第八届江苏技能状元大赛

信息通信网络运行管理（学生组）赛项

样

卷

模块A职业素养

本模块主要考查选手在信息通信网络施工与运维场景下的安全意识、规范操作、现场管理、团队协作与赛场纪律，全面体现技工院校信息技术类专业学生应具备的职业行为习惯与职业素养。

一、总体要求

1.严格遵守信息通信行业安全操作规范与赛场安全文明生产要求，杜绝违规操作，严防人身伤害、设备损坏、电路短路、操作失控等安全事故。

2.着装整洁规范，操作流程标准有序，工具使用规范熟练，物料摆放整齐统一，展现良好职业形象。

3.注重过程管理，资料归档规范、现场环境整洁，做到工完场清、文明施工。

4.尊重裁判、遵守纪律、服从管理，体现良好职业操守与团队协作能力。

二、具体行为规范

1.安全防护规范:进行网络综合布线施工等实操环节时，必须按要求佩戴安全帽，做好个人安全防护，杜绝不规范施工行为。

2.工具与物料管理:施工所用工具、材料、设备须统一放置在施工桌面，严禁随意摆放在地面、机柜上盖、网络设备及服务器表面；工具使用完毕及时归位。

3.现场环境管理:竞赛全程及结束后，施工区域保持卫生整洁；剩余材料、器件集中放置于施工桌面，施工废料、垃圾及时投入垃圾桶，工具放入工具包。

4.文档资料管理:过程性文档按竞赛要求规范存放，纸质试题、任务单等资料整理整齐，统一放置于施工桌面，做到归档完整、条理清晰。

5.团队协作要求:熟悉竞赛环境与施工流程，团队成员合理分工、充分沟通、高效配合，体现良好的组织协调与协作施工能力。

6.赛场纪律要求:竞赛期间未经裁判允许，不得擅自离开施工区域；遇到问题、疑问或需协助时，举手向裁判示意，服从裁判指挥，遵守赛场各项纪律，不喧哗、不违规交流、不干扰他人竞赛。

三、评分导向

本模块以安全、规范、整洁、有序、守纪、协作为核心评价标准，对违反安全规范、现场混乱、物料乱放、文档缺失、不服从管理、擅自离岗等行为将酌情扣分，全面体现选手职业素养水平。

模块 B 数据中心网络搭建（网络链路安装）

一、赛题说明：

1.总体要求：选手根据提供的多功能综合实训机柜正面展开设备安装布线施工图，完成网络综合布线的施工和测试。重点考查参赛选手的网络基础设备建设的能力。

2.综合布线识图要求：能够读懂施工图纸（多功能综合实训机柜正面展开图），并按照图示位置进行安装和布线。

3.综合布线技能要求：能够完成设备与底盒安装、线管铺设与固定、跳线制作与测试、线缆铺设与端接、信息点安装与标识等。

二、注意事项：

1.进入竞赛施工现场，施工人员需佩戴安全帽（未参与网络综合布线模块施工选手除外）；

2.竞赛所用工具、器材、耗材，在竞赛开始前已全部发放到各个竞赛工位，保证充分满足竞赛需求。竞赛开始前，请仔细核对材料明细表，并于比赛开始前签字确认（未签字确认前禁止开始比赛）。竞赛过程中，不再另行发放工具、材料；

