

第八届江苏技能状元大赛信息通信网络 运行管理（学生组）项目技术文件

第八届江苏技能状元大赛组委会技术工作组

2026 年 5 月

目录

一、 技术描述	3
(一) 项目概要	3
(二) 基本知识与能力要求	3
二、 试题与评判标准	11
(一) 试题内容	11
(二) 评判标准	12
三、 竞赛细则	16
(一) 赛程安排	16
(二) 裁判员分组和职责	16
(三) 赛场管理制度	17
(四) 技术违规处理	19
(五) 问题或争议处理	21
四、 竞赛场地、设施设备等安排	21
(一) 赛场规格要求	21
(二) 场地布局图	22
(三) 基础设施清单	23
五、 安全、健康要求	31
(一) 赛场人员安全要求	31
(二) 场地设备安全要求	31
(三) 赛事安全要求	32
(四) 开放赛场要求	33

(五) 绿色环保要求	33
六、试题公布说明	34
七、附件：样题	35

一、技术描述

（一）项目概要

本赛项以《信息通信网络运行管理员》职业标准为依据，面向为大中小型商业组织及政府部门提供 IT 服务、保障网络系统稳定运行的从业人员，重点考察选手网络系统架构、实施、运维、网络信息系统安全、渗透与防护、技术支持及建议指导等综合应用能力。

（二）基本知识与能力要求

本竞赛是对信息通信网络运行管理项目相关技能的展示与评判，选手需掌握操作所必备的理论知识，具有相应的知识水平，包括网络系统架构、实施、运维、网络信息系统安全、渗透与防护、技术支持等。该项目不涉及理论考试，只进行实际操作竞赛。参加信息通信网络运行管理项目竞赛的选手，应具备的知识和能力要求如下表：

相关要求		权重比例(%)
1	职业素养与团队合作	5%
基本知识	参赛选手需知道并了解： ——健康与安全规程、义务、条例及文件 ——需使用个人防护装备的情况，例如：ESD(静电放电) ——当在某些领域因缺少经验或知识而出现问题时，能向同伴提出援助请求 ——保证用户设备和信息完整及安全的重要性 ——废物处置及循环利用安全的重要性 ——规划，调度及设置优先等级的技术	

相关要求		权重比例(%)
工作能力	<ul style="list-style-type: none"> —精确度，校验以及注意细节对所有实践工作的重要性 —系统性地进行操作工作的重要性 —沟通及研究的方法和技巧 —管理自身专业发展的价值 —IT 系统变更的速度以及保持信息流通的需求 —聆听在有效沟通中的重要性 —同伴的角色和要求，以及最有效的沟通方式 —构建和维持与同事及管理者之间富有成效的工作关系的重要性 —有效的团队工作技巧 —消除误会和争执的技巧 —在管理紧张和愤怒的气氛过程中来解决困难处境 	
	<p>—参赛选手应能：</p> <ul style="list-style-type: none"> —遵守健康及安全标准，规则及规章 —保持一个安全的工作环境 —确定及使用合适的个人静电放电防护装备 —安全地选择，使用，清洁，维持并保存工具及设备 —把工作区域规划好使其发挥最大作用，做好定期整理工作。 —根据优先顺序表，定期计划，重新计划及多任务组织 —有效地工作并定期检查过程和成果 —密切关注最新“实操执照”要求及保持信息流通 —始终运用周密而有效的研究方法来支持知识的增长 —保持对新方法，技术的热诚以及致力于促进改变 —能与同伴有效地合作，并把工作效率和学习能力发挥到最大 —以项目团队成员的身份，有效地进行工作 	

相关要求		权重比例(%)
	<ul style="list-style-type: none"> —通过强大的聆听及提问技巧来加深对复杂环境的理解 —管理与同事间持续有效的口头和书面交流 —认识及适应同伴不断变更的需求 —积极主动地为强大及有效率的团队做出贡献 —与同事们分享知识及专业资料，从而发展相互支持的学习环境 —通过有效地管理紧张/愤怒，给予他们能够解决问题的信心 	
2	数据中心网络搭建（网络链路安装）	
基本知识	<p>参赛选手需知道并理解：</p> <ul style="list-style-type: none"> —综合布线系统的组成及各子系统功能（工作区子系统、水平子系统、垂直干线子系统、设备间子系统、管理子系统、建筑群子系统、进线间子系统） —常用布线材料的特性及适用场景，例如：双绞线（超五类、六类、七类）、光纤（单模、多模）、配线架（超五类、六类、七类）、跳线（铜缆、光缆）、信息插座、网络模块、铜缆端接器、光纤适配器、线槽、线管、桥架等。 —综合布线的相关行业标准及规范，例如：TIA/EIA-568、GB50311-2016《综合布线系统工程设计规范》 —布线环境的影响因素，例如：温度、湿度、电磁干扰、物理防护，以及不同场景（办公区、机房、室外）的布线要求 —布线系统的传输性能指标，例如：衰减、串扰、回波损耗，以及如何保障传输质量 —综合布线与网络设备、终端设备的适配原则，以及布线系统与网络架构的衔接逻辑 —布线施工中的安全规范，以及预防施工过程中损坏线缆、设备或 	15%

相关要求		权重比例(%)
	<p>造成安全隐患的方法</p> <p>—布线系统的测试标准、测试工具及测试流程，以及测试结果的解读方法</p> <p>—布线系统的归档要求，包括布线图纸、各类表格、材料清单、测试报告、施工记录的整理与留存的重要性</p>	
工作能力	<p>参赛选手应能：</p> <p>—根据用户需求、场地条件及行业规范，设计合理的综合布线方案，明确各子系统的布局、线缆选型及路由规划</p> <p>—结合客户预算，选择性价比高的布线材料及设备，提供合理的成本预估及优化建议</p> <p>—按照施工规范及设计方案，规范执行布线施工操作，包括线缆敷设、端接、跳线制作、配线架安装及固定等</p> <p>—使用专业测试工具（如网络线缆测试仪）对布线系统进行全面测试，排查并解决传输性能异常、接触不良等问题</p> <p>—针对不同场景（如高密度办公区、机房、室外远距离传输），调整布线策略，规避电磁干扰、物理损伤等风险</p> <p>—与用户、同伴及管理者沟通布线方案的细节，听取意见并优化方案，达成一致共识</p> <p>—规范整理布线施工过程中的各类记录，包括施工日志、材料使用清单、测试报告等，完成归档工作</p> <p>—对已完成的布线系统进行验收准备，配合用户及相关人员完成验收工作，获取验收认可并记录</p> <p>—识别布线系统中的潜在隐患，提出维护及优化建议，确保布线系统的稳定性和可扩展性</p>	

相关要求		权重比例(%)
	<ul style="list-style-type: none"> —根据设备升级、网络扩容需求，对现有布线系统进行改造、扩展，保障与新设备、新网络架构的兼容 —依据施工图，完成网络设备的规范安装，如吸顶式 AP、面板式 AP 等。 	
3	数据中心网络搭建（网络设备连接与调试）	
基本知识	<p>参赛选手需知道并理解：</p> <ul style="list-style-type: none"> —网络环境 —网络协议例如：IPv6 —根据客户要求完成网络服务 —构建网络的过程，以及如何配置能增加有效交流的网络设备的方法 —网络设备的工作范围。例如：路由器，VoIP，IP 设备，无线接入口，内部网络连接 —预防在操作设备上增添服务后因改变网络配置而引起的问题 —对最终的配置设置（必要的及所有）进行归档的重要性 	20%
工作能力	<p>参赛选手应能：</p> <ul style="list-style-type: none"> —根据行业认证要求，解释用户需求及设计要求 —根据所要求的流程进行工作，以完成配置 —为达到客户要求，选择合适的服务 —在所可能在网络环境出现的网络设备上，例如：路由器协议，网络安全，Wi-Fi，VoIP 等等设计并执行灾难恢复流程 —与相关人员讨论解决方案，并达成一致。例如：用户、同伴及经理 —保留配置记录 	

相关要求		权重比例(%)
3	网络服务与系统运维（Windows、Linux）	30%
基本知识	<p>参赛选手应知道并理解：</p> <ul style="list-style-type: none"> —操作系统使用范围及满足用户特殊需求的能力，给予客户预算指引 —为不同种类的硬件选择合适的驱动器的过程 —硬件的基础功能以及组装的过程 —听从指令的重要性及不听从指令的后果/代价 —预防措施：安装及升级前的注意事项 —安装完成后或升级后文件编制的目的 	
工作能力	<p>参赛选手应能：</p> <ul style="list-style-type: none"> —仔细倾听，转化及准确地认识用户的需求以达到用户期望 —选择操作系统：专用/开源，参照客户成本预估购买的总成本 —为满足用户/生产商的需求，确定正确的硬件及合适的软件驱动 —为了获得最新的“工作流程”，不断地核实生产厂商的指引 —选择操作系统/服务器系统的角色及/或特性例如：活动目录域服务（角色）及 Windows 服务器备份（特性） —与相关人员讨论并确定角色/特性的初步概念，例如：用户，同事及管理者 —准备一份能反映该解决方案的细则的技术文档，签名以示同意 —根据生产厂商的指引或者组织的最佳实践结果配置合适的角色/特性 —测试并改正所有的问题，若有需要，进行重新测试 —获得用户的认可和记录 	

