2023 年全国职业院校技能大赛
网络建设与运维赛项

赛题

2023 年 7 月 26 日

赛题说明

一、竞赛项目简介

“网络建设与运维”竞赛共分为模块一：网络理论测试；模块二：网络建设与调试；模块三：服务搭建与运维等三个模块。竞赛安排和分值权重见表 1。

表 1 竞赛时间安排与分值权重

模块		比赛时长	分值	答题方式
模块一	网络理论测试	0.5 小时	10%	在线测试
模块二	网络建设与调试	6.5 小时	40%	设备实操
模块三	服务搭建与运维		50%	设备实操
合计		7 小时	100%	

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按照答题要求保存相关结果。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。

5. 竞赛完成后，竞赛设备、软件和赛题请保留在座位上，禁止将

竞赛所用的所有物品（包括试卷等）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，禁止在提交资料上填写与竞赛无关的标记，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<U 盘>/soft 文件夹中。

8. 请在贴有“pc1-赛位号”U 盘（赛位号从 001-101 变化）根目录新建“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 U 盘中“答案提交指南.txt”要求生成答案文档，将答案文档复制到选手目录。

9. server1 管理 web 网址 http://192.168.100.100/dashboard，管理员为 admin，密码为 admin。server1 底层操作系统 root 用户密码为 Key-1122。Windows 虚拟机中 Administrator 用户密码为 Key-1122，题目中所有未指定的密码均用该密码。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。

10. server2 管理 web 网址 http://192.168.2.10，管理员为 Admin，密码为 Admin@123。

11. 使用完全合格域名访问网络资源。

模块二：网络建设与调试

（共计 40 分）

任务背景描述:

某集团公司原在城市 A 建立了总公司,后在城市 B 建立了分公司，又在城市 C 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。

随着企业数字化转型工作进一步推进，为持续优化运营创新，充分激活数据要素潜能，为社会创造更多价值，集团决定在总公司建立两个数据中心，在某省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。

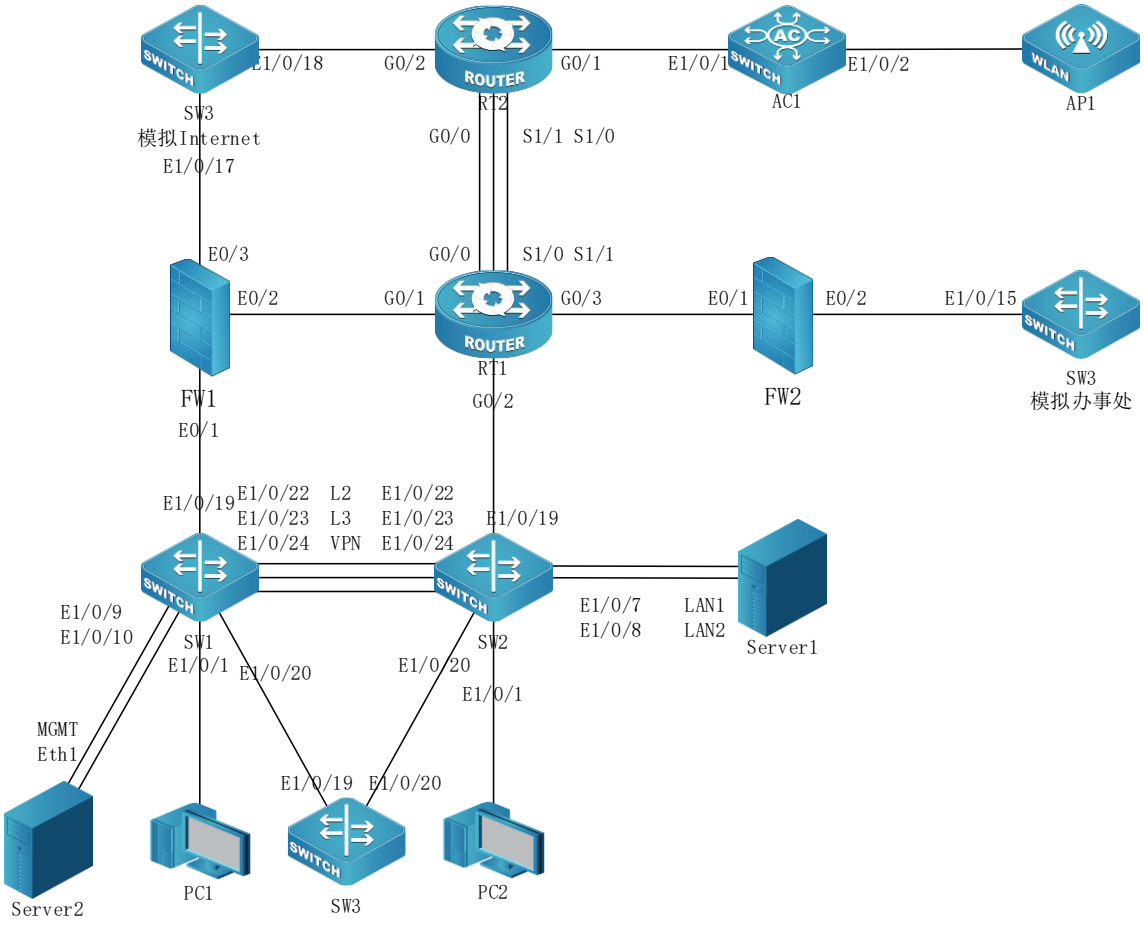
集团、分公司及办事处的网络结构详见拓扑图。编号为 SW1 的设备作为总公司 1#DC 核心交换机，编号为 SW2 的设备作为总公司 2#DC 核心交换机；编号为 SW3 的设备作为某省灾备 DC 核心交换机；编号 FW1 的设备作为总公司互联网出口防火墙；编号为 FW2 的设备作为办事处防火墙；编号为 RT1 的设备作为总公司核心路由器；编号为 RT2 的设备作为分公司路由器;编号为 AC1 的设备作为分公司的有线无线智能一体化控制器，通过与 AP1 配合实现所属区域无线覆盖。

