2020年全国职业院校技能大赛改革试点赛

赛项规程

一、赛项名称

赛项编号：ZZ-2020004

赛项名称：网络搭建与应用

英文名称：Network Establishment and Application

赛项组别：中职组

专业大类：信息技术类

二、竞赛目的

为贯彻党中央、国务院对职业教育工作的决策部署，落实《国家职业教育改革实施方案》，加快职业教育制度创新，促进职业教育高质量发展，以立德树人为根本任务，推进“三全育人”、深化“三教改革”，“以赛促教、以赛促学，以赛促改、以赛促建”，培养德智体美劳全面发展的高素质劳动者和技术技能人才，选拔中等职业学校信息技术类网络搭建与应用方向优秀技术技能型人才，开展本竞赛。

以职业需求为导向、以实践能力培养为重，竞赛内容主要检验参赛选手的计算机网络拓扑和IP地址规划、综合布线施工测试、设备配置与连接、网络安全管理与维护、服务器搭建与调试、故障排除和验证、应用接入与测试、中英文技术文档阅读、工程现场问题分析处理、组织管理与团队协调和理论技能综合应用等能力。在检验学生专业知识和技能熟练掌握的同时，更加重视了实践应用水平的提升，真正验证了职业教育的教学效果和应用价值，展现专业人才培养成果。

引领中职学校信息技术类专业教学发展方向，落实国家教学标准，

育训结合、书证融通；引导各地学校关注绿色、安全、智能的计算机网络技术发展趋势和产业应用方向，引导专业建设紧密对接新一代信息技术产业链、创新链的专业体系，提升学生能力素质与企业用人标准的吻合度。以技能大赛为抓手，产教融合、校企合作，切实提高学生的综合职业能力，真正促进教学改革，以适应新一轮科技革命、产业变革和新经济发展。

借鉴世赛理念，向世界高水平看齐，赛项通过真实完整工作任务，公开和临场故障创设等多样性的考核手段，工作效果和具体参数比对等精细化的评价方式，虚拟云、弹性网络、IPV6 等新技术、新工艺、新规范的应用，提高难度、加大时长，通过竞赛、体验、直播、互动与观摩，加强信息技术网络专业领域的交流与专业引领，既兼顾了中国特色，又面向世界一流看齐。

充分促进职业技能水平提升，积极推广职业技能，充分展示中职学校网络技术和系统服务技能人才培养的教育教学成果和师生良好的精神风貌，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，营造了崇尚技能、学习技能、弘扬工匠精神的良好社会氛围，激励广大青年走技能成才、技能报国之路。

三、竞赛内容

根据行业企业的业务背景开展网络业务需求、技术应用环境和实际的工程应用与业务架构分析，针对中职计算机网络毕业生主要从事系统集成、系统应用、网络工程、网络安全及售后技术支持等岗位的需求，在竞赛规定时间内完成网络搭建及安全部署、服务器配置及应用两个方面内容。

（一）竞赛主要内容

主要分为两部分:

1. 网络搭建及安全部署。主要涉及网络组建与安全配置与防护，利用本届赛项提供的计算机、网络等设备完成标识与连接、链路质量检测、端口检测; IP 地址规划与实施; 交换机、路由器、无线和防火墙等网络设备的配置与调试，局域网和广域网的相关部署与测试，并保证网络安全。

2. 服务器配置及应用。主要涉及云平台部署、虚拟化技术、Windows 和 Linux 各类服务器系统配置与管理、数据库安装调试、存储配置与管理、网站搭建与维护等。最终达到在安全的网络环境下，实现服务器、存储、网络无缝对接，云部署、系统服务与网络设备协同工作，并合理实现信息应用。

（二）重点考查技能

本竞赛项目重点考查参赛学生网络方面的实践技能，具体包括:

1. 参赛学生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。

2. 参赛学生能够完成线缆制作、合理配置路由器、交换机、无线控制器、无线 AP 和防火墙等网络设备，实现网络的正常运行。

3. 参赛学生能够根据业务需求和应用环境，安装部署服务器、数据库、存储等相关服务; 并根据网络业务需求配置各种策略，以达到网络互联互通，实现云平台和网络资源适应业务需求。

4. 参赛学生能够根据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及病毒、构建和维护绿色网络的实战能力。

5. 大赛设计与世赛接轨，在竞赛前发布竞赛设备、设备技术文档、

竞赛试题中的主要网络环境和技能点等竞赛相关信息，参赛选手可以有充分的时间思考网络架构、查找网络资料、针对性训练，提高技能水平；在实际竞赛中，基于已经发布的网络环境、技术要求的临场变化和故障预置，选手可根据掌握的技术原理参考设备技术文档进行解决。通过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。

（三）比赛时间

本赛项为团体赛项目，竞赛时间 4 小时

（四）竞赛内容与成绩比例

序号	具体内容		分值及评分细则
1	网络配置 50%	网络综合布线安装和施工	能完成设备连接，保证和测试物理连通性
2		IP 地址划分实施	能完成子网划分、IP 规划实施
3		网络调试	能完成指定的交换、路由、广域网和无线的配置，实现网络联通
4		网络优化	能完成各种网络优化配置
5		设备安全技术	通过防火墙等网络设备配置安全策略，能完成安全防护
6	系统配置管理 48%	云主机创建 Windows 与 Linux	能完成虚拟主机的创建与基本设置
7		配置常用服务 Windows 与 Linux	能完成各类服务器系统配置与管理、数据库安装调试、存储配置与管理、网站搭建与维护等
8		云平台部署	能使用云平台规划和分配资源、配置已生成的实例接入网络工作
9		操作系统安全技术	能完成操作系统的安全配置
10	职业素养 2%	职业规范与素养	能整理赛位，工具、设备归位，保持赛后整洁有序 能保证竞赛过程无因选手原因导致设备损坏 能恢复网络调试现场，保证网络及系统安全可靠运行