相关要求		权重比例(%)
4	秘密挑战（信息安全、网络系统故障排除）	
基本知识	<p>参赛选手需知道并理解：</p> <ul style="list-style-type: none"> —信息系统安全保障的核心原则（保密性、完整性、可用性、可控性、可审查性）及核心范畴 —常见网络安全威胁及攻击方式，例如：病毒、木马、勒索软件、DDoS 攻击、SQL 注入、跨站脚本（XSS）、网络钓鱼等 —网络安全相关法律法规及行业标准，例如：《网络安全法》《数据安全法》《个人信息保护法》、等保 2.0（网络安全等级保护） —网络安全防护技术及设备的工作原理，例如：防火墙、入侵检测/防御系统（IDS/IPS）、VPN、杀毒软件、数据加密、访问控制等 —网络安全风险评估的基本流程、方法及核心指标，以及风险防控的基本思路 —数据安全保护的相关要求，包括数据收集、存储、传输、使用、销毁全流程的安全规范 —网络安全应急响应的基本流程，以及常见安全事件的处置原则 —网络设备、服务器、终端设备的安全配置要点，以及默认配置的安全隐患 —网络安全日志的作用、收集方法及分析要点，以及安全记录归档的重要性 —人员安全管理的基本要求，包括权限分配、密码管理、安全培训及保密规范 —冷静及专心的问题解决方式的重要性 —IT 系统的意义，个人的依赖性及公司的持续可用性 —常见的硬件/软件/布线/系统错误类型 	30%

相关要求		权重比例(%)
	<ul style="list-style-type: none"> —诊断式和分析式的问题解决方法 —个人知识/技能/职权的界线，以及支持/程序升级的起源 —常见问题的标准解决时间 	
工作能力	<ul style="list-style-type: none"> —根据信息系统的规模、用途及行业规范，识别网络安全风险，制定合理的网络安全保障方案 —配置各类网络安全设备（防火墙、IDS/IPS、VPN等），优化安全策略，防范各类网络攻击 —对网络、服务器、终端设备进行安全检测，排查安全漏洞，及时进行补丁更新和漏洞修复 —实施数据安全保护措施，包括数据加密、备份与恢复，确保数据的保密性和完整性 —执行网络安全风险评估，撰写风险评估报告，提出针对性的风险防控建议并落地实施 —处理常见网络安全事件（如病毒感染、网络入侵），启动应急响应流程，降低安全事件造成的损失 —规范配置网络设备及终端的安全参数，管理用户权限，落实密码安全管理要求 —收集、分析网络安全日志，识别异常行为，排查安全隐患，形成安全分析报告并归档 —与用户、同伴及管理者沟通网络安全保障方案，解读安全规范，达成共识并推动方案落地 —定期开展网络安全自查，更新安全防护策略，适应新型网络威胁，保障信息系统长期安全稳定运行 —在解决问题时，拥有能使用户们冷静下来的信心 	

相关要求		权重比例(%)
	—定期检查工作以预防/减少后期阶段的问题 —质疑不正确的信息以预防/减少问题 —在处理问题时表现出顺应力及毅力 —快速地认识并理解问题，能自我解决问题及管理过程。 —对于复杂的问题/情况能进行彻底地研究及分析，并进行故障探测 —选择并使用诊断软件和工具以发现问题 —通过简易、指引及指导的方式引导用户解决问题 —必要时寻求专家帮助，防止问题损耗后果 —当问题解决后检查用户满意程度 —准确地记录问题并提供解决报告	
合计		100

二、试题与评判标准

（一）试题内容

1. 试题简介

项目参考国家职业技能标准（三级/高级工以上），借鉴中华人民共和国第三届职业技能大赛网络系统管理（国赛精选）项目的相关内容，结合信息通信网络系统管理行业企业新技术和新需求的基础上进行设计。

竞赛只进行技能实操，涉及数据中心网络搭建(网络链路安装)、数据中心网络搭建(网络设备连接与调试)、网络服务与系统运维(Windows、Linux)、秘密挑战(网络故障排除、网络故障排错)4个部分，根据赛题要求，对竞赛现场环境的网络服务项目进行分析、设计、连接、配置、调试、故障排查及解决；对服务器和客户端进行相应配置，解决故障，实现互联互通。

2. 竞赛模块

模块编号	模块名称
------	------

A	职业素养与团队合作
B	数据中心网络搭建（网络链路安装）
C	数据中心网络搭建（网络设备连接与调试）
D	网络服务与系统运维（Windows、Linux）
E	秘密挑战（信息安全、网络系统故障排除）

3. 样题及赛题变化

信息通信网络运行管理竞赛项目遵循公平、公正原则，命题流程借鉴样题公开的命题方式，采取以下方式确定并公布样题：本赛项样题将随技术文件公布，公布后，裁判长组织各参赛队围绕命题思路、关键考核要点等进行讨论，对提出的问题及时解答，吸收合理的意见建议，并作相应修改。正式赛题在样题的基础上有不超过 30%的改动。

（二）评判标准

1. 竞赛试题配分

（1）竞赛方式

本赛项采用 2 人组队的比赛模式，通过阅读赛场提供的任务书（赛题）明确竞赛内容，完成模块

A：职业素养与团队合作

B：数据中心网络搭建（网络链路安装）；

C：数据中心网络搭建（网络设备连接与调试）；

D：网络服务与系统运维（Windows、Linux）；

E：秘密挑战（信息安全、网络系统故障排除）。

（2）竞赛内容

本次竞赛（各模块）难度等级应等价（包含）于以下认证水平：

信息通信网络运行管理员（技师）；

信息通信网络线务员（技师）

参赛选手需按要求完成以下 5 项任务。

模块 A：职业素养与团队合作

考核选手节约耗材、规范施工的能力，主要考核网络线缆、模块、跳线、施工材料和工具的合理使用、减少浪费；设备规范操作、无损坏，物品与工具摆放合规等方面。安全包括网络设备安全、用电安全和人身安全，违规操作或发生安全事故将按评分细则扣分；团队具备出色的协作能力，能高效沟通、情绪稳定、主动分享与担当，充分发挥自身效能，助力打造互信互助、高效协同的团队；卫生包括竞赛工位场地、设备表面及周边环境的清洁，存在垃圾、余料、污渍、设备摆放等情况。

模块 B：数据中心网络搭建（网络链路安装）

选手根据提供的网络布线设计图、施工规范及相关材料，完成工作区子系统、配线子系统、干线子系统、管理间子系统、设备间子系统等区域的布线施工，包括设备和材料安装，线缆的敷设、捆扎、端接、测试，标识制作，信息点安装、跳线制作与测试，确保布线规范、连接可靠，满足网络传输性能要求。

模块 C：数据中心网络搭建（网络设备连接与调试）

选手根据数据中心网络架构设计要求，完成交换机、路由器、防火墙等网络设备的部署、连线与配置，搭建 VLAN、路由协议、链路聚合等核心网络功能，实现数据中心内部网络互联互通及与外部网络的安全对接，保障网络架构稳定高效。

模块 D：网络服务与系统运维（Windows、Linux）

选手根据任务要求，完成服务器、网络设备、终端设备及各类应用程序的日常运维工作，包括设备状态监测、故障排查与修复、系统参数优化、数据备份与恢复，

确保信息系统持续、稳定、安全运行。

模块 E：秘密挑战（信息安全、网络系统故障排除）

选手根据信息安全防护要求，完成网络安全配置、网络安全运维、网络安全攻击与防护，排查系统安全漏洞，防止网络攻击、数据泄露等安全风险，保障信息系统及数据的保密性、完整性和可用性。

选手在网络环境下的综合分析和故障排除能力。主要内容包括 VLAN、STP 和 V LAN 间路由、VOIP、VRRP、静态路由、RIP、OSPF、BGP 等路由协议、多路由协议共存、IPv4.Ipv6 地址规划、NAT、NAT64 的使用、访问控制列表的使用，多种形式的 VPN、网络安全等故障排除；选手须根据故障现象找出故障点，利用结构化理论方法进行故障点分析，制定故障排除解决方案，自行设定步骤进行故障排除，使服务器能正常提供相应服务。

分数权重，详见表 2-1。

表 2-1 竞赛模块分数权重表

模块 编号	模块名称	配分			评价方式
		评价分	测量分	总计	
A	职业技能素养	5	0	5	评价
B	数据中心网络搭建（网络链路安装）	0	15	15	测量
C	数据中心网络搭建(网络设备连接与调试)	0	20	20	测量
D	网络服务与系统运维（Windows、Linux）	0	30	30	测量
E	秘密挑战（信息安全、网络系统故障排除）	0	30	30	测量

总计	5	95	100	
----	---	----	-----	--

2.成绩计算方式

本项目采用 100 分制，各个评分项的分数应精确到小数点后一位，各任务原始成绩直接相加即为参赛选手最终竞赛成绩。

3.评判方法

（1）测量评分（客观）

测量评分时每个评分项除非另有说明，只能给予满分或 0 分。如果需要使用 0 分到满分之间分数，该项中应有清晰的解释说明。

举例：测量分评分准则样例如表 2-2 所示。

表 2-2 测量分评分准则样例表

示例	最高分值	正确分值	不正确分值
网络策略配置成功生效	1	1	0
网络策略配置成功生效	1	1	0

（2）评判方法（主观）

竞赛开始的前 1 天（C-1），各参赛队伍按照裁判长的安排进行裁判分组。每个小组的裁判只对裁判长分配指定的对应模块及指定的评分项进行评分，评判的过程完全按照评分标准进行测量分评分。