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。请完成所有配置后，需从客户端进行测试，确保能正常访问到相应应用。

网络拓扑图及 IP 地址表：

1. 网络拓扑图



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	10.4.1.1/32 2001:10:4:1::1/128
	Loopback2	10.4.1.2/32 2001:10:4:1::2/128
	Vlan11	10.4.11.1/24 2001:10:4:11::1/64
	Vlan12	10.4.12.1/24 2001:10:4:12::1/64
	Vlan13	10.4.13.1/24 2001:10:4:13::1/64
	Vlan14	10.4.14.1/24 2001:10:4:14::1/64
	Vlan15	10.4.15.1/24 2001:10:4:15::1/64
	Vlan1019	10.4.255.14/30
	Vlan1020	10.4.255.5/30
	Vlan1023	10.4.255.1/30
	Vlan1024 vpn	10.4.255.1/30
SW2	Loopback1 ospfv2 ospfv3 bgp	10.4.2.1/32 2001:10:4:2::1/128
	Loopback2	10.4.2.2/32 2001:10:4:2::2/128
	Vlan21	10.4.21.1/24 2001:10:4:21::1/64
	Vlan22	10.4.22.1/24 2001:10:4:22::1/64
	Vlan23	10.4.23.1/24 2001:10:4:23::1/64
	Vlan24	10.4.24.1/24 2001:10:4:24::1/64
	Vlan25	10.4.25.1/24 2001:10:4:25::1/64
	Vlan1019	10.4.255.22/30
	Vlan1020	10.4.255.9/30
	Vlan1023	10.4.255.2/30
	Vlan1024 vpn	10.4.255.2/30

设备名称	设备接口	IP 地址
SW3	Loopback1 ospfv2 ospfv3 bgp	10.4.3.1/32 2001:10:4:3::1/128
	Vlan31	10.4.31.1/24 2001:10:4:31::1/64
	Vlan32	10.4.32.1/24 2001:10:4:32::1/64
	Vlan33	10.4.33.1/24 2001:10:4:33::1/64
	Vlan34	10.4.34.1/24 2001:10:4:34::1/64
	Vlan1019	10.4.255.6/30
	Vlan1020	10.4.255.10/30
SW3 模拟办事处	Loopback2	10.4.3.2/32 2001:10:4:3::2/128
	Vlan110	10.4.110.1/24 2001:10:4:110::1/64
	Vlan120	10.4.120.1/24 2001:10:4:120::1/64
	Vlan1015	10.4.255.30/30
SW3 模拟 Internet	Vlan1017	200.200.200.1/30
	Vlan1018	200.200.200.5/30
AC1	Loopback1 ospfv2 ospfv3	10.4.4.1/32 2001:10:4:4::1/128
	Loopback2 rip ripng	10.4.4.2/32 2001:10:4:4::2/128
	Loopback3	10.4.4.3/32 2001:10:4:4::3/128
	Vlan1001	10.4.255.46/30
	Vlan130 无线管理	10.4.130.1/24 2001:10:4:130::1/64
	Vlan140 无线 2.4G 产品	10.4.140.1/24 2001:10:4:140::1/64
	Vlan150 无线 5G 营销	10.4.150.1/24 2001:10:4:150::1/64
RT1	Loopback1 ospfv2 ospfv3 bgp mpls	10.4.5.1/32 2001:10:4:5::1/128
	Loopback2 rip ripng	10.4.5.2/32 2001:10:4:5::2/128

