2022 年全国职业院校技能大赛
网络搭建与应用赛项
正式赛卷

第二部分 网络搭建及安全部署

竞赛总分　　450 分

竞赛时长　　3 小时

2022 年（中职组）网络搭建与应用赛项专家组

2022 年 8 月

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：

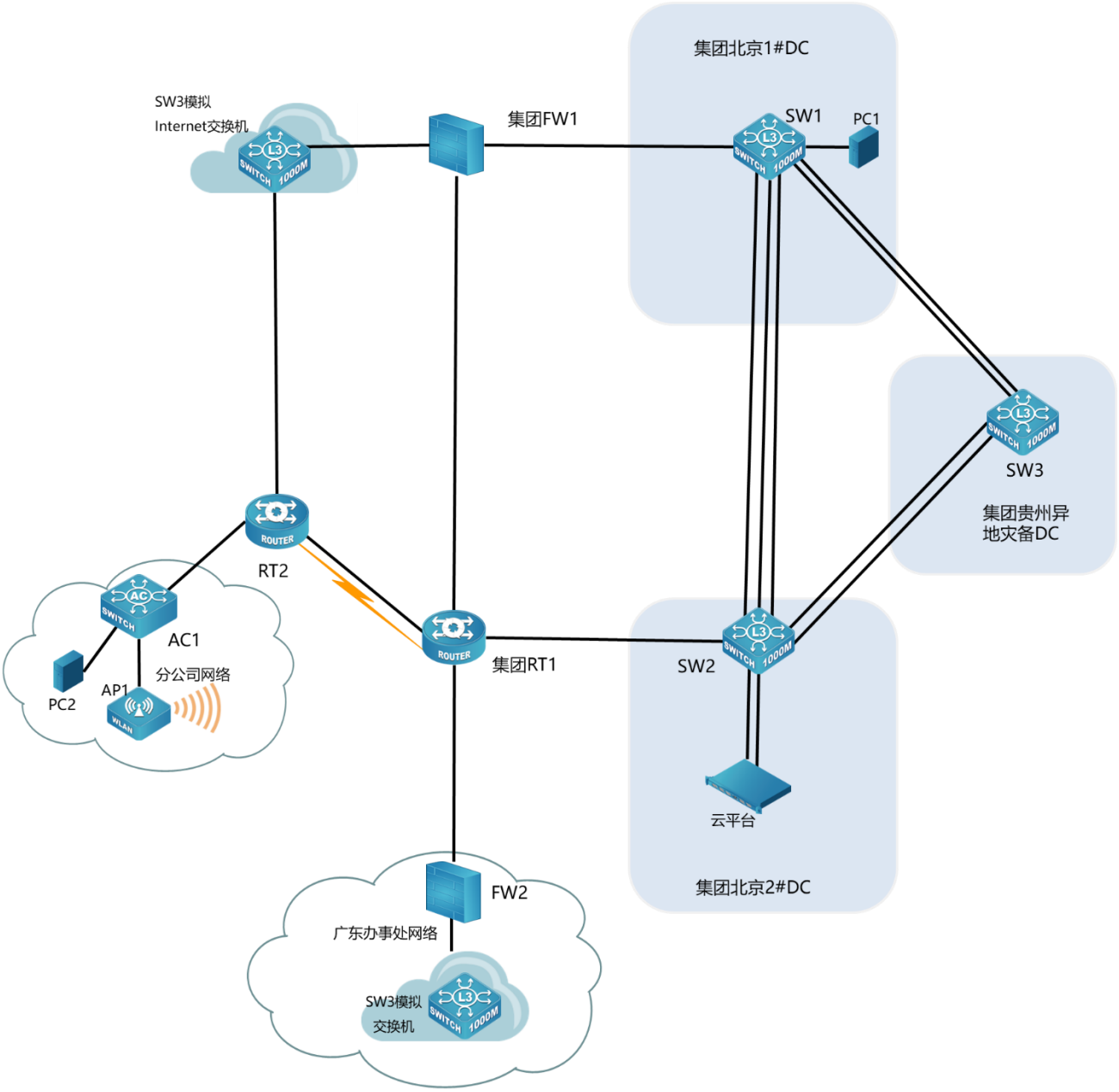
集团北京1#DC
SW3模拟
Internet交换机
集团FW1
SW1
PC1
SW3
集团贵州异
地灾备DC
RT2
AC1
PC2
AP1
分公司网络
集团RT1
SW2
云平台
集团北京2#DC
FW2
广东办事处网络
SW3模拟
交换机