3.对设备上未标注端口编号的配线架和信息点面板，规定端口号均为面向，依次从左向右从小到大编号（左……1、2、3……n……右）；

三、项目简介：

某集团公司新建内部网络，需要进行综合布线技术设施建设，请根据图 1 多功能综合实训机柜正面展开设备安装布线施工图，并根据具体要求，完成网络综合布线模块的施工。

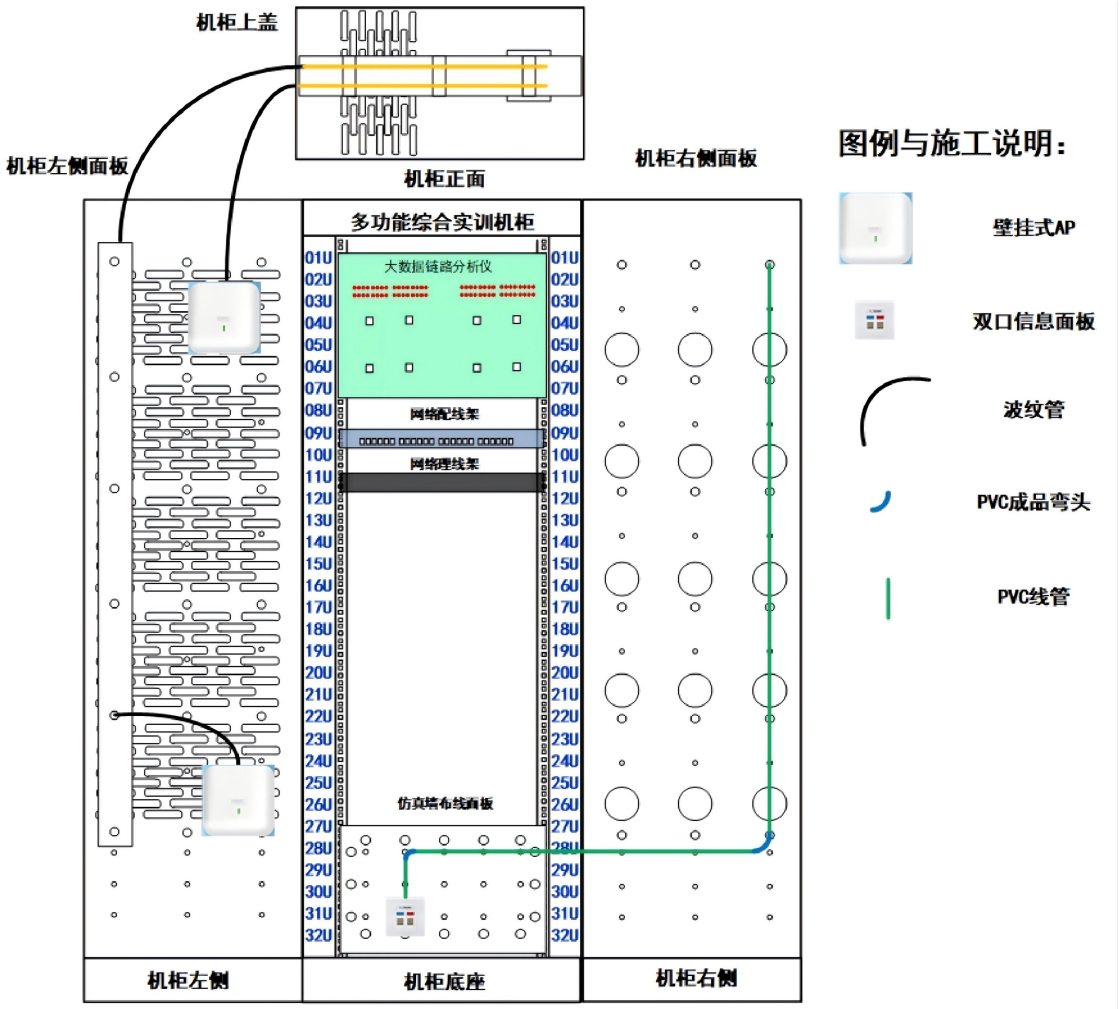


图 1 多功能综合实训机柜正面展开设备安装布线施工图

四、具体施工项目：

1. 在机柜侧布线面板的相应位置，安装壁挂式 AP、信息点底盒。（使用材料：壁挂式 AP、明装底盒、螺丝、塑料卡口）

2. 完成配线子系统 PVC 线管安装。（使用材料：Φ20PVC 冷弯管、管卡、直接头、成品弯头、PVC 锁母）

3. 完成双口信息点线管线缆铺设，在Φ20PVC 内铺设 2 根六类双绞线，一端接入明装底盒、一端进入机柜铺设到机柜内六类配线架位置。，注意线缆预留和标注。（使用材料：六类双绞线、P 型标签）