四、竞赛方式

竞赛以单场次团队赛组队方式进行,每支参赛队由2名选手组成，须为同校在籍学生，其中队长1名，同一学校参赛队不超过1支；每队限报2名指导教师。

五、竞赛流程

（一）比赛场次

本赛项为单场次团体赛项目。

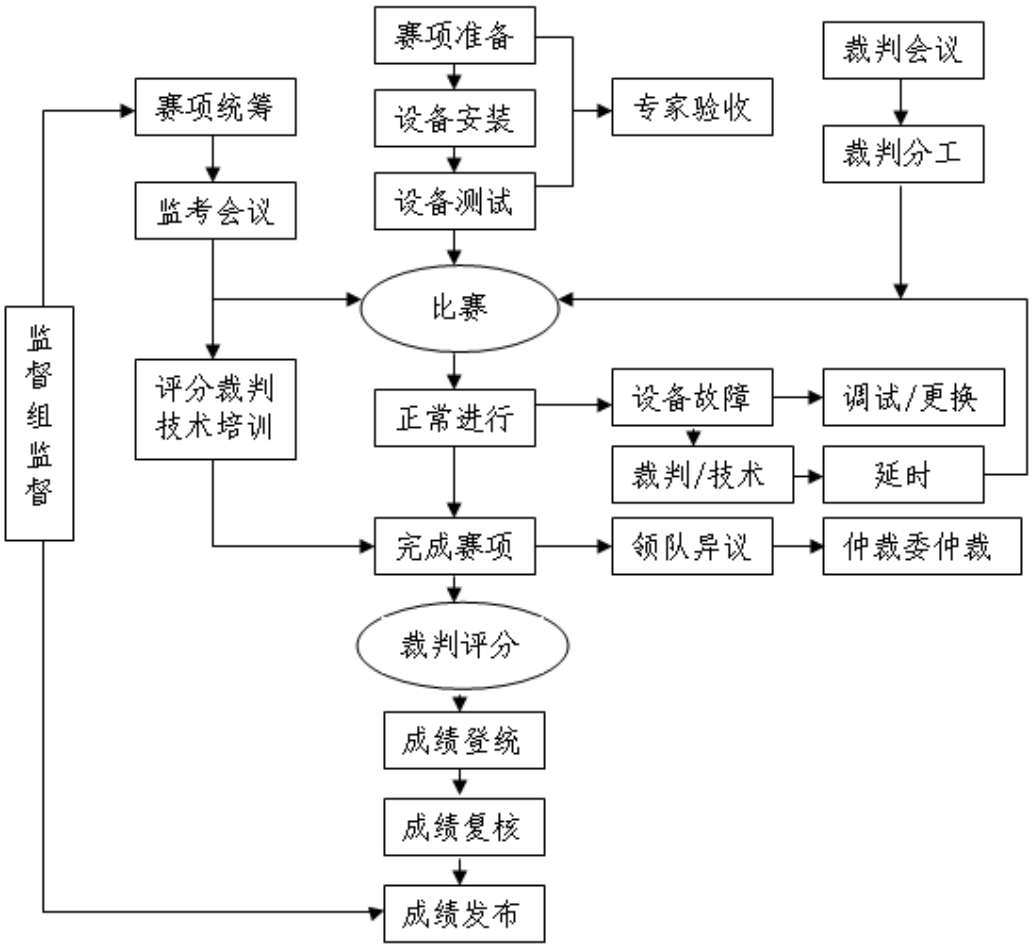
（二）日程安排

竞赛时间4小时，赛程具体安排分配如下:

日期	时间	事项	参加人员	地点
竞赛前2日	20:00前	裁判、仲裁、监督报到	工作人员	住宿酒店
竞赛前1日	09:00-12:00	参赛队报到，安排住宿，领取资料	工作人员、参赛队	住宿酒店
	09:00-12:00	裁判工作会议	裁判长、裁判员、监督组	会议室
	13:00-13:40	开赛式	各参赛队	礼堂
	13:50-14:30	领队会	各参赛队领队、裁判长	会议室
	15:00-16:00	熟悉赛场	各参赛队选手	竞赛场地
	16:00	检查封闭赛场	裁判长、监督组	竞赛场地
	16:00	返回酒店	参赛领队，参赛选手	竞赛场地
竞赛当天	07:30	参赛队到达竞赛场地前集合	各参赛队、工作人员	竞赛场地前
	07:30-07:40	大赛检录	参赛选手，检录工作人员	竞赛场地前
	07:40-08:00	第一次抽签加密（抽序号）	参赛选手、第一次加密裁判、监督	一次抽签区域
	08:00-08:20	第二次抽签加密（抽工位号）	参赛选手、第二次加密裁判、监督	二次抽签区域
	08: 00	依次进入赛场	现场裁判、裁判长、监督	竞赛场地
	08:20-08:30	就位并领取比赛任务	参赛队	竞赛场地
	08:20	比赛选手就位，裁判	参赛选手、现场裁判、	竞赛场地

日期	时间	事项	参加人员	地点
		员宣读竞赛须知	裁判长、监督	
	08: 30-12: 30	正式比赛	参赛选手、现场裁判、裁判长、监督	竞赛场地
	08: 30-11: 30	评分裁判培训会议	裁判、监督、专家组	会议室
	11: 30-12: 30	午餐	评分裁判、仲裁、监督、专家组	承办校安排
	12: 30-13: 30		现场裁判	
	12: 30	回酒店，午餐	参赛选手、指导教师、领队	住宿酒店
	12: 30-评判完毕	评判	评分裁判、裁判长、专家、监督	竞赛场地
	评判完毕后	成绩汇总报送，成绩公布	评分裁判、裁判长、专家、监督	竞赛场地和参赛队住宿酒店
竞赛后 1 日	13: 00-14: 00	专家讲评	领导、嘉宾、裁判组、各参赛队、专家组、监督组	礼堂
		闭赛式		

（三）比赛流程



（四）竞技过程

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、配置与测试网络设备、安装配置操作系统，部署安全策略等，完成网络搭建与应用整体工作项目实施。操作顺序和分工，由参赛队自行商定。