设备名称	设备接口	IP 地址
	Loopback3 isis	10.4.5.3/32 2001:10:4:5::3/128
	Loopback4 集团与办事处互联	10.4.5.4/32 2001:10:4:5::4/128
	Loopback5 vpn 财务	10.4.5.5/32 2001:10:4:5::5/128
	G0/0	10.4.255.33/3 0
	G0/1	10.4.255.18/30
	G0/2	10.4.255.21/30
	G0/3	10.4.255.25/30
	S1/0	10.4.255.37/30
	S1/1	10.4.255.41/30
RT2	Loopback1 ospfv2 ospfv3 bgp mpls	10.4.6.1/32 2001:10:4:6::1/128
	Loopback2 rip ripng	10.4.6.2/32 2001:10:4:6::2/128
	Loopback3 isis	10.4.6.3/32 2001:10:4:6::3/128
	Loopback4 ipsecvpn	10.4.6.4/32 2001:10:4:6::4/128
	Tunnel4 ipsecvpn	10.4.255.50/30
	Loopback5 vpn 财务	10.4.6.5/32 2001:10:4:6::5/128
	G0/0	10.4.255.34/30
	G0/1	10.4.255.45/30
	G0/2	200.200.200.6/30
	S1/0	10.4.255.42/30
	S1/1	10.4.255.38/30
FW1	Loopback1 ospfv2 ospfv3 trust	10.4.7.1/32 2001:10:4:7::1/128
	Loopback2 rip ripng trust	10.4.7.2/32 2001:10:4:7::2/128
	Loopback3 isis trust	10.4.7.3/32 2001:10:4:7::3/128
	Loopback4 ipsecvpn trust	10.4.7.4/32 2001:10:4:7::4/128
	Tunnel4 ipsecvpn VPNHUB	10.4.255.49/30
	E0/1 trust	10.4.255.13/30

设备名称	设备接口	IP 地址
	E0/2 trust	10.4.255.17/30
	E0/3 untrust	200.200.200.2/30
FW2	Loopback1 ospfv2 ospfv3 trust	10.4.8.1/32 2001:10:4:8::1/128
	E0/1 dmz	10.4.255.26/30
	E0/2 trust	10.4.255.29/30

(一)工程统筹（本题共 10 分）

1.职业素养

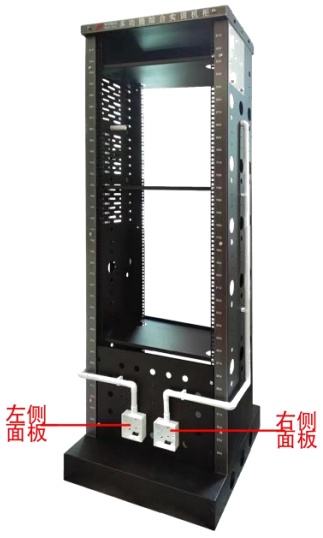
整理赛位，工具、设备归位，保持赛后整洁有序。

无因选手原因导致设备损坏。

恢复调试现场，保证网络和系统安全运行。

2.网络布线

机架立面示意图



左侧面板编号 101；右侧面板编号 102。

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。

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	W1-06-102-1	W1	102	2	06

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，并且安装上信息点面板，并标注标签。

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。

(二)交换配置（本题共 10 分）

1.配置 SW1、SW2、SW3 的 Vlan，二层链路只允许下面 Vlan 通过，不限制 vlan1。

设备	Vlan 编号	端口	说明
SW1	Vlan11	E1/0/1	产品 1 段
	Vlan12	E1/0/2	营销 1 段
	Vlan13	E1/0/3	法务 1 段
	Vlan14	E1/0/4	人力 1 段
	Vlan15	E1/0/5	财务 1 段
SW2	Vlan21	E1/0/1	产品 2 段
	Vlan22	E1/0/2	营销 2 段

设备	Vlan 编号	端口	说明
	Vlan23	E1/0/3	法务 2 段
	Vlan24	E1/0/4	人力 2 段
	Vlan25	E1/0/5	财务 2 段
SW3	Vlan31	E1/0/1	产品 3 段
	Vlan32	E1/0/2	营销 3 段
	Vlan33	E1/0/3	法务 3 段
	Vlan34	E1/0/4	人力 3 段
	Vlan110	E1/0/11	办事处产品
	Vlan120	E1/0/12	办事处营销

2.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 Finance，RD 为 1:1。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 passive；采用目的、源 IP 进行实现流量负载分担。

3.为方便后续验证与测试，SW3 的 E1/0/22 连接其他合适设备的一个接口，配置为 trunk，允许 Vlan31-34、110、120 通过。

4.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 Office,RD 为 1:1。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，RD 为 2:2。

5.SW1 配置 SNMP，引擎 id 分别为 1000；创建组 GroupSkills，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 UserSkills，采用 aes 算法进行加密，密钥为 Key-1122，哈希算法为 sha，密钥为 Key-1122；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 10.4.15.120、2001:10:4:15::120，采用最高安全级别；当法务部门的用户端口发生 updown 事件时禁止发送 trap 消息至上述集团网管服务器。

6.对 SW1 与 FW1 互连流量镜像到 SW1 E1/0/1，会话列表为 1。

7.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；

8.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。

(三)路由调试（本题共 10 分）

1.配置所有设备主机名，名称见“网络拓扑”。启用所有设备的 ssh 服务，用户名和明文密码均为 admin；配置所有设备 ssh 连接超时为 9 分钟，console 连接超时为 30 分钟。

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，其他设备为 ntp client，请求报文时间间隔 1 分钟，用 SW1 Loopback1 IPv6 地址作为 ntp server 地址。

3.配置接口 IPv4 地址和 IPv6 地址，互联接口 IPv6 地址用本地链路地址。FW1 和 FW2 接口仅启用 ping 功能以及 Loopback1 的 ssh 功能。

