2023年江苏省职业院校技能大赛中职赛项规程

一、赛项名称

赛项编号：JSZ202338

赛项名称：网络搭建与应用

赛项组别：学生组、教师组

赛项归属专业大类：信息技术类

二、竞赛目的

贯彻落实《国家职业教育改革实施方案》《关于推动现代职业教育高质量发展的意见》、全国职业教育大会精神和国家新职业教育法，进一步强化职业院校本专业学生职业技能训练和职业能力的综合运用，促进校企合作、产教融合，完善“岗课赛证”教学模式，培育工匠精神，推动职业院校“双师型”师资队伍建设，大力培养适应我省经济与社会发展的高素质劳动者和技术技能型人才，为建设“强、富、美、高”新江苏和建成技能型社会提供人才和技能支撑。进一步提升中职院校计算机类专业学生能力素质与企业用人标准的吻合度，为在新形势下全面提高信息技术类专业教学质量、为扩大就业创业、运用新技术新模式赋能传统产业转型升级、培育经济发展新动能做出新贡献。

三、竞赛内容

（一）学生组竞赛内容

本赛项竞赛主要考核选手理论知识、实操技能和职业素养。其中：

1.理论知识考核占比15%，考核内容主要包含：（1）计算机网络基础理论；（2）Linux系统的基础理论；（3）Windows系统的基本基础理论；（4）虚拟化、集群与云计算等基本理论等。

2.实操技能考核占比80%，考核内容主要包含：（1）网络组建与配置部分：网络综合布线安装和施工、交换配置、路由配置、无线配置、广域网配置、防火墙配置、网络优化配置、VPN技术等；（2）云平台配置部分：云平台部署、虚拟化、集群等配置；（3）Windows服务器配置部分：常用Windows服务配置、Windows操作系统安全技术等；（4）Linux服务器配置部分：常用Linux服务配置、Linux操作系统安全技术等。

3.职业素养考核占比 5%，考核内容主要包含：（1）团队配合；（2）操作科学规范。

（二）教师组竞赛内容

本赛项竞赛主要考核选手理论知识、实操技能和职业素养。其中：

1.理论知识考核占比 15%，考核内容主要包含：(1)计算机网络基础理论；(2) Linux 系统的基础理论；（3）Windows 系统的基本基础理论；（4）虚拟化、集群与云计算等基本理论等。(5) 除计算机网络专业需求的基础理论外，还应包括计算机科学与技术的基础理论，如：计算理论、信息与编码理论、程序理论、算法分析和计算复杂度理论、并行与分布处理理论等。

2.实操技能考核占比 80%，考核内容主要包含：（1）网络组建与配置部分：网络综合布线安装和施工、交换路由配置、无线配置、防火墙配置、网络性能优化配置、VPN 技术、网络设备安全配置等；（2）云平台配置部分：云平台部署、集群、虚拟化技术完成特定环境配置等；（3）Windows 服务器配置部分：常用 Windows 服务配置、Windows 操作系统安全技术、操作系统等；(4) Linux 服务器配置部分：常用 Linux 服务配置、Linux 操作系统安全技术等；（5）实训指导文档：撰写指导指导学生技能训练的实训文档。

3.职业素养考核占比 5%，考核内容主要包含：（1）团队配合；（2）操作科学规范。

四、竞赛方式

本赛项为团体赛。

学生组团体赛参赛要求：每组参赛队 2 名选手。每市学生组可报名 4 组，原则上同一所学校报名组数不得超过 1 组。

教师组团体赛参赛要求：每组参赛队 2 名选手。每市教师组可报名 2 组，原则上同一所学校报名组数不得超过 1 组。

如有变化见 2023 年江苏省职业院校技能大赛通知。

五、竞赛流程

（一）学生组竞赛流程

1.学生组竞赛流程安排如下表所示：

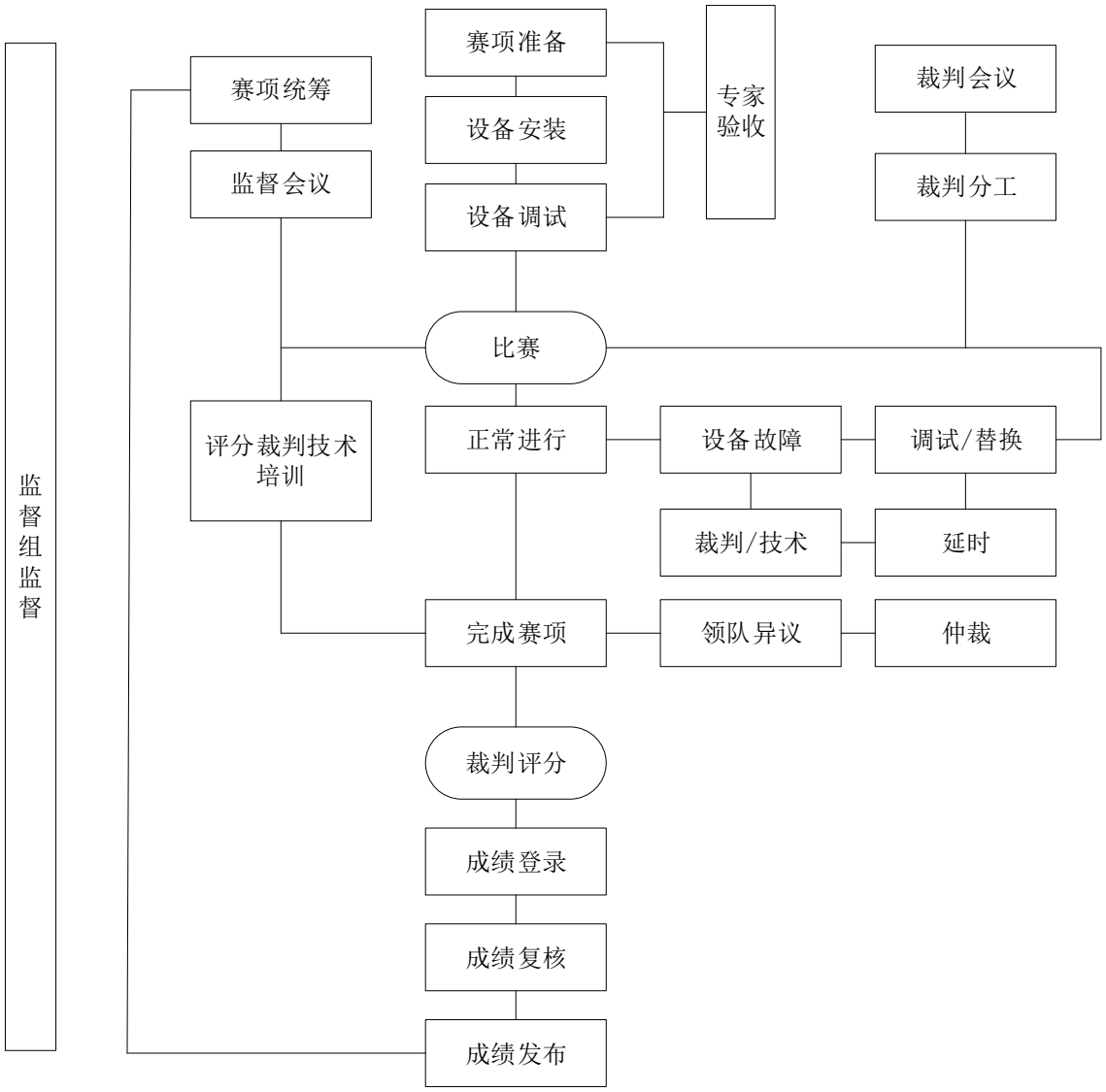
网络搭建与应用赛项学生组竞赛流程安排表

竞赛阶段	时间安排	工作内容	责任方	备注
赛前（竞赛前一天）	10:00 前	组织人员报到	专家组长	专家组、裁判长、仲裁、监督、联络员到报到
	10:00-11:00	专家组会议	专家组长	专家组成员、裁判长、仲裁、监督、联络员等参会
	12:30-18:30	印制试卷	专家组长	专家组成员负责印制
赛中（比赛第一天）	10:00 前	裁判报到	裁判长	
	09:00-12:00	参赛队报到	赛点学校	安排住宿，领取资料
	10:00-12:00	检查封闭赛场	裁判长	裁判、专家组、监督员、技术人员参加
	12:00-12:30	赛场工作人员会议	赛点负责人	巡视员、裁判长、专家组长、监督员、联络员、赛场技术人员、场外工作人员参加
	12:30-14:00	领队会	裁判长	巡视员、专家组长、赛点负责人、监督员、联络员、各参赛队领队参加
	14:00-14:30	裁判员会议	裁判长	巡视员、专家组、裁判、联络员、监督员、赛场技术人员参加
	14:30-15:30	第一次抽签	加密裁判	加密（抽序号）
	15:00-16:00	理论考试	裁判长	
	16:00-16:30	参观赛场	裁判长	
	16:30	返回酒店	参赛领队	
赛中（比赛第二天）	07:30	到技能赛场	各参赛队领队	
	07:30-08:00	大赛检录	检录员	参赛选手，检录工作人员
	08:00-08:20	第二次抽签	加密裁判	加密（抽工位号）
	08:00	依次进入赛场	裁判长	按要求入赛场
	08:20	宣读竞赛须知	裁判长	

	08:20-08:30	领取比赛任务	裁判长	
	08:30-12:30	正式比赛	裁判长	
	08:30-11:00	评分裁判培训会议	专家组	
	11:30-12:00	午餐	大赛联络员	评分裁判、监督、仲裁、专家组、巡视员、联络员会议室就餐
	12:40-13:10		各领队	参赛选手、指导教师、领队到学校食堂就餐
			裁判长	现场裁判会议室就餐
	13:30	回酒店	各领队	参赛选手、指导教师、领队回住宿酒店
	15:00		裁判长	现场裁判回住宿酒店
	12:40-18:40	评判	裁判长	
	18:40-20:30	恢复赛场	裁判长	裁判、专家组、监督员、技术人员参加
	18:40-20:30	成绩汇总与解密	裁判长	评分裁判、裁判长、专家、监督、大赛组委会联络员参加
	20:30	回酒店	裁判长	
赛中（第三天）	17:00	赴成绩发布会现场	裁判长	乘车前往赛场参加成绩发布会
	17:35-17:50	赛项测评	各市领队	各市领队、指导老师参加测评
	18:00-18:40	成绩发布会	巡视员	同时公布国赛集训名单
	18:40	回酒店或返程	承办校负责人	
赛后（竞赛后一天）	8:00—17:00	提交赛项文档	裁判长	
	8:00—17:00	提交大赛总结和点评文档	专家组长	

注：学生组比赛天数可根据报名人数和承办校比赛场地情况进行调整。

2.学生组竞赛流程图如下图所示：



学生组网络搭建与应用赛项竞赛流程图

（二）教师组竞赛流程

1.教师组竞赛流程安排如下表所示：

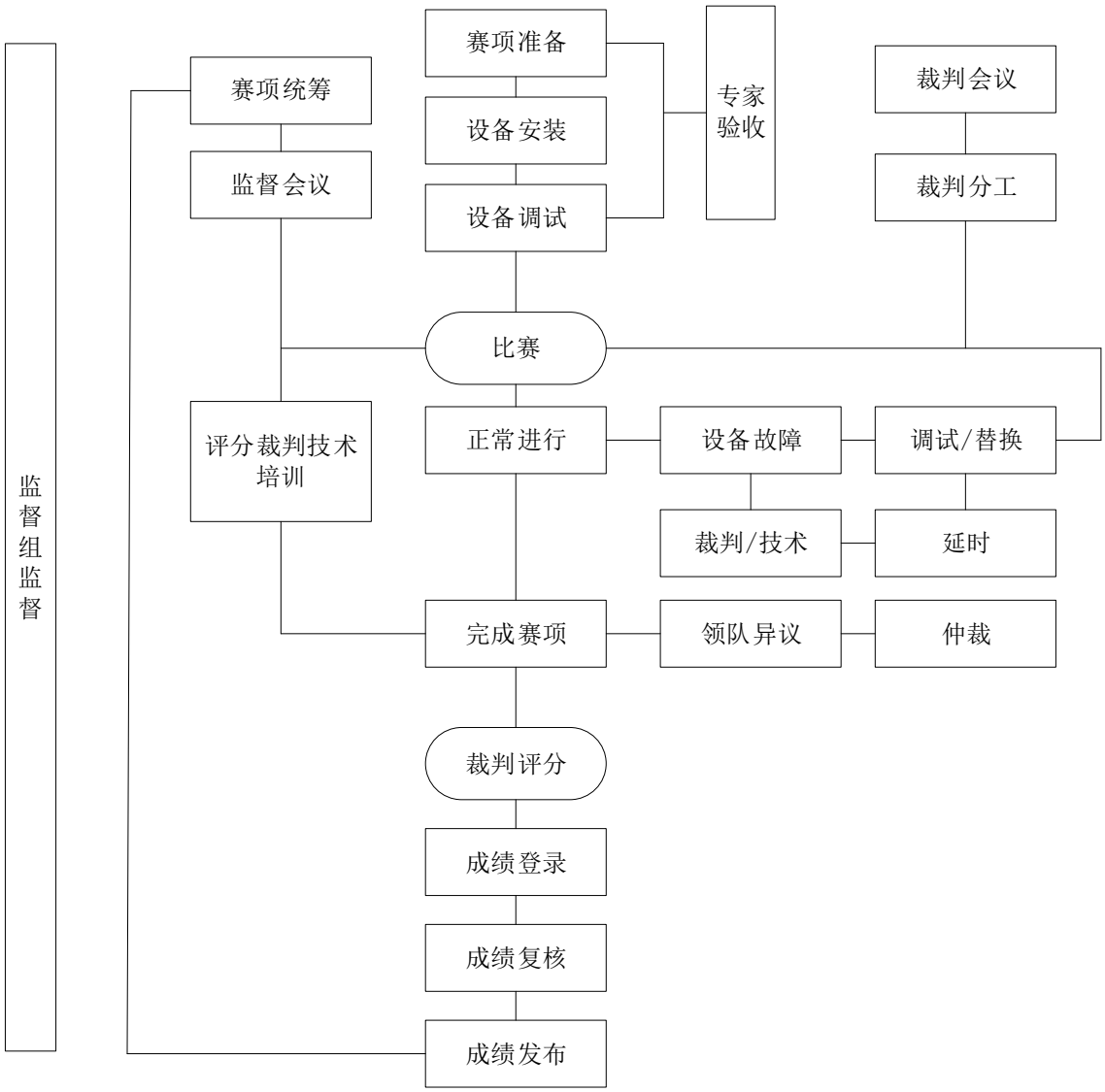
网络搭建与应用赛项教师组竞赛流程安排表

竞赛阶段	时间安排	工作内容	责任方	备注
赛前（竞赛前一天）	10:00 前	组织人员报到	专家组长	专家组、裁判长、仲裁、监督、联络员到报到
	10:00-11:00	专家组会议	专家组长	专家组成员、裁判长、仲裁、监督、联络员等参会
	12:30-18:30	印制试卷	专家组长	专家组成员负责印制
赛中	10:00 前	裁判报到	裁判长	

（比赛第一天）	09:00-12:00	参赛队报到	赛点学校	安排住宿，领取资料
	10:00-12:00	检查封闭赛场	裁判长	裁判、专家组、监督员、技术人员参加
	12:00-12:30	赛场工作人员会议	赛点负责人	巡视员、裁判长、专家组长、监督员、联络员、赛场技术人员、场外工作人员参加
	12:30-14:00	领队会	裁判长	巡视员、专家组长、赛点负责人、监督员、联络员、各参赛队领队参加
	14:00-14:30	裁判员会议	裁判长	巡视员、专家组、裁判、联络员、监督员、赛场技术人员参加
	14:30-15:30	第一次抽签	加密裁判	加密（抽序号）
	15:00-16:00	理论考试	裁判长	
	16:00-16:30	参观赛场	裁判长	
	16:30	返回酒店	参赛领队	
赛中（比赛第二天）	9：30—10：00	观摩现场	裁判长	
赛中（比赛第三天）	07:30	到技能赛场	各参赛队领队	
	07:30-08:00	大赛检录	检录员	参赛选手，检录工作人员
	08:00-08:20	第二次抽签	加密裁判	加密（抽工位号）
	08:00	依次进入赛场	裁判长	按要求入赛场
	08:20	宣读竞赛须知	裁判长	
	08:20-08:30	领取比赛任务	裁判长	
	08:30-12:30	正式比赛	裁判长	
	08:30-11:00	评分裁判培训会议	专家组	
	11:30-12:00	午餐	大赛联络员	评分裁判、监督、仲裁、专家组、巡视员、联络员会议室就餐

	12:40-13:10		各领队	参赛选手、指导教师、领队到学校食堂就餐
			裁判长	现场裁判会议室就餐
	13:30	回酒店	各领队	参赛选手、指导教师、领队回住宿酒店
	15:00		裁判长	现场裁判回住宿酒店
	12:40-16:40	评判	裁判长	
	16:40-17:50	成绩汇总与解密	裁判长	评分裁判、裁判长、专家、监督、大赛组委会联络员参加
	17:00	赴成绩发布会现场	裁判长	乘车前往赛场参加成绩发布会
	17:35-17:50	赛项测评	各市领队	各市领队、指导老师参加测评
	18:00-18:40	成绩发布会	巡视员	
	18:40	回酒店或返程	承办校负责人	
赛后（竞赛后一天）	8:00—17:00	提交赛项文档	裁判长	
	8:00—17:00	提交大赛总结和点评文档	专家组长	