六、竞赛赛卷

（一）大赛执委会下设的赛项专家工作组负责网络搭建与应用赛项命题工作。

（二）本赛项公开涉及主要比赛内容的 5 套赛卷和网络环境。比

赛完成后，赛卷进行封闭回收。

（三）具体内容将于距国赛开始日 1 个月之前公开发布在大赛网络信息发布平台上(http://www.chinaskills-jsw.org)。

竞赛样卷详见附件 1：2020 年全国职业院校技能大赛网络搭建与应用竞赛样卷

七、竞赛规则

（一）选手报名资格

参赛选手 2 名，须为 2020 年度中等职业学校全日制在籍学生；五年制高职的一至三年级（含三年级）学生可参加比赛。年龄须不超过 21 周岁(年龄计算的截止时间以 2020 年 11 月 1 日为准)，不得跨校组队，同一学校报名参赛队不超过 1 支；凡在往届本赛项全国职业院校技能大赛中获一等奖的学生，不再参加本项目的比赛。

参赛队可配指导教师，指导教师不得超过 2 人，指导教师须为本校专兼职教师。

（二）参赛要求

1. 参赛选手应严格遵守赛场纪律，服从指挥，着参赛服装、仪表端庄整洁，自觉遵守赛场纪律，服从赛项执委会的指挥和安排，爱护大赛场地的设备和器材，严格遵守安全操作流程，防止发生安全事故。不得以任何方式泄露参院校、选手姓名等涉及竞赛场上应该保密的信息。选手必须佩带参赛证提前 60 分钟列队参赛，比赛场地通过加密抽签决定，粘贴参赛号于左臂，对号入座。

2. 参赛队在赛前 20 分钟领取比赛任务并进入比赛工位，比赛正式开始后方可进行相关操作。

3. 现场裁判引导参赛选手检查比赛环境，宣读《竞赛规则》和《选

手须知》。

4. 参赛队自行决定选手分工、工作程序。

5. 比赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和指示，如遇问题须举手向裁判人员提问。若因选手原因造成设备故障或损坏而无法继续比赛的，裁判长有权决定终止该队比赛；若非因选手个人原因造成设备故障的，必须经现场裁判确认，安排技术人员予以解决，故障中断时间不计比赛时长；比赛结束前，需打扫整理赛位，保持整洁有序。

6. 当听到比赛结束命令时，参赛选手应立即停止所有操作，关闭显示器，不得以任何理由拖延比赛时间。比赛结束（或提前完成）后，参赛队要确认已成功提交竞赛要求的配置文件和文档，裁判员与参赛队队长一起确认，参赛队在确认后离场。

7. 竞赛所需的硬件、软件和辅助工具统一提供，参赛队不得使用自带的任何有存储和网络功能的电子设备，如硬盘、光盘、U 盘、手机、手环等。离开赛场时，不得将与比赛有关的物品带离现场。

（三）赛事规定

1. 参赛选手和指导教师必须遵守赛项规程和相关要求。

2. 领队代表参赛省市负责管理参赛选手和指导教师，应当严格遵守大赛制度的有关规定，有效管理参赛选手和指导教师，遵守申诉与仲裁程序。

3. 专家、裁判、监督和仲裁人员必须按制度规定履行职责，严格执行保密制度、遵守竞赛规程，公平公正履职。

4. 赛务工作人员必须遵守规章制度，认真负责履行有关赛务岗位职责。

八、竞赛环境

竞赛现场设置场内竞赛区、现场裁判工作区、技术支持区、观摩区、场外互动区、服务区等。

（一）竞赛工位

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，接地≤4Ω。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 40 支参赛队并保证赛位前后、左右间距 1 米及以上的竞赛场地。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、5 类非屏蔽双绞线 20 米、5 类水晶头 40 个和一个垃圾箱，留有出入和消防通道。

（二）赛场环境

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，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，并配备急救人员与设施。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：4 小时，电池类型：输出电压：220V ± 5%V；市电采用双路供电。

（三）其他区域

场外互动区可设置成果展示区、体验区，设直播观摩区让所有参赛师生和社会人员观看比赛；场内设有观摩区，在不影响选手竞赛的前提下组织领队或指导教师进行有组织有纪律现场观摩。

九、技术规范

（一）教学标准

中等职业学校专业教学标准——信息技术类。

（二）行业标准

序号	标准号	中文标准名称
1	GB50311-2016	《综合布线系统工程设计规范》
2	GB50312-2016	《综合布线系统工程验收规范》
3	GB50174-2017	《电子信息系统机房设计规范》
4	GB21671-2018	《基于以太网技术的局域网系统验收测评规范》
5	GB50348-2018	《安全防范工程技术标准》
6	GB/T18729-2011	《基于网络的企业信息集成规范》
7	GB/T22239-2018	《信息系统安全等级保护基本要求》

（三）职业技术标准

网络设备调试达到并超过行业内各知名厂商 NA/NE（网络工程师）级别，接近 NP（高级网络工程师）级别；WINDIWS 服务器调试达到微软 MCSE（系统工程师）级别；Linux 服务器调试达到并超过 RHCSA（系统管理员）级别，接近 RHCE（系统工程师）级别。

（四）主要竞赛知识点和技能点

序号	内容模块	具体内容	说明
1	网络基本配置	网络综合布线安装和施工	综合布线基础：网络布线、设备连接、端口标识、电源接入；物理连通性检测、链路质量（基于 GB50312-2016）检测、端口检测等
2		IP 地址划分实施	VLSM、CIDR 等
3		交换基本配置	LAN、STP、RSTP、MSTP、802.1X、ARP、交换机虚拟化、交换安全、端口聚合、端口镜像、VRRP、VRRP V3、IPV6、PBR、IPV6 PBR、ACL、DHCPV6、DHCP Snooping、QOS、BFD、Keepalive gateway、基于流的重定向等
4		广域网和路由配置	E1 链路捆绑、PPP 或者 HDLC 协议、静态、RIP、OSPF、OSPFV3、BGP、MBGP4+等单播路由协议、PIM、IGMP 等组播协议、NTP、DHCP、TELNET、策略路由、IPV6、NAT、