4. 完成桥架线缆铺设，从面板式 AP 底盒和壁挂式 AP 处，通过桥架分别铺设 1 根六类双绞线到机柜内六类配线架位置。注意线缆在桥架上铺设时每个支撑点都

要进行捆扎；线缆在进入桥架前要安装波纹管和锁母（机柜内线缆无需安装）；线缆预留和标注。（使用材料：六类双绞线、扎带、波纹管、锁母）

5.完成线缆端接，将 AP 信息点的 2 根双绞线端接水晶头、将双口面板信息点的 2 根双绞线端接六类模块，并安装信息点面板；4 根双绞线的另外一端按照表 1 线缆端接对应表的关系，端接到机柜内六类配线架相应端口；注意线缆预留和标记。（使用材料：水晶头、六类模块、六类配线架、P 型标签、双口信息面板）

表 1 线缆端接对应表

序号	信息点类型	配线架类型	端口号	端接标准	线缆标注
1	壁挂式 AP	CAT6UTP	01	T568B	AP01
2	面板式 AP	CAT6UTP	02	T568B	AP02
3	信息面板 01 口	CAT6UTP	03	T568B	D01
4	信息面板 02 口	CAT6UTP	04	T568B	D02

6.完成跳线制作与测试，制作 2 根合适长度的网络跳线。使用大数据链路分析仪进行测试，并将结果填入表 2 跳线测试结果表；其中第 1 根一端接入 PC1，另一端接入双口面板 01 号端口；第 2 根一端接入 PC2，另一端接入双口面板 02 号端口；注意线缆预留和标记。（使用材料：水晶头、六类双绞线、P 型标）

表 2 跳线测试结果表

序号	跳线标签	端接标准	测试是否连通	线序是否正确
1	T01	T568B		
2	T02	T568B		

7.完成 AP-AC 设备线缆连接，使用 2 根成品跳线，按照拓扑图要求，一端接入配线架的相应端口，另外一端接入 AC 相应端口；使用 2 根成品跳线，按照拓扑图要求，一端接入配线架的相应端口，另外一端接入交换机相应端口；注意线缆预留和理线。（使用材料：成品跳线、扎带、理线架）

模块C数据中心网络搭建（网络设备连接与调试）

本考核的拓扑为某公司总部与分部的网络架构。

根据任务的要求，完成本次考核。

《注意事项》：
配置及时保存，按照答题卡要求截图答题卡为唯一评分依据。

任务清单

（一）基础配置

1.根据下文拓扑图及下文地址规划表，配置设备接口信息。

2.在网络设备上，均开启SSH服务端、Telnet服务端功能。其中，用户名和密码为admin、Test@123，密码为明文类型，特权密码为Test@123。

3.分部交换设备上部署SNMP功能。配置所有设备SNMP消息，向主机192.168.100.100发送Trap消息版本采用V2C,读写的Community为“Test@123”，开启Trap消息。

（二）有线网络配置

1.在全网Trunk链路上做VLAN修剪，仅允许规划VLAN通过。

2. 在局域网接入设备启用边缘端口和BPDU防护功能；检测到环路后处理方式为关闭端口。如果端口检测进入禁用状态，设置300秒后会自动恢复。

3. 局域网接入设备启用环路检测功能，规避不同设备间、同一设备不同端口、同一设备单点下的多种环路现象，检测到环路后的处理方式为shutdown-port。

4.在总部配置DHCP服务且DHCP服务器搭建于EG1上，为有线用户 VLAN10与无线用户配置地址，地址池名依据地址表VLAN名称，DHCP对外服务使用loopback 0地址，根据拓扑配置DHCP中继。在分部R2设备上为无线用户配置DHCP服务，地址池名依据地址表VLAN名称；

5.在S1交换机部署DHCP Snooping+DAI功能。其中，DAI功能主要针对VLAN10启用ARP防御。

6.配置MSTP多生成树协议防止二层环路。要求所有数据流经过S2转发，S2失效时经过S1转发。region-name为test。revision版本为1。S2作为实例1的主根，S1作为实例1的从根。其中，主根优先级为4096，从根优先级为8192。

7.在S1和S2交换机上配置VRRP，实现主机的网关冗余，所需配置的参数要求见

表 1。在交换机 S1、S2 上配置的各 VRRP 组中，设置高优先级设置为 150，低优先级设置为 120，S1、S2 的 2 条互联链路（Gi0/3、Gi0/4）上，配置二层链路聚合，采取 LACP 动态聚合模式。