2.教师竞赛流程图如下图所示：



教师组网络搭建与应用赛项竞赛流程图

六、竞赛赛卷

（一）学生组赛卷

根据学生组竞赛内容，由专家组负责本赛项命题工作。本赛项公开赛卷（1 套）和主要网络环境（10 套），比赛时由监督员抽取其中一套赛卷进行比赛（注：若因报名人数和承办校比赛场等地情况需要分两天比赛，则抽取两套赛卷），比赛完成后，赛卷进行封闭回收。具体内容将于省赛前一个月由大赛组委会统一公开发布。正式赛题与公开赛卷原则上修改部分不超过 30%。为贯彻公开、公平、公正原则，本赛卷的样卷见附件一、学生组赛卷样卷。

（二）教师组赛卷

根据教师组竞赛内容，由专家组负责本赛项命题工作。本赛项公开赛卷（1 套）和主要网络环境（10 套），比赛时由监督员抽取其中一套赛卷进行比赛，比赛完成

后，赛卷进行封闭回收。具体内容将于省赛前一个月由大赛组委会统一公开发布。正式赛题与公开赛卷原则上修改部分不超过30%。为贯彻公开、公平、公正原则，本赛卷的样卷见附件二、教师组赛卷样卷。

七、竞赛规则

（一）选手报名

1.学生组参赛对象为中等职业学校（含技工学校）在校生及五年制高职一至三年级学生；教师组参赛对象为中等职业学校在编教师或已连续聘用的在聘教师（即2020年9月以前在聘教师）。获得过省赛、国赛学生组一等奖的学生选手不得参加同一赛项2023年度竞赛。获2021年、2022年教师组一等奖的教师不得参加2023年同一赛项竞赛。

2.团体赛不得跨校组队，同一学校相同项目报名参赛队原则上不超过1支；个人赛同一学校相同项目报名人数原则上不超过2人。

3.各职业院校按照大赛组委会规定的报名要求，通过“江苏省职业院校技能大赛网络报名系统”报名参赛。

4.参赛选手和指导教师报名，获得确认后不得随意更换。比赛前参赛选手和指导教师因故无法参赛，须由学校在相应赛项开赛前10个工作日出具书面说明，并按参赛选手资格补充人员并接受审核，经省大赛组委会办公室同意后予以更换。

5.各设区教育行政部门负责本地参赛师生的资格审查工作。

（二）熟悉场地

比赛前一天下午安排参赛队熟悉比赛场地，召开领队会议，宣布竞赛纪律和有关事宜。

（三）赛场规范

赛前准备：选手抽签加密入场，参赛队就位并领取比赛任务，完成比赛设备、线缆和工具检查等准备工作。

正式比赛：参赛选手需按题目要求规划IP地址，设备连接、配置网络设备、安装配置操作系统，部署安全策略等，完成企业级网络搭建及应用项目实施。操作顺序和分工，由参赛队自行商定。

（四）成绩评定与结果公布

成绩评定和结果公布由裁判组、监督组和仲裁组组成的成绩管理机构负责。

1.裁判组实行“裁判长负责制”，设裁判长1名，全面负责赛项的裁判分工、裁

判评分审核、处理比赛中出现的争议问题等工作。

2.裁判员根据比赛需要分为检录裁判、加密裁判、现场裁判和评分裁判。

检录裁判：负责对参赛队伍（选手）进行点名登记、身份核对等工作；

加密裁判：负责组织参赛队伍（选手）抽签，对参赛队信息、抽签代码等进行加密；

现场裁判：按规定做好赛场记录，维护赛场纪律，评定参赛队的过程得分；

评分裁判：负责按评分细则评定成绩。

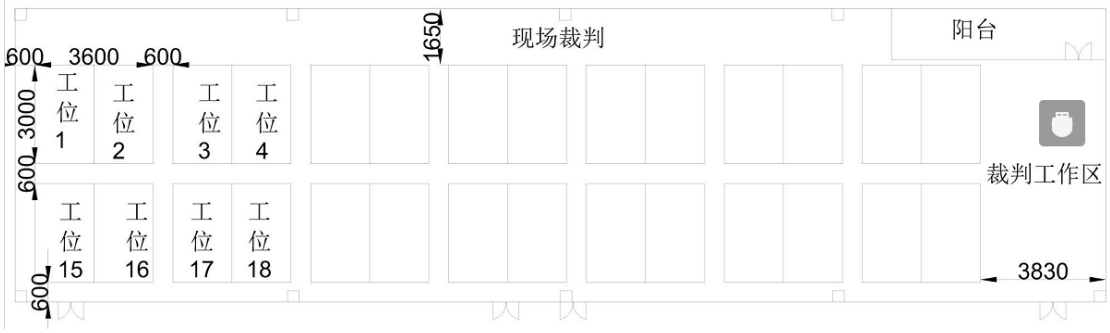
3.监督组对裁判组的工作进行全程监督，并对竞赛成绩抽检复核。

4.仲裁组负责接受由参赛队领队提出的对裁判结果的申诉，组织复议并及时反馈复议结果。

5.最终成绩经裁判组、监督组和仲裁组审核无误后正式公布。

八、竞赛环境

（一）竞赛场地安排



（二）理论竞赛环境要求

每个工位需提供一台 PC 机（安装 WINDOWS 10/11、谷歌浏览器、内网带宽 1000Mbps），工位数不低 160 个，每工位配备 220V 电源（带漏电保护装置），工位内的电缆线应符合安全要求。竞赛工位标明工位号，要求保证赛场采光(大于500lux)、照明通风良好、温度湿度适宜。

（三）技能竞赛环境要求

竞赛工位内设有操作平台，每工位配备220V电源（带漏电保护装置），工位内的电缆线应符合安全要求。每个竞赛工位面积6-9㎡，确保参赛队之间互不干扰，具备至少安排28支参赛队的技能赛场。竞赛工位标明工位号和参赛设备号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于500lux)、

照明通风良好、温度湿度适宜；为每支参赛队提供一套网络布线工具、6类双绞线60米、水晶头40个和一个垃圾箱，留有出入和消防通道。比赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护，承办单位应提供保证应急预案实施的条件，必须明确制度和预案。安装 UPS，采用UPS 防止现场因突然断电导致的系统数据丢失，额定功率：3KVA，后备时间：5小时，电池类型：输出电压：220V±5%V；市电采用双路供电，备用线路切换无间隔。

（四）医疗服务及要求

配备防疫和急救人员与设施。

（五）裁判员工作场所及要求

现场裁判工作场地与要求详见（一）竞赛场地安排；评分裁判需要2间各30平米的房间，每间需要提供两张不小于3*2的方桌，每张方桌配置6把靠椅，配备220V电源（带漏电保护装置），提供打印机一台。

（六）赛场保密场所及要求

保密室需要提供可容纳160*50张A4纸的保险柜，两台不低于20张/分钟的激光打印机及用于装订试卷的必要设备设施。

（七）赛场摄像头安装要求

指导教师、领队、参赛选手可在直播室观看选手操作现场。

（八）其他需要说明的内容

九、技术规范

（一）国家技术技能标准

1、GB/T 25069-2022 《信息安全技术 术语》

2、GB/T 41269-2022 《网络关键设备安全技术要求 路由器设备》

3、GB/T 41268-2022 《网络关键设备安全检测方法 路由器设备》

4、GB50311-2016 《综合布线系统工程设计规范》

5、GB50312-2016 《综合布线系统工程验收规范》

6、GB50174-2017 《电子信息系统机房设计规范》

7、GB21671-2018 《基于以太网技术的局域网系统验收测评规范》

8、GB50348-2018 《安全防范工程技术标准》

9、GB/T22239-2018 《信息系统安全等级保护基本要求》

（二）行业技术技能标准

1、YD/T 4059-2022《混合云平台安全能力要求》

2、JGJ/T121-2015 《工程网络计划技术规程》

（三）职业素养规范及要求

1、认识网络——网络基本知识能力；

2、理解网络——网络的特征和功能；

3、安全触网——高度网络安全意识；

4、善用网络——网络信息获取能力；

5、从容对网——网络信息识别能力；

6、理性上网——网络信息评价能力；

7、高效用网——网络信息传播能力；

8、智慧融网——创造性地使用网络；

9、阳光上网——坚守网络道德底线；

10、依法上网——熟悉常规网络法规。

十、技术平台

（一）竞赛设备、设施、附件

序号	设备类型	设备规格及型号
1	综合布线设备	1 台综合布线机柜（含机架、强弱电综合布线钢墙、24 口六类配线架，2 个底盒。
2	网络组建设备	（1）3 台三层交换机（参考型号：神州数码 CS6200-28X-EI）； （2）2 台防火墙（参考型号：神州数码 DCFW-1800S-H-V2）； （3）1 台无线控制器（参考型号：神州数码 DCWS-6028）； （4）1 台无线 AP（参考型号：神州数码 DCWL-7962AP 或 WL8200-I2）。
3	通用设备	（1）2 台普通计算机（CPU>=四核心四线程、主频≥3.0GHz；内存≥16GB；硬盘≥1TB； DVD 光驱），支持硬件虚拟化，2 块千兆位有线网卡； （2）2 台高性能计算机（CPU>=四核心四线程、主频≥3.5GHz；内存≥32GB；硬盘≥4TB；DVD 光驱，支持硬件虚拟化，2 块

		千兆位有线网卡）或 1 台云实训平台（参考型号：神州数码 DCC-CRL1000）。

（二）竞赛工具清单

一套网络布线工具。

（三）竞赛材料及耗材清单

1个垃圾箱和各类相关耗材若干。

（四）竞赛用软件清单

序号	软件参数	备注
1	Windows 10 /11 中文专业版	赛场提供
2	Rocky8.3	赛场提供
3	Windows Server 2022 中文数据中心版	赛场提供
4	WPS Pro 2022 专业试用版	赛场提供
5	SecureCRT -SecureFX9 及以上	赛场提供
6	kubernetes 的 rpm 包	赛场提供
7	tomcat10 及以上	赛场提供
8	oracle jdk-17 及以上	赛场提供
9	VLC media player 播放器	赛场提供

（五）允许选手翻阅的技术资料清单

所有硬件设备使用手册。

（六）劳保用品清单

遵循疫情防控要求。

（七）裁判工作需要的办公用品及设备、测量设备、场所等要求及清单

1.赛点提供两间评分裁判工作室；竞赛区域需设置现场裁判工作区域，需配备计算机和打印机各一台。

2.裁判用的办公用品主要包括：黑色和红色水笔、订书机、计算器、A4打印纸等。

（八）其他需要列出的清单

无

（九）现场需要配备的技术支持、志愿者、工作人员的要求及数量等

技术支持3名，1名负责计算机的维护，2名负责网络设备的维护；志愿者6名；工作人员4名。

十一、成绩评定

（一）评分方法

1.裁判队伍组成

成绩评定实行裁判长负责制，裁判组独立完成成绩评定工作。由竞赛裁判经验丰富的人员组成，具体组成和要求如下表。

裁判员组成与执裁资格要求

序号	裁判员类别	知识能力要求	工作经历	专业技术职称或资格等级	人数
1	加密裁判	能熟练运用电脑办公软件，认真细致负责完成加密工作	有责任心，与参赛队无利益关系	中级以上职称	2
2	现场裁判	掌握网络布线和计算机网络方面知识和技能	省级以上执裁经验或5年以上相关专业教学经验或相关行业工作经验	专业相关中级职称（高级职业资格证书/技能等级）	6
3	评分裁判	掌握网络布线、网络调试、操作系统和虚拟化方面知识和技能	省级以上执裁经验或5年以上相关专业教学经验或相关行业工作经验	专业相关中级职称（高级职业资格证书/技能等级）	12
4	统分裁判	能熟练运用电脑办公软件，认真细致负责完成加密工作	有责任心，与参赛队无利益关系	中级以上职称	2
裁判员总数：22					

2.裁判评分方法

理论考核部分在线提交后，系统自动评判，现场出分，每参赛队两位选手平均成绩计入团队分数；

实操技能考核部分采用分步得分、累计总分的积分方式，按照网络配置设备和虚拟机的配置及测试结果文件维度分别计算得分，只记录团队分数， 不计参赛选手个人得分；

职业素养考核由现场裁判根据选手的实操过程表现，按职业素养要求独立打

分，每组由2位裁判打分，取两位裁判的平均值作为团队该项的分数；

三部分分数合计为参赛队总分。

3.成绩产生方法

除职业素养考核部分带有一定的主观性，由两位裁判的平均值作为该项团队的分数，另外两部分即理论考核部分和实操技能考核部分均为客观评分，能保证成绩评定的公开、公平、公正。

4.成绩审核方法

各裁判员首先审核自身对选手的原始打分成绩，并签名；裁判长对所有裁判员的打分成绩进行审核，并签名。

（二）成绩复核与解密

监督、仲裁组将对赛项总成绩排名前30%的所有参赛队伍（选手）的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖率不得低于15%。如发现成绩错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。复核、抽检错误率超过5%的，裁判组将对所有成绩进行复核。

成绩复核、确认无误后进行成绩排名，得出排名结果后进行解密，不允许先解密后排序。

（三）成绩公布

记分员将解密后的各参赛队竞赛成绩进行汇总制表，经裁判长、监督仲裁组签字后在指定地点，以纸质形式向全体参赛队进行公布。公布2小时无异议后，将赛项总成绩的最终结果录入赛务管理系统，经裁判长、监督仲裁组长在导出成绩单上审核签字后，在闭赛式上宣布。

（四）评分标准

1、学生组：

任务（或模块） (一级指标)	任务组成 (二级指标)	技能点、知识点或难易度 （三级指标）	比例
一、理论考试	计算机网络理论	计算机网络的组成，体系结构及协议，	6%

（15%）	（7%）	局域网标准及主流局域网技术，广域网及网络互连技术，无线网络技术	
		网络应用等理论知识	1%
	网络操作系统理论（7%）	Linux系统的基础知识，基本命令及应用，文件系统及服务器配置，网络安全等理论知识；	3.5%
		Windows 系统的基本概念，用户与组、域与策略、磁盘与文件管理、网络安全与服务器配置等理论知识点；	3.5%
	虚拟化、集群等（1%）	虚拟化、集群与云计算等基本概念，与其服务配置相关的理论知识点等。	1%
二、实操技能考核（80%）	网络配置（35%）	设备连接，保证和测试物理连通性，IP地址划分实施	3%
		指定的交换、路由、广域网和无线的配置	20%
		企业网防火墙相关策略配置	4%
		网络优化配置、VPN 配置	6%
		无线网络安全配置	2%
	Windows（20%）	Windows 操作系统的安装和配置	3%
		Windows 安装配置各类应用服务和数据库安装调试	13%
		WINDOWS 操作系统方面安全技术配置	4%
	Linux（20%）	Linux 操作系统的安装和配置	3%
		Linux 安装配置各类应用服务和数据库安装调试	13%
		Linux 操作系统方面安全技术配置	4%
	云平台配置（5%）	虚拟化与服务器集群技术	5%
三、职业素养（5%）	1、团队合作默契，做好个人防护；		1%
	2、科学专业施工，耗材做到最简；		1%
	3、整理赛位，工具、设备归位，保持赛后整洁有序；		1%
	4、无因参赛选手的原因导致设备损坏等。		2%

2、教师组：（要求与学生组相同）

任务（或模块） (一级指标)	任务组成 (二级指标)	技能点、知识点或难易度 （三级指标）	比例
一、理论考试 （15%）	计算机网络理论（6%）	计算机网络的组成，体系结构及协议，局域网标准及主流局域网技术，广域网及网络互连技术，无线网络技术	5%
		网络应用等理论知识	1%
	网络操作系统理论（6%）	Linux系统的基础知识，基本命令及应用，文件系统及服务器配置，网络安全等理论知识；	3%
		Windows 系统的基本概念，用户与组、域与策略、磁盘与文件管理、网络安全与服务器配置等理论知识点；	3%
	虚拟化、集群等（1%）	虚拟化、集群与云计算等基本概念，与其服务配置相关的理论知识点等；	1%
	计算机科学与技术的基础理论（2%）	计算理论、信息与编码理论、程序理论、算法分析和计算复杂度理论、并行与分布处理理论等。	2%
二、实操技能考核 （80%）	网络配置 （35%）	设备连接，保证和测试物理连通性，IP地址划分实施	3%
		指定的交换、路由、广域网和无线的配置	20%
		企业网防火墙相关策略配置	4%
		网络优化配置、VPN 配置	6%
		无线网络安全配置	2%
	Windows（16%）	Windows 操作系统的安装和配置	3%
		Windows 安装配置各类应用服务和数据库安装调试	9%
		WINDOWS 操作系统方面安全技术配置	4%
	Linux（16%）	Linux 操作系统的安装和配置	3%
		Linux 安装配置各类应用服务和数据库安装调试	9%
		Linux 操作系统方面安全技术配置	4%

	云平台配置（8%）	虚拟化与服务器集群技术	8%
	实验教学设计文档（5%）	规范撰写实训指导文档	5%
三、职业素养（5%）	1、团队合作默契，做好个人防护；		1%
	2、科学专业施工，耗材做到最简；		1%
	3、整理赛位，工具、设备归位，保持赛后整洁有序；		1%
	4、无因参赛选手的原因导致设备损坏等。		2%

