：本地目录为D:\share\home，共享名为home，允许所有域用户完全控制。该文件夹将设置为所有域用户的home目录，skills域用户登录计算机成功后，自动映射挂载到T卷。禁止用户在该共享文件中创建“\*.exe”文件，文件组名和模板名为SKILLS。

2.创建目录D:\share\work，共享名为work，仅Administrator组和manager组有完全控制的安全权限和共享权限，其他认证用户有读取执行的安全权限和共享权限。在ADDS中发布该共享。

# 打印服务

**任务描述：请采用共享打印服务，实现共享打印的安全性。**

**任务要求：**

1.在 windows4 上安装打印机，驱动程序为“Ms Publisher Color Printer”，名称和共享名称均为“Printers”；在域中发布共享；使用组策略部署在"Default Domain Policy"的计算机。

2.网站名称为 printers，http 和 https 绑定主机 ip 地址，仅允许使用域名访问，启用 hsts，实现 http 访问自动跳转到 https（使用“计算机副本”证书模板）。

3.用浏览器访问打印机虚拟目录 printers 时，启用匿名身份认证，匿名用户为 manager00。

4.新建虚拟目录 dev，对应物理目录 C:\Development，该虚拟目录启用windows 身份验证，默认文档 index.html 内容为"Development"。

# ftp服务

**任务描述：**请采用ftp服务器，实现文件安全传输。

**任务要求：**

1.把windows3配置为ftp服务器，ftp站点名称为ftp，站点绑定本机ip地址，站点根目录为C:\ftp。

2.站点通过active directory隔离用户，用户目录为C:\ftp，用户目录名称与用户名相同，使用dev00和dev01测试。

# DHCP服务

**任务描述：**请采用DHCP服务器，实现ip地址及其他网络参数动态分配。

**任务要求：**

1.配置windows4和windows5为DHCP服务器，只绑定该主机的ipv4地址，DHCPipv4的作用域名称为SKILLS，地址范围为10.10.110.10-10.10.110.19，租约期3小时，网关为10.10.110.1，dns为10.10.110.101和10.10.110.102，dns域名为skills.com。

2.两台DHCP服务器实现故障转移，故障转移关系名称为skills，最长客户端提前期为2小时，模式为“负载平衡”，负载平衡比例各为50%，状态切换间隔1小时，启用消息验证，共享机密为Pass-1234。

# iscsi服务

**任务描述：**请采用iscsi，实现集中管理存储。

**任务要求：**

1.在windows3上添加4块硬盘，初始化为gpt磁盘，配置raid5，创建1个iscsi磁盘，存放在E:\iscsi，磁盘名称和目标名称分别为file，磁盘大小为动态扩展5GB，目标的iqn名称为iqn.2022-05.com.skills:server使用dns名称建立目标。发起程序的iqn名称为iqn.2022-05.com.skills:client。

2.windows4使用FQDN连接windows3的iscsi磁盘，初始化为GPT分区表，创建NTFS分区，驱动器号为E。

# 脚本

**任务描述：**请采用powershell脚本,实现快速批量的操作。

**任务要求：**

1.在windows5上编写C:\createfile.ps1的powershell脚本,创建20个文件C:\file\file00.txt至C:\file\file19.txt，如果文件存在，则删除后再创建；每个文件的内容同主文件名，如file00.txt文件的内容为“file00”。

Linux系统服务配置

# dns服务

**任务描述：**创建dns服务器，实现企业域名访问。

**任务要求：**

1.所有linux主机启用防火墙，防火墙区域为public，在防火墙中放行对应服务端口。

2.利用chrony，配置linux1为其他linux主机提供ntp服务。

3.所有linux主机root用户使用完全合格域名免密码ssh登录到其他linux主机。

4.利用bind和bind-utils，配置linux1为主dns服务器，linux2为备用dns服务器。为所有linux主机提供冗余dns正反向解析服务。

5.在linux1上安装ansible，作为ansible的控制节点。linux2-linux7作为ansible的受控节点。在linux1编写/root/skills.yaml剧本，实现在linux1创建文件/root/ansible.txt，并将该文件复制到所有受控节点的/root目录。

6.配置linux1为CA服务器,为linux主机颁发证书。证书颁发机构有效期10年，公用名为linux1.skills.com。申请并颁发一张供linux服务器使用的证书，证书信息：有效期=5年，公用名=skills.com，国家=CN，省=Beijing，城市=Beijing，组织=skills，组织单位=system，使用者可选名称=\*.skills.com和skills.com。将证书skills.crt和私钥skills.key复制到需要证书的linux服务器/etc/ssl目录。浏览器访问https网站时，不出现证书警告信息。