序号	内容模块	具体内容	说明
			QOS 等
5		无线配置	AP 到 AC 二、三层注册，AP 配置管理、AC 射频管理、无线认证和接入配置，QOS 配置、安全配置，限时策略、强制漫游、负载均衡配置等
6		安全配置	配置 GRE 隧道、IPSEC 隧道，安全域、接口、地址与服务，安全策略、NAT、安全控制、网络行为控制、攻击防护、日志配置、Secure Connect VPN 或者 L2TP VPN 等
7	服务器配置与管理	操作系统安装 Windows 与 Linux	虚拟主机的创建与基本设置
8		配置常用服务 Windows 与 Linux	能够根据企业的应用需求，熟练安装和配置 AD、DNS、WEB、E-MAIL、DHCP、DFS、NTP、NIS、KDC、Mariadb、Apache、NFS、Samba、Tomcat、iSCSI 等常用服务并进行数据库配置与管理，并能实际运用。能够熟练掌握虚拟化技术完成特定环境配置;使用服务器群集技术来实现网络的负载均衡、故障转移、群集管理等
9		云平台部署	在云平台配置资源模板、创建网络、创建卷等
10		操作系统安全技术	域安全配置、文件系统安全配置、权限管理、配置 CA 服务、系统防火墙防护等

十、技术平台

（一）硬件平台

每赛位需配备

序号	设备名称	设备型号	数量	备注
1	路由器	神州数码 DCR-2655	2	
2	路由器线缆	神州数码 CR-V35MT-V35FC	2	
3	三层交换机	神州数码 CS6200-28X-EI	2	每台标配: DAC-SFPX-3M VSF 虚拟化连接套件

序号	设备名称	设备型号	数量	备注
4	二层交换机	神州数码 S4600-28P-SI	1	
5	多核防火墙	神州数码 DCFW-1800E-N3002	2	标配: USG-N3002-LIC 特征库升级许可
6	无线交换机	神州数码 DCWS-6028	1	
7	无线接入点	神州数码 WL8200-I2	1	
8	云实训平台	神州数码 DCC-CRL1000	1	
9	POE 模块	神州数码 DCWL-PoEINJ-G+	1	
10	PC 机	CPU 主频>=3.5GHZ,>=四核心八线程 内存>=8G 硬盘>=1T 支持硬件虚拟化	2	承办校提供
11	网络设备机柜	JZ-ONPTC-1.8M	1	开放机柜，配线架等
12	网络布线工具	JZ-ONPTT	1	工具箱含综合布线常用工具，压线钳，打线钳，测线仪，美工刀等等

（二）软件技术平台

主要为比赛的应用系统环境提供的操作系统软件和办公软件，操作系统主要由 Windows 系统和 Linux 系统两部分组成，软件主要为 WPS Office 和解压缩工具等。

Windows 系统平台主要由服务器版和桌面版组成，桌面版主要采用 Windows 10(中文版)，服务器版主要采用 Windows Server 2016 (中文版)；Linux 系统平台主要采用 Centos7.4 服务器版本；办公软件的版本为 WPS Office。

每赛位具体软件参数如下所示:

序号	软件参数	备注

1	Windows 10 中文专业版	承办校电脑自带
2	Centos 7.4（64 位）	云实训平台镜像
3	Windows Server 2016 中文版	云实训平台镜像
4	WINRAR 5.21 中文试用版	赛场提供
5	WPS Pro 2019 专业试用版	赛场提供
6	SecureCRT -SecureFX8.7.3.2279 及以上	赛场提供
7	Apache Tomcat 9.0.38.tar.gz 及以上	赛场提供
8	JDK-11.0.8_linux-x64.tar.gz 及以上	赛场提供
9	Microsoft Edge Enterprise X64 浏览器	赛场提供
10	VLC media player 播放器	赛场提供

十一、成绩评定

（一）评分原则

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考察参赛选手以下三个方面的能力和水平:

1. 网络系统组建、配置与应用、安全配置与防护的正确性、规范性和合理性。

2. 相关文档的准确性与规范性。

3. 团队风貌、职业素养、协作与沟通、组织与管理能力。

（二）评分细则与知识点

评分细则与知识点		
序号	具体内容	分值及评分细则
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

评分细则与知识点		
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 23 分
4.	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
5.	硬件防火墙配置	完成企业网的相关策略配置，满分为 5 分
6.	网络配置优化	完成网络优化配置，满分为 10 分
7.	VPN 技术	完成 VPN 配置，满分为 4 分
8.	无线网络安全技术	完成无线网络安全配置，满分为 1 分
9.	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
10.	职业规范与素养	整理赛位，保持整洁有序，无因选手原因导致设备损坏，满分为 2 分
满分		100 分

（三）具体评分方法

1. 参赛队成绩评定采用结果评分。99%为客观评分，由两名评分裁判独立评分。

2. 裁判组遵照大赛执委会要求成立，需要裁判长 1 人，另安排具备中级以上网络或操作系统技术水平裁判 16 名，包括现场裁判 4 人、评分裁判 10 人、加密裁判 2 人。

3. 在监督人员监督下，每组 2 名评分裁判按照赛题评分标准的规定分步同时评判，及时、准确地将各自评分结果和平均分记录在相应的评分登记表中并签名，保证评判独立、公正。

4. 整体评分工作采取分步得分、累计总分的积分方式，分别计算环节得分，只记录团队分数，不计参赛选手个人得分。

5. 在竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为的，由裁判长按照规定扣减相应分数，情节严重的取消比赛资格，比赛成绩记 0 分。

6. 为保障成绩评判的准确性，监督组对赛项总成绩排名前 30%的所有参赛队伍的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖

率不低于15%。监督组需将复检中发现的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。若复核、抽检错误率超过5%，裁判组需对所有成绩进行复核。

7. 赛项成绩解密后，在赛项执委会指定的地点，以纸质形式向全体参赛队进行公布。成绩无异议后，在闭赛式上予以宣布。

8. 本赛项各参赛队最终成绩由承办单位信息员录入赛事管理系统。承办单位信息员对成绩数据审核后，将系统中录入的成绩导出打印，经赛项裁判长审核无误后签字。承办单位信息员将裁判长确认的电子版赛项成绩信息上传系统，同时将裁判长签字的纸质打印成绩单报送大赛执委会。

9. 赛项结束后专家工作组根据裁判判分情况，分析参赛选手在比赛过程中对各个知识点、技术的掌握程度，并将分析报告报备大赛执委会办公室，执委会办公室根据实际情况适时公布。