十二、奖项设定

（一）参赛选手奖

根据竞赛成绩，从高到低排序，个人赛按参赛人数、团体赛按参赛队的数量，其中10%设一等奖，20%设二等奖，30%设三等奖。

（二）指导教师奖

对获得一、二、三等奖选手的指导教师颁发指导教师奖。

十三、赛场预案

赛前成立由巡视员、专家组长、裁判长、监督组长、仲裁组长、承办校领导等相关人员组成的应急处理小组，比赛期间发生任何意外事故（如赛卷、设备、安全等），发现者应第一时间报告专家组长，立即采取措施避免事态扩大，启动应急预案予以解决并报告大赛组委会。赛项出现重大安全问题可以停赛，是否停赛由赛项组委会决定。事后，应向大赛组委会报告详细情况。

（一）医疗及安全事故预案

1.现场布置急救设施（如：120急救车和供电车场馆外等候等）。

2.赛场内设置医疗救护区(如:竞赛期间,安排医生随时处理突发的医疗事故)。

3.竞赛期间偶发大规模意外事件，立即启动《偶发大规模意外事件处理应急预案》(采取中止比赛、快速疏散人群等措施避免事态扩大，并第一时间报告赛区执委会)。

（二）水电事件应急预案

制订责任到人的事件处理小组，竞赛时现场值守，突发水、电供给不良时及时响应，维持秩序的同时，调配专业的人员，及时查明原因、排除故障。(如现场配置水桶、应急发电车值守等)。

（三）火灾事件应急预案

制订责任到人的事件处理小组，竞赛时现场值守。如发生火灾，及时组织人员疏散、切断电源，将易燃易爆物品及时转移到安全地段，同时组织人员使用适宜的灭火器材灭火。对轻伤人员有医疗人员进行处置，对重伤人员及时送往医院进行救治。

（四）竞赛设备损坏应急预案

制订责任到人的竞赛设备损坏应急处理小组，竞赛时现场值守。赛场每个工位由赛场工作人员或厂方技术人员负责，及时解决比赛中突发的设备故障，解决不了的，启用备用工位，保证竞赛正常进行。

（五）赛卷应急预案

比赛过程中一旦出现赛卷密等问题，立即由巡视员、专家组长、裁判长、监督组长和仲裁组长会商，并向大赛组委会报告，启用备用赛卷。

（六）竞赛作品提交预案

1、在赛场规定的场所递交；

2、在竞赛规定的时间递交；

3、按照规定的程序递交；

4、递交现场及过程全程录像。

5、如提交电脑（电子）作品的，应有参赛选手自己操作，参赛选手完成提交操作后，由参赛选手和裁判签字确认。

十四、赛项安全

赛项安全是技能竞赛一切工作顺利开展的先决条件，是赛项筹备和运行工作必须考虑的核心问题。采取切实有效措施保证大赛期间参赛选手、指导教师、裁判员、工作人员及观众的人身安全。

（一）比赛环境

在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。承办单位赛前须按照赛项规程要求排除安全隐患。

赛场周围要设立警戒线，防止无关人员进入发生意外事件。比赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁

判员要严防选手出现错误操作。

承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、可能有坠物、大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

承办单位制定开放赛场和体验区的人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，须增加引导人员，并开辟备用通道。

大赛期间，承办单位应在赛场管理的关键岗位增加力量并建立安全管理日志。

参赛选手进入工位、赛事裁判工作人员进入工作场所，严禁携带通讯、照相摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（二）生活条件

比赛期间，统一安排参赛选手和指导教师食宿。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

比赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由提供宿舍的学校负责。

大赛期间承办单位须保障比赛期间选手、指导教师和裁判员、工作人员的交通安全。

各赛项的安全管理，除了可以采取必要的安全隔离措施外，应严格遵守国家相关法律法规，保护个人隐私和人身自由。

（三）参赛队责任

1. 各学校组织参赛队时，须安排除参赛选手、指导教师、领队以外的随行人员购买大赛期间的人身意外伤害保险。

2. 各学校参赛队组成后，须制定相关管理制度，并对所有选手、指导教师进行安全教育。

3. 各参赛队伍须加强对参与比赛人员的安全管理，实现与赛场安全管理的对接。

（四）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项专家组长，同时采取措施避免事态扩大，立即启动预案予以解决并报告组委会。赛项出现重大安全问题可以停赛，应向组委会报告详细情况。

（五）处罚措施

1.因参赛队伍原因造成重大安全事故的，取消其获奖资格。

2.参赛队伍有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续比赛的资格。

3.赛场工作人员违规，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

十五、竞赛须知

（一）参赛队须知

1.参赛队名称统一使用规定的代表队名称。

2.参赛队员在报名获得审核确认后，原则上不再更换，如筹备过程中，选手因故不能参赛，所在学校需出具书面说明并按相关规定补充人员并接受审核；开赛前10日以内，参赛队不得更换参赛队员，允许缺员比赛。

3.参赛队按照大赛赛程安排凭大赛组委会颁发的参赛证和有效身份证件参加比赛及相关活动。

4.各参赛队统一安排参加比赛前熟悉场地环境的活动。

5.各参赛队准时参加赛前领队会，领队会上举行抽签仪式抽取场次号。

6.各参赛队要注意饮食卫生，防止食物中毒。

7.各参赛队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。

（二）指导老师须知

1.各指导老师要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。指导老师经报名、审核后确定，一经确定不得更换。

2.对申诉的仲裁结果，领队和指导老师应带头服从和执行，还应说服选手服从和执行。

3.指导老师应认真研究和掌握本赛项比赛的技术规则和赛场要求，指导选手做好赛前的一切准备工作。

4.领队和指导老师应在赛后做好技术总结和工作总结。

（三）参赛选手须知

1.参赛选手应遵守比赛规则，尊重裁判和赛场工作人员，自觉遵守赛场秩序，服从裁判的管理。

2.参赛选手应佩戴参赛证，带齐身份证、注册的学生证。在赛场的着装，应符

合职业要求。在赛场的表现，应体现自己良好的职业习惯和职业素养。

3.进入赛场前须将手机等通讯工具交赛场相关人员保管，不能带入赛场。未经检验的工具、电子储存器件和其他不允许带入赛场物品，一律不能进入赛场。

4.比赛过程中不准互相交谈，不得大声喧哗；不得有影响其他选手比赛的行为，不准有旁窥、夹带等作弊行为。

5.参赛选手在比赛的过程中，应遵守安全操作规程，文明的操作。通电调试设备时，应经现场裁判许可，在技术人员监护下进行。

6.比赛过程中需要去洗手间，应报告现场裁判，由裁判或赛场工作人员陪同离开赛场。

7.完成比赛任务后，需要在比赛结束前离开赛场，需向现场裁判示意，在赛场记录上填写离场时间并签工位号确认后，方可离开赛场，离开赛场后不可再次进入。未完成比赛任务，因病或其他原因需要终止比赛离开赛场，需经裁判长同意，在赛场记录表的相应栏目填写离场原因、离场时间并签工位号确认后，方可离开；离开后，不能再次进入赛场。

8.裁判长发出停止比赛的指令，选手（补时选手除外，等延时结束）应立即停止操作进入通道，在现场裁判的指挥下离开赛场。

9.遇突发事件，立即报告裁判和赛场工作人员，按赛场裁判和工作人员的指令行动。

（四）工作人员须知

1.工作人员必须服从赛项组委会统一指挥，佩戴工作人员标识，认真履行职责，做好服务赛场、服务选手的工作。

2.工作人员按照分工准时上岗，不得擅自离岗，应认真履行各自的工作职责，保证竞赛工作的顺利进行。

3.工作人员应在规定的区域内工作，未经许可，不得擅自进入竞赛场地。如需进场，需经过裁判长同意，核准证件，有裁判跟随入场。

4.如遇突发事件，须及时向裁判长报告，同时做好疏导工作，避免重大事故发生，确保竞赛圆满成功。

5.竞赛期间，工作人员不得干涉及个人工作职责之外的事宜，不得利用工作之便，弄虚作假、徇私舞弊。如有上述现象或因工作不负责任的情况，造成竞赛程序无法继续进行，由赛项组委会视情节轻重，给予通报批评或停止工作，并通知其所在单位做出相应处理。

（五）裁判员须知

1.裁判员执裁前应参加培训，了解比赛任务及其要求、考核的知识与技能，认真学习评分标准，理解评分表各评价内容和标准。不参加培训的裁判员，取消执裁资格。

2.裁判员执裁期间，统一佩戴裁判员标识，举止文明礼貌，接受参赛人员的监督。

3.遵守执裁纪律，履行裁判职责，执行竞赛规则，信守裁判承诺书的各项承诺。服从赛项专家组和裁判长的领导。按照分工开展工作，始终坚守工作岗位，不得擅自离岗。

4.裁判员有维护赛场秩序、执行赛场纪律的责任，也有保证参赛选手安全的责任。时刻注意参赛选手操作安全的问题，制止违反安全操作的行为，防止安全事故的出现。

5.裁判员不得有任何影响参赛选手比赛的行为，不得向参赛选手暗示或解答与竞赛有关的问题，不得指导、帮助选手完成比赛任务。

6.公平公正的对待每一位参赛选手，不能有亲近与疏远、热情与冷淡差别。

7.赛场中选手出现的所有问题如：违反赛场纪律、违反安全操作规程、提前离开赛场等，都应在赛场记录表上记录，并要求学生签工位号确认。

8.严格执行竞赛项目评分标准，做到公平、公正、真实、准确，杜绝随意打分；对评分表的理解和宽严尺度把握有分歧时，请示裁判长解决。严禁利用工作之便，弄虚作假、徇私舞弊。

9.竞赛期间，因裁判人员工作不负责任，造成竞赛程序无法继续进行或评判结果不真实的情况，由赛项组委会视情节轻重，给予通报批评或停止裁判资格，并通知其所在单位做出相应处理。

十六、申诉与仲裁

（一）各参赛队对不符合赛项规程规定的设备、工具、材料、计算机软硬件、竞赛执裁、赛场管理及工作人员的不规范行为等，可向赛项仲裁组提出申诉。

（二）申诉主体为参赛队领队。

（三）申诉启动时，参赛队以该队领队签字同意的书面报告的形式递交赛项仲裁组。报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。非书面申诉不予受理。

（四）提出申诉应在赛项比赛结束后2小时内提出。超过2小时不予受理。

（五）赛项仲裁组在接到申诉报告后的2小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由领队向大赛仲裁工作组提出申诉。大赛仲裁工作组的仲裁结果为最终结果。

（六）申诉方不得以任何理由拒绝接收仲裁结果；不得以任何理由采取过激行为扰乱赛场秩序。仲裁结果由申诉人签收，不能代收；如在约定时间和地点申诉人离开，视为自行放弃申诉。

（七）申诉方可随时提出放弃申诉。

十七、竞赛观摩

1.观摩期间，必须服从现场工作人员的指挥，保持安静，不得大声喧哗，不得在观摩区来回走动影响他人观摩。

2.各参赛队人员需提前15分钟到达观摩区入口处进行证件核查。

3.视频观摩地点由承办院校安排，观摩人员在观摩期间，不得吸烟，不得携带水或液体食品进入观摩区。

十八、竞赛直播

1.赛场内部署无盲点录像设备，能实时录制并播送赛场情况；

2.赛场外有大屏幕或投影，同步显示赛场内竞赛状况；

3.条件允许时，本赛项进行网上直播。

十九、其他

1.参赛选手及相关工作人员，由赛项承办院校赛统一安排食宿，费用自理。

2.本技术文件的最终解释权归大赛组织委员会。

附件一、学生组赛卷样卷

附件二、教师组赛卷样卷

附件一、学生组赛卷样卷

2023 年江苏省职业院校技能大赛网络搭建与应用赛项中职组样卷

技能要求

竞赛说明

1. 竞赛内容分布

“网络搭建与应用”竞赛共分五个部分，其中：

第一部分：网络组建与配置（35 分）

第二部分：云平台配置（5 分）

第三部分：Windows 系统配置（20 分）

第四部分：Linux 系统配置（20 分）

第五部分：职业素养（5 分）

2. 项目简介

某集团公司原在北京建立了总部，在郑州设立了办事处。总部设有销售、产品、法务、财务、信息技术 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 动态路由协议和静态路由协议进行互连互通。

公司规模在 2020 年快速发展，业务数据量和公司访问量增长巨大。为了更好管理数据，提供服务，集团决定建立自己的中型数据中心及业务服务平台，以达到快速、可靠交换数据，以及增强业务部署弹性的目的。

集团、办事处的网络结构详见“主要网络环境”拓扑图。

其中一台 CS6200 交换机编号为 SW-3，用于实现终端高速接入；两台 CS6200 交换机作为总部的核心交换机；两台 DCFW-1800 分别作为集团、郑州办事处的防火墙；一台 DCWS-6028 作为集团的有线无线智能一体化控制器，编号为 DCWS，通过与 WL8200-I2 高性能企业级 AP 配合实现集团无线覆盖。

第一部分：网络组建与配置（35 分）

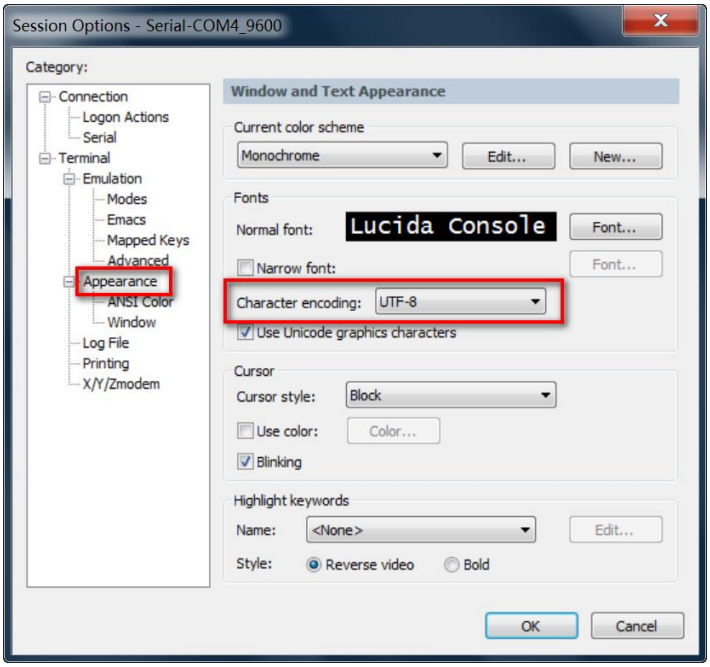
【说明】

1. 交换机、 DCWS、防火墙使用同一条 console 线；

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。所有提交的文档必须按照赛题所规定的命名规则命名；所有需要提交的文档均放置在 PC1 桌面的“比赛文档_X”（X 为赛位号）文件夹中；

3. 保存文档方式如下：

- 交换机、DCWS 要把 show running-config 的配置、防火墙要把 show configuration 的配置保存在 PC1 桌面上的“比赛文档_X”文件夹中，文档命名规则为：设备名称.txt。例如：SW-1 交换机文件命名为：SW-1.txt；
- 无论通过 SSH、telnet、Console 登录防火墙进行 show configuration 配置收集，需要先调整 CRT 软件字符编号为：UTF-8，否则收集的命令行中文信息会显示乱码。CRT 软件调整字符编号配置如图：



一、 网络布线与基础连接

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	W1-06-102-1	W1	102	1	06

（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 568A 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. PC1 连接 102 底盒 1 端口、PC2 连接 101 底盒 1 端口。

二、 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。具体要求如下：

1. 配置合理，所有链路上不允许不必要 VLAN 的数据流通过，包括 VLAN 1；

2. 集团接入交换机与核心交换机之间的互连接口发送 AP&交换机管理 VLAN 的报文时不携带标签，发送其它 VLAN 的报文时携带标签，要求禁止采用 trunk 链路类型；

3. 当财务业务 VLAN 物理端口接收到的流量大于端口缓存所能容纳的大小时，端口将通知向其发送流量的设备减慢发送速度，以防止丢包；当法务业务 VLAN 物理端口收包 BUM 报文速率超过 2000packets/s 则关闭端口，10 分钟后恢复端口。

4. 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	VLAN 名称	端口	说明
SW-3	VLAN10	XS	E1/0/6	销售
	VLAN20	CP	E1/0/7	产品
	VLAN30	FW	E1/0/8	法务
	VLAN40	CW	E1/0/9	财务
	VLAN50	XXJS	E1/0/10 至 E1/0/12	信息技术
	VLAN200	GL	E1/0/13	AP&交换机管理 VLAN

(二) 在集团核心交换机 SW-1 和 SW-2、接入交换机 SW-3 间运行一种协议，具体要求如下：

1. 实现销售、产品、信息技术业务优先通过 SW-1 至 SW-3 间链路转发，法务、财务、AP&交换机管理等业务优先通过 SW-2 至 SW-3 间链路转发，从而实现 VLAN 流量的负载分担与相互备份；

2. 设置路径开销值的取值范围为 1-65535，BPDU 支持在域中传输的最大跳数为 7 跳；同时不希望每次拓扑改变都清除设备 MAC/ARP 表，全局限制拓扑改变进行刷新的次数；

3. 加速接入交换机所有业务端口收敛，当接口收到 BPDU 丢弃报文并关闭端口，如果 5 分钟内没有收到 BPDU 报文，则恢复该端口。

(三) 在集团核心交换机 SW-1 和 SW-2 运行一种容错协议，为所有业务 VLAN 实现网关冗余，具体要求如下：

1. 虚地址使用该 VLAN 中的最后一个可用 IP、SW-1 使用该 VLAN 中的倒数第三可用 IP、SW-2 使用该 VLAN 中的倒数第二可用 IP，SW-1 为销售、产品、信息技术业务的 Master，SW-2 为法务、财务、AP&交换机管理等业务的 Master，且互为备份；每隔 3s，VRRP 备份组中的 Master 发送 VRRP 报文来向组内的三层交换机通知自己工作状态；