4.SW2 配置 DHCPv4 和 DHCPv6，分别为 Vlan11、Vlan21、Vlan130、Vlan140、Vlan150 分配地址。DHCPv4 地址池名称分别为 PC1、PC2、AP1、POOLv4-VLAN11、POOLv4-VLAN21、POOLv4-VLAN130、POOLv4-VLAN140、POOLv4-VLAN150，排除网关，DNS 为 10.4.210.101 和 10.4.220.101。DHCPv6 地址池名称分别为 POOLv6-VLAN11、POOLv6-VLAN21、POOLv6-VLAN130、POOLv6-VLAN140、POOLv6-VLAN150，DHCPv6 地址池用网络前缀表示，排除网关，DNS 为 2400:3200::1。PC1 保留地址 10.4.11.9（DHCPv4 地址池名称为 PC1）和 2001:10:4:11::9，PC2 保留地址 10.4.21.9(DHCPv4 地址池名称为 PC2)和 2001:10:4:21::9，AP1 保留地址 10.4.130.9（DHCPv4 地址池名称为 AP1）和 2001:10:4:130::9。SW1、AC1 中继地址为 SW2 Loopback1 地址。SW1 启用 DHCPv4 和 DHCPv6 snooping 功能，如果 E1/0/1 连接 DHCPv4 服务器，则关闭端口，恢复时间为 10 分钟。

5.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网络地址，按照 IP 地址从小到大的顺序发布。每个 prefix-list 的序号从 5 开始，按照 IP 地址从小到大的顺序递增 5；route-map 的序号从 10 开始，递增 10，route-map 名称与 prefix-list 名称相同。每个 ACL 序号从

10 开始，按照 IP 地址从小到大的顺序递增 10)。

SW1、SW2、SW3、RT1、RT2、FW1 之间 OSPFv2 和 OSPFv3 协议，process 1,area 0,分别发布 Loopback1 地址路由和产品路由,FW1 通告 type1 默认路由。

RT2 与 AC1 之间运行 OSPFv2 协议，process 1，area 1 nssa no-summary；AC1 发布 Loopback1 地址路由、管理、产品和营销路由，用 prefix-list 重发布 Loopback3,prefix-list 名称为 AC1-Loopback3-IPv4。

RT2 与 AC1 之间运行 OSPFv3 协议，process 1，area 1 stub no-summary；AC1 发布 Loopback1 地址路由、管理、产品和营销路由。

RT1、FW2、SW3 模拟办事处之间运行 OSPFv2 和 OSPFv3 协议，process 2，area 2。SW3 模拟办事处发布 Loopback2、产品和营销路由。FW2 发布 Loopback1 路由。RT1 发布 Loopback4 路由,向该区域通告 type1 默认路由；RT1 用 prefix-list 匹配 SW3 模拟办事处 Loopback2 和产品路由、FW2 Loopback1 路由(prefix-list 名称分别为 SW3-FW2-IPv4 和 SW3-FW2-IPv6)、RT1 与 FW2 直连 IPv4 路由(prefix-list 名称为 RT1-FW2-IPv4)，以上路由重发布到 process 1。

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。

6.RT1 串行链路、RT2 串行链路、FW1、AC1 之间分别运行 RIP 和 RIPng 协议，分别发布 Loopback2 地址路由（FW1 的 RIPng 发布路由时用接口名称）。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 ACL-RIP-IPv4，IPv6 的 ACL 名称为 ACL-RIP-IPv6。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 Key-1122。

7.RT1 以太链路（物理速率为 2048000）、RT2 以太链路、FW1 之间运行 ISIS 协议，instance 1，实现 Loopback3 之间 IPv4 互通和 IPv6 互通。RT1、RT2、FW1 的 NET 分别为 10.0000.0000.0005.00、10.0000.0000.0006.00、10.0000.0000.0007.00，路由器类型是 Level-2，互联接口网络类型为点到点。

8.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。

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 和 IPv6 BGP 邻居。SW1 和 SW2 的 Loopback2 IPv4 互通采用静态路由;IPv6 互通采用 OSPFv3，process 2，area 2。

SW1、SW2、SW3 分别只发布营销、法务、人力、财务等 IPv4 和 IPv6

路由；RT1 发布办事处营销 IPv4 和 IPv6 路由到 BGP；RT2 发布分公司营销 IPv4 和 IPv6 路由到 BGP。

SW3 营销分别与 SW1 和 SW2 营销 IPv4 和 IPv6 互访优先在 SW1-SW3 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 SW2-SW3 链路转发，主备链路相互备份；在 SW3 上用 prefix-list、route-map 和 BGP 路径属性进行选路，新增 AS 65000。

（SW1 和 SW2 营销路由 prefix-list 名称分别为 SW1-SW2-YX-IPv4 和 SW1-SW2-YX-IPv6、法务及人力路由 prefix-list 名称分别为 SW1-SW2-FWRL-IPv4 和 SW1-SW2-FWRL-IPv6;SW3 营销路由 prefix-list 名称分别为 SW3-YX-IPv4 和 SW3-YX-IPv6、法务及人力路由 prefix-list 名称分别为 SW3-FWRL-IPv4 和 SW3-FWRL-IPv6）