10. 赛项每个比赛环节裁判判分的原始材料和最终成绩等结果性材料经监督组人员和裁判长签字后装袋密封留档，并由赛项承办院校封存，委派专人妥善保管。

十二、奖项设定

本赛项设参赛选手团体一、二、三等奖。以赛项实际参赛队(团体赛)总数为基数，一、二、三等奖获奖比例分别为10%、20%、30%(小数点后四舍五入)。获得一等奖的参赛队(团体赛)的指导教师获“优秀指导教师奖”。

十三、赛场预案

1. 竞赛过程中出现设备掉电、故障等意外时，现场裁判需及时确认情况，安排技术支持人员进行处理，现场裁判登记详细情况，填写

补时登记表，报裁判长批准后，可安排延长补足相应选手的比赛时间。

2. 预留 4-5 套备用机位和充足备用 PC 及设备，当出现非选手原因设备掉电、故障等意外时，经现场裁判认可，裁判长确认，由赛场技术支持人员予以及时更换。

3. 本赛项竞赛时为各参赛队独立作业，不涉及连接统一实时竞赛进程和评分相关服务器以致影响比赛成绩的情况发生。如竞赛时某赛位参赛队出现意外境况不会影响其它赛位正常比赛，不会由此对成绩产生影响。

4. 赛场双路供电，备用 UPS，设有应急医疗点，120 急救车和供电车场馆外等候。

5. 比赛期间发生大规模意外事故和安全问题，发现者应第一时间报告赛项执委会，赛项执委会应采取中止比赛、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。赛项出现重大安全问题可以停赛，是否停赛由赛区执委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

十四、赛项安全

赛事安全是技能竞赛一切工作顺利开展的先决条件，是赛事筹备和运行工作必须考虑的核心问题。赛项执委会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）组织机构

1. 成立由赛项执委会主任为组长的赛项安全保障小组，成员包括承办院校主抓安全的校领导、学生工作处、后勤处、保卫处、合作企业技术工程师等相关人员。

2. 与地方行政、交通、司法、安全、消防、卫生、食品、质检等

相关部门建立协调机制，制定应急预案，及时处置突发事件，保证比赛安全进行。

（二）赛项安全管理要求

1. 赛项合作企业提供的器材、设备应符合国家有关安全规定，并在比赛现场安排技术支持人员，保障赛项设备安全稳定。

2. 在竞赛工位张贴安全操作说明，并由裁判长在比赛开始前 10 分钟宣读安全操作说明。

3. 评判期间，对所有涉及相关人员进行封闭管理，直至赛项比赛结束。所有涉及竞赛赛题的人员必须签署保密协议。

4. 赛题在具有相关印刷资质的印刷企业进行印刷，并于第一时间由安保人员送往承办校具有双锁保密室的保密铁柜内，由赛项执委会指定专人和保密室负责人共同负责保管。

5. 赛题领取人必须由专人在赛项监督人员的监督下于考前 30 分钟内到保密室领取试卷，并核对好数量，查验试卷的密封是否完整，做好移交工作。

6. 竞赛用的所有赛题、成绩评定过程材料等都要回收，并妥善保存在赛项承办院校。

7. 赛项所有裁判与参赛队住宿须在不同酒店。在竞赛当天进入赛场相关区域前，由竞赛执委会工作人员收缴裁判所有通信设备，直至评判结束，监督审核，成绩提交后再归还裁判。

8. 竞赛期间，除现场裁判外，其余裁判由竞赛执委会统一安排休息场所。在此期间，裁判人员不得随意出入，避免与参赛队代表取得联系。

（三）比赛环境

1. 执委会须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执委会要求排除安全隐患。

2. 赛场周围要设立警戒线，要求所有参赛人员必须凭执委会印发的有效证件进入场地，防止无关人员进入发生意外事件。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。

3. 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。

4. 严格控制与参赛无关的易燃易爆以及各类危险品进入比赛场地，不许随便携带书包进入赛场。

5. 配备先进的仪器，防止有人利用电磁波干扰比赛秩序。大赛现场需对赛场进行网络安全控制，以免场内外信息交互，充分体现大赛的严肃、公平和公正性。

6. 执委会须会同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。

7. 大赛期间，承办单位须在赛场管理的关键岗位，增加力量，建立安全管理日志。

8. 参赛选手、赛项裁判、工作人员严禁携带通讯摄录设备和未经许可的记录用具进入比赛区域；如确有需要，由赛项承办单位统一配置，统一管理。赛项可根据需要配置安检设备，对进入赛场重要区域的人员行安检，可在相关区域安放无线屏蔽设备。

（四）生活条件

1. 比赛期间，原则上由执委会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。

2. 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、饮食安全等由执委会和提供宿舍的学校共同负责。

3. 大赛期间有组织的参观和观摩活动的交通安全由执委会负责。执委会和承办单位须保证比赛期间选手、指导教师和裁判员、工作人员的交通安全。

4. 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。

（五）组队责任

1. 各学校组织代表队时，须安排为参赛选手购买大赛期间的人身意外伤害保险。

2. 各学校代表队组成后，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。

（六）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. 赛事工作人员违规的，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. 参赛队应该参加赛项承办单位组织的开闭赛式等各项赛事活动。

2. 在赛事期间，领队及参赛队其他成员不得私自接触裁判，凡发现有弄虚作假者，取消其参赛资格，成绩无效。

3. 所有参赛人员须按照赛项规程要求按照完成赛项评价工作。

4. 对于有碍比赛公正和比赛正常进行的参赛队，视其情节轻重，按照相关规定给予警告、取消比赛成绩、通报批评等处理。

5. 由省、自治区、直辖市、计划单列市、新疆生产建设兵团教育行政部门确定赛项领队 1 人，赛项领队应该由参赛院校中层以上管理人员或教育行政部门人员担任，熟悉赛项流程，具备管理与组织协调能力。

6. 参赛队领队应按时参加赛前领队会议，不得无故缺席。

7. 参赛队领队负责组织本省参赛队参加各项赛事活动。

8. 参赛队领队应积极做好本省参赛队的服务工作，协调各参赛队与赛项组织机构、承办院校的对接。

9. 参赛队认为存在不符合竞赛规定的设备、工具、软件，有失公正的评判、奖励，以及工作人员的违规行为等情况时，须由领队向赛项仲裁组提交书面申诉材料。各参赛队领队应带头服从和执行申诉的最终仲裁结果，并要求指导教师、选手服从和执行。