为确保评分过程的公平性和公正性，评分过程采取回避制度，裁判执裁过程中不能与自己的选手进行任何交流，评分过程中不参与自己选手的评分。无相应模块（评分项）执裁任务的裁判不得进入选手工位，不得干扰和影响其他裁判的执裁工作。

裁判长和裁判长助理原则上不参与评分。

4.成绩并列

按比赛总成绩从高到低排列参赛人员的名次。如遇比赛总成绩相同则由模块 E 成绩高低进行排序，如果成绩还是相同，则依次由模块 D、模块 C、模块 B、模块 A

模块成绩同理决定排名。如果仍然相同则按照模块 E 完成的时间短者为优进行判定。

三、竞赛细则

（一）赛程安排

比赛在 3 天内进行，赛项竞赛时间为 6 小时，具体安排如下：

表 3-1 竞赛实施安排

竞赛日期	竞赛时间	工作内容	参与人员
C-1	全天	裁判、选手报到	参赛选手、裁判员
C-1	全天	裁判员技术培训、选手熟悉场地	参赛选手、裁判员、裁判长、裁判长助理、场地经理、技术
C-1	全天	选手技术培训，熟悉场地、抽签、分组	参赛选手、裁判员、裁判长、裁判长助理、技术支持人员
C1	上午 (8:30-11:30)	模块 A、B、C、D 考核	裁判长、助理、项目裁判员、参赛选手
C1	下午	裁判 A、B、C、D 模块评分	裁判长、助理、项目裁判员
C2	上午 (8:30-11:30)	模块 A、E 考核	裁判长、助理、项目裁判员、参赛选手
C2	下午	裁判 A、E 模块评分 宣布成绩、技术点评	裁判长、助理、项目裁判员、参赛选手、指导老师

注：以上竞赛日程仅供参考。竞赛开始前或将根据实际情况做适当调整。以竞赛现场公布的时间表为准。

（二）裁判员分组和职责

本次竞赛设立裁判组，裁判组由裁判长 1 名、裁判长助理 1 名和若干名裁判员组成。裁判长负责组织全体裁判员（含裁判长助理）做好赛前技术准备及竞赛各环

节的技术工作，组织本项目开展技术总结和技术点评。裁判长助理协助裁判长组好执裁各项组织工作，完成裁判长安排的相关任务。裁判组接受竞赛组委会的领导。

1.裁判长

裁判长按照本项目技术文件，对裁判员进行培训和工作分工，带领裁判员对本项目比赛设备设施和现场布置情况进行检验；组织选手进行安全培训并熟悉赛场及设备，保障所有选手在比赛前掌握必备的安全知识和安全操作规范；比赛期间组织裁判员执裁，并按照相关要求和程序，处理项目内出现的问题；组织统计、汇总并及时录入大赛成绩等工作；赛后组织开展技术点评。裁判长应公平公正组织执裁工作，不参与评分。

2.裁判员

裁判员由各代表队择优推荐，每个参赛队限推荐1名裁判员。经省组委会技术工作组审核确定后承担裁判员执裁工作。全部裁判工作均采取回避制度，裁判员不对来自同一参赛队的选手进行评判。如裁判员人数不能满足工作需要，由项目裁判长在赛前提出增加裁判员人选申请，由省组委会技术工作组遴选确定后增补。裁判员应服从裁判长工作安排，认真做好本职工作；熟练掌握竞赛技术规则，参加赛前培训和技术讨论；对有争议的问题提出客观、公正、合理的意见和建议；公平公正执裁，不徇私舞弊；坚守岗位，严格遵守执裁时间安排，保证执裁工作正常进行。

3.工作人员

包括技术支持人员、录分员及赛务保障人员等。按照大赛统一要求，在裁判长领导下做好相应的竞赛保障工作。

（三）赛场管理制度

1. 所有参观人员的活动必须在参观通道内，不得进入竞赛区域；

2. 现场保持安静，不得大声交谈及喧哗；
3. 现场参观允许拍照，严禁使用闪光灯，赛场内部禁止拍照（如需拍照由裁判长指定人员进行）；
4. 竞赛开始前选手根据赛场情况可以熟悉比赛工位和设备。如需携带工具，需在规定时间内将自带工具经裁判检验后放入指定场所进行存放，比赛日禁止带任何工具、设备入场；
5. 在比赛前选手可以在工位内准备自己的物品和工具，在裁判宣布比赛开始前禁止触碰竞赛设备或开启电源，否则做扣分处理；
6. 竞赛期间选手禁止携带拍照、存储及通信设备，如带到赛场，需要交给本单位场外人员保管或由赛场工作人员集中保管；
7. 正式比赛开始前，选手可以对试题表述方面提问，过程中禁止与裁判员或其他选手进行一切形式的交流；
8. 选手必须在任务区内对题目进行仔细审核，如有问题及时向现场裁判反映，由裁判长决定是否修改或调整题目，如有修改必须对所有参赛队公示说明，比赛开始后选手禁止提出针对题目的疑义或建议；
9. 选手上交的电子文档由工作人员用赛场指定 U 盘进行拷贝传递或指定网络上传，比赛成果由工作人员打印并由选手确认签字；
10. 各参赛单位场外人员在竞赛过程中严禁与任何选手交谈或作出任何提示、影响、干扰行为，如被发现将相应扣除当事人所在参赛队的成绩；
11. 题目下发后比赛开始前，禁止裁判员与选手做任何形式的交流与沟通，仅限于选手与裁判长指定人员的公开问答形式；
12. 竞赛期间，选手需要通过提示牌与现场裁判进行应答或举手交流，本代表

队裁判需要回避，由其他代表队裁判员前去处理；

13. 比赛期间，本代表队的裁判与选手禁止任何形式的交流；

14. 场内现场裁判执裁过程中，除选手示意禁止主动进入选手工位内，如需要裁判进入工位必须 2 名以上非选手市裁判同时前往处理；

15. 选手如怀疑设备问题，可向裁判示意，并选择两种处理方式：1 是技术工作人员检查设备时同时工作，不予补时，2 是离开工位让技术工作人员检查设备，如是设备问题给予相应补时，如设备无恙则不予补时；

16. 严禁在竞赛过程中向赛场内传递任何物品，如有需要必须经过现场裁判确认后由裁判转交；

17. 在相关操作过程中，选手需要佩戴必要的防护用品,禁止做违规操作；

18. 竞赛现场发布的试卷禁止带出场外，竞赛结束后由现场裁判统一收回存档；

19. 竞赛过程中除记者外，禁止定点长期摄像及逗留；

20. 竞赛现场任何位置严禁吸烟；

21. 其他未尽事宜，参照世界技能大赛相关标准要求。

（四）技术违规处理

1.不得携带其他未经组委会认可的设备、工具、机具、材料等参赛，不听劝告的取消比赛资格。

2.竞赛过程中，选手不得接受场外送进的材料、加工过的半成品等。

3.选手不得损坏、拆卸、改装赛场提供的设备、工具和工作台等设施。

4.选手不得在任何竞赛区域、位置、赛件上作任何涉嫌作弊的标记。如比赛开始前发现有明显痕迹，可上报裁判员进行处理，严重者可按作弊处理。

5.在完成竞赛任务的过程中，因操作不当导致事故，扣 1-5 分，情况严重者取

消比赛资格。

6.因违规操作损坏赛场提供的设备、污染赛场环境等不符合职业规范的行为，视情节扣 1-5 分。

7.扰乱赛场秩序，干扰裁判员工作，视情节扣 1-5 分，情况严重者取消比赛资格。

8.在完成竞赛任务的过程中，有不符合职业规范的行为，因操作不当导致事故，依据表 3-2 进行扣分。

表 3-2 违规扣分参考表（此表应该和后面的评分表保持一致）

序号	考核内容		扣分标准	扣分情况
1	操作规范不符合要求	布线时线缆敷设用力过猛导致线缆破损、断裂	0.5 分/次	
2		运维时误操作删除系统文件、修改关键参数，导致系统无法正常运行	3 分/次	
3		设备通电前未检查线路，导致设备短路、损坏	1 分/次	
4		操作过程中人为干预设备正常运行（如强行断电、损坏设备等）	1 分/次	
5	工艺不符合要求	网络设备固定不牢固，摆放在地上。	0.5 分/处	
6		工具和耗材应发放在机柜底座上，把放在其他位置的。	0.5 分/处	
7	违反赛场纪律扰乱赛场秩序	裁判长发出开始比赛指令前提前操作	1 分/次	
8		不服从裁判指令、顶撞裁判	1 分/次	
9		裁判长发出结束比赛指令后，继续操作	1 分/次	
10		选手签名时，使用真实姓名或具体参赛队信息	取消比赛资格	
11		擅自离开本参赛队赛位，未向裁判报备	取消比赛资格	
12		与其他赛位选手交流、传递物品，泄露赛题相关信息	取消比赛资格	
13		裁判长发出开始比赛指令前提前操作	取消比赛资格	