表 1 S1 和 S2 的 VRRP 参数表

VLAN	VRRP 备份组号（VRID）	VRRP 虚拟 IP
VLAN10	10	192.168.10.254
VLAN20	20	192.168.20.254
VLAN50	50	192.168.50.254
VLAN60	60	192.168.60.254
VLAN100	100	192.168.100.254

8.南京总部 AC、S1、S2 与 EG1 设备之间运行 OSPF 协议，使用 OSPF 进程号 12，规划单区域 0，AC 不参与 DR\BDR 选举；苏州分部 EG2、R2 使用运行 OSPF 协议，使用 OSPF 进程号 22，规划单区域 0；EG1、EG2 使用默认路由访问运营商网络。

9.总部 EG1 重分布默认路由使得内网所有设备路由表中都有指向 EG1 的默认路由；

10. 要求终端网段中不出现 OSPF 协议报文；减少非必须 OSPF 协商报文；需要发布 Loopback 地址；优化 OSPF 相关配置，尽量加快 OSPF 收敛（S1\S2\AC 除外）；外部路由引入采用第一类外部路由模式。

11.运营商网络 S2 设备只做中转设备，禁止部署任何路由协议。

12.S1、S2 与 R1 设备之间运行 OSPF 协议建立邻居，OSPF 协议参数自定义，达到总分部之间的通信。

（三）无线网络配置

1.创建总部 SSID 1 为 Test-ZB_XX(XX 为工位号)，AP-Group 为 ZB；创建分部 SSID 2 为 Test-FB_XX(XX 为工位号)，AP-Group 为 FB；

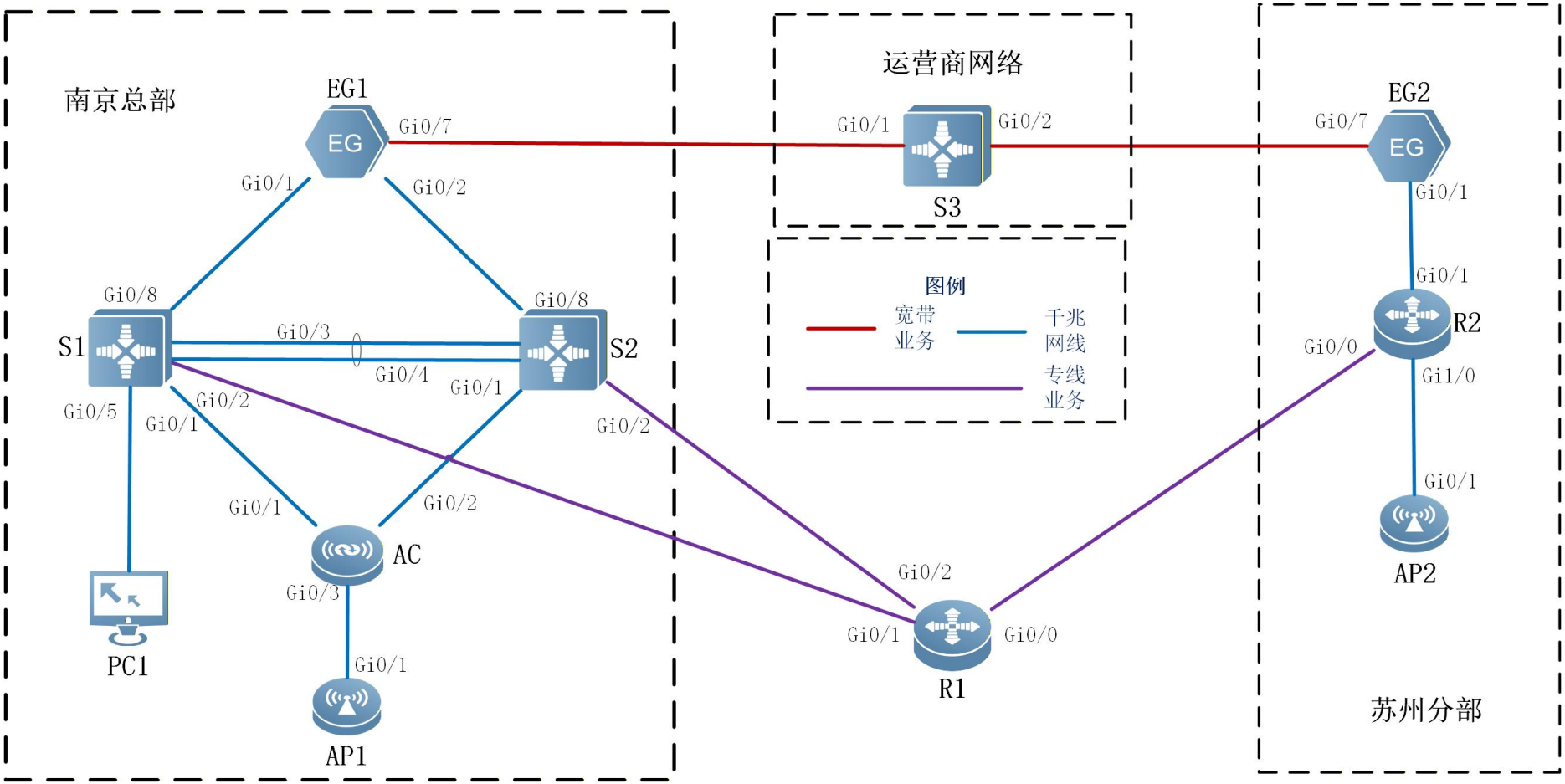
2.AP1、AP2 均为瘦 AP 分别与 AC 建立隧道，AC 提供无线管理服务；