（二）指导教师须知

1. 指导教师应该根据专业教学计划和赛项规程合理制定训练方案，认真指导选手训练，培养选手的综合职业能力和良好的职业素养，克服功利化思想，避免为赛而学、以赛代学。

2．指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

3．指导教师应该根据赛项规程要求做好参赛选手保险办理工作，并积极做好选手的安全教育。

4．指导教师参加赛项观摩等活动，不得违反赛项规定进入赛场，干扰比赛正常进行。

（三）参赛选手须知

1．参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

2．参赛选手凭统一印制的参赛证参加竞赛。

3．参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

4．参加选手请勿携带与竞赛无关的电子设备、通讯设备及其他资料与用品进入赛场。

5．参赛选手应按照规定时间抵达赛场，凭参赛证、学生证复印件和身份证复印件检录，按要求入场，不得迟到早退，遵守比赛纪律，以整齐的仪容仪表和良好的精神风貌参加比赛。

6．参赛选手应增强角色意识，科学合理分工与合作。

7．参赛选手应按有关要求在指定位置就坐，在比赛开始前 10 分钟，认真阅读《比赛任务书》，须在确认竞赛内容和现场设备等无误后在裁判长宣布比赛开始后打开显示器参与竞赛，如果违规先行做诸如打开显示器、制作线缆等任何操作，经裁判提示注意后仍无效，将酌情扣分，情节严重的经裁判长批准后将立即取消其参赛资格，由此引发的后续问题参赛队全部承担。

8．参赛选手必须在指定区域，按规范要求安全操作竞赛设备，严

格遵守比赛纪律。如果违反，经裁判提示注意后仍无效，将酌情扣分，情节严重的终止其比赛。一旦出现较严重的安全事故，经裁判长批准后将立即取消其参赛资格。

9. 在竞赛过程中，确因计算机或设备软件或硬件故障，只是操作无法继续的，经赛项裁判长确认，予以启用备用计算机或设备，由此耽误的比赛时间将予以补时。经现场技术人员、裁判和裁判长确认，如因个人操作导致设备系统故障，不予以补时处理。

10. 竞赛时间终了，选手应全体起立，关闭显示器，结束操作。将资料和工具整齐摆放在操作平台上，经与裁判签字确认，工作人员清点后可离开赛场，离开赛场时不得带走任何资料。

11. 在竞赛期间，未经赛项执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

（四）工作人员须知

1. 树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项执委会的领导下，按照各自职责分工和要求认真做好岗位工作。

2. 所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3. 注意文明礼貌，保持良好形象，熟悉赛项指南。

4. 自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5. 提前 30 分钟到达赛场，严守工作岗位，不迟到，不早退，不无故离岗，特殊情况需向工作组组长请假。

6. 熟悉竞赛规程，严格按照工作程序和有关规定办事，遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

7. 工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8. 保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。

十六、申诉与仲裁

各参赛队对不符合大赛和赛项规程规定的仪器、设备、工装、材料、物件、计算机软硬件、竞赛使用工具、用品，竞赛执裁、赛场管理，以及工作人员的不规范行为等，可向赛项仲裁组提出申诉。申诉主体为参赛队领队。参赛队领队可在比赛结束后（选手赛场比赛内容全部完成）2 小时之内向仲裁组提出书面申诉。

书面申诉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，并由领队亲笔签名。非书面申诉不予受理。

赛项仲裁工作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，可由省（市）领队向赛区仲裁委员会提出申诉。赛区仲裁委员会的仲裁结果为最终结果。

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。

申诉方可随时提出放弃申诉，不得以任何理由采取过激行为扰乱赛场秩序。

十七、竞赛观摩

本赛项提供公开观摩区进行公开观摩。

参加观摩人员应遵守竞赛制度和规程，按照赛项执委会有序组织参加赛项观摩等活动，不得违反赛项规定进入赛场，干扰比赛正常进行，观摩时需按照沿指定路线、在指定时间和规定区域内到现场观赛。

十八、竞赛直播

赛项全过程、全方位安排现场直播，并设直播观摩区让所有参赛师生和社会人员观看比赛。

本赛项赛前对赛题印制、设备安装调试、软件安装等关键环节进行实况摄录。

十九、资源转化

依照有关要求，赛项资源转方案按要求与规程同时公布；于赛后30日内向大赛执委会办公室提交资源转化实施方案，作为十三年的老赛项会在三个月完成新资源的补充与完善，半年内完成全部资源的转化工作。

（一）竞赛过程中获得的主要资源

1. 竞赛样题、试题库;

2. 竞赛赛题的评分标准;

3. 考核环境描述;

4. 竞赛过程音视频记录;

5、评委、裁判、专家点评和技术分析报告;

6. 优秀选手、指导教师访谈。

（二）资源转化基本方案与呈现形式

资源转化成果按照行业标准、契合课程标准、突出技能特色、展现竞赛优势，形成满足职业教育教学需求、体现先进教学模式、反映职业教育先进水平的共享性职业教育教学资源。资源转化成果包含基

本资源和拓展资源，充分体现本赛项技能考核特点:

资源转化成果应包含基本资源和拓展资源。

1. 基本资源

基本资源按照风采展示、技能概要、教学资源三大模块设置。

（1）风采展示。赛后即时制作时长 15 分钟左右的赛项宣传片，以及时长 10 分钟左右的获奖代表队（选手）的风采展示片。供专业媒体进行宣传播放。

（2）技能概要。包括技能介绍、技能操作要点、评价指标等。

（3） 教学资源。教学资源充分涵盖赛项内容。包括教学方案、训练 指导、作业/任务、实验/实训/实习资源等，其呈现形式主要是演示文稿、图片、操作流程演示视频、动画及相关微课程、微资源等。