（五）问题或争议处理

大赛期间，与竞赛有关的问题或争议，各方应通过正当渠道并按程序反映和申诉，不得擅自传播、扩散未经核查证实的言论、信息。对竞赛期间出现的问题或争议按以下程序解决：

1. 竞赛项目内解决。参赛选手、裁判员发现竞赛过程中存在问题或争议，应向裁判长反映。裁判长依据相关规定处理或组织比赛现场裁判员研究解决。处理意见需比赛现场全体裁判员表决的，须获全体裁判员半数以上通过。最终处理意见应及时告知意见反映人，并填写《中华人民共和国第三届职业技能大赛江苏省选拔赛问题或争议处理记录表》。处理期间，执委会技术保障部和组委会技术工作组应给予支持和指导。

2. 监督仲裁组解决。对项目内处理结果有异议的，在参赛选手成绩最终确认锁定前，领队可向监督仲裁组出具署名的书面反映材料并举证。监督仲裁组在执委会监督仲裁协助部协助下受理并开展调查。其中，经调查确认所反映情况属技术性问题的，仍交由竞赛项目内解决。属非技术性问题的，由监督仲裁组作最终裁决。各类问题或争议处理情况，由执委会监督仲裁协助部填写《争议处理记录表》报监督仲裁组备案。

四、竞赛场地、设施设备安排

（一）赛场规格要求

1. 赛场整体规划

赛场内选手工位独立，确保选手正常开展比赛，不受外界影响；工位集中布置，保证竞赛氛围。设置安全通道和警戒线，确保进入赛场的竞赛参观、采访、视察的人员限定在安全区域内活动，以保证大赛安全有序进行。根据赛项流程设置选手集合报到区、选手休息区、技术支持休息区、赛事办公工作（储物）区、录分室、裁判休息交流等区域（如有需要，可再设其他空间）。

2. 竞赛工位规划

竞赛工位：每个工位占地约 3m×4m，标明工位号，并配备网络通信运行管理综合实践平台 1 套、装配桌 1 张、电脑桌 2 张、座椅 2 把、通用虚拟化计算机 2 台（安装了大赛所需的必要软件）。

赛场每工位提供独立控制并带有 3 组断路器保护装置的 220V 单相三线的交流电源（3 组电源分别控制），供电系统有必要的安全保护措施。

3. 竞赛工位规划

照度大于 500Em（lx）。

4. 场地消防和逃生要求

（1）赛场必须留有安全通道。竞赛前必须明确告知选手和裁判员安全通道和安全门位置。

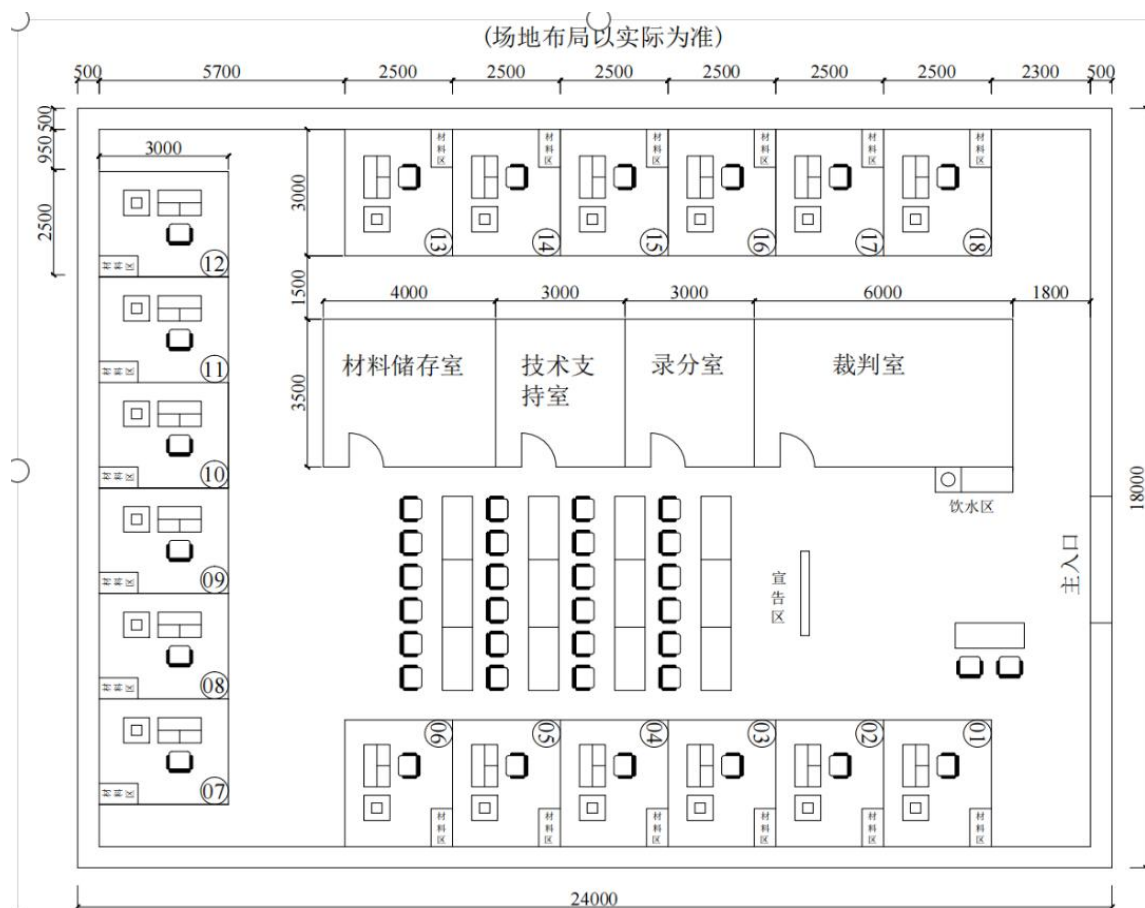
（2）赛场必须配备灭火设备，并置于显著位置。

（3）赛场应具备良好的通风、照明和操作空间的条件。

（4）承办单位应做好竞赛安全、健康和公共卫生及突发事件预防与应急处理等工作。

（二）场地布局图

最终比赛场地以实际场地为主



(三) 基础设施清单

1. 赛场硬件设备

赛场提供设施、设备清单表根据竞赛需要，赛场还需准备如下辅助设施，见表 4-1。

表 4-1 赛场提供的设备工具清单表

序号	名称	型号（备注）	单位	数量
1	竞赛设备	<p>一、数据中心网络搭建（网络链路安装）模块（1 套）</p> <p>1、多功能综合实训机柜（1 套）</p> <p>技术要求：</p> <p>（1）开放式多功能机柜包含：底座（1 个）、侧面板（2 个）、上盖（1 个）、层板（3 个）、布线仿真墙（1 个）、侧面仿真桥架（1 个）、顶部仿真桥架（1 个）、服务器支架（1 个）组成。</p> <p>（2）、开放式多功能机柜上所有螺母必须采用焊接工艺，不得使用拉铆、压铆等工艺。</p> <p>（3）、底座包含进线孔（1 个），地弹式插座安装孔（1 个）。</p>	套	15

序号	名称	型号（备注）	单位	数量
		<p>(4)、侧面板开有 3 种不同的进线孔和卡扣孔，能实现基本布线实训以及设备安装的需求。</p> <p>(5)、机柜上盖开有仿真进线孔，与顶部仿真桥架相连，实现桥架布线入机柜的实训需求。</p> <p>(6)、层板开有过线孔，模拟垂直竖井实训。</p> <p>(7)、布线仿真墙开有进线孔和螺母矩阵。</p> <p>2、大数据链路分析仪（1 台）</p> <p>技术要求：1.物理规格：6U（26.67cm）*19 英寸（48.56cm）机架式，配置 1 个 USB-B 端口、两对 Modbus 接口；</p> <p>测试模块：四组测试模块，每组含 16 个 led 显示灯 + 2 个测试网口，配备 1 个 speed 按钮可切换 led 显示效果；3.提供 4 组 RJ-45 网络端口链路数据分析，同时提供自动上传测试数据，实时监测现场所有设备网络链路安装情况</p> <p>3、综合实训工具箱（1 套）</p> <p>技术要求：配备综合布线全流程常用工具，含压线钳、打线钳、斜口钳、剥线器、线管剪刀等，满足综合布线实训的工具操作需求</p> <p>4、综合布线耗材</p> <p>技术要求：配备综合布线常用耗材，含双绞线、信息点底盒、面板、扎带、线管、标签、模块等，满足竞赛需要。</p> <p>二、数据中心网络搭建（网络设备连接与调试）模块（1 套）</p> <p>1、路由器设备（2 台）</p> <p>技术要求：WAN 口不少于 4 个千兆电口、LAN 口不少于 24 个千兆电口，含电源模块；</p> <p>2、三层可控交换机设备（3 台）</p> <p>技术要求：</p>		