# tomcat 服务

**任务描述：**采用tomcat搭建动态网站。

**任务要求：**

1.配置linux2为nginx服务器，默认文档index.html的内容为“HelloNginx”；仅允许使用域名访问，http访问自动跳转到https。

2.利用nginx反向代理，实现linux3和linux4的tomcat负载均衡，通过https://tomcat.skills.com 加密访问 tomcat，http访问时永久自动跳转到https。

3.配置linux3和linux4为tomcat服务器，网站默认首页内容分别为“TomcatA”和“TomcatB”，仅使用域名访问http80端口和https443端口；证书路径均为/etc/ssl/skills.jks。

# ftp 服务

**任务描述：**请采用 ftp 服务器，实现文件安全传输。

**任务要求：**

1.配置 linux1 为 ftp 服务器，安装 vsftpd，新建本地用户 jack，本地用户登陆 ftp 后的目录为/var/ftp/pub，可以上传下载。

2.配置 ftp 虚拟用户认证模式，虚拟用户 ftp1 和 ftp2 映射为 ftp，ftp1 登录 ftp 后的目录为/var/ftp/vdir/ftp1，可以上传下载,禁止上传后缀名为.sh 的文件；ftp2 登录 ftp 后的目录为/var/ftp/vdir/ftp2，仅有下载权限。

# samba服务

**任务描述：**请采用samba服务，实现资源共享。

**任务要求：**

1.在linux3上创建user00-user19等20个用户；user00和user01添加到dev组，user02和user03添加到sale组。把用户user00-user03添加到samba用户。

2.配置linux3为samba服务器,建立共享目录/srv/sharesmb，共享名与目录名相同。dev组用户对sharesmb共享有读写权限，sale组对sharesmb共享有只读权限；用户对自己新建的文件有完全权限，对其他用户的文件只有读权限，且不能删除别人的文件。在本机用smbclient命令测试。

3.在linux4修改/etc/fstab,使用用户user00实现自动挂载linux3的sharesmb共享到/sharesmb。

# wordpress服务

**任务描述：**请采用wordpress服务，为企业建立博客。

**任务要求：**

1.安装apache2、mariadb-server、php和wordpress。

2.创建数据库wordpress，供wordpress服务使用。创建用户xiao，对wordpress数据库有完全权限。

3.创建数据库userdb；在数据库中创建数据表userinfo，在表中插入2条记录，分别为(1,user1，2005-8-1，男)，(2,user2，2005-8-2，女)，口令与用户名相同，password字段用password函数加密，表结构如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 数据类型 | 主键 | 自增 |
| id | int | 是 | 是 |
| name | varchar(10) | 否 | 否 |
| birthday | datetime | 否 | 否 |
| sex | char(8) | 否 | 否 |
| password | char(200) | 否 | 否 |

4.备份数据库userdb到/var/mariadbbak/userdb.sql（含创建数据库命令）；将表userinfo中的记录导出，并存放到/var/mariadbbak/userinfo.sql文件中。

5.网站默认文档/var/www/html/index.html的内容为"wordpress"。

6.利用wordpress搭建博客网站，站点标题为"skillsblog"。

# postgresql 服务

**任务描述：**请采用 postgresql 服务，实现数据存储。

**任务要求：**

1.配置 linux5 为 postgresql 服务器，创建数据库 userdb；在库中创建表 userinfo，在表中插入 2 条记录，分别为（1,user1，2005-6-1），（2,user2，2005- 6-2），口令与用户名相同，password 字段用 md5 函数加密，表结构如下：

|  |  |  |
| --- | --- | --- |
| 字段名 | 数据类型 | 主键 |
| id | serial | 是 |
| name | varchar (10) | 否 |
| birthday | date | 否 |
| password | varchar (100) | 否 |

2.设置可以直接在 shell 下操作数据库，然后备份数据库 userdb（含创建 数据库命令）到/var/postgresqlbak/userdb.sql；备份 userinfo 表记录到 /var/postgresqlbak/userinfo.sql.

# mail服务

**任务描述：**请采用postfix邮件服务器，实现安全的邮件服务。

**任务要求：**

1.配置linux5为mail服务器，安装postfix和dovecot。

2.仅支持smtps和pop3s连接。

3.创建用户mail1和mail2，向all@skills.com发送的邮件，每个用户都会收到。

4.安装mailx使用本机测试。

# redis服务

**任务描述：**请采用redis服务，实现高并发数据和海量数据的读写。

**任务要求：**

1.利用linux5搭建rediscluster集群，使用端口8001-8003模拟主节点，8004-8006模拟从节点，让其他主机可以访问redis集群。

# 脚本

**任务描述：**请采用脚本,实现快速批量的操作。

**任务要求：**

1.在linux5上编写/root/createfile.sh的shell脚本，创建20个文件/root /file00至/root/file19，如果文件存在，则删除后再创建；每个文件的内容同文件名，如file00文件的内容为“file00”