（四）出口网络配置

1.出口 EG1、EG2 上进行 NAT 配置，实现机构内网终端及服务器，均可访问互联网，通过 NAPT 方式将内网 IP 地址转换到互联网接口上。

2.在 EG1 与 EG2 出口网关之间启用 GRE 功能。

拓扑图


南京总部
EG1
EG
Gi0/7
Gi0/1
Gi0/2
运营商网络
Gi0/1
Gi0/2
S3
EG2
Gi0/7
EG
Gi0/1
Gi0/1
R2
Gi0/0
Gi1/0
Gi0/1
AP2
图例
宽带业务
千兆网线
专线业务
Gi0/8
S1
Gi0/3
Gi0/4
Gi0/8
S2
Gi0/1
Gi0/5
Gi0/2
Gi0/1
Gi0/2
Gi0/1
Gi0/2
AC
Gi0/3
Gi0/1
PC1
AP1
Gi0/2
Gi0/1
Gi0/0
R1
苏州分部

地址规划表

设备	接口或 VLAN	VLAN 名称	二层或三层规划	说明
S1	VLAN 10	Production	192.168.10.252/24	生产网
	VLAN 20	Office	192.168.20.252/24	办公网
	VLAN 50	APManage	192.168.50.252/24	AP 管理网
	VLAN 60	APuser	192.168.60.252/24	AP 用户网
	VLAN 100	Manage	192.168.100.252/24	有线管理网
	Gi0/2		10.3.0.1/30	级联 R1
	Gi0/8		10.1.0.1/30	级联 EG1
	LoopBack 0	\	11.1.1.31/32	回环接口
S2	VLAN 10	Production	192.168.10.253/24	生产网
	VLAN 20	Office	192.168.20.253/24	办公网
	VLAN 50	APManage	192.168.50.253/24	AP 管理网
	VLAN 60	APuser	192.168.60.253/24	AP 用户网
	VLAN 100	Manage	192.168.100.253/24	有线管理网
	Gi0/2		10.3.0.5/30	级联 R1
	Gi0/8		10.1.0.5/30	级联 EG1
	LoopBack 0	\	11.1.1.32/32	回环接口
S3	Gi0/1	\	202.1.0.2/30	级联 EG1
	Gi0/2	\	202.2.0.2/30	级联 EG2
EG1	Gi0/1	\	10.1.0.2/30	级联 S1
	Gi0/2	\	10.1.0.6/30	级联 S2
	Gi0/7	\	202.1.0.1/30	级联 S3
	Tunnel 0	\	11.1.5.1/30	GRE
	LoopBack 0	\	11.1.1.11/32	回环接口
EG2	Gi0/1	\	10.2.0.2/30	级联 R2
	Gi0/7	\	202.2.0.1/30	级联 S3
	Tunnel 0	\	11.1.5.2/30	GRE
	LoopBack 0	\	11.1.1.12/32	回环接口
R1	Gi0/1	\	10.3.0.2/30	级联 S1
	Gi0/2	\	10.3.0.6/30	级联 S2
	Gi0/0	\	10.3.0.10/30	级联 R2
	LoopBack 0	\	11.1.1.1/32	回环接口
R2	Gi0/0	\	10.3.0.9/30	级联 R1
	Gi0/1	\	10.2.0.1/30	级联 EG2
	VLAN 50	APManage	172.16.50.254/24	AP 管理网
	VLAN 60	APuser	172.16.60.254/24	AP 用户网
	LoopBack 0	\	11.1.1.2/32	回环接口
AC	VLAN 10	Production	\	生产网
	VLAN 20	Office	\	办公网