序号	名称	型号（备注）	单位	数量
		<p>千兆电口不少 24 个，万兆光口不少于 4 个，含电源模块；</p> <p>3、网关设备 （2 台）</p> <p>技术要求：</p> <p>千兆电口不少 8 个，含电源模块；</p> <p>4. 无线控制设备（1 台）</p> <p>技术要求：</p> <p>千兆电口不少 8 个，光口不少于 2 个，可管理 AP License 不少于 32 个，含电源模块；</p> <p>5. 无线接入设备 （2 台）</p> <p>技术要求：</p> <p>胖、瘦一体 AP，含 POE 电源模块；</p> <p>三、网络服务与系统运维（Windows、Linux）模块</p> <p>1、信息系统运维服务虚拟化平台 （1 台）</p> <p>技术要求：</p> <p>提供 Windows 和 Linux 虚拟化服务，满足自动化评分，提供 3D 态势分析。提供 Windows 和 Linux 虚拟化服务，适配赛项所需的服务器配置、服务部署等实操需求，支持自动化评分功能，可精准评判选手操作规范性与任务完成度。同时兼容 X86、ARM 架构仿真，能模拟真实运维场景，保障竞赛公平高效，贴合“岗课赛证”融合的竞赛要求，助力赛项实操考核有序开展。</p> <p>四、秘密挑战（信息安全、网络系统故障排除）模块</p> <p>1、信息系统安全保障靶场平台（1 套）</p>		

序号	名称	型号（备注）	单位	数量
		<p>技术要求：</p> <p>支持理论答题，单兵闯关，内网渗透，公有靶场四个资源模块,支持 3D 攻防态势分析等功能，四种比赛模式可独立配置与管理，每个比赛模式下都有比赛管理、赛题管理、比赛关卡、靶机部署、动态展示和成绩查询等。支持 FLAG 自动更新、违规监测、自动扣分等机制。</p> <p>2、网络故障排错系统平台（1 套）</p> <p>支持快速搭建路由交换、无线、安全等典型企业网络拓扑，可批量预设链路中断、配置错误、协议故障、设备异常等网络故障点。提供可视化操作界面，支持故障点自定义、随机下发与分步解锁，适配竞赛与实训不同场景。具备实时监控、操作日志记录、自动评分与成绩导出功能，实现竞赛过程公平、评判高效。</p> <p>3、硬件配置要求（1 台）</p> <p>专用 2U 虚拟化平台，固化业务背板，固化千兆网络接口≥ 2 个，外接 USB 口≥ 2 个；数据及系统硬盘容量配置$\geq 1T$，内存$\geq 64G$；采用双路设计，处理器≥ 1 颗,总内核≥ 20 核心,主频$\geq 2.0GHz$；采用 KVM 虚拟化管理，单台设备虚机并发≥ 30</p>		

序号	名称	型号（备注）	单位	数量
2	通用电脑	CPU：Intel i7 及以上 内存：16G 及以上 硬盘：512G 的 SSD 固态硬盘及以上 网卡：千兆网卡（1 块）；无线网络适配器（1 块） 自带串口用于连接调试线缆 19 英寸及以上显示器 键鼠及电源线	台	36
3	工作台	装配及施工工作台	台	20
4	电脑桌	标准学生电脑桌椅	套	20
5	局域网	所有电脑，局域网互联互通	套	1

2.赛场软件环境

序号	软件名称	说明	单位	数量
1	Windows Server	Windows Server 2022 Data Center 中文版	套	1
2	Windows	Windows 10 Enterprise 中文版	套	1
3	CentOS Linux	Version 7 及以上	套	1
4	办公软件	WPS Office Version 2022 及以上	套	1
5	Putty	Version 0.7 及以上	套	1
6	Tftpd	Version 4.6 及以上	套	1
7	解压缩软件	RAR4.0 及以上	套	1
8	PDF 阅读器	Adobe Reader X111 及以上	套	1
9	网络调试工具	SercureCRT8.1 及以上	套	1
10	截图工具	FScapture6.5 以上	套	1

11	FTP 客户端	FlashFXP5.4 以上	套	1
12	浏览器	Firefox 85 以上	套	1

3.赛场辅助设施

赛场辅助设施根据竞赛需要，赛场还需准备如下辅助设施，见表 4-2。

表 4-2 赛场提供辅助设备表

序号	名称	规格	数量	备注
1	音响及扩音器	能涵盖整个赛场	1 套	
2	无线麦克风		2 个	与音响配套
3	口哨		2 个	
4	赛场时钟	具有时/分/秒/毫秒计时	1 套	赛场都可见
5	计时秒表		若干	
6	打印机		1 台	
7	打印纸	A4	2 箱	
8	签字笔	红、黑	若干	
9	订书机及钉		1 套	
10	评分夹		若干	
11	文件柜		1 套	用于存放赛场资料
12	饮水机		若干	根据赛场布置
13	桶装水		若干	

序号	名称	规格	数量	备注
14	讨论区工作台		若干	摆放在讨论区
15	讨论区桌椅		若干	摆放在讨论区
16	隔离栏（或隔板）		若干	包围赛场
17	安全标志		若干	
18	常用急救药盒		2 套	常用药品
19	灭火器		若干	根据赛场布置

4.竞赛用耗材

竞赛用耗材根据竞赛需要，赛场提供如下耗材，见表 4-3。

表 4-3 赛场提供的耗材清单

序号	名称	技术规格	单位	数量
1	Cat6 双绞线	CAT6/非屏蔽	盘	1
2	网络跳线	1 米/条（每组 30 根）	批	1
3	PVC 线管	Φ20	米	2
4	明装底盒	86*86	个	2
5	面板	双口 86 型	个	1
6	波纹管	Φ20	米	1
7	管卡	Φ20	个	6
8	弯头	Φ20	个	5
9	直通	Φ20	个	4
10	网络模块	六类 RJ45	个	3

序号	名称	技术规格	单位	数量
11	水晶头	RJ45	包	1
12	标签纸	P 型	张	1

以上耗材为单组基本需求

5.竞赛配套物品清单

根据比赛需要，现场统一提供工具，具体工具清单见表 4-4。

表 4-4 赛场提供配套工具清单表

序号	名称	技术规格	数量
1	单口打线刀	单口	1 套/组
2	线管剪刀	Φ25	1 套/组
3	剥线器	三挡	1 套/组
4	螺丝刀	十字型	1 套/组
5	斜口钳	6 寸	1 套/组
6	压线钳	RJ45/RJ11	1 套/组
7	记号笔	油性	1 套/组
8	剪刀	小型，剪纸用	1 套/组
9	头盔	施工用	1 套/选手

6. 参赛选手禁止使用的物品和材料

选手禁止携带的设备和材料，见表 4-5 所示，违规者不得参赛。

表 4-5 参赛选手禁止使用物品和材料清单表

序号	名称
1	存储设备，如 U 盘、移动硬盘、录音笔等；电子设备，如平板、手机、多媒体播放器、录音器，照相机，摄影机等
2	带有身份标示的物品

3	防锈清洗剂、酒精、汽油、有毒有害物、易燃易爆物
4	气动工具、特制工具

五、安全、健康要求

根据国家相关法规要求，结合本项目实际，提出安全、健康要求及职业操作规范要求，并明确违反后的处理规定。特别是根据本项目具体情况的诸如人身防护，有毒、有害物品携带、存放，防火、防爆等措施。

（一）赛场人员安全要求

以参赛选手为重点，说明进入竞赛区和非竞赛区等竞赛场地的各类人员需进行哪些检测、所需的注意事项（如废弃物不能随意丢、不能使用明火等）、赛场文明要求（竞赛场地禁止吸烟、不能携带手机、照相机等）、所带物品安全检测以及参观人员和宣传人员的安全要求（不能进入竞赛区等）。

1. 现场裁判、选手、工作人员在竞赛期间应该遵守组委会和执委会的安全规定和要求。
2. 参赛选手进入竞赛场地后，须听从并尊重裁判人员的管理，文明参赛。
3. 参赛选手必须在确保人身安全和设备安全的前提下开始竞赛，发现或发生有关安全问题，应立即向裁判报告。
4. 参赛选手必须按照主办地的安全标准要求，配备个人防护用品，包括工作服、绝缘防砸鞋。
5. 参赛选手在本竞赛工位内操作，不得影响其他选手操作。
6. 未经许可，不得进入标有警告标示的危险区。

（二）场地设备安全要求

场地设备安全要求包括设施设备安全操作要求、赛场消防安全要求、安全标识

张贴要求、设备安全操作规程。

1. 设施设备安全操作要求

(1) 禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。

(2) 承办单位应设置专门的安全防卫组，负责竞赛期间健康和安​​全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

(3) 赛场须配备相应医疗人员和急救人员，并备有相应急救设施。

2. 赛场消防安全要求

消防设施、器材和消防安全标志全都在位且功能完整。消防安全重点部位人员正常在岗工作。

3. 安全标识张贴要求

安全出口、疏散通道保证畅通，安全疏散指示标志、应急照明完好无损，竞赛场地安全疏散通道禁止被占用。

4. 设备安全操作规程

(1) 现场电力规格为单相 220V 交流电，安全用电，禁止使用不符合安全要求的机具，禁止使用连接 220V 电线供电的手电钻，禁止擅自使用电气设备。

(2) 在进行任何安装或维护工作前，必须确认操作对象处于停止或断电状态。

(三) 赛事安全要求

禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。

承办单位应设置专门的安全防卫组，负责竞赛期间健康和安​​全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