2. 监视上行链路状态，当上行链路故障时，Slave 设备能够接管 Master 设备转发数据；而当链路故障恢复后，原 Master 设备接管 Slave 设备转发数据。

(四) 因集团销售人员较多、同时也为了节约成本，在集团接入交换机下挂两个 8 口 HUB 交换机实现销售业务接入，集团信息技术部已经为销售业务 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。

(五) 集团接入交换机与核心交换机之间的互连采用光纤接口且跨楼层，当发现单向链路后，要求自动地关闭互连端口；发送握手报文时间间隔为 5s，以便对链路连接错误做出更快的响应，如果某端口被关闭，经过 30 分钟，该端口自动重启。

(六) SW-2 既作为集团核心交换机，同时又使用相关技术将 SW-2 模拟为 Internet 交换机，实现集团内部业务路由表与 Internet 路由表隔离。

(七) 集团预采购多个厂商网流分析平台对集团整体流量进行监控、审计，分别连接在 SW-1 核心交换机 E1/0/10-E1/0/11 接口测试，将核心交换机与接入交换机、防火墙互连流量提供给多个厂商网流分析平台。

三、 路由配置与调试

(一) 尽可能加大集团防火墙与核心交换机之间链路带宽；

(二) 规划集团使用 OSPF 协议进行互连互通，进程号为 1，具体要求如下：

1. 集团防火墙与集团核心交换机之间、集团核心交换机与集团核心交换机之间均属于骨干区域；

2. 借助 OSPF 相关特性，尽可能保证骨干区域完整性；

3. 针对骨干区域启用区域 MD5 验证，验证密钥为：DCN2019，调整接口的网络类型加快邻居关系收敛；

4. 集团防火墙将访问郑州办事处业务网段的静态路由引入 OSPF。

(三) 实现集团销售&产品&信息技术&无线业务、统一通过集团防火墙访问 Internet，轮询使用 NAT 地址为：202.99.192.4/30，针对上述源地址，限制单个 IP 地址能建立 NAT 翻译表项的最大数目为 100；配置一对一地址转换，实现通过 Internet 任意位置访问 202.99.192.8/32 都可以访问至集团 OA 平台 10.XX.10.1/32（XX 与“主要网络环境”地址中相应网段一致）进行数据查询；郑州办事处业务网段通过郑州办事处防火墙访问 Internet，NAT 地址池为接口公网 IP。

(四) 集团防火墙与郑州办事处防火墙之间使用与 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，郑州办事处通过静态路由协议访问集团销售网段在通过运营商网络传输时，就不用担心被监视、篡改和伪造，可以安全上传郑州办事处相关销售业务数据。

(五) 为了合理分配集团业务流向，保证来回路径一致，业务选路具体要求如下：

1. 集团核心交换机与集团无线控制器 DCWS 之间采用静态路由协议，使用 OSPF 相关特性实现集团无线业务与 Internet 互访流量优先通过 DCWS_SW-1_FW-1 间链路转发，DCWS_SW-2_FW-1 间链路作为备用链路；

2. 实现销售、产品、信息技术业务分别与 Internet、办事处互访流量优先通过 SW-1_ FW-1 间链路转发，法务、财务、AP&交换机管理等业务分别与分公司、办事处互访流量优先通过 SW-2_ FW-1 间链路转发，从而实现流量的负载分担与相互备份。

四、 无线配置

(一) 集团无线控制器 DCWS 与核心交换机互联，无线业务网关位于 DCWS 上，

VLAN220 为业务 VLAN；核心交换机侧配置使用 DHCP 进行 AP 管理地址分配，利用 DHCP 方式让 AP 发现 DCWS 进行三层注册，采用 MAC 地址认证。

(二) 配置一个 SSID DCNXX：DCNXX 中的 XX 为赛位号，访问集团及 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 Dcn12345678。

(三) 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 7:00 触发信道调整功能。

五、 安全策略配置

(一) 根据题目要求配置郑州办事处防火墙相应的业务安全域、业务接口；郑州办事处业务网段通过 VPN 隧道只可以访问集团销售业务网段 http&https 业务,通过公网接口可以访问 Internet 业务；集团所有业务网段均可以与郑州办事处业务网段双向互 ping，方便网络连通性测试与排障。

(二) 集团计划在郑州办事处进行 https 认证试点，对郑州办事处业务网段上网的用户进行控制，认证服务器为本地防火墙，只有在认证页面输入用户名和密码分别为 dcn01 或者 dcn02 才可以访问外部网络，强制用户在线时常超过 1 天后必须重新登录。

(三) 郑州办事处只有 100M Internet 出口，在郑州办事处防火墙上限制该业务网段每个 IP 上下行最多 4M 带宽；对 Internet 出口 http 流量整形到 10Mbps，从而实现流量精细化控制，保障办事处其它关键应用和服务的带宽。

六、 IPV6 配置

集团公司为贯彻落实中共中央办公厅、国务院办公厅印发的《推进互联网协议第六版（IPv6）规模部署行动计划》，加快推进基于互联网协议第六版（IPv6）基础网络设施规模部署和应用系统升级，现准备先在集团公司开始 IPv6 测试，要求如下：

(一)在集团核心交换机 SW-1 配置 IPv6 地址，使用相关特性实现销售业务的 IPv6 终端可自动从网关处获得 IPv6 有状态地址。

(二)在集团核心交换机 SW-2 配置 IPv6 地址，开启路由公告功能，路由公告的生存期为 2 小时，确保产品业务的 IPv6 终端可以获得 IPv6 无状态地址。

(三)在集团两台核心交换机之间通过互联 ipv4 链路使用相关特性，实现销售业务的 IPv6 终端与产品业务的 IPv6 终端可以互访。

集团测试 IPv6 业务地址规划如下，其它 IPv6 地址自行规划：

业务	IPV6 地址
销售	2001:XX:10::254/64 （XX 与“主要网络环境”地址中相应网段一致）
产品	2001:XX:20::254/64 （XX 与“主要网络环境”地址中相应网段一致）

举例：“主要网络环境”中销售业务 IPv4 地址为：10.30.10.0/24，对应 IPv6 地址为：2001:30:10::254/64。

第二部分：云平台配置（5 分）

【竞赛技术平台说明】

1．云服务实训平台相关说明：

（1） 云服务实训平台管理 ip 地址默认为 192.168.100.100，访问地址 http://192.168.100.100/dashboard 默认账号密码为 admin/dcncloud，ssh 默认账号密码为 root/dcncloud，考生禁止修改云服务实训平台账号密码及管理 ip 地址，否则服务器配置及应用项目部分计 0 分；

（2） 云服务实训平台中提供镜像环境，镜像的默认用户名密码以及镜像信息，参考《云服务实训平台用户操作手册（江苏省赛版）》；

名称	用户名	密码	ssh	rdp
Win10	admin	Qwer1234	否	是
Win2008	administrator	Qwer1234	否	是
Win2019	administrator	Qwer1234	否	是
Rocky8.3	root	dcncloud	是	否

（3） 所有 windows 主机实例在创建之后都直接可以通过远程桌面连接操作，Rocky8.3 可以通过 CRT 软件连接进行操作，所有 linux 主机都默认开启了 ssh 功能，Linux 系统软件镜像位于”/opt”目录下；

（4） 要求在云服务实训平台中保留竞赛生成的所有虚拟主机。

2．云服务实训平台和服务器 PC1 和 PC2 相关服务说明：

（1） 题目中所有未指明的密码均参见“表 6.云主机和服务器密码表”，若未按照要求设置密码，涉及到该操作的所有分值记为 0 分；

（2） 虚拟主机的 IP 属性设置请按照“拓扑结构图”以及“表 3.服务器 IP 地址分配表”的要求设定；

（3） 除非作特殊说明，在 PC1 和 PC2 上需要安装相同操作系统版本的虚拟机时，可采用 VMwareWorkstation 软件自带的克隆系统功能实现。

（4） PC1 和 PC2 上所有系统镜像文件及赛题所需的其它软件均存放在每台主机的 D:\soft 文件夹中；

（5） PC1 和 PC2 要求的虚拟机均安装于每台在 D 盘根目录下自建的名为 virtualPC 文件夹中，即路径为 D：\virtualPC\虚拟主机名称。

（6） 请在 PC2 桌面上，选手自己建立 BACKUP_X（X 为赛位号）文件夹，并将 PC2 上 D 盘 soft 文件夹中的《云实训平台安装与应用报告单》、《Windows 操作系统-云平台部分竞赛报告单》和《Linux 操作系统竞赛报告单》复制到 PC2 桌面的“BACKUP_X”（X 为赛位号）文件夹中、将 PC1 上 D 盘 soft 文件夹中的《Windows 操作系统-虚拟机部分竞赛报告单》复制到 PC1 桌面的“BACKUP_X”（X 为赛位号）文件夹中，并按照截图要求填写完整；如报告单、截图等存放位置错误，涉及到的所有操作分值记为 0 分；

（7） 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，否则会扣除该服务功能一定分数。

【云实训平台安装与运用】

（一）按照《主要网络环境》要求新建网络。

（二）按照《主要网络环境》要求新建云主机类型。

（三）按照《主要网络环境》要求新建虚拟主机；

所有虚拟主机 IP 地址与《主要网络环境》中的一致，且手动设置为该虚拟机自动获取的 IP 地址。

（四）按照下述题目相关要求新建硬盘，并连接到虚拟主机。

第三部分：Windows 系统配置（20 分）

一、在云实训平台上完成如下操作

（一）完成虚拟主机的创建

将按照“表 5：虚拟主机信息表”生成的虚拟主机加入到 skillsJiangSu.com 域环境；

（二）在云主机 1 中完成链路聚合的部署

添加安装一块网卡，第一块网卡和第二块网卡为提供链路聚合网卡，完成链路聚合操作，组名为“AggNic1”，成组模式为“静态成组”，负载均衡模式为“地址哈希”，为主域和辅助域之间的传输提升速度。

（三）在云主机 1 中完成 DNS 服务器的部署

1. 将此服务器配置为主 DNS 服务器，具体要求：

（1）正确配置 skillsJiangSu.com 域名的正向及反向解析区域；

（2）创建对应服务器主机记录，正确解析 skillsJiangSu.com 域中的所有服务器；

（3）关闭网络掩码排序功能；

（4）设置 DNS 服务正向区域和反向区域与活动目录集成；

（5）启用 Active Directory 的回收站功能；

2. 为了防止域控制器的 DNS 域名解析服务造成大量不必要的数据流，公司技术人员决定禁用 DNS 递归功能，请您使用 PowerShell 禁用 DNS 递归功能。

（四）在云主机 1 中完成域控制器及 CA 服务器的部署

1. 将云主机 1 的服务器配置成 CA 服务器：

（1）安装证书服务，为企业内部自动回复证书申请；

（2）设置为企业根，有效期为 6years；

（3）颁发的证书有效期年份为 3years；

2. 创建 3 个用户组，组名采用对应部门名称的中文全拼命名，每个部门都创建 2 个用户，行政部用户：adm1~adm2、销售部用户：sale1~sale2、技术部用户：sys1~sys2（如有需要可将技术部员工加入管理员组），所有用户不能修改其用户口令，并要求用户只能在上班时间可以登录（每周一至周五 9:00~18:00）；

3. 配置域中技术部的所有员工必须启用密码复杂度要求，密码长度最小为 9 位，密码最

长存留 30 天，允许失败登录尝试的次数、重置失败登录尝试计数都为 5 次，帐户将被锁定的时间为 5 分钟，直至管理员手动解锁账户；

4. 配置相关策略，防止用户随意退出域，实现所有行政部的用户登录域后自动去除“计算机”的上下文菜单中的“属性”；

5. 配置相关策略，实现所有销售部的计算机开机后自动弹出“温馨提示”的对话框，显示的内容为“请注意销售数据的安全！”。

（五）在云主机 1 中完成 DNS 安全防护的部署

1.新建一条主机记录，主机名称为 dnss、IP 地址为 10.30.30.140；

2.对云主机 1 的 skillsJiangSu.com 区域中的 dnss 主机记录提供完整性验证，来保证数据在传输的过程中不被篡改。

（六）在云主机 2 中完成链路聚合的部署

1.添加安装一块网卡，第一块网卡和第二块网卡为提供链路聚合网卡，完成链路聚合操作，组名为“AggNic2”，成组模式为“静态成组”，负载均衡模式为“地址哈希”，为主域和辅助域之间的传输提升速度。

（七）在云主机 2 中完成从属证书及磁盘阵列的部署

1.将云主机 2 的服务器升级成 skillsJiangSu.com 域的的辅助域控制器；

2.将云主机 2 的服务器设置为证书颁发机构：

（1）安装证书服务，为企业内部自动回复证书申请；

（2）设置为企业从属 CA，负责整个 skillsJiangSu.com 域的证书发放工作；

（八）在云主机 2 中完成 AD RMS 及网络打印服务的部署

1.安装 AD RMS 权限管理服务：

（1）要求安装“AD 权限管理服务器”和“联合身份验证支持”角色服务；

（2）使用 Windows 的内部数据库；

（3）指定群集地址为：https://adrms.skillsJiangSu.com；

（4）配置联合身份验证支持的服务器名称为：https://adrms.skillsJiangSu.com。

2.将云主机 2 的服务器配置成打印服务器：

（1）添加一台虚拟打印机，名称为“HP-Print”；

（2）将“HP-Print”发布到 AD 域；

（3）客户端访问网络打印服务器，能够通过访问“https://Print.skillsJiangSu.com”查看打印机，证书由本机进行签署颁发。

（九）在云主机 3 中完成文件服务器的部署

1.添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 10G，并创建 RAID5 卷，盘符为 E 盘；

2.在 E 盘上新建文件夹 FilesWeb，并将其设置为共享文件夹，共享名为 FilesWeb，开放共享文件夹的读取/写入权限给 everyone 用户；

3.在 FilesWeb 文件夹内建立两个子文件夹：

（1）子文件夹为“FilesConfigs”，用来存储共享设置；

（2）子文件夹为“FilesConts”，用来存储共享网页。

（十）在云主机 3 中完成 DHCP 及 WDS 服务的部署

1.安装 DHCP 服务，为服务器网段部分主机动态分配 IPv4 地址，建立作用域，作用域的名称为 dhcpser，地址池为 220-225，仅允许“服务器 3”的服务器获取 DHCP 服务器的最后一个地址；

2.安装 WDS 服务，目的是通过网络引导的方式来安装 Windows server 2008 R2 CORE 操作系统，运用适当技术手段，让此 WDS 的客户端，只获取到对应 WDS 服务器端 DHCP 下发的 IP 地址。

（十一）在云主机 3 中完成 DNS 转发服务器和 DNSSEC 签名的部署

1.安装 DNS 服务器角色，设置转发器为“云主机 1”的服务器，负责转发“云主机 6”的域名解析的查询请求；

2.在云主机 3 上导入 skillsJiangSu.com 区域的 DNSKEY 签名，来保证数据来自正确的名称服务器。

（十二）在云主机 4 中完成 WEB 服务器 1 的部署

1.添加安装二块网卡，第一块网卡为提供负载均衡网卡，完成网络负载均衡操作；第二块网卡为心跳线网卡；

2.安装 IIS 组件，创建 www.skillsJiangSu.com 站点：

(1)将该站点主目录指定到\\WDF\FilesWeb\FilesConts 共享文件夹；

(2)将 PC1 中“D:\Soft\IIS”目录下的主页文件拷贝到文件服务器中的共享文件夹\\WDF\FilesWeb\FilesConts 内；

(3)启动 www.skillsJiangSu.com 站点的共享配置功能，通过输入物理路径、用户名、密码、确认密码和加密秘钥，将该站点的设置导出、存储到\\WDF\FilesWeb\FilesConfigs 内；

3.设置网站的最大连接数为 1000，网站连接超时为 60s，网站的带宽为 1000KB/S；

4.使用 W3C 记录日志，每天创建一个新的日志文件，文件名格式：

（1）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；

（2）日志文件存储到“C:\WWWLogFile”目录中；

5.创建证书申请时，证书必需信息为：

（1）通用名称=“www.skillsJiangSu.com”；

（2）组织=“skillsJiangSu”；

（3）组织单位=“sales”；

（4）城市/地点 =“NanJing”；

（5）省/市/自治区=“JiangSu”；

（6）国家/地区=“CN”。

（十三）在云主机 4 中完成 NLB 群集服务器的部署

1.安装 NLB 负载平衡服务，其群集 IPv4 地址自行设定，新建群集优先级为 6，群集名称为 www.skillsJiangSu.com，采用多播方式；

2.客户端在访问 www.skillsJiangSu.com 站点时，要求只允许使用域名通过 SSL 加密访问。

（十四）在云主机 5 中完成 WEB 服务器 2 的部署

1.添加安装二块网卡，第一块网卡为提供负载均衡网卡，完成网络负载均衡操作；第二块网卡为心跳线网卡；

2.安装 IIS 组件，实现 www.skillsJiangSu.com 站点的共享配置，启动 www.skillsJiangSu.com 站点的共享配置功能，通过输入物理路径、用户名、密码、确认密码和加密密钥密码，使得让该站点可以使用位于\\WDF\FilesWeb\FilesConfigs 内的共享配置；

3.设置网站的最大连接数为 1000，网站连接超时为 60s，网站的带宽为 1000KB/S；

4.使用 W3C 记录日志，每天创建一个新的日志文件，文件名格式：

（1）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；

（2）日志文件存储到“C:\WWWLogFile”目录中；

5.创建证书申请时，证书必需信息为：

（1）通用名称=“www.skillsJiangSu.com”；

（2）组织=“skillsJiangSu”；

（3）组织单位=“sales”；

（4）城市/地点 =“NanJing”；

（5）省/市/自治区=“JiangSu”；

（6）国家/地区=“CN”。

（十五）在云主机 5 中完成 NLB 群集服务器的部署

1.安装 NLB 负载平衡服务，其群集 IPv4 地址自行设定，完整的 Internet 名称为 www.chinaskills.com，优先级为 11，采用多播方式；