设备	接口或 VLAN	VLAN 名称	二层或三层规划	说明
	VLAN 50	APManage	\	AP 管理网
	VLAN 60	APuser	\	AP 用户网
	VLAN 100	Manage	192.168.100.1/24	有线管理网
	LoopBack 0	\	11.1.0.172/32	回环接口

模块 D 网络服务与系统运维（Windows、Linux）

选手根据任务要求，完成 Windows 系统、linux 系统运维服务，并完成相应服务配置。

一、完成 WINDOWS 系统运维服务：

Windows 虚拟机信息表：（系统为：windows 2022 或者 windows 2025）

虚拟机名称	vcpu	内存	磁盘	IPv4 地址	主机名称
Windows1	4	4096MB	100GB	10.0.0.101/24	Windows1
Windows2	4	4096MB	100GB	10.0.0.102/24	Windows2
Windows3	4	4096MB	100GB	10.0.0.103/24 10.0.1.103/24 10.0.2.103/24	Windows3

（1）、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 activedirectory 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 activedirectory 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。

（2）、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。

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 10 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。

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。

（3）、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。

（4）、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 dotnetclrv4.0，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。客户端访问时，必需有 ssl 证书。

网站目录为 C:\web\index，默认文档 index.aspx 内容为"HelloUser"享。

二、完成 linux 系统运维服务

虚拟机名称	vcpu	内存	磁盘	IPv4 地址	主机名称
linux1	2	4096MB	100GB	10.4.1.101/24	linux1
linux2	2	4096MB	100GB	10.4.1.102/24	linux2
linux3	2	4096MB	100GB	10.4.1.103/24	linux3

Linux 虚拟机信息表：

（1）、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，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 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 5 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。

（2）、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、linux3 作为 ansible 的受控节点。

（3）、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。

（4）、任务描述：请采用 samba 服务，实现资源共享。

在 linux3 上创建 vip00-vip19 等 20 个用户；vip00 和 vip01 添加到 manager 组，vip02 和 vip03 添加到 dev 组。 把用户 vip00-vip03 添加到 vsftp 用户。

配置 linux3 为 ftp 服务器 ,建立 ftp 主目录/srv/shareftp，。manager 组用户对 shareftp 有读写权限，dev 组对 shareftp 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 ftp 命令测试。

（5）、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 5555 端口到容器的 80 端口，在容器内安装 httpd，默认网页内容为“HelloUser”。

