2023年全国职业院校技能大赛

网络搭建与应用赛项

公开赛卷

（二）

第一部分 网络搭建及安全部署

2023年（中职组）网络搭建与应用赛项专家组

2023年 3月 8日

竞赛说明

一、 竞赛内容分布

本赛卷共分七项，其中：

第一项：职业规范与素养 （50分）

第二项：网络布线与基础连接（50分）

————以下为（400分）————

第三项：交换配置与调试

第四项：路由配置与调试

第五项：无线网络配置

第六项：安全策略配置

第七项：业务选路与组播配置

二、 竞赛注意事项

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，需要及时保存配置命令。

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。

6. 比赛完成后，禁止将比赛所用的所有物品（包括赛卷）带离赛场。

7. 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。

8. 与比赛相关的软件和《网络搭建及安全部署竞赛结果提交指南》存放在物理机的 D:\soft 文件夹中。

9. 请在物理机 PC1 桌面上新建“XXX”文件夹作为“选手目录”，用以保存按照《网络搭建及安全部署竞赛结果提交指南》要求自动生成的全部结果文档。（XXX 为赛位号。举例：1 号赛位，文件夹名称为“001”）**重要提示：选手目录如缺少文档，相应分值计为 0 分。**

三、 竞赛说明

1. 请根据物理机“D:\soft\网络搭建及安全部署竞赛结果提交指南.docx”的要求生成文档，将生成的文档复制到选手目录。

2. 收集防火墙信息时，需要先调整 SecureCRT 软件字符编号为：UTF-8（提示：默认是 UTF-8），否则收集的命令行中文信息会显示乱码。

竞赛题目

- **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，又在广东设立了一个办事处。集团设有营销、产品、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 RIP、ISIS、OSPF 和 BGP 路由协议进行互联互通。

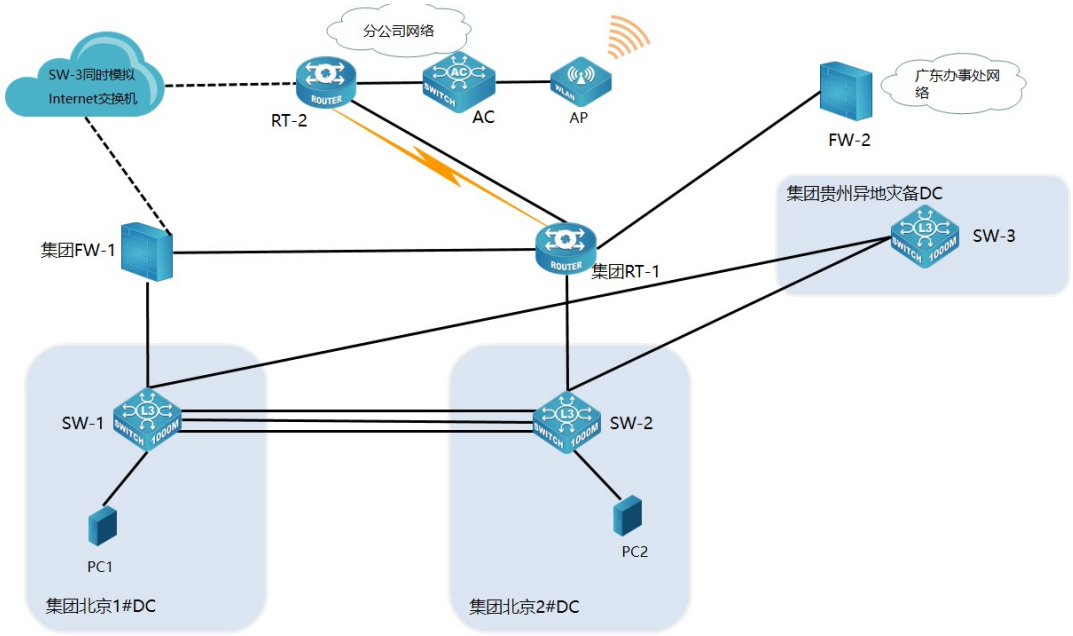
2023年在党的坚强领导下，全年公司规模保持快速增长，业务数据量和公司访问量增长巨大，不断开创新局面，向着全面建成社会主义现代化强国的第二个百年奋斗目标迈进。为了更好管理数据，提供服务，集团决定在北京建立两个数据中心，在贵州建立异地灾备数据中心，以达到快速、可靠交换数据，增强业务部署弹性的目的，完成向两地三中心整体战略架构演进，更好的服务于公司客户。

集团、成都分公司及广东办事处的网络结构详见拓扑图。编号为 SW-1 和 SW-2 分别作为集团北京两个 DC 的核心交换机；编号为 SW-3 作为灾备 DC 的核心交换机；两台防火墙编号 FW-1 和 FW-2 分别作为集团互联网出口、广东办事处的防火墙；编号为 RT-1 作为集团的核心路由器；编号为 RT-2 作为分公司的路由器；一台 AC 设备作为分公司的有线无线智能一体化控制器，通过与高性能企业级 AP 配合实现分公司无线覆盖。

请注意：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
RT-1	G0/0	RT-2	G0/0
RT-1	G0/1	FW-2	E0/1
RT-1	G0/2	FW-1	E0/1
RT-1	G0/3	SW-2	E0/23
RT-1	S1/0	RT-2	S1/1
RT-1	S1/1	RT-2	S1/0

A设备连接至B设备			
设备名称	接口	设备名称	接口
RT-2	G0/2	AC	E1/0/24
RT-2	G0/3	SW-3模拟Internet交换机	E1/0/18
FW-1	E0/2	SW-3模拟Internet交换机	E1/0/19
FW-1	E0/3	SW-1	E1/0/22
SW-1	E1/0/21	SW-3	E1/0/21
SW-1	E1/0/26(实现三层IP业务承载)	SW-2	E1/0/26（实现三层IP业务承载）
SW-1	E1/0/27(实现VPN业务承载)	SW-2	E1/0/27(实现VPN业务承载)
SW-1	E1/0/28(实现二层业务承载)	SW-2	E1/0/28(实现二层业务承载)
SW-2	E1/0/22	SW-3	E1/0/22
SW-1	E1/0/15	PC1	NIC

A设备连接至B设备			
设备名称	接口	设备名称	接口
SW-2	E1/0/15	PC2	NIC
AC	E1/0/10	AP	

- 表2-网络设备IP地址分配表

设备名称	设备接口	IP地址
RT-1	Loopback1 (ospfv2、ospfv3、bgp使用)	10.60.255.6/32 2001:10:60:255::6/128 (集团内使用)
	Loopback2	10.60.255.7/32 (集团与广东办事处互联使用)
	Loopback3	10.60.255.11/32 2001:10:60:254::11/128 (集团与分公司互联使用)
	Loopback10	10.60.64.2/32 (模拟集团财务业务使用)
	G0/0	10.60.254.18/30 2001:10:60:254::18/120
	G0/1	10.60.254.21/30 2001:10:60:254::6/127
	G0/2	10.60.254.25/30 2001:10:60:254::25/120
	S1/0	10.60.254.29/30 2001:10:60:254::8/127
	S1/1	10.60.254.33/30 2001:10:60:254::A/127
RT-2	Loopback3	10.60.255.12/32