2.客户端在访问 www.skillsJiangSu.com 站点时，要求只允许使用域名通过 SSL 加密访问。

（十六）在云主机 6 中完成相关功能

配置“连接安全规则”，保证和“服务器 2”之间的通信安全，要求入站和出站都要求身份验证，完整性算法采用 SHA-1，加密算法采用 AES-CBC 128，预共享的密钥为 JiangSuskills。

二、在 PC1 上完成如下操作

（一）完成虚拟主机的创建

1.安装虚拟机“服务器 1”，其内存为 768MB，硬盘 40G；

2.安装虚拟机“服务器 2”，其内存为 768MB，硬盘 40G；

3.安装虚拟机“服务器 3”，其内存为 768MB，硬盘 40G，通过“云主机 3”的 WDS 服务进行网络引导和安装，安装完成后停止“云主机 3”中 DHCP 中服务器网段的作用域。

（二）在主机“服务器 2”中完成域及安全部署

1.将“服务器 2”的服务器，升级为子域 cz.skillsJiangSu.com 域控；

2.配置“连接安全规则”，保证和“云主机 6”之间的通信安全，要求入站和出站都要求身份

验证，完整性算法采用 SHA-1，加密算法采用 AES-CBC 128，预共享的密钥为 JiangSuskills。

（三）在主机“服务器 1”中完成域控制器的部署

1.将“服务器 1”服务器升级为域服务器，域名为 JiangSuskills.com;

2.在“服务器 1”中添加二块 SCSI 虚拟硬盘，其每块硬盘的大小为 4G。将二块硬盘配置为 RAID0，对应磁盘盘符为 e:\；同时需要在 e:\启用卷影副本功能，设置每周工作六的晚上 20:30 创建卷影副本，将副本存储于 c:\。

（四）在主机“服务器 1”中完成域控制器信任的部署

1.在 E 盘下新建文件夹 share，并将其文件夹进行共享，权限为任何人完全控制，共享名为 share；

2.通过使用单向信任关系，实现 skillsJiangSu.com 域的技术部的员工可以访问 JiangSuskills.com 域的共享资源 share 文件夹，反之不可以。

（五）在主机“服务器 3”中完成 Core 服务器的部署

1.使用命令修改“服务器 3”服务器的主机名为 wscore，修改“服务器 3”服务器的 IP 地址为表 3 中要求的地址，并按照题目要求设置默认网关；

2.将其“服务器 3”服务器加入 AD DS 域 JiangSuskills.com 中；

3.关闭“服务器 3”服务器的防火墙；

4.在“服务器 3”服务器上安装并启动 DHCP 服务。

第四部分：Linux 系统配置（20 分）

（一）Linux CA 服务及 chrony 时间同步配置配置

【任务描述】为保障企业提供的网络服务具有加密功能，提供证书服务，配置 CA 服务器。

1. 启用所有 Linux 服务器的防火墙。

2. 配置服务后，该服务开机自启动。

3. 所有 Linux 服务器的时区设为“上海”。

4. Linux-1 安装 chrony，为所有 Linux 服务器提供时间同步，Linux-2 ~Linux-7 与 Linux-1 的时间同步。

5. 把 Linux-1 配置为 CA 服务器，证书通用名称均为主机的完全合格域名，CA 证书有效期 20 年，CA 颁发证书有效期 10 年，证书其他信息：

(1) 国家=“CN”。

(2) 省=“Beijing”。

(3) 市/县=“Beijing”。

(4) 组织=“skills”。

(5) 组织单位=“system”。

（二）Linux 智能 DNS 服务配置

【任务描述】随之企业服务对象的不断扩大，在网络边界实现了多运营商接入的情况下，为保障企业提供的网络服务外网的高速访问，同时为了实现区域服务优化，对企业的 DNS 服务实现升级，为模拟相关功能，请使用 Linux-1、Linux-2、Linux-3、Linux-4、Linux-5 模拟完成相关功能配置及实际测试。

6. 在 Linux-1 上安装配置 DNS 主服务器。

7. 实现【服务器 IP 地址分配表】中 Linux-1~linux-5 的域名的解析。

8. 在 Linux-2 上安装配置对应备份服务器。

9. 添加【服务器 IP 地址分配表】中 Linux-6~linux-7 的域名的解析。

10. 修改上述 Linux-1、Linux-2 的 DNS 相关配置，实现 Linux-3（Jiangsu）、Linux-4（Beijing）、Linux-5（Shanghai）不同地区主机解析 tomcat.skills.com 返回不同 IP 地址。【使用 hosts 文件不得分!】

11. 配置服务后，相关服务开机自启动。

（三）FTP 服务配置

【任务描述】为实现文件的安全访问，采用传统的 FTP，实现企业内部资源管理，在 Linux-3 服务器上安装配置 VSFTP 服务，具体要求为：

（1）安装配置 vsftp 及 ftp 客户端软件，开机启动 FTP 服务，系统启用 SELinux 和防火墙，请正确配置相关参数，保证网络正常访问。

（2）为了服务器安全及加强使用规范，为网络部、技术部、市场部、行政部分别创建访客账号，分别为 netftp，techftp，markftp，admftp，用户密码为本竞赛统一要求的密码，指定默认访问路径分别为：/opt/ftp/账号名，不允许本地登录；各部门员工可以在各自部门的相关目录下实现资源的上传与下载

（3）匿名用户不允许访问此 FTP 服务器，用户 nic 不允许登录此 FTP 服务器，最大连接数上限 50，空闲超时 60s 后自动断线。

（4）配置完成重启相关服务，并验证检查相关状态，设置相关服务开机自启。

（四）samba 服务配置

【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，实现 Windows 操作系统和 Linux 操作系统的资源共享。

12. 在 Linux-4 上创建 user101~user120 等 20 个用户；user101 和 user102 属于 hr 组，user103 属于 sale 组，user104 属于 fin 组；

13. 配置 Linux-4 为 Samba 服务器,建立共享目录/share/hr_share, /share/sale_share, /share/public_share，共享名与目录名相同；

14. hr 组用户对 hr_share 和 public_share 有共享读写权限，sale 组用户对 sale_share 和 public_share 有共享读写权限，fin 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。

（五）Mariadb 服务配置

【任务描述】为按数据结构来存储和管理数据，请采用 Mariadb，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。

15. 配置 Linux-3 为 Mariadb 服务器，创建数据库用户 Jack，只能在 Linux-4 主机上对所有数据库有完全权限。

16. 配置 Linux-4 为 Mariadb 客户端，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,user01，1995-7-1，男)，(2,user02，1995-9-1，女)，口令与用户名相同， password 字段用 password 函数加密，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
birthday	datetime	否	否
sex	char(5)	否	否
password	char(200)	否	否

17. 修改表 userinfo 的结构，在 name 字段后添加新字段 height(数据类型为 float)，更新 user1 和 user2 的 height 字段内容为 1.61 和 1.62。

18. 把物理机 d:\soft\mysql.txt 中的内容导入到 userinfo 表中，password 字段用 password 函数加密。

19. 将表 userinfo 中的记录导出，并存放到/var/databak/mysql.sql 文件中。

20. 每周五凌晨 1:00 备份数据库 userdb 到/var/databak/userdb.sql。

（六）基于 Nginx 的反向代理和负载均衡

【任务描述】随着企业规模的不断扩大，为了进一步提高企业 WEB 服务的可靠性、提升 WEB 服务的效能，同时有效保护前期 IT 投资， 请采用 Nginx、Tomcat、Apache 配置 Web 服务，实现基于 Nginx 的反向代理和初步的简单负载均衡，有效整合资源，实现对企业网站的高效、安全、有效的访问。

21. 安装 Nginx1.18.0 到 Linux-5 的/usr/local/nginx，配置启用网站 https，默认文档 index.html 的内容为“Nginx 加密访问！”；证书由 Linux-1 颁发,证书路径为/etc/pki/nginx-1.crt，私钥路径为/etc/pki/nginx-1.key，网站虚拟主机配置文件路径为/usr/local/nginx/conf/nginx.conf。

22. 使用 Nginx 的 proxy_pass 配置 HTTP 反向代理，使用 upstream 配置负载均衡实现 Linux-5 主机 WEB 为前端，Linux-2 主机（权重为 1，max_fails 为 3，超时为 30 秒）和 Linux-3 主机（权重为 2，max_fails 为 3，超时为 20 秒）的相关 web 服务为后端。

23. 配置 Linux-2 为 web 服务器，网站根目录为/https，默认文档 index.html 的内容为“Apache 加密访问！”；仅允许使用域名访问，证书由 Linux-1 颁发,证书路径为/etc/pki/www.crt，私钥路径为/etc/pki/www.key，网站虚拟主机配置文件路径为/etc/httpd/conf.d/vhost.conf。

24. 配置 Linux-3 为 Tomcat 服务器，tomcat 安装目录为/usr/local/tomcat。将 D:\soft\jndsjs 中全部微网站应用程序，复制到 tomcat 的相关目录，仅允许使用域名正常访问且页面信息

正确无误，通过修改配置文件的方法，使用 443 端口；证书由 Linux-1 颁发，证书路径为<安装目录>/conf/tomcat.pfx，证书格式为 pfx。

25. 利用 systemd 实现 tomcat 开机自启动，服务名称为 tomcat.service。

（七）Docker 虚拟化服务配置

【任务描述】随着虚拟化技术的发展，企业把测试环境迁移到 docker 容器中，考虑到一些安全方面的问题，公司决定启用 podman 兼容 Docker。

26. 在 Linux-6 上安装 podman。

27. 导入 hello 镜像，镜像存放在物理机 D:\soft\skills\hello.tar，仓库名为 hello-skills，TAG 标签为 1.0。

28. 测试运行 hello-skills。

29. 导入 nginx 镜像，镜像存放在物理机 D:\soft\skills\nginx.tar，仓库名为 nginx-skills，TAG 标签为 1.0。

30. 创建 docker 自定义网络，名称：skillsnet01，IP：172.16.77.0/24，网关：172.16.77.254。

31. 使用 nginx-skills 镜像创建后台运行容器，名称 nginx01，网络使用 skillsnet01，将容器 nginx01 的 80 口映射到主机 80 口，挂载 nginx01 容器的/usr/share/nginx 到 Linux-6 的/usr/share/nginx01 文件夹。

32. 修改容器 nginx01 默认网页内容为“欢迎来到容器世界!! ”。

第五部分：职业素养（5分）

1、团队合作默契，做好个人防护；

2、科学专业施工，耗材做到最简；

3、整理赛位，工具、设备归位，保持赛后整洁有序；

4、无因参赛选手的原因导致设备损坏等。

网络环境要求

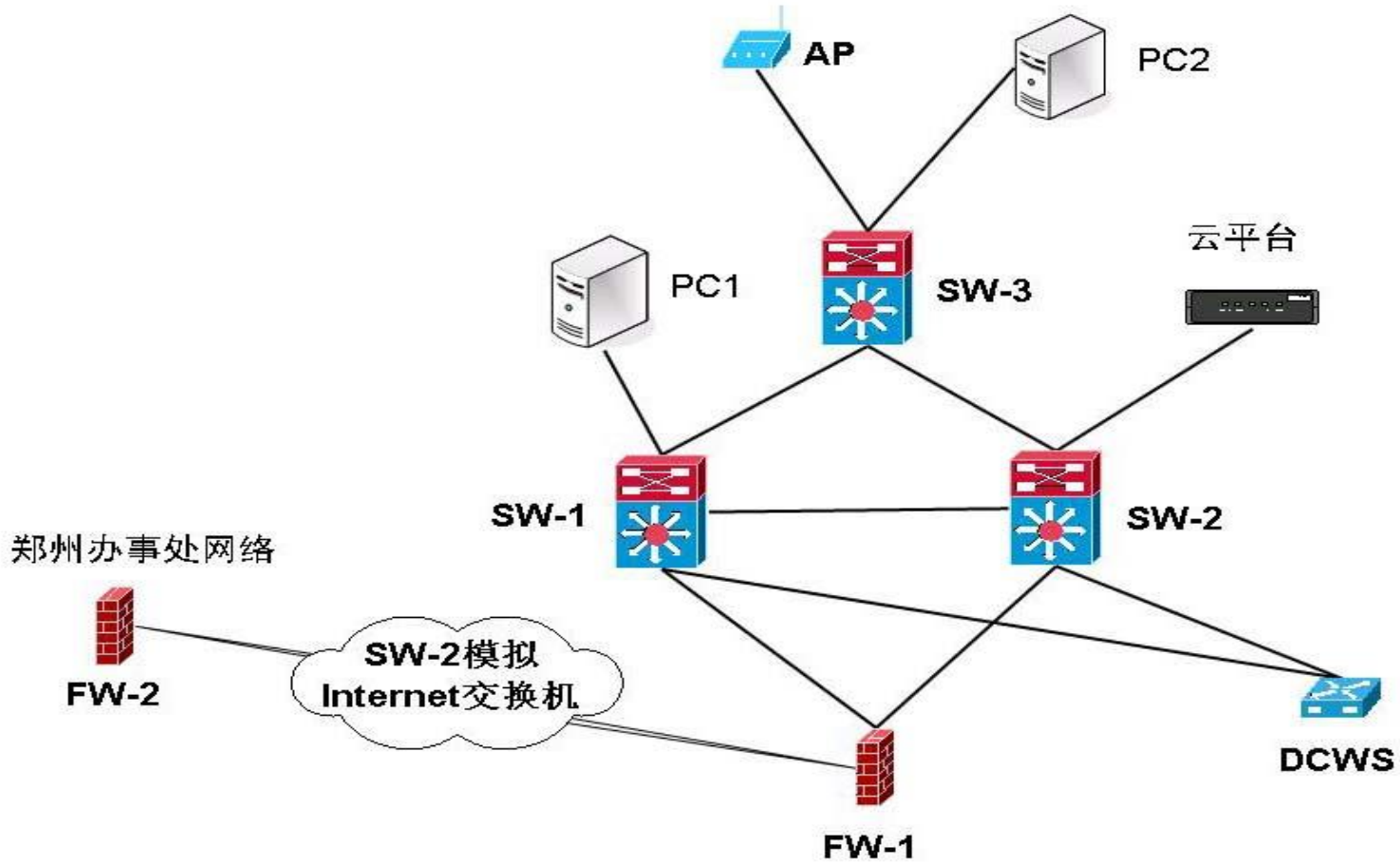


图 1 网络拓扑图

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
SW-1	E1/0/23	SW-2	E1/0/23
SW-1	E1/0/24	SW-3	E1/0/27
SW-2	E1/0/24	SW-3	E1/0/28
SW-1	E1/0/22	DCWS	E1/0/23
SW-2	E1/0/22	DCWS	E1/0/24
SW-1	E1/0/21	FW-1	G0/3
SW-2	E1/0/21	FW-1	G0/4
FW-1	E0/1	SW-2 模拟 Internet 交换机	E1/0/17
FW-2	E0/1	SW-2 模拟 Internet 交换机	E1/0/18
SW-1	E1/0/1	PC1	NIC
SW-2	E1/0/1	云平台	管理口
SW-2	E1/0/2	云平台	业务口
SW-3	E1/0/13	AP	
SW-3	E1/0/14	PC2	NIC

表 2.网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
三层交换机	SW-1	Loopback 1	10.60.255.1/32
		VLAN10 SVI	10.60.10.0/24
		VLAN20 SVI	10.60.20.0/24
		VLAN30 SVI	10.60.30.0/24
		VLAN40 SVI	10.60.40.0/24
		VLAN50 SVI	10.60.50.0/24
		VLAN200 SVI	10.60.200.0/24
		VLAN1000 SVI	10.60.254.9/30
		VLAN1001 SVI	10.60.254.1/30
		VLAN4094 SVI	10.60.254.253/30
	SW-2	Loopback 1	10.60.255.2/32
		VLAN10 SVI	10.60.10.0/24
		VLAN20 SVI	10.60.20.0/24
		VLAN30 SVI	10.60.30.0/24
		VLAN40 SVI	10.60.40.0/24
		VLAN50 SVI	10.60.50.0/24
		VLAN200 SVI	10.60.200.0/24
		VLAN1002 SVI	10.60.254.13/30
		VLAN1001 SVI	10.60.254.5/30
		VLAN4094 SVI	10.60.254.254/30
	SW-2 模拟 Internet 交换机	VLAN4000 SVI	202.99.192.2/30
		VLAN4001 SVI	202.99.192.65/30
		Loopback100	202.100.100.100/32
	SW-3	VLAN200 SVI	10.60.200.250/24
防火墙	FW-1	Loopback1	10.60.255.5/32
		Eth0/1	202.99.192.1/30（untrust 安全域）
		Eth0/3	10.60.254.2/30（trust 安全域）
		Eth0/4	10.60.254.6/30（trust 安全域）
		Tunnel 1	10.60.254.33/30

			（VPNHub 安全域）
	FW-2	Eth0/1	202.99.192.66/30 （untrust 安全域）
		Eth0/2	172.30.30.254/24 （trust 安全域）
		Tunnel 1	10.60.254.34/30 （VPNHub 安全域）
无线控制器	DCWS	VLAN1000 SVI	10.60.254.10/30
		VLAN1002 SVI	10.60.254.14/30
		VLAN220 SVI	10.60.220.254/24