2. 拓展资源

拓展资源是指反映技能特色、可应用于各教学与训练环节、支持技能教学和学习过程的较为成熟的多样性辅助资源。

（三）资源的技术标准

资源转化成果以文本文档、演示文稿、视频文件、Flash 文件、图形/图像素材和网页型资源等。

（四）资源的提交方式与版权

赛项资源转化成果的版权由技能大赛执委会和赛项执委会共享。

（五）资源的使用与管理

资源转化成果的使用与管理由大赛执委会统一使用与管理，会同赛项承办单位、赛项有关专家，联系出版社编辑出版有关赛项实训教材等精品资源。

（六）资源转化项目工作进程表

资源名称			表现形式	资源数量	资源要求	完成时间	实施人员
基本资源	风采展示	宣传片	视频	1	15 分钟以上	赛后 5 日	承办校
		风采展示片	视频	1	10 分钟以上	赛后 5 日	承办校
	技能概要	技能介绍	文本	1	补充完善	赛后 60 日	专家组
		训练大纲	文本	1	补充完善	赛后 60 日	专家组
		评价指标	文本	1	补充完善	赛后 60 日	专家组
	教学资源	专业教材	教材	1 本以上	补充完善定期再版	赛后 90 日	专家组 技术支持单位
		技能训练指导书	教材	1 本以上	补充完善定期再版	赛后 90 日	专家组 技术支持单位
	仿真微课		资源库	1 套	微课平台补充完善	赛后 90 日	专家组 技术支持单位
	优秀选手访谈		视频	1	20 年赛事	赛后 90 日	承办校

赛后还需加强师资队伍建设，促进资源转化能够在教学中有效应用。2020 年大赛完毕后计划进行 2 期研讨会，以及 2 期师资培训。

序号	活动名称	计划时间	备注
1	研讨会第 1 期	2020 年 12 月	
2	师资培训第 1 期	2020 年 12 月	
3	师资培训第 2 期	2021 年 1 月	
4	研讨会第 2 期	2021 年 1 月	

（七）资源转化说明

1. 计算机网络技术专业系列教材补充完善。

2. 计算机网络技能训练指导书。系统梳理计算机网络技术专业的岗位需求、核心知识点和能力点及历年竞赛考核内容与评分要点。

3. 仿真实训微课的制作。在 2014 年搭建的“云微课平台”和 “在线交互式仿真实训课件”的基础上补充完善新资源。

附件 1：竞赛样卷

2020 年全国职业院校技能大赛改革试点赛中职组

“网络搭建与应用”赛项竞赛样卷

（总分 1000 分）

网络拓扑图

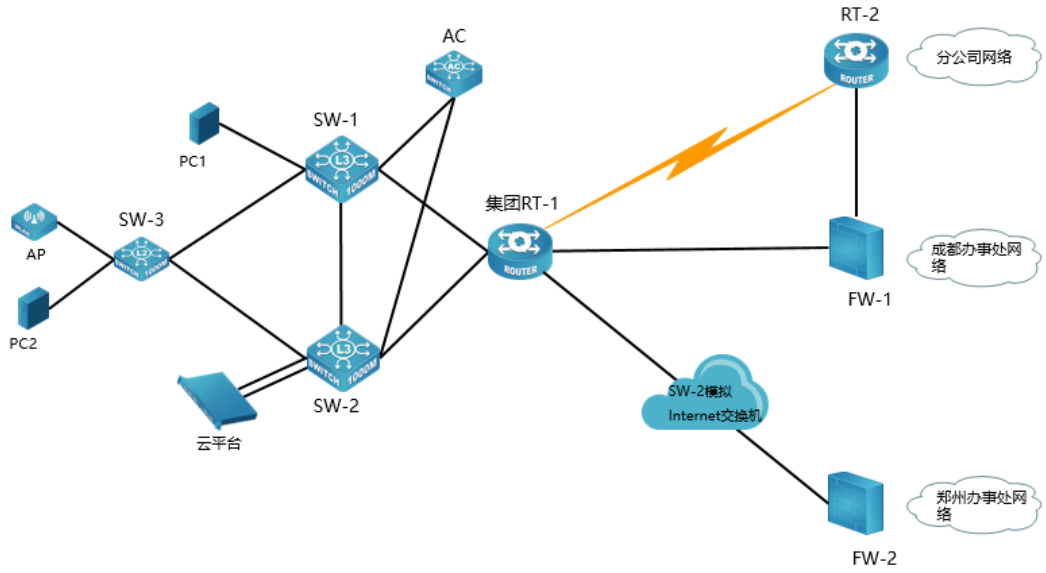


表 1. 网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
RT-1	G0/5	FW-1	E0/1
RT-1	S0/1	RT-2	S0/2
RT-1	S0/2	RT-2	S0/1
RT-2	G0/5	FW-1	E0/2
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	AC	E1/0/23
SW-2	E1/0/22	AC	E1/0/24
SW-1	E1/0/21	RT-1	G0/3
SW-2	E1/0/21	RT-1	G0/4
RT-1	G0/6	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
路由器	RT-1	Loopback1	10.30.255.3/32
		G 0/3	10.30.254.2/30
		G 0/4	10.30.254.6/30
		G 0/5	10.30.254.25/30
		G 0/6	202.99.192.1/30
		S 0/1-2	10.30.254.17/30
		Tunnel 1	10.30.254.33/30
	RT-2	Loopback1	10.30.255.4/32
		G 0/5	10.30.254.29/30
		G 0/4	172.30.10.254/24
		S 0/1-2	10.30.254.18/30
三层交换机	SW-1	Loopback 1	10.30.255.1/32
		VLAN10 SVI	10.30.10.0/24
		VLAN20 SVI	10.30.20.0/24
		VLAN30 SVI	10.30.30.0/24
		VLAN40 SVI	10.30.40.0/24
		VLAN50 SVI	10.30.50.0/24
		VLAN200 SVI	10.30.200.0/24
		VLAN1000 SVI	10.30.254.9/30
		VLAN1001 SVI	10.30.254.1/30
		VLAN4094 SVI	10.30.254.253/30
	SW-2	Loopback 1	10.30.255.2/32
		VLAN10 SVI	10.30.10.0/24

		VLAN20 SVI	10.30.20.0/24
		VLAN30 SVI	10.30.30.0/24
		VLAN40 SVI	10.30.40.0/24
		VLAN50 SVI	10.30.50.0/24
		VLAN200 SVI	10.30.200.0/24
		VLAN1002 SVI	10.30.254.13/30
		VLAN1001 SVI	10.30.254.5/30
		VLAN4094 SVI	10.30.254.254/30
	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
防火墙	FW-1	Loopback1	10.30.255.5/32
		Eth0/1	10.30.254.26/30（untrust 安全域）
		Eth0/2	10.30.254.30/30（untrust 安全域）
		Eth0/3	172.30.20.254/24（trust 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	10.30.254.34/30（VPNHub 安全域）