设备名称	设备接口	IP 地址
		2001:10:60:254::12/128 (分公司与集团互联使用)
	Loopback10	10.60.64.2/32 (模拟分公司财务业务使用)
	G0/0	10.60.254.19/30 2001:10:60:254::19/120
	G0/1.100	172.16.100.254/24
	G0/1.200	172.16.200.254/24 2001:172:16:200::254/64
	G0/3	10.40.254.26/30 2001:10:40:254::26/120
	S1/1	10.60.254.30/30 2001:10:60:254::9/127
	S1/0	10.60.254.34/30 2001:10:60:254::B/127
SW-1	Loopback 1 (ospfv2、bgp 使用)	10.60.255.1/32
	Loopback 2 (ospfv3 使用)	10.60.255.2/32 2001:10:60:255::2/128
	VLAN10 SVI	10.60.11.254/24
	VLAN20 SVI	10.60.12.254/24 2001:10:60:12::254/64
	VLAN30 SVI	10.60.13.254/24 2001:10:60:13::254/64
	VLAN40 SVI	10.60.14.254/24
	VLAN50 SVI	10.60.15.254/24 2001:10:60:15::254/64
	VLAN1000 SVI	10.60.254.14/30
	VLAN1001 SVI	10.60.254.6/30 2001:10:60:254::3/127
	VLAN4093 SVI	10.60.254.1/30 (实现 VPN 业务承载)
	VLAN4094 SVI	10.60.254.1/30 2001:10:60:254::/127
SW-3	VLAN4000 SVI	202.60.100.1/30

设备名称	设备接口	IP 地址
	VLAN4001 SVI	202.60.100.5/30
SW-2	Loopback 1 (ospfv2、bgp 使用)	10.60.255.3/32
	Loopback 2 (ospfv3 使用)	10.60.255.4/32 2001:10:60:255::4/128
	VLAN10 SVI	10.60.21.254/24
	VLAN20 SVI	10.60.22.254/24 2001:10:60:22::254/64
	VLAN30 SVI	10.60.23.254/24 2001:10:60:23::254/64
	VLAN40 SVI	10.60.24.254/24
	VLAN50 SVI	10.60.25.254/24 2001:10:60:25::254/64
	VLAN1000 SVI	10.60.254.10/30 2001:10:60:254::5/127
	VLAN1001 SVI	10.60.254.22/30 2001:10:60:254::7/127
	VLAN4093 SVI	10.60.254.2/30 （实现 VPN 业务承载）
	VLAN4094 SVI	10.60.254.2/30 2001:10:60:254::1/127
SW-3	Loopback 1 (ospfv2、bgp 使用)	10.60.255.8/32
	Loopback 2 (ospfv3 使用)	10.60.255.9/32 2001:10:60:255::9/128
	VLAN10 SVI	10.60.31.254/24
	VLAN20 SVI	10.60.32.254/24 2001:10:60:32::254/64
	VLAN30 SVI	10.60.33.254/24 2001:10:60:33::254/64
	VLAN50 SVI	10.60.35.254/24 2001:10:60:35::254/64
	VLAN1000 SVI	10.60.254.5/30 2001:10:60:254::2/127
	VLAN1001 SVI	10.60.254.9/30 2001:10:60:254::4/127

设备名称	设备接口	IP 地址
SW-3 模拟 Internet 交换机	VLAN4000 SVI	202.60.100.2/30
	Loopback100	202.60.100.100/32 2001:202:50:100::100/128
FW-1	Loopback1	10.60.255.5/32 （trust 安全域）
	E0/1	10.60.254.13/30 （trust 安全域） 2001:10:60:254::13/120
	E0/2	10.60.254.17/30 （trust 安全域） 2001:10:60:254::17/120
	E0/3	202.60.100.6/30 （untrust 安全域）
FW-2	Loopback1	10.60.255.10/32 （trust 安全域）
	E0/1	10.60.254.26/30 （dmz 安全域）
	E0/2.10 （营销网段业务）	172.16.10.254/24 （trust 安全域）
	E0/2.20 （产品网段业务）	172.16.20.254/24 （trust 安全域）

一、 职业规范与素养（50 分）

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、 网络布线与基础连接（50 分）

右侧布线面板立面示意图

左侧布线面板立面示意图

【说明】

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表所示。

PC1、PC2 配线点连线对应关系表

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	W1-04-102-1	W1	102	1	04

(一) 铺设线缆并端接

1. 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。

2. 将 2 根双绞线的一端，根据“PC1、PC2 配线点连线对应关系表“的要求，端接在配线架的相应端口上。

3. 将 2 根双绞线的另一端，根据“PC1、PC2 配线点连线对应关系表”的要求，端接上 RJ45 模块，并且安装上信息点面板，并标注标签。

(二) 跳线制作与测试

1. 再截取 2 根当长度的双绞线，两端制作标签，根据“PC1、PC2 配线点连线对应关系表”的要求，链接网络信息点和相应计算机，端接水晶头，制作网络跳线，所有网络跳线要求按 568B 标准制作。

2. 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，制作网络跳线， 根据题目要求，插入相应设备的相关端口上;（包括设备与设备之间、设备与配线架之间）;

3. 实现 PC、信息点面板、配线架、设备之间的连通;（提示:可利用机柜上自带的设备进行通断测试）。

4. 按照“PC1、PC2 配线点连线对应关系表”连接机柜两侧底盒端口。

三、 交换配置与调试

(一) 为了减少广播，需要根据题目要求规划并配置 VLAN。要求配置合理,所有链路上不允许不必要 VLAN 的数据流通过，包含 VLAN1。核心交换机 SW-1 和核心交换机 SW-2 之间实现二层业务承载的裸光缆通道目前暂时只允许 VLAN10、VLAN20、VLAN30、VLAN40、VLAN50 通过，禁止配置 VLAN 及接口的描述信息。根据下述信息及表，在交换机上完成 VLAN 配置和端口分配。

设备	VLAN 编号	端口	说明（非 VLAN 描述信息）
SW-1	VLAN10	E1/0/1	营销 1 段
	VLAN20	E1/0/2	产品 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
SW-2	VLAN10	E1/0/1	营销 2 段
	VLAN20	E1/0/2	产品 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
SW-3	VLAN10	E1/0/1	营销 3 段
	VLAN20	E1/0/2	产品 3 段
	VLAN30	E1/0/3	法务 3 段
	VLAN50	E1/0/5	人力 3 段