9.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 Finance，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。

10.RT2 配置 IPv4 NAT，ACL 名称为 ACL-NAT，实现 AC1 IPv4 产品用 RT2 外网接口 IPv4 地址访问 Internet。RT2 配置 NAT64，ACL 名称为 ACL-NAT64，实现 AC1 IPv6 产品用 RT2 外网接口 IPv4 地址访问 Internet，IPv4 地址转 IPv6 地址前缀为 64:ff9b::/96。

(四)无线部署（本题共5分）

1.AC1 与 AP1 相连接口只允许 Vlan140 和 Vlan150 通过。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Vlan140,用Network 140和radio1（profile 1, mode 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Key-1122，用第一个可用VAP发送2.4G信号。SKILLS-5G对应Vlan150，用Network 150和radio2（profile 1, mode 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。

(五)安全维护（本题共5分）

说明:按照IP地址从小到大的顺序用“IP/mask”表示,IPv4 Any地址用0.0.0.0/0，IPv6 Any地址用::/0，禁止使用地址条目。

1.FW1配置IPv4 NAT,id为1,实现集团产品1段IPv4访问Internet IPv4，转换ip/mask为200.200.200.16/28，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。

2.FW1配置NAT64，id为2，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 段和产品 2 段访问 SW3 模拟办事处 Loopback2 IPv4、FW2 Loopback1 IPv4、办事处产品 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。RT2 的 ACL 名称为 ACL-VPN，transform-set 名称为 SET-1，crypto map 名称为 MAP-1。FW1 的 isakmp proposal 名称为 P-1，isakmp peer 名称为 PEER-1，ipsec proposal 名称为 P-2，tunnel ipsec 名称为 IPSEC-1，tunnel gre 名称为 GRE-1。

模块三：服务搭建与运维

（共计 50 分）

任务背景描述：

随着信息技术更迭，集团计划 2023 年把部分业务由原有的 X86 架构服务器上迁移到 ARM 架构服务器上，同时根据目前的部分业务需求进行了部分调整和优化。

(一)X86 架构计算机安装与管理（本题共 5 分）

1.PC1 系统为 ubuntu-desktop-amd64 系统，登录用户为 xiao，密码为 Key-1122，配置该用户免密码执行 sudo 命令。

2.安装 remmina，用该软件连接 server1 上的虚拟机，并配置虚拟机上的相应服务。

(二)ARM64 架构计算机操作系统安装与管理（本题共 5 分）

1.从 U 盘启动 PC2，安装 kylin-desktop-arm64（安装语言为英文），安装时创建用户为 xiao，密码为 Key-1122，配置该用户免密码执行 sudo 命令。

2.配置 minicom，用该软件连接网络设备。

(三)Windows 云服务配置（本题共 15 分）

1.创建实例

网络信息表

网络名称	Vlan	子网名称	网关	IPv4 地址池
Network210	210	Subnet210	10.4.210.1/24	10.4.210.100-10.4.210.199
Network211	211	Subnet211	none	10.4.211.100-10.4.211.199
Network212	212	Subnet212	none	10.4.212.100-10.4.212.199

实例类型信息表（提示：删除所有已有实例类型）

名称	id	vcpu	内存	磁盘
Skills	1	4	4096MB	100GB

实例信息表

实例名称	镜像	实例类型	IPv4 地址	主机名称
windows1	windows2022	Skills	10.4.210.101	windows1
windows2	windows2022	Skills	10.4.210.102	windows2
windows3	windows2022	Skills	10.4.210.103	windows3
windows4	windows2022	Skills	10.4.210.104	windows4
windows5	windows2022	Skills	10.4.210.105 10.4.211.105	windows5
windows6	windows2022	Skills	10.4.210.106 10.4.211.106	windows6
windows7	windows2022	Skills	10.4.210.107 10.4.211.107	windows7
windows8	windows2022	Skills	10.4.210.108	windows8

实例名称	镜像	实例类型	IPv4 地址	主机名称
			10.4.211.108 10.4.212.108	
windows9	windows2022	Skills	10.4.210.109 10.4.211.109 10.4.212.109	windows9

2.域服务

任务描述：请采用域环境，管理企业网络资源。

配置所有 windows 主机 IP 地址和主机名称。

配置 windows1 为 skills.lan 域控制器；安装 dns 服务，dns 正反向区域在 active directory 中存储，负责该域的正反向域名解析。

配置 windows2 为 skills.lan 辅助域控制器；安装 dns 服务，dns 正反向区域在 active directory 中存储,负责该域的正反向域名解析。

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

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.lan。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.lan，国家=CN，省=Beijing，城市=Beijing，组织=skills，组织单位=system，使用者可选名称=*.skills.lan 和 skills.lan。浏览器访问 https 网站时，不出现证书警告信息。

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

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，不能修改其口令，密码永不过期。manager00 拥有域管理员权限。