表 3.服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4地址信息
云实训平台	云主机 1	dc.skillsJiangSu.com	域服务 DNS 服务 CA 服务	WindowsServer2019	10.60.10.101/24
	云主机 2	slave.skillsJiangSu.com	辅助域服务 辅助 DNS 服务 从属 CA 服务 DFS 服务 网络打印服务	WindowsServer2019	10.60.10.102/24
	云主机 3	www1.skillsJiangSu.com	DNS 转发 DFS 服务 文件服务 DHCP 服务 WDS 服务	WindowsServer2019	10.60.10.103/24
	云主机 4	www2.skillsJiangSu.com	NLB 服务 WEB 服务 DFS 服务	WindowsServer2019	10.60.10.104/24 10.60.10.105/24
	云主机 5	nlb.skillsJiangSu.com	NLB 服务 WEB 服务	WindowsServer2019	10.60.10.106/24 10.60.10.107/24
	云主机 6	sec.skillsJiangSu.com	安全服务	WindowsServer2019	10.60.10.108/24
	Linux-1	dns.skills.com	DNS、CA 服务 chrony 服务	Rocky 8.3	10.60.30.101/24
	Linux-2	web.skills.com	辅助 DNS 服务 Apache 服务	Rocky 8.3	10.60.30.102/24
	Linux-3	ftp.skills.com	FTP 服务 Tomcat 服务 Mariadb 服务	Rocky 8.3	10.60.30.103/24
	Linux-4	smb.skills.com	samba 服务	Rocky 8.3	10.60.30.104/24
	Linux-5	proxy.skills.com	nginx 服务 Proxy 服务	Rocky 8.3	10.60.30.105/24
PC1（IP 为 10.60.10.0/24 网段）	服务器 1	dc.JiangSuskills.com	域控服务 域信任配置 卷影副本	WindowsServer2019	10.60.10.109/24
	服务器 2	dc1.cz.skillsJiangSu.com	子域域控 安全服务	WindowsServer2019	10.60.10.110/24
	服务器 3	wscore.jiangSuskills.com	DHCP 服务	WindowsServerCore	10.60.10.111/24
PC2（IP 为 10.60.30.0/24 网段）	Linux-6	docker.skills.com	docker 服务	Rocky 8.3	10.60.30.105/24
	Linux-7	test.skills.com	测试服务	Rocky 8.3	10.60.30.106/24

表 4.云平台网络信息表

网络名称	Vlan 号	外部网络	子网名称	子网网络地址	网关 IP	激活 DHCP	地址池范围
Vlan10	10	是	Vlan10-subnet	10.60.10.0/24	10.60.10.254	是	10.60.10.100~200
Vlan20	20	是	Vlan20-subnet	10.60.20.0/24	10.60.20.254	是	10.60.20.100~200
Vlan30	30	是	Vlan30-subnet	10.60.30.0/24	10.60.30.254	是	10.60.30.100~200

表 5.虚拟主机信息表

虚拟主机名称	镜像模板 (源)	云主机类型(flavor)	VCPU数量	内存、硬盘信息	网络名称	备注
Windows-1	WindowsServer2019	Large	2	4G，40G		
Windows-2	WindowsServer2019	Large	2	4G，40G		HD1~HD3
Windows-3	WindowsServer2019	Large	2	4G，40G		
Windows-4	WindowsServer2019	Large	2	4G，40G		
Windows-5	WindowsServer2019	Large	2	4G，40G		
Windows-6	WindowsServer2019	Large	2	4G，40G		
Linux-1 至 Linux-7	Rocky8.3.3	Small	1	2G，40G		

表 6.云主机和服务器密码表

云主机和服务器密码	Netw@rkCZ!@#（注意区分大小写）

注：需把云主机的默认密码改为表 6.云主机和服务器密码表要求的密码

附件二、教师组赛卷样卷

2023 年江苏省职业院校技能大赛网络搭建与应用赛项教师组样卷

技能要求

竞赛说明

1. 竞赛内容分布

“网络搭建与应用”竞赛共分六个部分，其中：

第一部分：网络组建与配置（35 分）

第二部分：云平台配置（8 分）

第三部分：Windows 系统配置（16 分）

第四部分：Linux 系统配置（16 分）

第五部分：实训指导文档（5 分）

第六部分：职业规范与素养（5 分）

2. 项目简介

某公司原在北京建立了总部，后在深圳建立了分部。总部设有研发、行政、营销、财务、信息技术 5 个部门，统一进行 IP 及业务资源的规划和分配，网络采用 OSPF 路由协议。

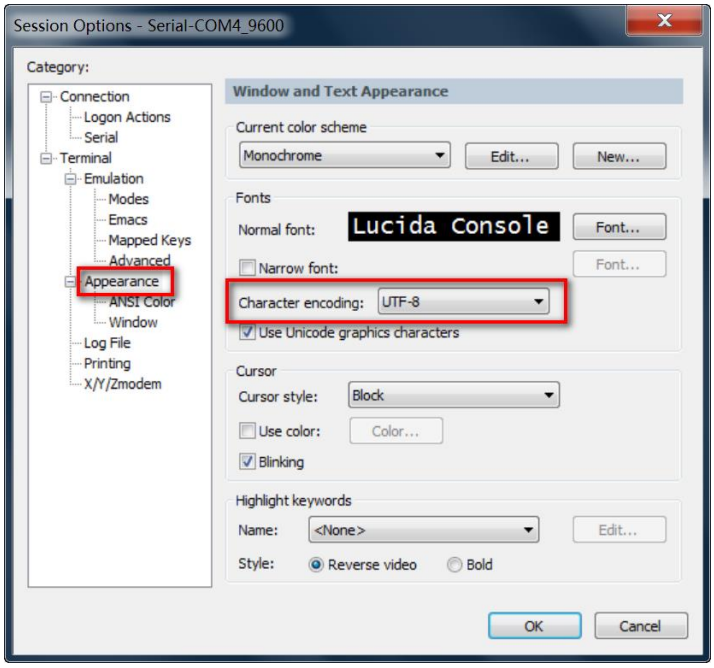
公司规模在 2023 年快速发展，业务数据量和公司访问量增长巨大。为了更好管理数据，决定建立自己的小型数据中心及业务服务平台，以达到快速、可靠交换数据等目的。总部及深圳分部的网络结构详见“主要网络环境”拓扑图。

其中一台 CS6200 交换机编号为 SW-3，用于实现终端高速接入；两台 CS6200 交换机 VSF 虚拟化后编号为 SW-Core，作为总部的核心交换机；一台 DCFW-1800 作为总部的内网防火墙，另一台 DCFW-1800 作为分部的防火墙；一台 DCWS-6028 作为分部机构的有线无线智能一体化控制器，编号为 DCWS，通过与 WL8200-I2 高性能企业级 AP 配合实现分部无线覆盖。

第一部分：网络组建与配置（35 分）

【说明】

1. 交换机、 DCWS、防火墙使用同一条 console 线；
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。所有提交的文档必须按照赛题所规定的命名规则命名；所有需要提交的文档均放置在 PC1 桌面的“比赛文档_X”（X 为赛位号）文件夹中；
3. 保存文档方式如下：
   - 交换机、DCWS 要把 show running-config 的配置、防火墙要把 show configuration 的配置保存在 PC1 桌面上的“比赛文档_X”文件夹中，文档命名规则为：设备名称.txt。例如：SW-1 交换机文件命名为：SW-1.txt；
   - 无论通过 SSH、telnet、Console 登录防火墙进行 show configuration 配置收集，需要先调整 CRT 软件字符编号为：UTF-8，否则收集的命令行中文信息会显示乱码。CRT 软件调整字符编号配置如图：



一、 网络布线与基础连接

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	W1-06-102-1	W1	102	1	06

(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. PC1 连接 102 底盒 1 端口、PC2 连接 101 底盒 1 端口。

二、 交换配置与调试

(一) 、总部两台核心交换机通过 VSF 物理端口连接起来形成一台虚拟的逻辑设备，用户对这台虚拟设备进行管理，来实现对虚拟设备中所有物理设备的管理。两台设备之间建立一个 vsf port-group，vsf port-group 编号都为 2，每个 vsf port-group 绑定两个千兆光端口，SW-1 的成员编号为 1，SW-2 的成员编号为 2，正常情况下 SW-1 负责管理整个 VSF，选定 VLAN 4090 进行 BFD MAD 分裂检测，SW-1 BFD MAD IP 地址为：1.1.1.1/30，SW-2 BFD MAD 接口 IP 地址为：1.1.1.2/30，配置 VSF 链路 down 延迟上报时间为 2s。

(二) 、为了减少广播，需要根据题目要求规划并配置 VLAN。具体要求如下：

1. 配置合理，所有链路上不允许不必要 VLAN 的数据流通过，包括 VLAN 1；
2. 配置研发业务 VLAN 每个物理端口最多允许每秒钟通过 640kbit 的广播数据包；营销业务 VLAN 每个物理端口最多允许每秒钟通过 1280kbit 的单播数据包。

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	VLAN 名称	端口	说明
SW-3	VLAN10	YF	E1/0/1	研发
	VLAN20	XZ	E1/0/2	行政
	VLAN30	YX	E1/0/3	营销
	VLAN40	CW	E1/0/4	财务
	VLAN50	XXJS	E1/0/5	信息技术
	VLAN200	GL		网络管理

(三) 、在总部两台核心交换机与接入交换机间运行一种协议，具体要求如下：

1. 实现研发、行政、信息技术业务优先通过 SW-1 至 SW-3 间链路转发，营销、财务、网络管理等业务优先通过 SW-2 至 SW-3 间链路转发，从而实现 VLAN 流量的负载分担

与相互备份；

2. 设置路径开销值的取值范围为 1-65535，BPDU 支持在域中传输的最大跳数为 5 跳；同时不希望每次拓扑改变都清除设备 MAC/ARP 表，全局限制拓扑改变进行刷新的次数；

3. 加速接入交换机所有业务端口收敛，当接口收到 BPDU 丢弃报文并关闭端口，如果 3 分钟内没有收到 BPDU 报文，则恢复该端口。

(四) 、总部为贯彻落实中共中央办公厅、国务院办公厅印发的《推进互联网协议第六版（IPv6）规模部署行动计划》，加快推进基于互联网协议第六版（IPv6）基础网络设施规模部署和应用系统升级,计划先对研发、信息技术各自部门业务终端启用 IPv6 测试，采用自动获取 IP 地址，总部两台核心交换机作为 DHCPv6 服务器进行 IP 地址分配；在接入交换机上配置相关特性，自动绑定上述业务端口通过 DHCPv6 方式获得 IPv6 地址信息。IPv6 业务地址规划如下：

业务	IPv6 地址
研发	2001:XX:10::254/64 （XX 与“主要网络环境”地址中相应网段一致）
信息技术	2001:XX:20::254/64 （XX 与“主要网络环境”地址中相应网段一致）

(五) 、要求尽可能加大总部核心交换机 SW-Core 与 FW-1 之间的带宽。

(六) 、SW-1 既作为总部核心交换机，同时又使用相关技术将 SW-1 模拟为 Internet 交换机，实现总部内部业务路由表与 Internet 路由表隔离。

(七) 、在总部接入交换机针对行政业务接入端口进行限速，带宽限制为 100M 比特/秒，突发值设为 8M 字节，超过带宽的该网段内的报文一律丢弃。

三、 路由配置与调试

总部与分部使用 OSPF 协议组网。FW-1、SW-Core 之间规划使用 OSPF 协议。

(一) 、尽可能加大总部 FW-1 与分部 FW-2 之间专线链路带宽。

(二) 、总部 FW-1、SW-Core 之间规划使用 OSPF 协议，进程号为 100，Area1，启用区域 MD5 验证，验证密钥为：Net2019，调整接口的网络类型加快邻居关系收敛，为了管理方便，需要发布 Loopback 地址，并尽量在 OSPF 域中发布，总部业务网段中不发送协议报文。

(三) 、实现总部行政&营销业务网段统一通过总部 FW-1 访问 Internet，使用 NAT 地址为：183.203.10.8/29，限制 NAT 翻译表项的最大数目为 5K；配置一对一地址转换，实现通过 Internet 任意位置访问 183.203.10.7/32 都可以访问至总部营销平台 172.XX.30.1/32（XX 与“主

要网络环境”地址中相应网段一致）进行数据访问；实现分部无线业务网段统一通过分部 FW-2 访问 Internet，NAT 地址池为接口公网 IP。

(四)　、总部 FW-1 与分部 FW-2 之间使用与 Internet 互联接口地址建立 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，这样有了 IPSec，总部与分部互访业务在通过运营商网络传输时，就不用担心被监视、篡改和伪造。

(五)　、总部 FW-1 配置路由重分布，与 OSPF 协议相互引入，实现总部只能学习到分部明细业务网段路由、分部只能学习到总部明细业务网段路由。

四、　无线配置

(一)　、无线控制器 DCWS 二层与分部 FW-2 互联，所有业务网关位于分部 FW-2 上，DCWS 配置 VLAN100 为 AP 管理 VLAN，VLAN10、20、30 为业务 VLAN；使用无线控制器为业务 VLAN 和 AP 管理 VLAN 提供 DHCP 服务，动态分配 IP 地址和网关，使用第一个地址作为 DCWS 管理地址，本地转发，AP 二层手工注册，启用 MAC 认证。

(二)　、设置三个 SSID FenZhiXX-YX、FenZhiXX-XZ、FenZhiXX-Internet，其中 FenZhiXX 中的 XX 为赛位号，具体要求如下：

1. SSID FenZhiXX-YX：访问总部营销业务，VLAN10，采用 WAPI 预共享密钥鉴别方式，配置密钥为 Net12345678；

2. SSID FenZhiXX-XZ：访问总部行政业务，VLAN20，采用 WPA-PSK 认证方式，加密方式为 WPA 个人版，配置密钥为 Dcn12345678；

3. SSIDFenZhiXX-Internet：访问 Internet，VLAN30，采用开放接入。

(三)　、配置 AP 通过周期性触发方式每隔 1 小时对发射功率进行一次调整；开启 AP 实时监测周边的射频环境功能，每隔 1 分钟执行一次跨信道扫描。

五、　安全策略配置

(一)　、总部相关设备配置安全策略，服务器业务网段只与总部业务网段、分部业务网段双向互访。

(二)　、分部相关设备配置安全策略，禁止总部所有业务网段与分部 FenZhiXX-Internet 业务网段双向访问。

(三)　、配置 SSID FenZhiXX-YX 访问总部营销业务最小保证带宽为 30M，SSID FenZhiXX-XZ 访问总部行政业务最小保证带宽为 20M。

六、 组播配置

计划在总部上线视频会议系统，实现多业务部门横向沟通、交流，提升工作效率，初步先在总部研发、信息技术部门启用组播协议进行测试，具体要求如下：

1. 在总部核心交换机运行协议独立组播－密集模式协议、因特网组管理协议第二版本；

2. 研发部门内部终端启用组播，使用 VLC 工具串流播放视频文件 1.mpg，组地址 228.10.10.10，端口：1234，实现信息技术部门内部终端可以通过组播查看视频播放。

第二部分：云平台配置（8 分）

【竞赛技术平台说明】

1．云服务实训平台相关说明：

（1） 云服务实训平台管理 ip 地址默认为 192.168.100.100，访问地址 http://192.168.100.100/dashboard 默认账号密码为 admin/dcncloud，ssh 默认账号密码为 root/dcncloud，考生禁止修改云服务实训平台账号密码及管理 ip 地址，否则服务器配置及应用项目部分计 0 分；

（2） 云服务实训平台中提供镜像环境，镜像的默认用户名密码以及镜像信息，参考《云服务实训平台用户操作手册（江苏省赛版）》；

名称	用户名	密码	ssh	rdp
Win10	admin	Qwer1234	否	是
Win2008	administrator	Qwer1234	否	是
Win2019	administrator	Qwer1234	否	是
Rocky8.3	root	dcncloud	是	否

（3） 所有 Windows 主机实例在创建之后都直接可以通过远程桌面连接操作，Rocky8.3 可以通过 CRT 软件连接进行操作，所有 Linux 主机都默认开启了 ssh 功能，Linux 系统软件镜像位于”/opt”目录下；

（4） 要求在云服务实训平台中保留竞赛生成的所有虚拟主机。

2．云服务实训平台和服务器 PC1 和 PC2 相关服务说明：

（1） 题目中所有未指明的密码均参见“表 6.云主机和服务器密码表”，若未按照要求设置密码，涉及到该操作的所有分值记为 0 分；

（2） 虚拟主机的 IP 属性设置请按照“拓扑结构图”以及“表 3.服务器 IP 地址分配表”的要求设定；

（3） 除非作特殊说明，在 PC1 和 PC2 上需要安装相同操作系统版本的虚拟机时，可采用 VMware Workstation 软件自带的克隆系统功能实现；

（4） PC1 和 PC2 上所有系统镜像文件及赛题所需的其它软件均存放在每台主机的 D:\soft 文件夹中；

（5） PC1 和 PC2 要求的虚拟机均安装于每台在 D 盘根目录下自建的名为 VirtualPC 文

件夹中，即路径为 D:\VirtualPC\虚拟主机名称。

（6） 请在 PC2 桌面上，选手自己建立 BACKUP_X（X 为赛位号）文件夹，并将 PC2 上 D 盘 soft 文件夹中的《云实训平台安装与应用报告单》、《Windows 操作系统-云平台部分竞赛报告单》和《Linux 操作系统竞赛报告单》复制到 PC2 桌面的“BACKUP_X”（X 为赛位号）文件夹中、将 PC1 上 D 盘 soft 文件夹中的《Windows 操作系统-虚拟机部分竞赛报告单》 复制到 PC1 桌面的“BACKUP_X”（X 为赛位号）文件夹中，并按照截图注意事项的要求填写完整；如报告单、截图等存放位置错误，涉及到的所有操作分值记为 0 分；