(二) 核心交换机 SW-1 和核心交换机 SW-2 之间线路租用运营商三条裸光缆通道实现两个 DC 之间互通，一条裸光缆通道实现三层 IP 业务承载、一条裸光缆通道实现 VPN 业务承载、一条裸光缆通道实现二层业务承载。核心交换机 SW-1 与核心交换机 SW-3 之间、核心交换机 SW-2 与核心交换机 SW-3 之间租用运营商 OTN 波分链路实现互通。具体要求如下:

1. 为了节约集团成本，设计实现 VPN 业务承载的裸光缆通道带宽只有 10Mbps，后续再根据业务使用情况考虑是否扩容; 使用相关技术分别实现集团财务 1 段、财务 2 段业务路由表与集团其它业务网段路由表隔离，财务业务位于 VPN 实例名称 CW 内。

2. 配置实现三层 IP 业务承载的裸光缆通道最大传输单元为 1700Bytes，满足后续集团双 DC VXLAN、EVPN 等新技术应用。

3. 目前设计实现二层业务承载的只有一条裸光缆通道，随着集团 1#DC 服务器数量快速扩容，预计未来 2-3 年集团 1#DC 与 2#DC 间服务器大二层流量会呈现爆发式增长，配置相关技术，方便后续链路扩容与冗余备份，编号为 1。

4. 配置核心交换机 SW-1、SW-2、SW-3 采用源、目的 IP 进行实现流量负载分担。

5. 核心交换机 SW-3 针对每个业务 VLAN 的第一个接口配置 Loopback 命令，模拟接口 UP，方便后续业务验证与测试。

(三) 核心交换机 SW-1 和核心交换机 SW-2 针对营销业务网段的每个物理接口限制收、发数据占用的带宽分别为 100Mbps、90Mbps; 针对产品业务网段的每个物理接口限制所有报文最大收包速率为 100packets/s，如果超过了设置交换机端口的报文最大收包速率则关闭此端口，10 分钟后再恢复此端口，来保证交换机对其他业务的正常处理。

(四) 要求禁止配置访问控制列表，实现核心交换机 SW-3 法务业务对应的物理端口间二层流量无法互通; 针对 SW-3 人力业务配置相关特性，每个端口只允许的最大安全 MAC 地址数为 1，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; 配置相关特性实现报文上送设备 CPU 的前端整体上对攻击报文进行拦截，开启日志记录功能，采样周期 10s 一次，恢复周期为 2 分钟，从而保障 CPU 稳定运行。

(五) 核心交换机 SW-1、SW-2、SW-3 分别配置简单网络管理协议，计划启用 V3 版本，V3 版本在安全性方面做了极大的扩充。配置引擎号分别为 62001、62002、62003；创建认证用户为 2023，采用 3des 算法进行加密，密钥为：20232023，哈希算法为 SHA，密钥为：20232023；加入组，采用最高安全级别；配置组的读、写视图分别为：2023_R、2023_W；当设备有异常时，需要使用本地的环回地址 Loopback2 发送 Trap 消息至集团网管服务器 10.60.15.120、2001:10:60:15::120，采用最高安全级别；当人力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。

(六) 使用相关技术将核心交换机 SW-3 模拟为 Internet 交换机，实现与集团其它业务网段路由表隔离，Internet 路由表位于 VPN 实例名称 Internet 内。

(七) 配置相关功能，使核心交换机 SW-1、核心交换机 SW-2、核心交换机 SW-3 设备能够在网络中相互发现并交互各自的系统及配置信息，以供管理员查询两端接口对应关系及判断链路的通信状况；配置所有使能此功能的端口发送更新报文的时间间隔为 1 分钟、更新报文所携带的老化时间为 5 分钟，配置租用运营商三条裸光缆通道相关端口使能 Trap 功能，Trap 报文发送间隔为 1 分钟。

(八) 配置相关功能，使集团核心交换机 SW-1 和 SW-2 设备能够在网络中相互发现并交互各自的系统及配置信息，以供管理员查询两端接口对应关系及判断链路的通信状况。

(九) 防止终端产生 MAC 地址泛洪攻击，在 SW-1，SW-2 的所有业务端口设置开启端口安全功能，配置端口允许的最大安全 MAC 数量为 20，发生违规阻止后续违规流量通过，关闭端口，恢复时间为 3 分钟。

(十) 因集团营销人员较多、同时也为了节约成本，在集团接入交换机下挂两个 8 口 HUB 交换机实现营销部接入，已经为营销业务 VLAN 分配 IP 主机位为 1-14，在集团接入交换机使用相关特性实现只允许上述 IP 数据包进行转发，对 IP 不在上述范围内的用户发来的数据包，交换机不能转发，直接丢弃，要求禁止采用访问控制列表实现。

四、 路由配置与调试

(一) 规划集团内部、集团与广东办事处之间使用 OSPF 协议，集团内使用进程号为 1，集团与广东办事处间使用进程号为 2，具体要求如下:

1. 核心交换机 SW-1 与 FW-1 之间、核心路由器 RT-1 与 FW-1 之间、核心路由器 RT-1 与 SW-2 之间、SW-1 与 SW-2 之间、SW-1 与 SW-3、SW-2 与 SW-3 均属于骨干区域；RT-1 与 FW-2 之间属于普通区域，区域号为 20。

2. 调整 OSPF 进程号 1 所有接口发送 Hello 包的时间间隔为 5 秒，如果接口在 3 倍时间内都没有收到对方的 Hello 报文，则认为对端邻居失效。

3. RT-1、SW-1、SW-2、SW-3、FW-1、FW-2 分别发布自己的环回地址路由；SW-1、SW-2、SW-3 只允许发布营销网段业务路由；FW-2 分别发布自身营销、产品网段业务路由。

4. 核心交换机 SW-1、SW-2、SW-3 OSPF 进程 1 的路由表中业务网段路由只允许学习到 FW-1 通告的 TYPE1 类型的缺省路由、集团营销业务网段路由、FW-2 环回地址与营销业务网段路由；由于 FW-2 路由条目支持数量有限，禁止学习到集团、分公司的所有互联地址与业务路由。

(二) 规划核心交换机 SW-1 与 SW-2 之间、SW-1 与 SW-3 之间、SW-2 与 SW-3、SW-2 与 RT-1 之间使用 OSPFv3 协议，均属于骨干区域，发布相应环回地址，禁止发布业务路由；SW-1 与 SW-2 之间通过两端三层 IP 业务承载的裸光缆通道进行互联互通。