3.组策略

任务描述：请采用组策略，实现软件、计算机和用户的策略设置。

复制 PowerShell-7.3.6-win-x64.msi 到 windows1 的 C:\soft。域中主机自动安装 powershell7（提示：如果部署不成功，则需要每台 windows 主机均手动安装，软件包在 U 盘 soft 目录。导出答案时使用 pwsh(powershell7)，而不是 powershell5。）

域中主机自动申请“ipsec”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”，有效期 5 年。

允许 manager 组本地登录域控制器，允许 manager00 用户远程登录到域控制器；拒绝 dev 组从网络访问域控制器。

登录时不显示上次登录，不显示用户名，无须按 ctrl+alt+del。

登录计算机时，在桌面新建名称为 vcsc 的快捷方式，目标为 https://www.vcsc.org.cn，快捷键为 ctrl+shift+f6。

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:\profiles，每个用户提供单独的配置文件文件夹。

4.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。

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。在本目录下为所有用户添加一个以用户名命名的文件夹，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”文件，文件组名和模板名为 my。

创建目录 D:\share\work，共享名为 work，仅 manager 组和 Administrator 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 AD DS 中发布该共享。

5.DFS 服务

任务描述：请采用 DFS，实现集中管理共享文件。

在 windows3-windows5 的 C 分区分别划分 2GB 的空间，创建 NTFS 主分区，驱动器号为 D。

配置 windows3 为 DFS 服务器，命名空间为 dfsroot，文件夹为 pictures，存储在 D:\dfs，所有用户都具有读写权限；实现 windows4 的 D:\pics 和 windows5 的 D:\images 同步。

配置 windows4 的 dfs IPv4 使用 34567 端口；限制所有服务的 IPv4 动态 rpc 端口从 10000 开始，共 2000 个端口号。

6.ASP 服务

任务描述：请采用 IIS 搭建 web 服务，创建安全动态网站,。

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

http 和 https 绑定本机与外部通信的 IP 地址，仅允许使用域名访问（使用“计算机副本”证书模板)。客户端访问时，必需有 ssl 证书（浏览器证书模板为“管理员”)。

网站目录为 C:\iis\contents，默认文档 index.aspx 内容为"HelloAspx"。

使用 windows5 测试。

7.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。

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

网站名称为 printer，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)。

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。

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"。

8.NLB 服务

任务描述：请采用 NLB，实现负载平衡。

配置 windows5 和 windows6 为 NLB 服务器。

windows5 群集优先级为 5，windows6 群集优先级为 6，群集 IPv4 地址为 10.4.210.60/24,群集名称为 www.skills.lan,采用多播方式。

配置 windows5 为 web 服务器，站点名称为 www，网站的最大连接数为 10000，网站连接超时为 60s，网站的带宽为 100Mbps。

共享网页文件、共享网站配置文件和网站日志文件分别存储到 windows1 的 D:\FilesWeb\Contents 、 D:\FilesWeb\Configs 和 D:\FilesWeb\Logs。网站主页 index.html 内容为"HelloNLB"。

使用 W3C 记录日志，每天创建一个新的日志文件，日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号。

网站仅绑定 https，IP 地址为群集地址，仅允许使用域名加密访问，使用“计算机副本”证书。

配置 windows6 为 web 服务器，要求采用共享 windows5 配置的方式，使用“计算机副本”证书。

9.iSCSI 服务

任务描述：请采用 iSCSI，实现故障转移。

在 windows7 上安装 iSCSI 目标服务器，并新建 iSCSI 虚拟磁盘，存储位置为 C:\iscsi；虚拟磁盘名称分别为 Quorum 和 Files，磁盘大小为动态扩展，分别为 1GB 和 5GB，目标名称为 win，访问服务器为 windows8 和 windows9，实行 CHAP 双向认证，Target 认证用户名和密码分别为 IncomingUser 和 IncomingPass，Initiator 认证用户名和密码分别为 OutgoingUser 和 OutgoingPass。目标 iqn 名称为 iqn.2008-01.lan.skills:server，使用 IP 地址建立目标。发起程序 iqn 名称分别为 iqn.2008-01.lan.skills:client1 和 iqn.2008-01.lan.skills:client2。

在 windows8 和 windows9 上安装多路径 I/O，10.4.210.0 和 10.4.211.0 网络为 MPIO 网络，连接 windows7 的虚拟磁盘 Quorum 和 Files，初始化为 GPT 分区表，创建 NTFS 主分区，驱动器号分别为 M 和 N。

配置 windows8 和 windows9 为故障转移群集；10.4.212.0 网络为心跳网络。

在 windows8 上创建名称为 cluster 的群集，其 IP 地址为 10.4.210.70。

在 windows9 上配置文件服务器角色，名称为 clusterfiles，其 IP 地址为 10.4.210.80。为 clusterFiles 添加共享文件夹，共享协议采用

“SMB”，共享名称为 clustershare，存储位置为 N:\share，NTFS 权限为仅域管理员和本地管理员组具有完全控制权限，域其他用户具有修改权限；共享权限为仅域管理员具有完全控制权限，域其他用户具有更改权限。