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。

模块 E 秘密挑战（信息安全、网络系统故障排除）

一、信息系统安全

选手根据任务要求，完成 Windows 系统应急响应、linux 系统应急响应、网络流量分析、WEB 安全渗透测试。

（1）、Linux 系统应急响应

任务描述：A 集团站点遭到攻击，你现在是一名安全服务工程师，请登录系统进行应急响应排查，找出黑客攻击站点的痕迹以及相关漏洞信息。

1.将攻击者使用的跳板机 IP 以及攻击的服务作为 flag 提交，提交格式：flag{IP,小写服务名}

2.将攻击者的公网 IP 作为 flag 提交，提交格式：flag{******}

3.将攻击者的后门首次执行的时间作为 flag 提交,以系统时区为主，提交格式：flag{2026/02/16 23:59:59}

4.将攻击者创建的后门用户名及密码作为 flag 提交，提交格式：flag{用户名/密码}

5.将攻击者留下的后门程序的 md5 值作为 flag 提交，提交格式：flag{******}

6.将攻击者留下的后门程序的连接密码作为 flag 提交，提交格式：flag{******}

（2）、网络流量分析

任务描述：A 集团 FTP 服务器被黑客攻击，请借助 Wireshark 对攻击流量包进行分析，来查找黑客留下的蛛丝马迹，还原攻击现场。

1 将黑客的 IP 地址作为 flag 提交,提交格式:flag{127.0.0.1}

2.将黑客扫描到开放的端口按照从小到大的顺序作为 flag 提交,提交格式:flag{port1,port2,port3}

3.将黑客真实的浏览器指纹(User-Agent)作为 flag 提交,提交格式:flag{*/* (***;***)} 截止到()结束部分。

4.将黑客目录扫描到的第一个响应状态码为 200 的请求的响应时间（UTC 时区）作为 flag 提交,提交格式:flag{2026/Feb/16 23:59:59}

5. 将黑客登录后台的账户密码作为 flag，提交格式:flag{username/password}

6.将黑客从服务器中获取的 flag 作为 flag 提交，提交格式:flag{******}

7.将服务器的操作系统名称作为 flag 提交，提交格式:flag{*******}

（3）、WEB 安全渗透测试

任务描述：你是一名网络安全服务工程师，现在需要你对 A 集团网站进行安全防护，找出其中的漏洞点。

1.通过信息收集,获取站点存在的 flag1，提交格式： flag{****}；

2.将数据库中存在 flag2 值进行提交，提交格式： flag{***}；

3.将后台中存在的 flag3 值进行提交，提交格式：flag{*******}；

4.查看服务器根目录下的 flag4 内容，提交格式：flag{*******}；

5.将 root 目录下的 flag 文件内容作为 flag5 进行提交，提交格式：flag{*********}；

二、网络故障排错

某中型科技公司在南京设有企业总部（Corporate Headquarters），并在苏州设立了分支机构（Branch Company），为满足跨地域协同办公需求，计划搭建一套稳定、冗余的企业内部网络，整体网络按标准企业三层架构规划部署，由 IT 人员完成设备连线与基础配置后，进行全网业务测试，测试过程中出现多处网络异常故障，现需要排错人员从零开始逐层排查网络拓扑、设备互联、VLAN 规划、网关配置、地址分发、跨网互通及外网访问等问题，修复所有故障，使全网恢复正常业务运行

故障现象：

1、分公司内网电脑无法自动获取 IP 地址，只能手动设置静态 IP 才能上网和内网互访，请检查网络配置，将修改部分做为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}

2、分公司内网用户可以访问内网网关，但是无法访问外网（ping 分公司路由器外网口地址），请检查网络配置，将修改部分做为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}。

3、分公司内网用户无法访问总公司路由器外网口地址，请检查网络配置，将修改部分做为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}。

4、总公司两台核心交换机一直在报错误信息，请检查网络配置，将修改部分作为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}。

5、总公司为了业务冗余配备了两台核心交换机，HO-Core-SW-2 为主设备 HO-Core-SW-3 为从设备，配置完成后发现设备运行状态有问题，请检查网络配置，将修改部分作为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}。

6、总公司业务部分无法自动获取 IP 地址，请检查网络配置，将修改部分做为 flag 提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名 1:修改内容|设备名 2:修改内容}。

7、总公司销售部门发现即使获取到 IP 地址后还是无法访问互联网，请检查网络配置，将修改部分做为 flag 提交。如涉及到多项内容，中间

用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名1:修改内容|设备名2:修改内容}。

8、为了测试总公司网络冗余性，将HO-Core-SW-2断电后发现，总公司办公部门无法访问互联网，将修改部分做为flag提交。如涉及到多项内容，中间用“|”分隔，提交格式：flag{***|***}；填写顺序按设备末尾序号。参考格式：flag{设备名1:修改内容|设备名2:修改内容}。