(三) 规划集团核心路由器 RT-1 与分公司路由器 RT-2 之间运行 ISIS 协议，实现两端环回地址 3 之间的互通。使用进程号为 10，设置路由器类型是 Level-2，接口网络类型为点到点链路，通过配置相关验证功能，验证密码为：Skills2023，验证密码将会按照设定的方式封装到 Level-2 报文中，并对收到的 Level-2 报文进行验证密码的检查，防止将不可信的路由信息注入当前路由域。

(四) 为了方便业务灵活调度，同时还规划集团北京两个 DC 与集团灾备 DC 之间、集团与分公司之间使用 BGP 协议，集团北京两个 DC 使用的 AS 号为 62021、集团灾备 DC 使用的 AS 号为 62023、分公司使用的 AS 号为 62023，具体要求如下：

1. 核心交换机 SW-1 与 SW-2 之间、SW-1 与 RT-1 之间、SW-2 与 RT-1 之间通过 OSPFv2 环回地址建立 IBGP 邻居，SW-1 与 SW-3 之间、SW-2 与 SW-3 之间、核心路由器 RT-1 与分公司路由器 RT-2 之间通过互联地址建立 EBGP 邻居。

2. 使用 BGP 协议实现集团 DC 之间 IPV6 业务、集团与分公司之间 IPV6 业务、北京 DC 之间财务业务互联互通，满足集团

DC之间、集团与分公司之间IPV6及北京DC之间财务业务发展的需要；其中要求SW-1、SW-2、SW-3之间实现DC间IPV6业务互联互通需使用环回地址建立BGP邻居；集团与分公司之间IPV6业务互联互通要求SW-1、SW-2与RT-1使用环回地址建立BGP邻居、核心路由器RT-1与分公司路由器RT-2采用互联地址建立BGP邻居。

3. 要求北京两个DC与贵州DC、分公司路由器RT-2禁止发布除产品、法务、财务、人力、无线业务网段外的其它路由; SW-1、SW-2、SW-3 BGP公网路由表中只允许学习到集团DC间产品&法务&人力业务网段、广东办事处产品业务网段路由、分公司无线业务业务网段路由。

4. 利用BGP相关功能特性，减少网络不稳定带来的过多的路由更新，抑制这些不稳定的路由信息，不允许这类路由参与路由选择。

(五) 为了合理分配集团内业务流向，保证来回路径一致，业务选路具体要求如下:

1. 实现核心交换机SW-1与分公司路由器RT-2、广东办事处IPV4互访流量优先通过SW-1_SW-2_RT-1之间链路转发，SW-1_FW-1_RT-1之间链路作为备用链路；实现核心交换机SW-2与分公司路由器RT-2、广东办事处IPV4互访流量优先通过SW-2_RT-1之间链路转发，SW-2_SW-1_FW-1_RT-1之间链路作为备用链路。

2. 实现核心交换机SW-1与Internet互访流量优先通过SW-1_FW-1之间链路转发，SW-1_SW-2_RT-1_FW-1之间链路作为备用链路；实现核心交换机SW-2与Internet互访流量优先通过

SW-2_SW-1_FW-1 之间链路转发，SW-2_RT-1_FW-1 之间链路作为备用链路。

3. 核心交换机 SW-3 与 SW-1、SW-2 IPv4 营销业务互访流量优先通过 SW-3_SW-2 之间链路转发，SW-3_SW-1 之间链路作为备用链路；实现 SW-3 与 SW-1、SW-2 DC 间 IPV6 业务互访流量优先通过 SW-3_SW-1 之间链路转发，SW-3_SW-2 之间链路作为备用链路。

(六) FW-1 集团 RT-1_RT-2 之间配置 RIPng，无线 IPv6 用户优先通过 RT-2 访问 INTERNET,RT-2 -FW1 为备份线路，如备份线路启用则优先使用专线传送数据;

(七) 北京 1#DC 和分公司之间用相关特性，实现无线的 IPv6 终端与产品业务的 IPv6 终端可以通过 RIPng 互访。

五、 无线网络配置

(一) 分公司无线控制器 AC 与 RT-2 互连，无线业务网关位于 RT-2 上，配置 VLAN100 为 AP 管理 VLAN，VLAN200，201 为业务 VLAN；AC 提供无线管理与业务的 DHCP 服务，动态分配 IP 地址和网关；分别使用第一个可用地址作为 AC 管理地址和无线业务管理地址; AP 二层自动注册，AP 采用 MAC 地址认证。

(二) 配置一个 SSID 2023，访问 Internet 业务，采用 WPA-PSK 认证方式，加密方式为 WPA 个人版，配置密钥为 20232023

(三) 配置所有无线接入用户相互隔离，Network 模式下限制 SSID 2023每天早上 0 点到 4 点禁止终端接入，开启 SSID 2023 ARP 抑制功能；配置当无线终端支持 5GHz 网络时，优先引导接入 5GHz 网络，从而获得更大的吞吐量，提高无线体验。

(四) 配置一个 SSID XXX_IPv6，属于 VLAN201，访问 Internet 业务，用户接入无线网络时需要采用基于 WPA-personal 加密方式，其口令为“12345678”，该网络中的用户从 RT-2 DHCP 获取 IPv6 地址，地址范围为：2001:172.40.201::254/64。

(五) 配置 2 个 SSID，分别为“skills-2.4”和“skills-5.0”。“skills-2.4”对应业务 Vlan 200，使用 network 200,用户接入无线网络时需要采用基于 WPA-personal 加密方式，其口令为“123456”；“skills-5.0”对应业务 Vlan201，使用 network 201，不需要认证，隐藏 SSID，“skills-5.0” 的 SSID 只使用倒数第一个可用 VAP 发送 5.0G 信号。