赛场须配备相应医疗人员和急救人员，并备有相应急救设施。

（四）开放赛场要求

1.公众要求

赛场内除指定的裁判、工作人员外，其他人员须经组委会同意或在组委会负责人陪同下，佩带相应的标志方可进入赛场内。

允许进入赛场的人员，只可在安全区内观摩竞赛，不得使用录像设备长时间拍摄选手工位、屏幕。

允许进入赛场的人员，应遵守赛场规则，不得与选手交谈，不得妨碍、干扰选手竞赛。

允许进入赛场的人员，不得在场内吸烟、喧哗。

2.对于赞助商和宣传的要求

经组委会允许的赞助商和负责宣传的媒体记者，按竞赛规则的要求进入赛场相关区域。上述相关人员不得妨碍、干扰选手竞赛，不得有任何影响竞赛公平、公正的行为。

（五）绿色环保要求

1.环境保护

赛场严格遵守我国环境保护法。

赛场所有废弃物应有效分类并处理，尽可能地回收利用。

赛场设置排烟除尘系统，尽可能地减少和控制烟尘。

2.可持续性

工位将被用于为 3 个与技能相对应的模块进行测试（第 1 天-第 3 天）。为了减少网络设备的数量，工位设备可用于多个模块的测试环境，比赛结束后设备可持续

使用。

六、试题公布说明

本项目赛前 7 天公布试题，赛前 1 天裁判长可结合赛场设备、材料状况，组织裁判人员对赛题进行试题试做，制定评分标准。试题经裁判长审核确认后即为本次竞赛的最终试题。最终试题确定后给予裁判组内部公开，但不对外公开发布。

七、附件：样题

重要说明

- 1.竞赛时间 360 分钟，选手不可以弃赛，不可提前离开赛场。
- 2.比赛共包括 5 个任务，总分 100 分，任务及配分见下表所示。

序号	模块	配分	备注
A	职业技能素养	5	
B	数据中心网络搭建（网络链路安装）	15	
C	数据中心网络搭建（网络设备连接与调试）	20	
D	网络服务与系统运维（Windows、Linux）	30	
E	秘密挑战（信息安全、网络系统故障排除）	30	
合计		100	

3.如发现任务书缺页、字迹不清等问题，请及时向裁判申请更换任务书；对照设备清单认真检查设备及工量具，如发现问题，请及时向裁判申请处理。

4.每个赛位配有 2 台计算机，装有 CRT/Xshell 等软件、相机及比赛相关软件，参考资料存放在计算机桌面“竞赛参考资料”文件夹下；选手创建的程序文件必须存储到“D:\技能竞赛\竞赛编号”（竞赛编号由场次+工位号组成，例如第二场第 1 号工位为 B1）文件夹下。赛题中所要求备份的文件请备份到对应到文件夹下，即使选手没有任何备份文件也要建立文件夹。

5.选手提交的资料不得出现学校、企业、姓名等与身份有关信息，擅自离开竞赛工位、与其他选手交流、不服从裁判指令，将依据扣分表进行处理。

6.由于操作不当等原因引起网络设备、路由交换设备、服务器等设备的损坏，将依据扣分表进行处理。严重损坏比赛设备将取消竞赛资格。

7.在完成任务过程中，请及时保存程序及数据，未能及时保存程序及数据，由于断电等意外情况造成的程序及数据丢失的责任将由选手自负。

8.选手必须认真填写各类文档，竞赛完成后所有文档按页码顺序一并上交；赛场提供

的任何物品，不得带离赛场。

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，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施建设的能力。

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。

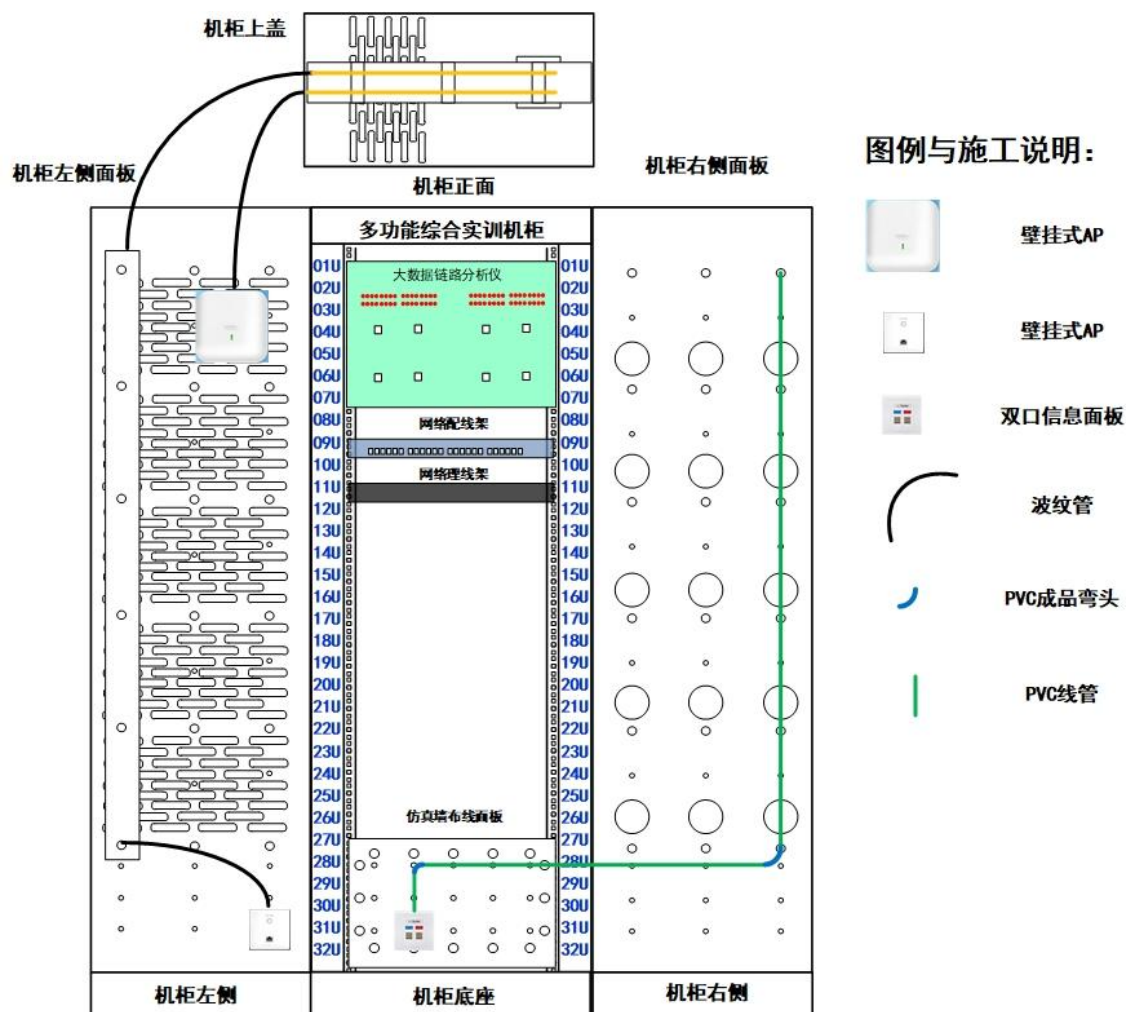


图 1 多功能综合实训机柜正面展开设备安装布线施工图

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）

一、赛题说明：

能够根据大赛提供的网络环境和技能要求，读懂文档需求，理解业务架构，实现项目应用。

1. 能够完成线缆制作、合理配置路由器、交换机、无线控制器、无线 AP 和出口网关等网络设备，实现网络的正常运行。
2. 根据网络业务需求配置各种策略，以达到网络互联互通，实现网络资源适应业务需求。
3. 能够预判网络运行中所面临的安全威胁，防范并解决网络恶意攻击行为；考查选手防御不良信息、构建和维护绿色网络的实战能力。
4. 能够充分理解竞赛前发布的竞赛设备列表、配套技术文档、竞赛网络环境和技术技能要点等信息，分析网络架构、查找技术资料、开展针对性训练，从而提高技能水平；能够基于竞赛现场发布的网络环境、技术要求和临场故障预置和变化，在实际竞赛中结合技术原理，参考设备技术文档进行合理解决。开放的形式一方面扩大了竞赛的公平性，另一方面可以与真实工作实践相符合，最终充分考察学生整体熟练运用知识原理解决技术问题的能力。

二、项目介绍：

某集团公司建立了上海管理中心、广东生产中心。上海管理中心设有生产、办公、管理 3 个部门，统一进行 IP 及业务资源的规划和分配，网络采用 OSPF、VPN 等路由协议。

总公司及分公司的网络拓扑结构如下图所示。

一台三层交换机编号为 S1，用于实现广州生产中心终端高速接入；一台三层交换机编号为 S2，作为广州生产中心的出口 HUB；两台 EG3210 编号为 GW1\GW2，作为广东生产中心的出口设备；一台三层交换机编号为 S3，作为上海分公司接入设备。一台 RSR20-X 路由器编号为 R1，作为 Internet 出口路由器；一台 RSR20-X 路由器编号为 R2，作为上海分公司出口路由器；一台 WS6008 作为上海管理中心机构的无线控制器，编号为 AC1，通过与 AP850 高性能企业级 AP 配合实现整体无线覆盖。