(四)Linux 云服务配置（本题共 15 分）

1.系统安装

PC1 web 连接 server2，给 server2 安装 rocky-arm64 CLI 系统（语言为英文)。

配置 server2 的 IPv4 地址为 10.4.220.100/24。

安装 qemu-kvm、libvirt 和 virt-install。

创建 rocky-arm64 虚拟机，虚拟机磁盘文件保存在默认目录，名称为 linuxN.qcow2(N 表示虚拟机编号 0-9，如虚拟机 linux1 的磁盘文件为 linux1.qcow2),虚拟机信息如下：

虚拟机名称	vcpu	内存	磁盘	IPv4 地址	主机名称
linux0	2	4096MB	100GB	none	
linux1	2	4096MB	100GB	10.4.220.101/24	linux1
linux2	2	4096MB	100GB	10.4.220.102/24	linux2
linux3	2	4096MB	100GB	10.4.220.103/24	linux3
linux4	2	4096MB	100GB	10.4.220.104/24	linux4
linux5	2	4096MB	100GB	10.4.220.105/24	linux5
linux6	2	4096MB	100GB	10.4.220.106/24	linux6
linux7	2	4096MB	100GB	10.4.220.107/24	linux7

linux8	2	4096MB	100GB	10.4.220.108/24	linux8
linux9	2	4096MB	100GB	10.4.220.109/24	linux9

安装 linux0，系统为 rocky9 CLI，网络模式为桥接模式，用户 root 密码为 Key-1122。

关闭 linux0，给 linux0 创建快照，快照名称为 linux-snapshot。

根据 linux0 克隆虚拟机 linux1-linux9。

2.dns 服务

任务描述：创建 DNS 服务器，实现企业域名访问。

配置 linux 主机的 IP 地址和主机名称。

所有 linux 主机启用防火墙（kubernetes 服务主机除外），防火墙区域为 public，在防火墙中放行对应服务端口。

所有 linux 主机之间（包含本主机）root 用户实现密钥 ssh 认证，禁用密码认证。

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

利用 bind，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。正向区域文件均为 /var/named/named.skills，反向区域文件均为 /var/named/named.10。

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.lan。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.lan，

国家=CN,省=Beijing,城市=Beijing,组织=skills,组织单位=system,使用者可选名称=*.skills.lan 和 skills.lan。将证书 skills.crt 和私钥 skills.key 复制到需要证书的 linux 服务器/etc/pki/tls 目录。浏览器访问 https 网站时，不出现证书警告信息。

3.ansible 服务

任务描述：请采用 ansible，实现自动化运维。

在 linux1 上安装系统自带的 ansible-core,作为 ansible 控制节点。linux2-linux9 作为 ansible 的受控节点。

4.apache2 服务

任务描述：请采用 Apache 搭建企业网站。

配置 linux1 为 Apache2 服务器,使用 skills.lan 或 any.skills.lan（any 代表任意网址前缀,用 linux1.skills.lan 和 web.skills.lan 测试)访问时,自动跳转到 www.skills.lan。禁止使用 IP 地址访问，默认首页文档/var/www/html/index.html 的内容为"HelloApache"。把/etc/pki/tls/skills.crt 证书文件和/etc/pki/tls/skills.key 私钥文件转换成含有证书和私钥的/etc/pki/tls/skills.pfx 文件；然后把/etc/pki/tls/skills.pfx 转换为含有证书和私钥的/etc/pki/tls/skills.pem 文件，再从/etc/pki/tls/skills.pem 文件中提取证书和私钥分别到/etc/pki/tls/apache.crt 和/etc/pki/tls/apache.key。

客户端访问 Apache 服务时，必需有 ssl 证书。

5.nginx 和 tomcat 服务

任务描述:利用系统自带 openjdk 和 tomcat,搭建 Tomcat 动态网站。

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。

利用 nginx 反向代理，实现 linux3 和 linux4 的 tomcat 负载均衡，通过 https://tomcat.skills.lan 加密访问 Tomcat，http 访问通过 301 自动跳转到 https。

配置 linux3 和 linux4 为 tomcat 服务器，网站默认首页内容分别为“tomcatA”和“tomcatB”,采用修改配置文件端口形式,仅使用域名访问 80 端口 http 和 443 端口 https。

6.samba 服务

任务描述：请采用 samba 服务，实现资源共享。

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

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。manager 组用户对 sharesmb 共享有读写权限，dev 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。

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

7.nfs 服务

任务描述：请采用 nfs，实现共享资源的安全访问。

配置 linux2 为 kdc 服务器，负责 linux3 和 linux4 的验证。

在 linux3 上，创建用户，用户名为 xiao，uid=2222，gid=2222，家目录为/home/xiaodir。

配置 linux3 为 nfs 服务器,目录/srv/sharenfs 的共享要求为:linux 服务器所在网络用户有读写权限，所有用户映射为 xiao，kdc 加密方式为 krb5p。

配置 linux4 为 nfs 客户端，利用 autofs 按需挂载 linux3 上的/srv/sharenfs 到/sharenfs 目录,挂载成功后在该目录创建 test 目录。