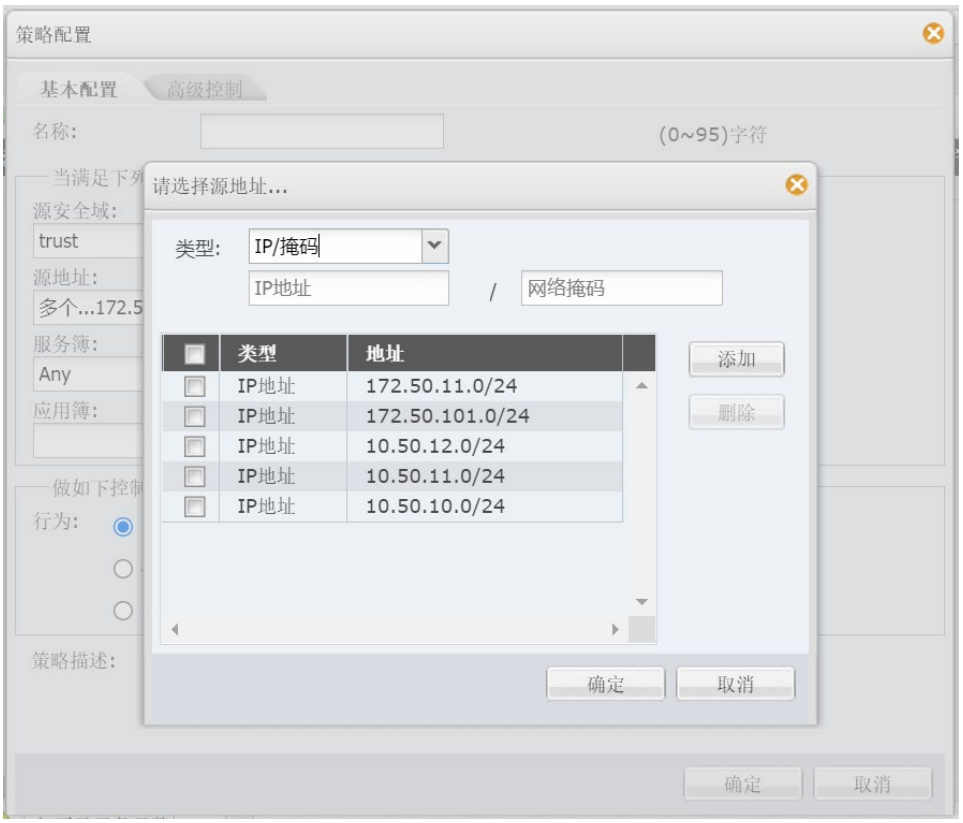
(六) 配置所有 Radio 接口：AP 在收到错误帧时，将不再发送 ACK 帧；打开 AP 组播广播突发限制功能；开启 Radio 的自动信道调整，每天上午 10:00 触发信道调整功能。

(七) 保障无线信息的覆盖性，无线 AP 的发射功率设置为 90%。禁止 MAC 地址为 80-45-DD-77-CC-48 的无线终端连接。针对 skills-5.0 开启内置 portal+本地认证的认证方式，账号为密码为 12345678，组编号为 1。

六、 安全策略配置

说明：为了统一结果，要求源地址和目的地址均使用“IP/掩码”

表示，禁止使用地址薄或地址条目表示，否则按零分处理。举例截图如下：



(一) 根据题目要求配置 FW-1、FW-2 相应的业务安全域、业务接口；2023年护网行动开展在即，调整全网防火墙安全策略缺省规则为拒绝;限制 FW-1 只允许集团营销业务、分公司无线 IPV4 业务、广东办事处营销业务访问 Internet 业务；在 FW-2 上限制广东办事处产品业务网段只可以访问集团产品网段 https、mysql 数据库类型业务，集团营销网段可以访问广东办事处营销业务网段任何端口。

(二) 为了避免集团内部业务直接映射至 Internet 成为攻击“靶心”，不断提升集团网络安全体系建设，在 FW-1 配置 L2TP VPN，名称为 VPN，满足远程办公用户通过拨号登陆访问集团营销业务，创建隧道接口为 tunnel 1、并加入 untrust 安全域，地址池名称为 AddressPool，LNS 地址池为 10.60.253.1/24-10.60.253.100/24，网关为最大可用地址，认证账号 2023001,密码 2023。

(三) 在 FW-1 配置网络地址转换，NAT 地址转换条件中源、目的 IP 均为 any，公网 NAT 地址池为：202.60.21.0/28；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 10.60.11.120 的 UDP 514 端口；开启相关特性，实现扩展 NAT 转换后的网络地址端口资源。

(四) 在 FW-2 开启安全网关的 TCP SYN 包检查功能，只有检查收到的包为 TCP SYN 包后，才建立连接；配置所有的 TCP 数据包每次能够传输的最大数据分段为 1460,尽力减少网络分片；配置对 TCP 三次握手建立的时间进行检查，如果在 1 分钟内未完成三次握手，则断掉该连接。

(五) FW-1 的出口带宽为 800Mbps，为集团内研发、营销、行政、财务 4 个业务网段更加合理使用出口资源，要求出口口带宽小于 480Mbps 时，每 IP 上下行最大 5Mbps 带宽；出口带宽大于 720Mbps 时，每 IP 上下行最大 2Mbps 带宽，规则名称为 JT。同时要求在流量变化期间带宽增长速率为 2 倍，在任何时候都要确保网页访问服务占每 IP 带宽的 40%。

(六) 为防止集团内部收到垃圾邮件，请在防火墙上配置邮箱过滤，规则名称和类别名称均为“商业中心”，过滤含有“商业中心”字样的邮件。

(七) 正常情况下集团 FW1 与分公司 RT-2 使用 BGP 连接，当连接断开时，集团 FW1 与分公司 RT-2 使用公网 VPN 作为备份链路，VPN 要求如下：集团 FW1 与分公司 RT-2 使用与 Internet 的接口互联地址建立 GRE 隧道，再使用 IPSEC 技术对 GRE 隧道进行保护，使用 IKE 协商 IPSec 安全联盟、交换 IPSec 密钥，两端加密访问列表名称都为 ipsecacl，这样有了 IPSec，集团与分公司在通过运营商网络传输时，就不用担心被监视、篡改和伪造。

(八) 为确保北京与广东之间业务数据的安全可靠性，两地防火墙之间使用Internet之间建立GRE隧道，使用IPSec技术对GRE隧道进行保护，使用IKE协商自行设置IPSec安全联盟、交换IPSec密钥。

七、业务选路与组播配置

(一) 考虑到从北京两个DC与贵州DC之间共有两条链路，贵州DC产品业务网段与北京两个DC产品业务网段IPV4协议栈互访优先在SW-3与SW-1之间链路转发；贵州DC法务&人力网段与北京两个DC法务&人力网段IPV4协议栈互访优先在SW-3与SW-2之间链路转发，主备链路相互备份。根据以上需求，在交换机上进行合理的业务选路配置。具体要求如下:

1. 使用IP前缀列表匹配上述业务数据流。

2. 使用BGP自治系统路径属性进行业务选路，允许新增的变量为AS 62000，只允许使用route-map来改变路径属性、路由控制。

(二) 计划在集团北京与分公司之间上线视频会议系统，实现多业务部门横向沟通、交流，提升工作效率，初步先在产品部启用组播协议进行测试，具体要求如下:

1. 在集团北京SW-1，SW-2，集团RT-1，分公司RT-2路由器运行协议独立组播－稀疏模式协议，集团RT-1路由器为RD，因特网组管理协议第二版本;

2. SW-1产品部门内部终端启用组播，此终端IP地址为:10.60.11.234/24，使用VLC工具串流播放视频文件“大赛宣传片.mp4”，模拟组播源，设置此视频循环播放，组地址228.50.50.50，

端口：2022，实现分公司无线业务部门内部终端可以通过组播查看视频播放。

2023年全国职业院校技能大赛

网络搭建与应用赛项

公开赛卷（二）

第二部分 服务器配置及应用

2023年（中职组）网络搭建与应用赛项专家组

2023年 3月 8日

竞赛说明

竞赛内容分布

本赛卷共分三项，其中:

第一项：云平台网络连接 （100 分）

第二项：Linux 服务配置 （200 分）

第三项：Windows 服务配置（200 分）

一、竞赛注意事项

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，需要及时保存配置命令。

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。

6.比赛完成后，禁止将比赛所用的所有物品（包括赛卷）带离赛场。

7.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。

8.与比赛相关的软件和《服务器配置及应用竞赛结果提交指南》存放在物理机的 D:\soft 文件夹中。

9.请在物理机 PC1 桌面上新建“XXX”文件夹作为“选手目录”，用以保存按照《服务器配置及应用竞赛结果提交指南》要求自动生成的全部结果文档。（XXX 为赛位号。举例：1 号赛位，文件夹名称为

“001”）重要提示：选手目录如缺少文档，相应分值计为 0 分。

二、赛项说明

1.请根据物理机“D:\soft\服务器配置及应用竞赛结果提交指南.docx”的要求生成文档，将生成的文档复制到“选手目录”。

2.虚拟主机的 IP 地址必须手动设置为该虚拟机自动获取的 IP 地址（提示：先新建固定 IP 地址的端口，为了测试的需要，关闭端口安全；然后创建实例并指定端口）。

3.所有 windows 虚拟机都启用了远程桌面连接，所有 linux 虚拟机都启用了 ssh。

4.修改 windows 虚拟机管理员 Administrator 的密码为 Pass-1234，windows 题目中所有未指明的密码均为管理员 Administrator 的密码；修改 linux 虚拟机管理员 root 的密码为 Pass-1234，linux 题目中所有未指明的密码均为管理员 root 的密码。提示：因密码设置错误导致无法评判计为 0 分。

5.所有服务器要求虚拟机系统重新启动后，均能正常启动和使用。

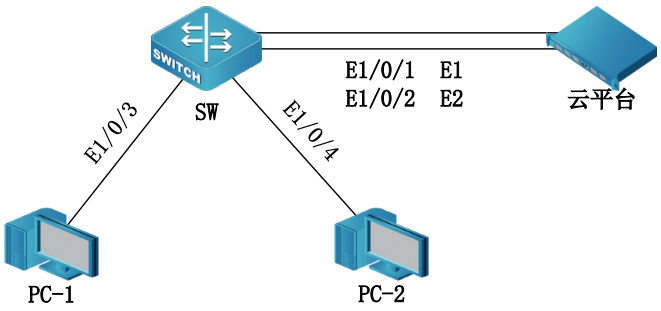
6.使用完全合格域名访问网络资源。

竞赛题目

一、云平台网络连接

【任务描述】 请按照下述拓扑结构和信息表，使用六类非屏蔽双绞线连接网络并设置云平台，保证系统服务正常运行。

1.拓扑结构



2.网络信息表

网络名称	VlanID	子网名称	网络地址	网关	IPv4 地址池
Network10	10	Subnet10	10.10.10.0/24	10.10.10.254	10.10.10.100-10.10.10.200
Network20	20	Subnet20	10.10.20.0/24	10.10.20.254	10.10.20.100-10.10.20.200

3.实例类型信息表

名称	ID	VCPU	内存(MB)	磁盘(GB)	实例名称	镜像模板
Large	1	4	4096	40	windows1 至 windows7	win2022
Small	2	1	2048	40	linux1 至 linux7	rocky9

4.实例信息表

实例名称	IPv4 地址	完全合格域名
windows1	10.10.10.101	windows1.skills.com
windows2	10.10.10.102	windows2.skills.com

实例名称	IPv4 地址	完全合格域名
windows3	10.10.10.103	windows3.skills.com
windows4	10.10.10.104	windows4.skills.com
windows5	10.10.10.105	windows5.skills.com
windows6	10.10.10.106	windows6.cnskills.com
windows7	10.10.10.107	windows7.bj.cnskills.com
linux1	10.10.20.101	linux1.skills.com
linux2	10.10.20.102	linux2.skills.com
linux3	10.10.20.103	linux3.skills.com
linux4	10.10.20.104	linux4.skills.com
linux5	10.10.20.105	linux5.skills.com
linux6	10.10.20.106	linux6.skills.com
linux7	10.10.20.107	linux7.skills.com

二、windows 服务配置

(一) 域服务

【任务描述】 为实现高效管理，请采用域控制器，提升企业网络安全程度，整合局域网内基于网络的资源。

1.配置 windows2 为 skills.com 域服务和 DNS 服务，DNS 正反向区域在 Active Directory 中存储，为 skills.com 域中主机提供正反向解析。

2.把 skills.com 域服务迁移到 windows1；安装 DNS 服务，DNS 正反向区域在 Active Directory 中存储，为 skills.com 域中主机提供正向解析，为 skills.com 林中主机提供反向解析。

3.将 windows6 升级为 skills.com 林中的 cnskills.com 域控制器，安装 DNS，负责该域的正反向域名解析。升级域控制器后，用 skills\administrator 身份登陆。

4.将 windows7 升级为 bj.cnskills.com 域控制器，安装 DNS，负责该域的正反向域名解析。升级域控制器后，用 skills\administrator 身份登陆。

5.把云平台其他 windows 主机加入到 skills.com 域。

6.在 windows1 上安装证书服务，证书颁发机构有效期为 20 年，颁发证书有效期 10 年，证书信息：公用名=skills.com，国家=CN，省=Beijing，城市=Beijing，组织=Skills，组织单位=System。chrome 浏览器访问 https 网站时，不出现证书警告提示信息。

7.在 windows2 上安装从属证书服务。

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 manager101-manager120、开发部 dev101-dev120、营销部 sale101-sale120，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。

(二) 组策略

【任务描述】 为了帮助系统管理员对计算机或是特定用户来进行不同配置，请采用组策略，实现软件、计算机和用户的策略设置。

1.部署软件 powershell7.2.msi，让域中主机自动安装 powershell

（从物理机复制 powershell7.2.msi 到 windows1 的 C:\soft）。

2.域中主机（含域控制器）自动申请“计算机”模板证书，自动注册“工作站身份验证”模板证书，该模板可用作“服务器身份验证”。windows3 和 windows4 之间通信采用 IPSec 安全连接，采用计算机证书验证。

3.拒绝 dev 组从网络访问域控制器，允许 manager 组本地登录域控制器。

4.登录计算机时，在桌面新建名称为 chinaskills 的快捷方式，目标为 https://www.chinaskills-jsw.org，快捷键为 Ctrl+Shift+F6