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

一、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、网络连接

左侧布线面板立面示意图

右侧布线面板立面示意图

1.机柜左侧布线面板编号101；机柜右侧布线面板编号102。

2.面对信息底盒方向左侧为1端口、右侧为2端口。所有配线架、模块按照568B标准端接。

3.主配线区配线点与工作区配线点连线对应关系如下：

序号	信息点编号	配线架编号	底盒编号	信息点编号	配线架端口编号
1	W1-02-101-1	W1	101	1	02
2	W1-06-102-2	W1	102	2	06

4.铺设线缆并端接。截取2根适当长度的双绞线，两端制作标签，穿过PVC线槽或线管。双绞线在机柜内部进行合理布线，并且通过扎带合理固定。将2根双绞线的一端，端接在配线架相应端口，另一端端接上RJ45模块，并且安装在信息点面板，并标注标签。

5.跳线制作与测试。截取2根当长度的双绞线，端接水晶头，所有网络跳线要求按568B标准制作，两端制作标签，连接网络信息点和相应计算机。根据网络拓扑要求，截取适当长度和数量的双绞线，端接水晶头，插入相应设备的相关端口上，实现PC、信息点面板、配线架、设备之间的连通。

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。

6.开启 SW1 日志记录功能和保护功能,采样周期 5s 一次,恢复周期为 100s，从而保障 CPU 稳定运行。

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；

10.SW1 和 SW2 所有端口启用链路层发现协议,更新报文发送时间间隔为 20s，老化时间乘法器值为 5，Trap 报文发送间隔为 10s，配置三条裸光缆端口使能 Trap 功能。

四、路由配置

1.启用所有设备的 ssh 服务，防火墙用户名 admin，明文密码 Pass-1234，其余设备用户名和明文密码均为 admin。

2.配置所有设备的时区为 GMT+08:00，调整 SW1 时间为实际时间，SW1 配置为 ntp server，其他设备用 SW1 loopback1 ipv4 地址作为 ntp server 地址，ntp client 请求报文时间间隔 1 分钟。

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。

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。

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。

(3)RT2 与 AC1 之间运行 OSPFv3 协议，进程 1，stub no-summary 区域 1；AC1 发布 loopback1 地址路由、产品和营销。

(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。

9.RT2 配置 ipv4 nat，实现 AC1 ipv4 产品部门用 RT2 外网接口 ipv4 地址访问 Internet。RT2 配置 nat64，实现 AC1 ipv6 产品部门用 RT2 外网接口 ipv4 地址访问 Internet，ipv4 地址转 ipv6 地址前缀为 64:ff9b::/96。

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。

12.SW1、SW2、RT1、RT2、AC1 运行 PIM-SM，RT1 loopback1 为 c-bsr 和 c-rp，RT2 运行 IGMPv3；SW1 产品部门（PC1 测试）终端启用组播，用 VLC 工具串流播放视频文件“1.mp4”,模拟组播源,设置此视频循环播放,组地址 232.1.1.1，端口 1234，实现分公司产品部门（PC2 测试）收看视频。

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。

2.当 AP 上线，如果 AC 中储存的 Image 版本和 AP 的 Image 版本号不同时，会触发 AP 自动升级。AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时。

3.MAC 认证模式为黑名单，MAC 地址为 80-45-DD-77-CC-48 的无线终端采用全局配置 MAC 认证。

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。

7.FW2 配置 L2TP Over IPSec VPN，名称为 VPNL2TP，远程用户通过 dmz 区域接口拨入,本地认证账号 UserL2TP,密码 Pass-1234,地址池名称为 POOLL2TP，地址池范围为 10.19.0.100/24-10.19.0.199/24。保持 PC2 位置不变，用 PC2 测试。L2TPVPN 连接成功后，本地私有地址为 10.19.0.199。

8.FW1 配置邮件内容过滤，规则名称和类别名称均为“Denied”，过滤含有“pornographic”字样的邮件。

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。

10.FW1 利用 iQoS，实现集团产品 1 段访问 Internet https 服务时，上下行管道带宽为 1000Mbps,限制每 IP 上下行最小带宽 100Mbps、最大带宽 200Mbps、优先级为 5，管道名称为 SKILLS，模式为管制。

2022 年中职组网络搭建与应用赛项分值表

项目	分值（分）	小计（分）
职业素养	50	50
网络布线	50	50
Net-AC1	26.5	
Net-FW1	46.8	
Net-FW2	14.8	
Net-RT1	51.7	
Net-RT2	51.2	
Net-SW1	74.0	
Net-SW2	51.2	
Net-SW3	33.8	
Net 小计		350
合计		450