8.kubernetes 服务

任务描述：请采用 kubernetes 和 containerd，管理容器。

在 linux5-linux7 上安装 containerd 和 kubernetes，linux5 作为 master node，linux6 和 linux7 作为 work node；使用 containerd.sock 作为容器 runtime-endpoint。pod 网络为 10.244.0.0/16，services 网络为 10.96.0.0/16。

master 节点配置 calico 作为网络组件。

导入 nginx.tar 镜像，主页内容为“HelloKubernetes”。用该镜像创建一个名称为 web 的 deployment，副本数为 2；为该 deployment 创建一个类型为 nodeport 的 service，port 为 80，targetPort 为 80，nodePort 为 30000。

9.iscsi 服务

任务描述：请采用 iscsi，搭建存储服务。

为 linux8 添加 4 块磁盘，每块磁盘大小为 5G，创建 lvm 卷，卷组名称为 vg1，逻辑卷名称为 lv1，容量为全部空间，格式化为 ext4 格式。使用/dev/vg1/lv1 配置为 iSCSI 目标服务器，为 linux9 提供 iSCSI 服务。iSCSI 目标端的 wwn 为 iqn.2008-01.lan.skills:server，iSCSI 发起端的 wwn 为 iqn.2008-01.lan.skills:client1.

配置 linux9 为 iSCSI 客户端，实现 discovery chap 和 session chap 双向认证，Target 认证用户名为 IncomingUser，密码为 IncomingPass；Initiator 认证用户名为 OutgoingUser，密码为 OutgoingPass。修改/etc/rc.d/rc.local 文件开机自动挂载 iscsi 磁盘到/iscsi 目录。

10.mariadb 服务

任务描述：请安装 mariadb 服务，建立数据表。

配置 linux3 为 mariadb 服务器，创建数据库用户 xiao，在任意机器上对所有数据库有完全权限。

创建数据库 userdb；在库中创建表 userinfo，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
height	float	否	否
birthday	datetime	否	否
sex	varchar(5)	否	否
password	varchar(200)	否	否

在表中插入 2 条记录，分别为(1,user1,1.61,2000-07-01，M)，(2,user2，1.62,2000-07-02，F)，password 字段与 name 字段相同，password 字段用 md5 函数加密。

新建/var/mariadb/userinfo.txt 文件，文件内容如下，然后将文件内容导入到 userinfo 表中，password 字段用 md5 函数加密。

3,user3,1.63,2000-07-03,F,user3

4,user4,1.64,2000-07-04,M,user4

5,user5,1.65,2000-07-05,M,user5

6,user6,1.66,2000-07-06,F,user6

7,user7,1.67,2000-07-07,F,user7

8,user8,1.68,2000-07-08,M,user8

9,user9,1.69,2000-07-09,F,user9

将表 userinfo 中的记录导出，并存放到/var/mariadb/userinfo.sql，字段之间用','分隔。

为 root 用户创建计划任务（day 用数字表示），每周五凌晨 1:00 备

份数据库 userdb(含创建数据库命令)到/var/mariadb/userdb.sql。（为便于测试，手动备份一次。）

11.podman 服务

任务描述：请采用 podman，实现容器虚拟化技术。

在 linux3 上安装 podman，导入 rockylinux-9.tar 镜像。

创建名称为 skills 的容器,映射本机的 8000 端口到容器的 80 端口，在容器内安装 httpd，默认网页内容为“HelloPodman”。

配置 https 访问的私有仓库，登录用户和密码均为 admin。导入 registry.tar 镜像，创建名称为 registry 的容器。

修改 rockylinux 镜像的 tag 为 linux3.skills.lan:5000/rockylinux:9，上传该镜像到私有仓库。

12.开发环境搭建

任务描述：搭建开发环境。

在 linux4 上搭建开发环境。

利用系统 iso 文件，搭建 c 语言、c++语言、rust 语言开发环境。

(五)网络运维（本题共10分）

1.网络运维

任务描述：某集团公司在更新设备后，路由之间无法正常通信，请修复网络达到正常通信。

（1） 请在server1“管理员”下拉菜单中选择“镜像”选项卡，点击 “创建镜像”按钮，弹出“创建镜像”对话框后，名称为eve-ng，镜像文件请在U盘soft目录下选择“eve-ng.qcow2”文件，“镜像格式”为qcow2格式，“最小磁盘”和“最低内存”不填，单击“创建镜像”按钮完成镜像创建。

（2） 用上述eve-ng镜像创建虚拟机，虚拟机名称为eve-ng，IP地址为10.4.210.110/24，虚拟机实例类型为Skills。

（3） 通过http://10.4.210.110运行eve-ng虚拟机，登录用户名为admin，密码为eve，html5 console，启动所有网络设备。

（4） 完善设备配置，请在最少改动设备路由协议的基础上，实现所有设备的loopback1之间通信。

（5） 在每台设备图标上右击，从弹出菜单中选择“export CFG”，在左侧的面板中选择“Startup-configs”，依次单击设备图标，复制右侧文本框内容，保存到选手目录中以设备名称命名的文本文件（R1.txt，R2.txt，R3.txt）。

2.系统运维

任务要求：为保证 linux9 系统稳定性，请在不破坏原有服务的基础上，升级 linux9 的内核 kernel，删除旧版本 kernel。