5.为正在登录此计算机的所有用户设置漫游配置文件路径为 windows1 的 C:\share，每个用户提供单独的配置文件文件夹。

6.用户的主文件夹为 windows1 的 C:\home,驱动器号为 X。

7.每个用户的“文档”文件夹重定向到 windows1 的 C:\Document，为每一用户创建一个文件夹。

8.所有域用户使用漫游用户配置文件，配置文件存储在 windows1 的 C:\Profiles 文件夹，为每个用户提供单独的配置文件文件夹。

9.新建 C:\DocShare 共享文件夹，共享名称为 ShareDoc，管理员组有完全访问权限，其他用户有只读权限；在 AD DS 中发布该共享。

10.允许 manager1 用户远程登录到域控制器，manager1 登录系统时，对 windows1 的 C:\DocShare 共享文件夹映射驱动器 Z。

（三）DHCP 服务

【任务描述】 为了提高 IP 地址的使用率，减少 IT 技术人员的工作量，请采用 DHCP 服务器，实现 IP 地址及其他网络参数的动态分配。

1.配置 windows4 和 windows5 为 DHCP 服务器，DHCP IPv4 的

作用域名称为 skills，地址范围为 10.10.10.10-10.10.10.19，租约期 3 小时，网关为 10.10.10.254，DNS 为 10.10.10.101 和 10.10.10.102，DNS 域名为 skills.com。

2.在 windows4 上安装 WDS，部署安装 Windows Server 2022 Datacenter Core。

3.两台 DHCP 服务器实现故障转移，故障转移关系名称为 dhcp，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 60 分钟，启用消息验证，共享机密为 Pass-1234。

(四)文件共享

【任务描述】为了使局域网中的特定用户，能够访问共享文件夹内的特定资源，请采用文件共享，实现共享资源的安全访问。

1.在 windows1 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，允许所有域用户可读可写。在本目录下为所有用户添加一个以名称命名的文件夹，该文件夹将设置为所有域用户的 home 目录，用户登录计算机成功后，自动映射挂载到 H 卷。禁止用户在该共享文件中创建“*.exe, *.bat, *.sh”文件，文件组名和模板名为 my。

2.创建 manager 组共享文件夹：本地目录为 D:\share\manager，共享名为 manager，仅允许 manager 用户组成员拥有完全权限，该共享对其他组成员不可见。

3.创建 public 公共共享文件夹：本地目录为 D:\share\public，共享名为 public，仅允许 manager 用户组成员拥有更改权限，其他认证用户只读权限。

（五）DFS 服务

【任务描述】 为建立一个高效率的存储架构，请采用 DFS，实现集中管理共享文件。

1.在 windows3 至 windows5 的 C 分区划分 2GB 的空间，创建 NTFS 分区，驱动器号为 D。

2.配置 windows3 为 DFS 服务器，命名空间为 DFSROOT，文件夹为 Pictures；实现 windows4 的 D:\Pics 和 windows5 的 D:\Images 同步。

3.配置 windows3 的 DFS IPv4 使用 34567 端口；限制所有服务的 IPv4 动态 RPC 端口从 8000 开始，共 1000 个端口号。

（六）Web 服务

【任务描述】 为客户获取公司产品信息和企业宣传的需要，创建安全动态网站，请采用 IIS 搭建 Web 服务。

1.把 windows3 配置为 ASP 网站，网站仅支持 dotnet CLR v4.0，站点名称为 asp。

2.http 和 https 绑定本机外部网络 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。

3.网站目录为 C:\IIS\Contents，主页文档 index.aspx 的内容为 "HelloAspx"。

4.启用 windows 身份验证，只有通过身份验证的用户才能访问到该站点。

5.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，只有通过身份验证的用户才能访问。

6.客户端访问时，必需有 SSL 证书，证书模板为“管理员”，使

用 windows5 测试。

(七)打印服务

【任务描述】为了提高打印服务效率，节省成本，请采用共享打印服务，实现共享打印的安全性。

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“SkillsPrinter”；在域中发布共享；使用组策略部署在"Default Domain Policy"的计算机。

2.通过浏览器访问打印机时，启用匿名身份认证，匿名用户为 dev1。

3.客户端访问时，必需有 SSL 证书，证书模板为 “管理员”，使用 windows5 测试。

(八)BitLocker

【任务描述】为了更好地保护计算机中的数据，请采用 BitLocker，加密 Windows 操作系统卷上存储的数据。

1.将 windows4 的 D 盘启用 BitLocker，使用密码解锁驱动器，仅加密已用磁盘空间，使用 XTS-AES 加密模式，启用自动解锁。

(九)脚本

【任务描述】 为了减少重复性任务的工作量，节省人力和时间，请采用脚本,实现快速批量的操作。

1.在 windows5 上编写 C:\CreateDir.ps1 的 powershell 脚本,创建 20 个文件夹 C:\test\dir00 至 C:\test\dir19，如果文件夹存在，则首先删除后，再创建。

三、Linux 服务

（一）DNS 服务

【任务描述】 创建 DNS 服务器，实现企业域名访问。

1.设置所有 linux 服务器的时区设为 “上海”，本地时间调整为实际时间。在防火墙中开启相应服务端口，设置服务开机自启动。

2.利用 chrony 配置 linux1 为其他 linux 主机提供 NTP 服务。

3.利用 bind9 软件，配置 linux1 为主 DNS 服务器，采用 rndc 技术提供不间断的 DNS 服务；配置 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。

4.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。

5.配置 linux1 为 CA 服务器,为所有 linux 主机颁发证书，不允许修改/etc/pki/tls/openssl.conf。CA 证书有效期 20 年，CA 颁发证书有效期均为 10 年,证书信息: 国家=“CN”, 省=“Beijing”, 城市=“Beijing”, 组织=“Skills”，组织单位=“System”，公用名=skills.com。证书路径均为/etc/ssl/skills.crt，私钥路径均为/etc/ssl/skills.key，chrome 浏览器访问 https 网站时，不出现证书警告提示信息。

（二）apache2 服务

【任务描述】为了搭建快速、可靠的网页服务器，请采用 Apache 服务器，实现对企业网站的安全有效访问。

1.配置 linux2 为 apache2 服务器，安装 apache2，http 访问时自动跳转到 https。

2.使用 skills.com 或 any.skills.com（any 代表任意网址前缀，用

linux2.skills.com 和 web.skills.com 测试）访问时，自动跳转到 www.skills.com。

3.客户端访问时，必需有 SSL 证书。

4.关闭不安全的服务器信息，在任何页面不会出现系统和 WEB 服务器版本信息。

（三）tomcat 服务

【任务描述】根据企业需要搭建动态网站，采用 tomcat 实现该需求。

1.配置 linux3 和 linux4 为 Tomcat 服务器，网站默认首页内容分别为“TomcatOne”和“TomcatTwo”，使用 80 端口访问 http 和 443 端口访问 https；证书路径均为/etc/ssl/skills.jks，证书密码 Pass-1234，格式为 jks。