（7） 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，否则会扣除该服务功能一定分数。

【云实训平台安装与运用】

一、云平台基础设置

1.按照“表 4：云平台网络信息表”要求创建五个外部网络，这些外部网络所使用的 VLAN 均为总部业务 VLAN，详细操作过程请参照“云服务实训平台用户操作手册（江苏省赛版）”；

2.创建 5 块云硬盘，卷命名为 hd1-hd5，其中 hd1-hd2 大小为 10G，h3-h5 大小自定；

注意事项：

（1）必须通过“项目”栏中的“计算”子栏中的“卷”功能来创建云硬盘；不能使用 “管理员”，“系统”栏下的“卷”功能，该功能使用不当会造成云硬盘创建失败，界面卡死。

（2）在云平台中可以创建多个云硬盘，所有云硬盘容量的总大小不能超过 100G，否则将创建失败。一个实例可以同时连接多个云硬盘，但一个云硬盘同时只能给一个实例作为扩展硬盘使用。

（3）在分离卷之前一定要保证使用该卷的 Linux 主机中，已经不存在该卷的任何挂载点。如果使用该卷的主机是 Windows 实例，必须保证该卷在主机的“磁盘管理”项目中处于脱机状态，否则会造成分离失败，或是一直显示“分离中”状态。

二、创建虚拟主机

1.按照“表 5：虚拟主机信息表”所示，按要求生成虚拟主机，详细操作过程请参照“云服

务实训平台用户操作手册（江苏省赛版）”；

2.云平台中所有虚拟机的 IP 地址，要求手动设置为该虚拟机 DHCP 获取的地址。

第三部分：Windows 系统配置（16 分）

一、在云实训平台上完成如下操作

（一）完成虚拟主机的创建

将按照“表 5：虚拟主机信息表”生成的虚拟主机加入到 JSSkill.com 域环境。

（二）在云主机 1 中完成链路聚合的部署

添加一块网卡，完成两块网卡的链路聚合操作，组名为“AggNic1”，成组模式为“静态成组”，负载均衡模式为“地址哈希”，为主域和辅助域之间的传输提升速度。

（三）在云主机 1 中完成 DNS 服务器的部署

为了防止域控制器的 DNS 域名解析服务造成大量不必要的数据流，公司技术人员决定禁用 DNS 递归功能，请您使用 PowerShell 禁用 DNS 递归功能。

（四）在云主机 1 中完成域用户管理及 CA 服务器的部署

1. 将配成 CA 服务器：安装证书服务；为企业内部自动回复证书申请；设置为企业根；有效期为 5 年；颁发的证书有效期年份为 4 年；

2. 新建名称为 hr、tech、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：人力部（hr101-hr120）、营销部（sale101-sale120）、技术部（tech101-tech120），所有用户不能修改其口令；必须启用密码复杂度要求、密码长度最小为 8 位、密码最长期限为 10 天、允许失败登录尝试的次数为 4 次、重置失败登录尝试计数（分钟）为 5 分钟、直至管理员手动解锁帐户，并且只能每天 8:00-18:00 可以登录;

3. 所有用户到任何一台域计算机登录，“文档”文件夹重定向到域控制器的 C:\Documents 文件夹；

4. 配置组策略，实现所有销售部的计算机开机后自动弹出“温馨提示”的对话框，显示的内容为“请注意销售数据的安全！”并测试。

（五）在云主机 1 中完成 DNS 安全防护的部署

1. 新建一条主机记录，主机名称为 dnsn、IP 地址为 172.19.20.140;

2. 对云主机 1 的 JSSkill.com 区域中的 dnsn 主机记录提供完整性验证，来保证数据在传输的过程中不被篡改；

3. 同时为所有区域设置老化/清理时间：无刷新间隔：5 天，刷新间隔：5 天。

（六）在云主机 2 中完成链路聚合的部署

添加一块网卡，完成两块网卡的链路聚合操作，组名为“AggNic2”，成组模式为“静态成组”，负载均衡模式为“地址哈希”，为主域和辅助域之间的传输提升速度。

（七）在云主机 2 中完成从属证书的部署

1. 将云主机 2 的服务器升级成 JSSkill.com 域的辅助域控制器；

2. 将云主机 2 的服务器设置为证书颁发机构：

（1）安装证书服务，为企业内部自动回复证书申请；

（2）设置为企业从属 CA，负责整个 JSSkill.com 域的证书发放工作。

（八）在云主机 2 中完成磁盘管理及 iSCSI 存储的部署

1. 添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 10G，将其配置为跨区卷，盘符为 E，开启数据删除重复功能，排除扩展名为.xlsx，.txt 的文件；

2. 安装 iSCSI 目标服务器和存储多路径，并新建 iSCSI 虚拟磁盘，存储位置为 E 盘，虚拟磁盘名称分别是 Quorum 和 Files，大小分别为 512M 和 5G，访问服务器为“云主机 4”和“云主机 5”。

（九）在云主机 3 中完成 DHCP 及 WDS 服务的部署

1. 将云主机 3 的服务器升级成 JSSkill.com 域的只读域控制器；

2. 安装 DHCP 服务，为服务器网段部分主机动态分配 IPv4 地址，建立作用域，作用域的名称为 dhcpserver，地址池为 225-230，仅允许“服务器 3”的服务器获取 DHCP 服务器的尾数为 228 的地址；

3. 安装 WDS 服务，目的是通过网络引导的方式来安装 Windows Server 2019 core 操作系统，运用适当技术手段，让此 WDS 的客户端，只获取到对应 WDS 服务器端 DHCP 下发的 IP 地址。

（十）在云主机 4 中完成 WEB 服务器的部署

1.添加安装三块网卡，第一块网卡和第二块网卡为提供 MPI 网卡，第三块网卡为心跳线网卡；

2.安装故障转移群集功能、文件服务器功能和存储多路径功能，在存储多路径功能的属性中，添加对 iSCSI 设备的支持；

3.使用 iSCSI 发起程序连接云主机 2 的 iSCSI 虚拟磁盘，实现对 Quorum 和 Files 的存储多路径功能，并能正常访问；

4.安装 IIS 组件，创建 www.JSSkill.com 站点：

（1）将该站点主目录指定到 N:\MyShare 共享文件夹，创建 JSSkill.aspx 主首页面，内容为“全国职业技能大赛网络搭建与应用江苏省赛时间为：<%=now()%>”,只允许使用域名通过 SSL 加密访问；

（2）配置站点同时支持 dotnet CLR v2.0 和 dotnet CLR v4.0；

（3）使用 W3C 记录日志，每天创建一个新的日志文件，文件名格式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；日志文件存储到“C:\WWWLogFile”目录中；

5.创建证书申请时，证书必需信息为：

（1）通用名称=“www.JSSkill.com”；

（2）组织=“JSSkill”；

（3）组织单位=“sys”；

（4）地点/城市=“ChangZhou”；

（5）省/市/自治区=“JiangSu”；

（6）国家/地区=“CN”。

（十一）在云主机 5 中完成故障转移群集及 WEB 服务器的部署

1.添加安装三块网卡，第一块网卡和第二块网卡为提供 MPIO 网卡，第三块网卡为心跳线网卡；

2.安装故障转移群集功能和存储多路径功能，在存储多路径功能的属性中，添加对 iSCSI 设备的支持；

3.使用 iSCSI 发起程序连接云主机 2 的 iSCSI 虚拟磁盘，实现对 iSCSI 虚拟磁盘 Quorum 和 Files 的存储多路径功能，成功连接后对其进行初始化和创建卷，设置驱动器号分别为 M 和 N，完成格式化操作；

4.在故障转移群集功能中，添加云主机 4 和云主机 5，并生成故障转移群集验证报告；

5.创建故障转移群集，群集名称为：webcluster，IP 地址尾数为 60；

6.添加文件服务器功能和配置文件服务器角色，名称为：MyClusterFiles，IP 地址尾数为61，为 MyClusterFiles 添加共享文件夹，共享协议采用“SMB”，共享名称为 MyShare，存储位置为 N 盘，共享权限采用管理员具有完全控制权限，其他用户具有读写权限，NTFS 权限采用域管理员具有完全控制权限，域其他用户具有修改权限；

7.安装 IIS 组件，创建 www.JSSkill.com 站点，将该站点主目录指定到 N:\MyShare 共享文件夹，创建 JSSkill.asp 主首页面，内容为“全国职业技能大赛网络搭建与应用江苏省赛时间为：<%=now()%>”,只允许使用域名通过 SSL 加密访问；

8. 配置站点同时支持 dotnet CLR v2.0 和 dotnet CLR v4.0；

9.使用 W3C 记录日志，每天创建一个新的日志文件，文件名格式；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；日志文件存储到“C:\WWWLogFile”目录中；

10.创建证书申请时，证书必需信息为：

（1）通用名称=“www.JSSkill.com”；

（2）组织=“JSSkill”；

（3）组织单位=“sys”；

（4）地点/城市=“ChangZhou”；

（5）省/市/自治区=“JiangSu”；

（6）国家/地区=“CN”。

（十二）在云主机 6 中完成相关功能

1. 配置“连接安全规则”，保证和“服务器 2”之间的通信安全，要求入站和出站都要求身份验证，完整性算法采用 SHA-256，加密算法采用 AES-CBC 192，预共享的密钥为 skills2022；

2. 访问 https://www.JSSkill.com 网站。

二、在 PC1 上完成如下操作

（一）完成虚拟主机的创建

安装虚拟机“服务器 3”，其内存为 768MB，硬盘 60G，通过“云主机 3”的 WDS 服务进行网络引导和安装，安装完成后停止“云主机 3”中 DHCP 中服务器网段的作用域。

（二）在主机“服务器 2”中完成域部署

1. 将“服务器 2”的服务器，升级为子域 cz.JiangSuskills.com；

2. 配置“连接安全规则”保证和“云主机 6“之间的通信安全，要求入站和出站都要求身份验证，完整性算法采用 SHA-256，加密算法采用 AES-CBC 192，预共享的密钥为 skills2022。

（三）在主机“服务器 1”中完成独立服务器和域控制器的部署

1. 将“服务器 1”服务器升级为域控服务器，域名为 JiangSuSkills.com；

2. 在 “服务器 1”中添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 5G。将三块硬盘配置为 RAID5，对应磁盘盘符为 E:\；同时需要在 E:\启用卷影副本功能，设置每周日的晚上 21:30 创建卷影副本，将副本存储于 c:\。

（四）在主机“服务器 1”中完成域控制器信任的部署

1.在 E 盘下新建文件夹 option，并将其文件夹进行共享，权限为任何人完全控制，共享名为 option；

2.通过使用单向信任关系，实现 JSSkill.com 域的行政部的员工可以访问 JiangSukills.com 域的共享资源 option 文件夹，反之不可以。

（五）在主机“服务器 3”中完成 Core 服务器的部署

1.使用命令修改“服务器 3”服务器的主机名为 ServerCore，修改“服务器 3”服务器的 IP 地址为表 3 中要求的地址，并按照题目要求设置默认网关；

2.将其“服务器 3”服务器加入 AD DS 域 JiangSuskills.com 中；

3.关闭“服务器 3”服务器的防火墙；

4.在“服务器 3”服务器上安装并启动 DHCP 服务。

第四部分：Linux 系统配置（16 分）

（一）Linux CA 服务配置

【任务描述】为保障企业提供的网络服务具有加密功能，提供证书服务，配置 CA 服务器，为模拟相关功能，请使用 Linux-1、Linux-2 模拟完成相关功能配置及实际测试。

1. 修改所有 Linux-1~Linux-7 主机的主机名为“服务器 IP 地址分配表”中标注的合格域名。

2. 把 Linux-1 配置为 CA 服务器，CA 的私钥 cakey.pem 使用 2048 位，私钥文件存放于 /etc/pki/CA/private 目录，只有拥有者可读写，CA 证书使用系统默认文件名：/etc/pki/CA/cacert.pem, 可以签发“省、市/县”名称不同的主机、web 服务等证书，有效期 20 年，CA 颁发证书有效期 10 年，证书其他信息：

(1) 国家=“CN”。

(2) 省=“Beijing”。

(3) 市/县=“Beijing”。

(4) 组织=“skills”。

(5) 组织单位=“system”。

3. 为 Linux-2 签发 http01.crt 证书，证书存放于 Linux-2 主机的/etc/pki/httpd/ssl 目录。

(1) 国家=“CN”。

(2) 省=“Jiangsu”。

(3) 市/县=“CZ”。

(4) 组织=“skills”。

(5) 组织单位=“NIC”。

(6) 服务器主机名=“web01.skills.com”

(7) 邮件名=nic@skills.com

4. 为 Linux-3 签发 http02.crt 证书，证书存放于 Linux-2 主机的/etc/pki/httpd/ssl 目录。

(1) 国家=“CN”。

(2) 省=“Jiangsu”。

(3) 市/县=“NJ”。

(4) 组织=“skills”。

(5) 组织单位=“NIC”。

(6) 服务器主机名=“web02.skills.com”

(7) 邮件名=nic@skills.com

（二）Linux 智能 DNS 服务配置

【任务描述】随之企业服务对象的不断扩大，在网络边界实现了多运营商接入的情况下，为保障企业提供的网络服务外网的高速访问，同时为了实现区域服务优化，对企业的 DNS 服务实现升级，为模拟相关功能，请使用 Linux-1、Linux-2、Linux-3、Linux-4 模拟完成相关功能配置及实际测试。

1. 在 Linux-1 上安装配置 DNS 主服务器。

2. 实现【服务器 IP 地址分配表】中 Linux-1~linux-5 的域名的解析。

3. 在 Linux-2 上安装配置对应备份服务器。

4. 添加【服务器 IP 地址分配表】中 Linux-6~linux-7 的域名的解析。

5. 修改上述 Linux-1、Linux-2 的 DNS 相关配置，实现 Linux-3（Jiangsu）、Linux-4（Beijing）不同地区主机解析 web.skills.com 返回不同 IP 地址。【使用 hosts 文件不得分！】

6. 配置服务后，相关服务开机自启动。

（三）FTP 服务配置

【任务描述】为实现文件的安全访问，采用传统的 FTP，实现企业内部资源管理，在 Linux-4 服务器上安装配置 VSFTP 服务，具体要求为：

7. （1）安装配置 vsftp 及 ftp 客户端软件，开机启动 FTP 服务，系统启用 SELinux 和防火墙，请正确配置相关参数，保证网络正常访问。

8. （2）为了服务器安全及加强使用规范，为网络部、技术部、市场部、行政部分别创建访客账号，分别为 netftp，techftp，markftp，admftp，用户密码为本竞赛统一要求的密码，指定默认访问路径分别为：/opt/ftp/账号名，不允许本地登录；各部门员工可以在各自部门的相关目录下实现资源的上传与下载

9. （3）匿名用户不允许访问此 FTP 服务器，用户 nic 不允许登录此 FTP 服务器，最大连接数上限 50，空闲超时 60s 后自动断线。

10. （4）配置完成重启相关服务，并验证检查相关状态，设置相关服务开机自启。

（四）Mariadb 服务配置

【任务描述】为按数据结构来存储和管理数据，请采用 Mariadb，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。

11. 配置 Linux-3 为 Mariadb 服务器，创建数据库用户 Jack，只能在 Linux-4 主机上对所有数据库有完全权限。

12. 配置 Linux-4 为 Mariadb 客户端，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,user01，1995-7-1，男)，(2,user02，1995-9-1，女)，口令与用户名相同， password 字段用 password 函数加密，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
birthday	datetime	否	否
sex	char(5)	否	否
password	char(200)	否	否

13. 修改表 userinfo 的结构，在 name 字段后添加新字段 height(数据类型为 float)，更新 user1 和 user2 的 height 字段内容为 1.61 和 1.62。

14. 把物理机 d:\soft\mysql.txt 中的内容导入到 userinfo 表中，password 字段用 password 函数加密。

15. 将表 userinfo 中的记录导出，并存放到/var/databak/mysql.sql 文件中。

16. 每周五凌晨 1:00 备份数据库 userdb 到/var/databak/userdb.sql。

（五）基于 Nginx 的反向代理和负载均衡

【任务描述】随着企业规模的不断扩大，为了进一步提高企业 WEB 服务的可靠性、提升 WEB 服务的效能，同时有效保护前期 IT 投资， 请采用 Nginx、Apache 配置 Web 服务，实现基于 Nginx 的反向代理和初步的简单负载均衡，有效整合资源，实现对企业网站的高效、安全、有效的访问。

17. 在 Linux-5 上安装 Nginx，配置启用网站 https，默认文档 index.html 的内容为“Nginx 加密访问！”；证书由 Linux-1 颁发,证书路径为/etc/pki/nginx-1.crt，私钥路径为/etc/pki/nginx-

1.key。

18. 使用 Nginx 的 proxy_pass 配置 HTTP 反向代理，使用 upstream 配置负载均衡实现 Linux-5 主机 WEB 为前端，Linux-2 主机（权重为 1，max_fails 为 3，超时为 30 秒）和 Linux-3 主机（权重为 2，max_fails 为 3，超时为 20 秒）的相关 web 服务为后端。

19. 配置 Linux-2 为 web 服务器，网站根目录为/https，默认文档 index.html 的内容为“Apache01 加密访问！”；仅允许使用域名访问，证书由 Linux-1 颁发,证书路径为/etc/pki/httpd/ssl/http01.crt，私钥路径为/etc/pki/httpd/ssl/http01.key，网站虚拟主机配置文件路径为/etc/httpd/conf.d/vhost.conf。