拓扑结构图

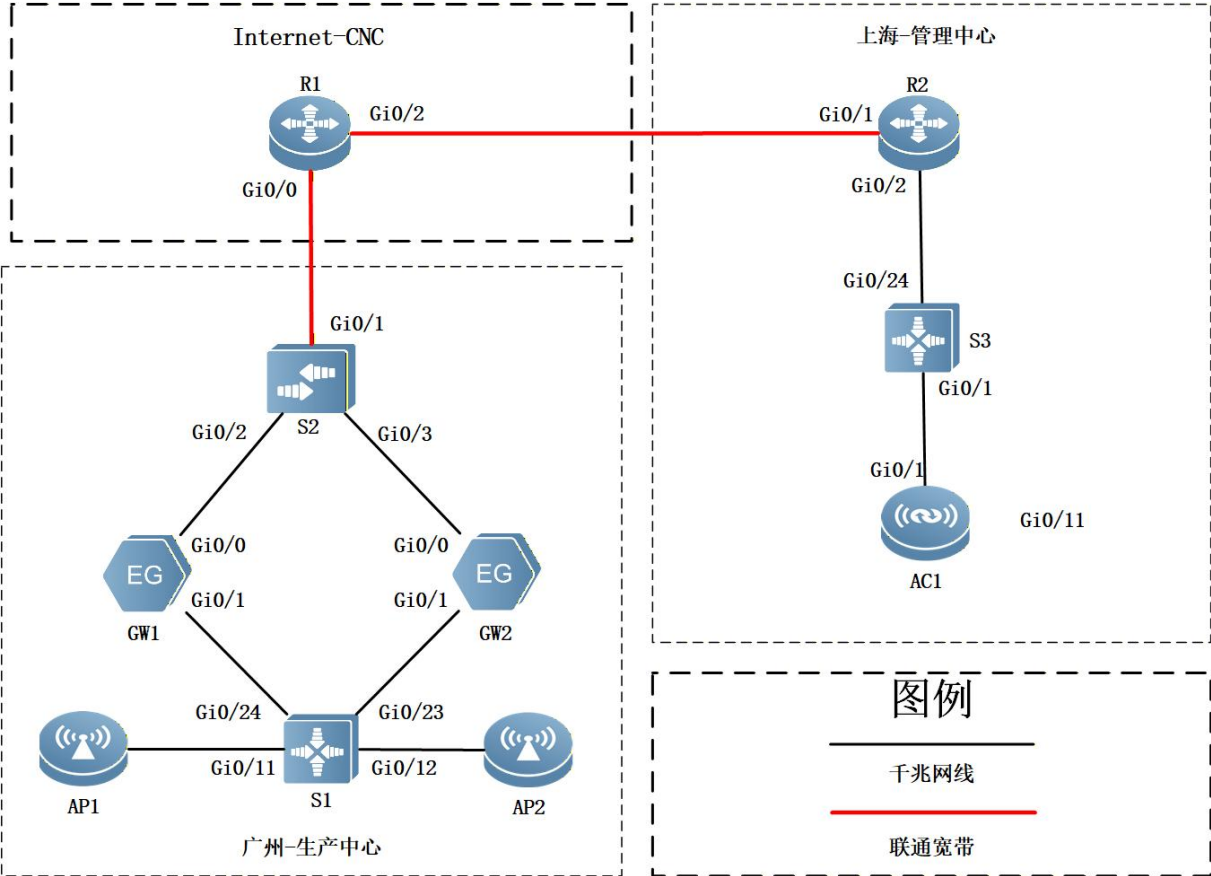


表 1：网络设备连接表：

编号	硬件型号
S3	RG-S5310-24GT4XS-E
S1	RG-S5310-24GT4XS-E
S2	RG-S5310-24GT4XS-E
GW1	RG-EG3210
GW2	RG-EG3210
R1	RSR20-X-28
R2	RSR20-X-28
AC1	RG-WS6008
AP1	RG-AP520
AP2	RG-AP520

表 2：网络地址规划表：

设备	接口/VLAN	接口/VLAN 描述	二层/三层规划	说明
R1	G 0/2	Connect_To_R3	13.1.1.1/29	
	G 0/0	Connect_To_S2	17.1.1.1/29	
	LoopBack 20	\	20.0.0.1/32	模拟 IPv4 公网

设备	接口/VLAN	接口/VLAN 描述	二层/三层规划	说明
				资源
R2	G 0/1	Connect_To_R1	13.1.1.2/29	
	G 0/2	Connect_To_S3	10.3.0.1/30	
	LoopBack 0	\	10.3.1.3/32	OSPF 20 Router id
	LoopBack 1	\	172.16.0.2/24	L2TP 隧道
S3	G 0/24	Connect_To_R3	10.3.0.2/30	
	G 0/1	Connect_To_AC1	10.3.0.10/30	G 0/1
	LoopBack 0	\	10.3.1.5/32	OSPF 20 Router id
AC1	G 0/1	Connect_To_S3	10.3.0.9/30	G 0/1
	LoopBack 0	\	10.3.1.12/32	
GW1	G 0/0	Connect_To_R1	17.1.1.2/29	
	G 0/1.10	SC1-Terminal	10.4.10.254/24	生产 1 终端
	G 0/1.11	SC2-Terminal	10.4.11.254/24	生产 2 终端
	G 0/1.20	AP-Manage	10.4.20.254/24	AP 管理
	G 0/1.30	Net-Manage	10.4.30.254/24	设备管理
	LoopBack 0	\	10.4.1.1/32	
	Virtual-ppp		172.16.0.3/24	L2tp 隧道
GW2	G 0/0	Connect_To_R1	17.1.1.3/29	
	G 0/1.10	SC1-Terminal	10.4.10.253/24	生产 1 终端
	G 0/1.11	SC2-Terminal	10.4.11.253/24	生产 2 终端
	G 0/1.20	AP-Manage	10.4.20.253/24	AP 管理
	G 0/1.30	Net-Manage	10.4.30.253/24	设备管理
	LoopBack 0	\	10.4.1.2/32	
	Virtual-ppp	\	172.16.0.4/24	L2tp 隧道
S1	VLAN10	SC1-Terminal	\	
	VLAN11	SC2-Terminal	\	
	VLAN20	AP-Manage	\	G 0/11-12 (AP)
	VLAN30	Net-Manage	10.4.30.1/24	设备管理
S2	VLAN1	HUB	17.1.1.4/29	

三、数据中心网络搭建及安全部署

【说明】

(1) 设备 console 线有两条。设备命名方式参考网络设备 IP 地址分配表。

(2) 设备配置完毕后，保存最新的设备配置。裁判以各参赛队提交的竞赛结果文档为主要评分依据，无文档相关环节视为 0 分。所有提交的文档必须按照赛题所规定的命名规则命名，否则按无效内容处理；所有需要提交的文档均放置在 PC1 桌面的“比赛文档

_X”（X 为工位号）文件夹中。

保存文档方式分为两种：

- 交换机、路由器、出口网关、AC 要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.txt,例如：R1 路由器文件命名为：R1.txt，然后放入到 PC1 桌面上“比赛文档_X”文件夹中；
- 交换机、路由器、出口网关、AC 除收集 show running-config 的配置外，还需收集其他命令一同保存在相关设备的“数据中心网络搭建答题卡.docx”文档中后转成 PDF 文件，保存到桌面指定位置中，每个设备收集的命令有所差异，详见表 4：数据中心网络搭建答题卡；

表 4：数据中心网络搭建答题卡

基础配置

S2 设备查看 snmp 配置状态信息 S2#show snmp host
R1 设备查看路由表条目 R1#show ip route exclude local host
S3 设备查看远程 SSH 登录信息 S3#show ssh

有线网络配置

S1 设备查看 21 口接口 Trunk 修剪信息 S1#show interfaces switchport include 30
S1 设备查看生成树环路自动恢复时间配置信息 S1#show run interface gigabitEthernet 0/1
R2 设备查看 L2TP 隧道建立状态信息 R2#show vpdn tunnel
R2 设备查看 ipsec 感兴趣流协商创建信息 R2#show crypto ipsec sa include remote

无线网络配置

AC 设备查看两个 AP 通过隧道关联到 AC 后的主机名，IP 地址，信道，功率等状态信息 AC1#show ap-config summary
AC 设备查看 user10 关联 GZ_SC_WEB_XX,认证成功后的状态信息 AC1#show web-auth user all
AC 设备查看无线用户限速的相关配置信息

AC1#show run include per-user-limit
查看 AP 限制关联用户数相关配置 AC1#show ap-config running AP1 include sta-limit

出口网络配置

GW1 设备查看路由表中 10.3.1.12 的状态信息
GW1 设备查看 nat 转换表项信息（无线终端连接 GZ_SC_WPA_XX 后 ping 20.0.0.1 连通截图）
GW1 设备查看 VRRP 协议处于备份状态的网关信息
GW2 设备查看路由表 10.3.1.12 路由状态信息
GW2 查看 nat 转换表项信息（无线终端连接 GZ_SC_WEB_XX 后 ping 20.0.0.1 连通截图）
GW1 设备查看黑名单状态信息 GW1#show url-class user-cfg include url

- 截图方式：使用上面指令查看其运行状态，并使用 FSCapture 截图软件或者其他截图功能软件进行截图，将输入结果的截图插入到“数据中心网络搭建答题卡.docx”文档中后转成 PDF 文档中，保存后放入到 PC1 桌面上“比赛文档_X”文件夹中；

3.1、线缆制作与基础配置

1. 根据网络拓扑图要求，使用赛场提供的成品网线，根据题目要求，插入相应设备的相关端口。特别提醒：成品跳线不够长的连接，可以使用赛场提供的双绞线和水晶头，自己制作网络跳线并使用。
2. 根据网络拓扑要求及网络地址规划表，对网络设备进行地址设置。
3. 对每个三层网络设备互联端口进行描述，例如对 R1 与 R2 连接的 R1 的端口描述为：“R1_to_R2”+R2 端口号。