2.配置 linux1 为 nginx 服务器，安装 nginx，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，证书路径为/etc/ssl/skills.crt，私钥路径为/etc/ssl/skills.key。

3.利用 nginx 反向代理，客户端通过 https://tomcat.skills.com 加密访问 Tomcat，实现 linux3 和 linux4 的两个 Tomcat 负载均衡，http 访问通过 301 自动跳转到 https。

（四）NFS 服务

【任务描述】 为了使局域网中的特定用户，能够访问共享文件夹内的特定资源，请采用文件共享，实现共享资源的安全访问。

1.配置 linux2 为 KDC 服务器，负责 linux3 和 linux4 的验证。

2.在 linux3 上，创建用户，用户名为 tom，uid=222，gid=222，家目录为/home/tomdir。

3.配置 linux3 为 NFS 服务器，目录/srv/share 的共享要求为：10.10.20.0/24 网络用户具有读写权限，所有用户映射为 tom；kdc 加密方式为 krb5p。目录/srv/tmp 的共享要求为：所有人都可以读写，都（含 root 用户）不改变身份；kdc 加密方式为 krb5p。

4.配置 linux4 为 NFS 客户端，新建/opt/share 和/opt/tmp 目录，分别挂载 linux3 上的/srv/share 和/srv/tmp。

（五）NIS 服务

【任务描述】为降低重复设定用户帐号密码的步骤，便于账号管理，请采用 NIS 服务器，集中管理网域中所有主机的帐号密码。

1.配置 linux5 为 NIS 服务器；新建 user1 和 user2 用户，用户目录分别为/home/user1 和/home/user2。采用 samba 方式共享 user1 和 user2 的 home 目录，用户测试。

2.配置 linux6 为 NIS 客户端，按需自动挂载 linux3 上的 user1 和 user2 用户目录到/home。

（六）Redis 服务

【任务描述】为了解决应用服务器的 CPU 和内存压力，减轻 I/O 的压力，请采用 Redis 服务，实现高并发数据和海量数据的读写。

1.利用 linux3 搭建 redis cluster 集群，使用端口 7001-7003 模拟主节点，7004-7006 模拟从节点。

（七）postgresql 服务

【任务描述】为按数据结构来存储和管理数据，请采用 PostgreSQL 服务，实现方便、严密、有效的数据组织、数据维护、数据控制和数据

运用。

1.配置 linux3 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,user1，1995-7-1），（2,user2，1995-9-1），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（50）	否

2.设置可以直接在 shell 下操作数据库，然后备份数据库 userdb 到/var/local/postgresqlbak/userdb.sql。

（八）PXE 服务

【任务描述】由于企业新购一批服务器，需要安装 linux 操作系统，请采用 PXE 服务实现需求。

1.配置 linux4 为 PXE 服务器，实现完全自动安装 Linux。

2.安装 DHCP 服务，地址范围为 10.10.20.10-10.10.20.19，网关为 10.10.20.254，DNS 为 10.10.20.101，域名为 skills.com。

3.安装 tftpd，为 PXE 客户端提供启动服务，TFTP 目录为默认值。

4.安装 apache2 服务，为 PXE 客户端提供软件包；挂载 linux 光盘文件到/var/www/html/cdrom。

（九）WordPress 服务

【任务描述】为了推广产品，提升品牌形象，合理利用资源，降低成本，请采用 WordPress 服务，为企业建立博客。

1.在 linux5 上安装图形界面，并设置默认启动模式为图形界面。安装 xrdp，物理机可以使用远程桌面连接该主机。

2.配置 C 语言和 C++语言的编译环境。

3.安装 nginx、mariadb、php、phpMyAdmin 和 wordpress，创建数据库 wordpress，数据库字符集为 utf8-unicode-ci；创建用户 test，对所有数据库有完全权限。

4.利用 linux5 上浏览器搭建 wordpress 博客，站点标题为 “This is my blog!”。

（十）Ansible 服务

【任务描述】为了提高了工作效率,由程序自动的、重复的执行任务，请采用 Ansible 服务，实现自动化运维。

1.在 linux1 上安装 ansible，作为 ansible 的控制节点。linux2-linux7 作为 ansible 的受控节点。

2.编写/root/my.yml 剧本，实现在 linux1 的/root 目录创建一个 ansible.txt 文件，然后复制到所有受控节点的/root 目录。

（十一）Kubernetes 服务

【任务描述】为了对容器进行更高级更灵活的管理，请采用 Kubernetes 服务，管理和控制容器。

1.在 linux5 上安装 kubernetes，linux6-linux7 作为 kubernetes 的节点，搭建一主二从的单集群。

2.使用 containerd 管理容器。

(十二) FTP 服务

【任务描述】为了提高文件的共享性，对用户进行透明和可靠高效地数据传送，请采用 FTP 服务器，实现文件安全传输。

1.配置 linux4 为 FTP 服务器，安装 vsftpd。

2.配置虚拟用户认证模式。虚拟用户 ftp1 和 ftp2 映射为 ftpuser（该账户不能登录系统，家目录为/home/ftpuser），ftp1 有完全权限,禁止上传后缀名为.docx 和.xlsx 的文件，上传文件所有者为 ftpuser; ftp2 仅有下载权限。ftp1 登录 ftp 后的目录为/home/ftpuser/ftp1，ftp2 登录 ftp 后的目录为/home/ftpuser/ftp2。

(十三) samba 服务

【任务描述】 为在 Linux 和 Windows 之间实现共享文件和打印机的安全访问，请采用 samba 服务器，实现 Windows 操作系统和 Linux 操作系统的资源共享兼容。

1.在 linux4 上创建 user101-user120 等 20 个用户；user101 和 user102 添加到 manager 组，user103 添加到 sale 组，user104 添加到 dev 组。

2.配置为 Samba 服务器,建立共享目录/share/ShareManager, /share/ShareSale, /share/SharePublic，共享名与目录名相同。

3.manager 组用户对 ShareManager 和 SharePublic 有共享读写权限，sale 组用户对 ShareSale 和 SharePublic 有共享读写权限，dev 组对所有共享均有读写权限；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。

4.把用户 user101-user104 添加到 samba 用户。

(十四)脚本

【任务描述】为了减少重复性任务的工作量，节省人力和时间，请采用脚本,实现快速批量的操作。

1.在 linux7 上编写/root/CreateFile.py 的 python3 脚本，创建 20 个文件/root/test/File01 至/root/test/File20，如果文件存在，则先删除再创建；每个文件的内容同文件名，如 File01 文件的内容为 “File01”。