20. 配置 Linux-3 为 Apache web 服务器，网站根目录为/https，默认文档 index.html 的内容为“Apache02 加密访问！”；仅允许使用域名访问，证书由 Linux-1 颁发,证书路径为/etc/pki/httpd/ssl/http02.crt，私钥路径为/etc/pki/httpd/ssl/http02.key，网站虚拟主机配置文件路径为/etc/httpd/conf.d/vhost.conf。在主机 PC2 上测试。

（六）Linux Rsyslog 服务配置

【任务描述】

随之企业的不断扩大，安全变得越来越重要，为了有效防范骇客，加强监控系统级安全，决定将主机登录、su 等相关日志统一保存，相关服务主机不再保存相关安全日志，将安全日志数据与服务主机系统分离，决定使用 Linux 的 RSYSLOG 服务实现相关功能，为模拟相关功能，请使用 Linux-5、Linux-6、Linux-7 模拟完成相关功能配置及实际测试。

21. 在 Linux-7 上配置 rsyslog 服务，作为统一安全事件日志服务器，将网络内相关 Linux 主机的登录、su 命令等产生的相关安全日志存储到/var/log/skills 文件。

22. 在 Linux-5 上配置 rsyslog 服务，将本主机的登录、su 命令等产生的相关安全日志使用 UDP 转发到 Linux-7 上的 rsyslog 服务，本机不再保存相关日志。

23. 在 Linux-6 上配置 rsyslog 服务，将本主机的登录、su 命令等产生的相关安全日志使用 TCP 转发到 Linux-7 上的 rsyslog 服务，本机不再保存相关日志。

24. 禁止 Linux-5 的 SSH 的 root 远程登录，将密码重试次数设为 3，在本主机添加账号 nic，密码为竞赛系统规定的统一密码。

25. 在 Linux-6 配置 sudo，在本主机添加账号 hic，密码为竞赛系统规定的统一密码，添

加 accounts 组，使得 hic 能通过任何主机以系统中任何其它类型的用户身份运行任何命令，accounts 组中的任何成员都能通过任何主机以 root 身份运行/usr/bin 下的 useradd、userdel 和 usermod 命令；

26. 在 PC2 上使用相关用户名及密码分别 ssh 连接 Linux-5、Linux-6 主机，并使用 su 等命令。

（七）Docker 虚拟化服务配置

【任务描述】随着虚拟化技术的发展，企业把测试环境迁移到 docker 容器中，考虑到一些安全方面的问题，公司决定启用 podman 兼容 Docker。

27. 在 Linux-6 上安装 podman。

28. 导入 hello 镜像，镜像存放在物理机 D:\soft\skills\hello.tar，仓库名为 hello-skills，TAG 标签为 1.0。

29. 测试运行 hello-skills。

第五部分：实训指导文档（5 分）

撰写本次比赛项目的实训指导文档，格式可参照“**实训指导文档模板”（模板为 2023 年实训指导文档，仅供参考，内容按照实际情况自行设定）**，要求对学生技能训练有指导意义。以“Train.docx”命名并保存至 PC2 的计算机桌面上。

实训指导文档模板

【实训项目】

网络组建与管理（说明：需要 2 人为一组）。

【实训环境】

1. 通用设备

2 台计算机（CPU>=四核心四线程、主频≥3.4GHz；内存≥16GB；硬盘≥1TB； DVD 光驱），支持硬件虚拟化，2 块千兆位有线网卡，2 块无线网卡（型号：TP-LINK TL-WN821N），1 台激光打印机和各类相关耗材若干。

2. 专用设备

2 台路由器（神州数码 DCR-2655），3 台三层交换机（神州数码 CS6200-28X-EI），2 台防火墙（神州数码 DCFW-1800S-H-V2 或 DCFW-1800E-N3002），1 台无线控制器（神州数码 DCWS-6028），1 台无线 AP（神州数码 DCWL-7962AP 或 WL8200-I2），1 台云实训平台（神州数码 DCC-CRL1000），1 台综合布线机柜（含机架、强弱电综合布线钢墙、24 口超五类配线架，2 个底盒），相应线缆及配置线若干。

3. 软件环境

（1）微软 Windows 7(64 位中文版) 试用版；

（2）Rocky8.3（64 位）；

（3）WINRAR 5.21(中文版) 试用版；

（4）微软 Microsoft Office 2013(中文版) 试用版；

（5）微软 Windows Server 2008 R2(中文版) 试用版；

（6）微软 Windows Server 2019 R2(中文版) 试用版；

（7）VMware workstation 12 免费版；

（8）SecureCRT；

（9）Apache Tomcat 7.0.27；

（10）JDK（Java Development Kit）1.7 及以上；

（11）谷歌浏览器(Google Chrome)官方正式版。

【实训目的】

通过该项的实训，提高实训者计算机网络的拓扑规划能力、IP 地址规划能力、设备配置与连接能力、网络安全管理与维护能力、服务器的搭建与调试能力、故障排除和验证能力、应用的接入与测试能力、中英文技术文档阅读和应用能力、工程现场问题的分析和处理能力、组织管理与团队协调能力、质量管理和成本控制意识。

【实训内容】

主要分为三部分：

1.网络组建：根据该项目提供的计算机、网络等设备完成设备标识与连接、链路质量检测、端口检测；IP 地址规划与实施；交换机、路由器和无线等网络设备的设置与调试，局域网和广域网的相关配置。

2.服务器配置及应用：安装服务器操作系统(Windows/Linux)并配置 DNS、Web、FTP、E-mail、DHCP 等服务(Windows/Linux)、数据库安装配置、服务器系统管理、虚拟化技术、云平台部署、服务器集群技术。

3.网络设备安全配置与防护：部署防火墙保证网络安全，包括实现路由、NAT 转换、防 DDoS 攻击、包过滤、URL 过滤、P2P 流量控制、入侵检测、病毒攻击、缓冲区溢出攻击、端口攻击等、利用 VPN 技术实现远程安全接入和站点到站点的 IPsec VPN；配置无线网络 WEP 加密、MAC 认证接入控制。

【实训步骤】

此处列出整个项目过程中实操的步骤（略）。补充说明两点：

1.主要包括综合布线，网络配置的路由器、交换机、防火墙、无线 AC、AP 设备的配置文档（综合布线内容可简单概括完成内容的步骤，网络配置文档部分只需要列出每个设备的关键步骤，用文字描述即可，无需导出完整的配置文档）。

2. 服务部分（包括 WINDOWS、LINUX、虚拟化与云平台），列出需要实现哪些功能，完成哪些服务即可，但内容需完整。

【学时分配】

一般 180 分钟（考虑安排一个下午的实训时间）。

【考核标准】

1.网络综合布线安装和施工，完成设备连接，保证和测试物理连通性，IP 地址划分实施，满分为 5 分。

2.网络调试，完成指定的交换、路由、广域网和无线的配置，满分为 25 分。

3.操作系统安装(Windows/Linux)，完成操作系统的安装和配置，满分为 5 分。

4.配置常用服务(Windows/Linux)，能够熟练安装配置各类应用服务和数据库安装调试、服务器集群技术，满分为 20 分。

5.云平台部署，掌握使用云平台规划和分配资源、配置生成实例接入网络工作，满分为 15 分。

6.硬件防火墙配置，完成企业网的相关策略配置，满分为 5 分。

7.网络配置优化，完成网络优化配置，满分为 10 分。

8.VPN 技术，完成 VPN 配置，满分为 4 分。

9.无线网络安全技术，完成无线网络安全配置，满分为 1 分。

10.操作系统安全技术，掌握操作系统方面安全技术配置，满分为 10 分。

【注意事项】

参与实训者注意保持工位整洁有序。

第六部分：职业规范与素养（5 分）

1、团队合作默契，做好个人防护；

2、科学专业施工，耗材做到最简；

3、整理赛位，工具、设备归位，保持赛后整洁有序；

4、无因参赛选手的原因导致设备损坏等。

2023 年江苏省职业院校技能大赛网络搭建与应用赛项教师组样卷

网络环境要求

拓扑结构图

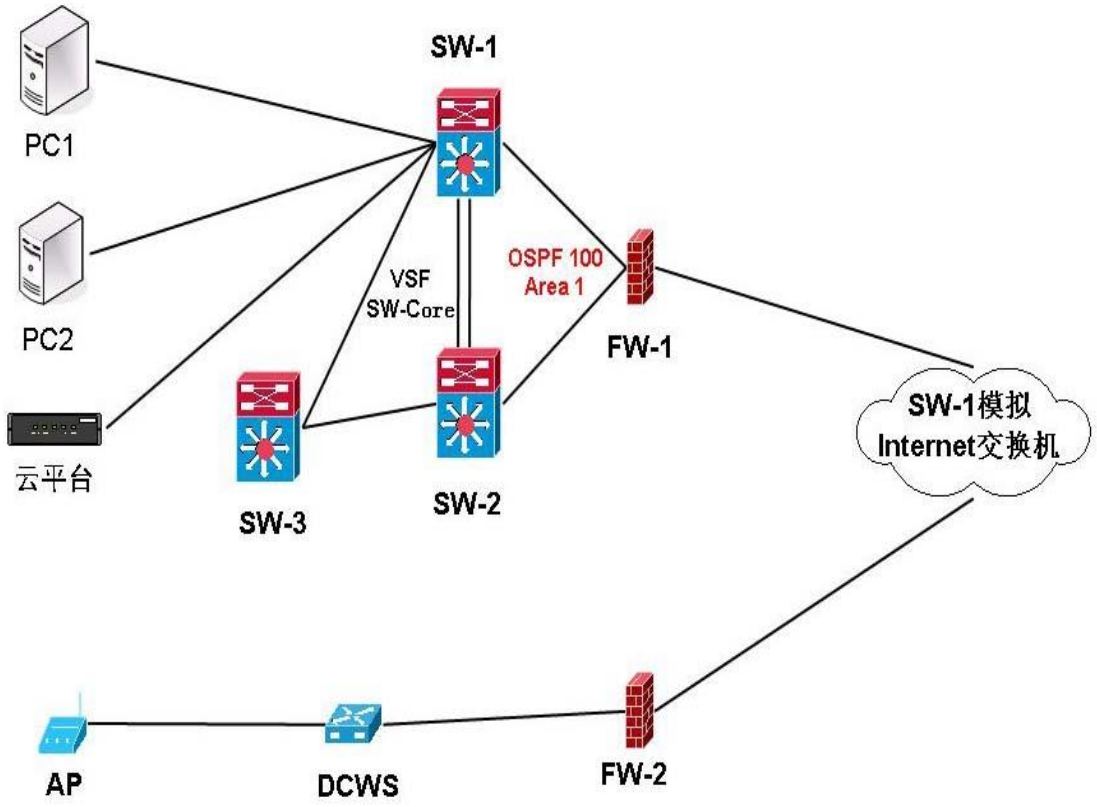


图 1 拓扑结构图

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
SW-1	E1/0/25	SW-2	E1/0/28
SW-1	E1/0/26	SW-2	E1/0/27
SW-1	E1/0/16	SW-2	E1/0/16
SW-1	E1/0/15	SW-3	E1/0/20
SW-2	E1/0/15	SW-3	E1/0/19
SW-1	E1/0/14	FW-1	E0/1
SW-2	E1/0/14	FW-1	E0/3
FW-1	E0/5	SW-1 模拟 Internet 交换机	E1/0/3
FW-2	E0/5	SW-1 模拟 Internet 交换机	E1/0/4
FW-2	E0/3	DCWS	E1/0/12
DCWS	E1/0/3	AP	
SW-1	E1/0/2	PC1	NIC
SW-1	E1/0/4	PC2	NIC
SW-1	E1/0/5	云平台	管理口
SW-1	E1/0/6	云平台	业务口

表 2.网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
防火墙	FW-1	Loopback1	172.19.254.2/32
		E0/1	172.19.255.10/30
		E0/3	172.19.255.14/30
		E0/5	183.203.10.1/30
		Tunnel 1	172.19.255.21/30
	FW-2	E0/5	183.203.10.129/30
		E0/3.10（VLAN10）	172.17.10.254/24
		E0/3.20（VLAN20）	172.17.20.254/24
		E0/3.30（VLAN30）	172.17.30.254/24
		E0/3.100(VLAN100)	172.17.100.254/24
		Tunnel 1	172.19.255.22/30
三层交换机	SW-Core	Loopback 1	172.19.254.1/32
		VLAN10 SVI	172.19.10.254/24
		VLAN20 SVI	172.19.20.254/24
		VLAN30 SVI	172.19.30.254/24
		VLAN40 SVI	172.19.40.254/24
		VLAN50 SVI	172.19.50.254/24
		VLAN200 SVI	172.19.200.254/24
		VLAN1000 SVI	172.19.255.1/30
		VLAN1001 SVI	172.19.255.9/30
		VLAN1002 SVI	172.19.255.13/30
	SW-1 模拟 Internet 交换机	VLAN4000 SVI	183.203.10.2/30
		VLAN4001 SVI	183.203.10.130/30
		Loopback100	183.100.100.100/32
二层交换机	SW-3	VLAN200 SVI	172.19.200.1/24

表 3.服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
云实训平台	云主机 1	dc.JSSkill.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2019	172.19.10.xx/24 172.19.10.xx/24
	云主机 2	Subdc.JSSkill.com	从属 CA 服务器 辅助域控制器 数据删重服务	Windows Server 2019	172.19.10.xx/24 172.19.10.xx/24
	云主机 3	Rodc.jsskill.com	只读域控制器 DHCP 服务器 WDS 服务器	Windows Server 2019	172.19.10.xx/24
	云主机 4	www1.JSSkill.com	WEB 服务器 故障转移集群服务	Windows Server 2019	172.19.10.xx/24 172.19.10.xx/24 172.19.10.xx/24
	云主机 5	www2.JSSkill.com	WEB 服务器 故障转移集群服务	Windows Server 2019	172.19.10.xx/24 172.19.10.xx/24 172.19.10.xx/24
	云主机 6	w10.JSSkill.com	Client	Windows 10	172.19.10.xx/24
	Linux-1	ca.skills.com	DNS、CA 服务	Rocky 8.3	172.19.30.xx/24
	Linux-2	Web01.skills.com	辅助 DNS 服务 Apache 服务	Rocky 8.3	172.19.30.xx/24
	Linux-3	Web02.skills.com	Apache 服务 Mariadb 服务	Rocky 8.3	172.19.30.xx/24
	Linux-4	ftp.skills.com	ftp 服务	Rocky 8.3	172.19.30.xx/24
	Linux-5	www.skills.com	nginx 服务 Proxy 服务 rsyslog 服务	Rocky 8.3	172.19.30.xx/24
PC1（IP 为 172.19.20.0/24 网段）	服务器 1	JSDC. JiangSuskills.com	域控制器 卷影副本	Windows Server 2019	172.19.20.20/24
	服务器 2	Server2.cz. JSSkill.com	子域控制器	Windows Server 2019	172.19.20.21/24
	服务器 3	Servercore. JiangSukills.com	CORE 系统 DHCP 服务器	Windows Server 2019 Core	172.19.20.22/24
PC2（IP 为 172.19.30.0/24 网段）	Linux-6	docker.skills.com	docker 服务 rsyslog 服务	Rocky 8.3	172.19.30.23/24
	Linux-7	log.skills.com	rsyslog 服务	Rocky 8.3	172.19.30.24/24

表 4.云平台网络信息表

网络名称	Vlan号	外部网络	子网名称	子网网络地址	网关 IP	激活 DHCP	地址池范围
Vlan10	10	是	Vlan10-subnet	172.19.10.0/24	172.19.10.254	是	172.19.10.100-200
Vlan20	20	是	Vlan20-subnet	172.19.20.0/24	172.19.20.254	是	172.19.20.100-200
Vlan30	30	是	Vlan30-subnet	172.19.30.0/24	172.19.30.254	是	172.19.30.100-200
Vlan40	40	是	Vlan40-subnet	172.19.40.0/24	172.19.40.254	是	172.19.40.100-200
Vlan50	50	是	Vlan50-subnet	172.19.50.0/24	172.19.50.254	是	172.19.50.100-200

表 5.虚拟主机信息表

虚拟主机名称	镜像模板(源)	云主机类型(flavor)	VCPU数量	内存、硬盘信息	网络名称	备注
云主机 1	windows2019	window-455	2	4G、55G	Vlan10	加入域
云主机 2	windows2019	window-465	2	4G、65G	Vlan10	连接卷 hd1-hd2 加入域
云主机 3	windows2019	window-465	2	4G、65G	Vlan10	加入域
云主机 4	windows2019	window-450	2	4G、50G	Vlan10	加入域
云主机 5	windows2019	window-465	2	4G、65G	Vlan10	加入域
云主机 6	Windows10	Window10-265	2	2G、65G	Vlan10	加入域
Linux1	Rocky8.3-mini-V2	linux-145	1	1G、45G	Vlan30	
Linux2	Rocky8.3-mini-V2	linux-130	1	1G、30G	Vlan30	
Linux3	Rocky8.3-mini-V2	linux-130	1	1G、30G	Vlan30	
Linux4	Rocky8.3-mini-V2	linux-140	1	1G、40G	Vlan30	
Linux5	Rocky8.3-mini-V2	linux-140	1	1G、40G	Vlan30	

表 6.云主机和服务器密码表

云主机和服务器密码	2021NetW@rk（注意区分大小写）

注：需把云主机的默认密码改为表 6.云主机和服务器密码表要求的密码