3.2、交换机配置

1. 根据附录 1 拓扑图、附录 2 地址规划表、附录 3 设备编号表，配置设备接口及主机名信息。
2. 在网络设备上均开启 SSH 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. 在网络设备上均部署 SNMP 功能，配置所有设备 SNMP 消息，向主机 192.1.100.100 发送 Trap 消息。版本采用 V2C，读写的 Community 为“Test@123”。
4. 在全网 Trunk 链路上做 VLAN 修剪。

5. 在 S1 开启边缘端口和 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 200 秒后会自动恢复。

3.3、路由器配置与调试

1. DHCP 服务器搭建于 GW1、GW2 设备上，为局域网络终端动态分配 IP 地址。
2. 上海管理中心 R2、S3 间运行 OSPF，归属区域 0，进程号 20。AC1 与 S3 间运行静态路由协议。
3. 各中心出口设备至互联网使用静态路由协议。
4. 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；所有路由协议都发布具体网段；需要发布 Loopback 地址；优化 OSPF 相关配置，加快 OSPF 收敛；外部路由引入采用第一类外部路由模式。

3.4、广域网配置

1. 上海管理中心局域网管理终端可通过出口路由器 R2 NAPT 方式访问互联网。
2. 广州生产中心局域网生产终端可通过出口网关 GW1/GW2 NAPT 方式访问互联网。
3. 广州生产中心出口网关内网启用 VRRP 功能，其中 GW1 为生产 1、AP 管理、网络设备管理网段的主设备，优先级 255；GW2 为生产 2 的主设备，优先级 255；两者互为备份，在其中一台宕机的情况下终端流量可以无缝切换到另一台设备，达到网关冗余备份的目的。
4. GW1/GW2 与 R2 间启用 L2TP 隧道，隧道内承载 OSPF 协议，使广州生产中心与北京综合服务中心内网连通。两者互为备份，在其中一台宕机的情况下业务流量可自动切换到另一条 L2TP 隧道进行转发。
5. L2TP 隧道验证用户名及密码均为 Test@123，L2TP 隧道密码为 Test@123。L2TP 用户地址池为 172.16.0.1—172.16.0.254，服务端 L2TP 隧道接口引用本地 loopback 1 接口地址。
6. IPsecVPN 针对 GRE 及 L2TP 隧道内数据进行加密，其中 isakmp 策略定义加密算法采用 3des。散列算法采用 md5，预共享密码为 Test@123。DH 使用组 2。此外，转换集 myset 定义加密验证方式为 esp-des esp-md5-hmac。加密图定义为 mymap。
7. 出口网关 GW1 上，设置黑名单禁止局域网用户通过浏览器访问 www.exam.com 网址。

3.5、无线配置

1. 无线网络采用 FIT AP+AC 方案，所有 AP 都关联到上海管理中心 AC 进行管理。

2. 广州生产中心使用 GW1/GW2 作为无线生产 1 用户（VLAN 10）、生产 2 用户（VLAN 11）和无线 FIT AP1（VLAN 20）无线 FIT AP2（VLAN 20）的 DHCP 服务器。

3. 广州生产中心无线网络部署中，AP1 关联创建 SSID 为：GZ_SC_WEB_X；WLANID 为 1；AP-GROUP 为 Admin_GZ；无线用户（认证用户名 user10、密码为 Y）关联 SSID 后使用 WEB 认证方式，可自动获取 VLAN10 地址；AP2 关联创建 SSID 为：GZ_SC_WPA_X；WLANID 为 2；AP-GROUP 为 Admin_GZ；无线用户（密码为 Y）关联 SSID 后使用 WPA2 认证方式，可自动获取 VLAN11 地址；（X 为工位号、Y 自设）。

4. 所有 AP 均通过 AC 的 loopback 0 接口建立隧道。

5. 无线用户的下行平均速率为 1000KB/s，突发速率为 1600KB/s。

6. 每 AP 最大带点人数为 25 人。

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
Windows4	4	4096MB	100GB	10.0.0.104/24 10.0.1.104/24 10.0.2.104/24	Windows4
Windows5	4	4096MB	100GB	10.0.0.105/24 10.0.1.105/24 10.0.2.105/24	Windows5

(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 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。

（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。

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。

（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 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。

(5)、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"。

(6)、任务描述：完成 DHCP 配置，实现内网地址自动分配。

配置 Windows3 和 Windows4 为 DHCP 服务器，DHCP IPv4 的作用域名称为

skills，地址范围为 10.0.0.200-10.0.0.219，租约期 4 小时，网关为 10.0.0.254，DNS 为 10.0.0.101 和 10.0.0.102，DNS 域名为 skills.lan；

在 Windows2 上安装 WDS,部署安装 Windows Server 2022 Datacenter Core。

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 Windows3 占 60%，Windows4 占 40%，状态切换间隔 60 分钟，启用消息验证，共享机密为 ycjdgc。

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
linux4	2	4096MB	100GB	10.4.1.104/24	linux4
linux5	2	4096MB	100GB	10.4.1.105/24	linux5

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（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。

(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-linux5 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 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。

(5)、任务描述：请采用 `iscsi`，搭建存储服务。

为 `linux4` 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 `linux5` 提供 `iSCSI` 服务。`iSCSI` 目标端的 `wwn` 为 `iqn.2026-01.lan.skills:server`，`iSCSI` 发起端的 `wwn` 为 `iqn.2026-01.lan.skills:client1`。

配置 `linux5` 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。

(6)、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。

(7)、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。

配置 `linux4` 为 `PXE` 服务器，实现完全自动安装 `Linux`。

安装 `DHCP` 服务，地址范围为 `10.4.1.10-10.4.1.19`，网关为 `10.4.1.254`，`DNS` 为 `10.4.1.101`，域名为 `skills.com`。

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

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`。

模块 E 秘密挑战 (信息安全、网络系统故障排除)

1. 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。

一、windows 系统应急响应

任务描述：X 集团的一台存储关键信息的 Windows 服务器遭受到了黑客的攻击，现在需要你对该服务器进行应急排查，该服务器的系统目录被上传恶意文件，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行检查，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

1. 找到黑客创建的后门用户，并将完整用户名作为 flag 进行提交，提交格式：flag{*****};

2. 将后门用户创建的时间作为 flag 进行提交，(以最后一次修改为主) 提交格式：flag{2023/1/01 10:10:10};

3. 将后门用户上传的恶意程序连接的恶意服务器 IP 地址作为 flag 进行提交，提交格式：flag{*****};

4. 将恶意程序所在绝对路径作为 flag 进行提交，提交格式：flag{*****};

5. 将 powerShell 执行过的历史命令中的关键信息作为 flag 进行提交，提交格式：flag{*****};

二、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. 对目标系统进行排查，找出攻击者的地址，将 IP 地址作为 flag 值提交，提交格式：flag{0.0.0.0}

2. 对目标系统进行排查，找出攻击者使用的渗透工具，将工具的具体名及版本号作为 flag 值提交，提交格式：flag{*****}

3. 对目标系统进行排查，找到攻击者上传的恶意文件，将恶意文件在系统中的路径及名称作为 flag 值提交，提交格式：flag{*****}

4. 对目标系统进行排查，找出攻击者第一次攻击成功的时间，将攻击时间作为 flag 值提交，提交格式：flag{11/Jun/2019:12:47:22}

5. 对目标系统进行排查，找出攻击者遗留的后门，将该后门创建的文件名称作为 flag 值提交，提交格式：flag{包含绝对路径的完整名称}

三、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. 统计流量包中基于 TCP 协议的应用层协议，将所有用到的协议作为 FLAG 提交，提交格式：flag{SSH,SMTP,MYSQL} (根据协议端口由小到大)；

2. 分析流量包，将通过 FTP 下载文件的第一个包的序号作为 FLAG 提交，提交格式：flag{*****}；

3. 分析流量包，将 FTP 文件传输协议的过滤表达式提交，提交格式：flag{*****}；

4. 分析流量包，将找到通过 FTP 传输的文件名作为 FLAG 提交，提交格式：flag{*****}；

5. 分析通过 FTP 传输的文件，将文件的类型作为 FLAG 提交，提交格式：flag{*****}；

6. 分析最后找到的文件，将文件中的 FLAG 信息提交，提交格式：flag{*****}。

四、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. 使用扫描器，获取靶机的 Web 服务端口号并提交，格式：flag{*****}；

2. 获取网站源码，将根目录下的文件夹个数提交，格式：flag{*****}；

3. 找出网站管理后台，提交后台页面的地址，格式：flag{*****}；

4. 找出数据库的密码并提交，格式：flag{*****}；

5. 登录靶机数据库，提交后台密码的密文，格式：flag{*****};
6. 重置网站后台密码，修改为“hacker”，将修改的内容提交（网页中有隐藏线索），格式：flag{*****};
7. 登录管理后台，将后台中隐藏的 flag 提交，格式：flag{*****};
8. 获取服务器根目录下的 flag 并提交，格式：flag{*****};

2. 网络故障排错

小 A 是某公司网络管理员，销售部告诉小 A 自己电脑无法访问外网，同时不能访问客户资料，客户资料存放在公司内部存储服务器里，请小 A 进行排查。

竞赛结束后由裁判分组评判!!!