无线控制器	DCWS	VLAN1000 SVI	10.30.254.10/30
		VLAN1002 SVI	10.30.254.14/30
		VLAN220 SVI	10.30.220.254/24
二层交换机	SW-3	VLAN200 SVI	10.30.200.250/24

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	ad.netskills.net	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2012 R2	10.30.30.xx/24
	云主机 2	print.netskills.net	从属 CA 服务器 辅助域控制器 打印服务器	Windows Server 2012 R2	10.30.30.xx/24
	云主机 3	WDF	WDS 服务器 DHCP 服务器 文件服务器	Windows Server 2012 R2	10.30.30.xx/24
	云主机 4	www1.netskills.net	WEB 服务器 负载均衡集群服务	Windows Server 2012 R2	10.30.30.xx/24 10.30.50.xx/24
	云主机 5	www2.netskills.net	WEB 服务器 负载均衡集群服务	Windows Server 2012 R2	10.30.30.xx/24 10.30.50.xx/24
	云主机 6	w10.netskills.net	Client	Windows 10	10.30.30.xx/24

	云主机 7	dns.chinaskills.net	域名服务器 证书服务器	Centos 7.4	10.30.40.xx/24
	云主机 8	www1.chinaskills.net	邮件服务器 WEB 服务器	Centos 7.4	10.30.40.xx/24
	云主机 9	www2.chinaskills.net	WEB 服务器 数据库服务器	Centos 7.4	10.30.40.xx/24
	云主机 10	ssm.chinaskills.net	Tomcat 服务器 磁盘管理	Centos 7.4	10.30.40.xx/24
PC1（IP 为 10.30.30.0/24 网段）	服务器 1	dc.netjnds.com	域控制器	Windows Server 2008 R2	10.30.30.30/24
	服务器 2	Server2.hm.netskills.net	子域控制器	Windows Server 2012 R2	10.30.30.29/24
PC2（IP 为 10.30.40.0/24 网段）	服务器 3		WEB 服务器	Centos 7.4	10.30.60.27/24
	服务器 4	www3.chinaskills.net	反向代理服务器	Centos 7.4	10.30.40.26/24 10.30.60.26/24
	服务器 5	www.chinaskills.net	负载均衡服务器	Centos 7.4	10.30.40.25/24

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
Vlan30	30	是	Vlan30-subnet	10.30.30.0/24	10.30.30.254	是	10.30.30.100, 10.30.30.200

Vlan40	40	是	Vlan40-subnet	10.30.40.0/24	10.30.40.254	是	10.30.40.100, 10.30.40.200
Vlan50	50	是	Vlan50-subnet	10.30.50.0/24	10.30.50.254	是	10.30.50.100, 10.30.50.200

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(实例规格)	VCPU数量	内存、硬盘信息	网络名称	备注
云主机 1	WindowsServer2012	windows-490	2	4G、90G	Vlan30	
云主机 2	WindowsServer2012	windows-485	2	4G、85G	Vlan30	加入域
云主机 3	WindowsServer2012	windows-480	2	4G、80G	Vlan30	连接卷 hd1-hd3
云主机 4	WindowsServer2012	windows-465	2	4G、65G	Vlan30 Vlan50	加入域
云主机 5	WindowsServer2012	windows-460	2	4G、60G	Vlan30 Vlan50	加入域
云主机 6	Windows10	windows10-260	2	2G、60G	Vlan30	加入域
云主机 7	Centos7-mini-V2	linux-140	1	1G、40G	Vlan40	
云主机 8	Centos7-mini-V2	linux-150	1	1G、50G	Vlan40	
云主机 9	Centos7-mini-V2	linux-170	1	1G、70G	Vlan40	
云主机 10	Centos7-mini	linux-120	1	1G、20G	Vlan40	连接

	-V2					hd4-hd5

表 6.云主机和服务器密码表

云主机和服务器密码	2019Netw@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

竞赛说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分三个部分，其中:

第一部分: 网络搭建及安全部署项目（500 分）

第二部分: 服务器配置及应用项目（480 分）

第三部分: 职业规范与素养（ 20 分）

二、竞赛注意事项

1. 禁止携带和使用移动存储设备、计算器、通信工具及参考资料。
2. 请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。
3. 请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。
4. 操作过程中，需要及时保存设备配置。
5. 比赛结束后，所有设备保持运行状态，评判以最后的硬件连接和配置为最终结果。
6. 比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。
7. 禁止在纸质资料、比赛设备、上填写任何与竞赛无关的标记，如违反规定，可视为 0 分。
8. 与比赛相关的工具软件放置在每台主机的 D 盘 soft 文件夹中。

项目简介:

某集团公司原在北京建立了总部，后在深圳建立了分部，又在成都、郑州设立了两个办事处。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 2019 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、分公司及两个办事处的网络结构详见“主要网络环境”拓扑图。

其中一台 S4600 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 分别作为成都办事处、郑州办事处的防火墙；一台 DCR-2655 路由器编号为 RT-1，作为集团的核心路由器；另一台 DCR-2655 路由器编号为 RT-2，作为分公司路由器;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。

请注意:结合网络环境和网络拓扑要求,合理规划网络和IP地址，保证网络搭建及安全部署项目和服务器配置及应用项目顺利实施。

网络搭建及安全部署项目

（500 分）

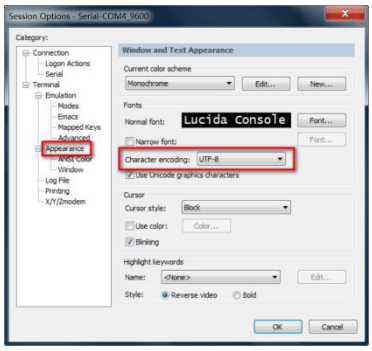
【说明】

1. 设备 console 线有不同两条。交换机、 AC、防火墙使用同一条 console 线，路由器使用另外一条 console 线;
2. 请将 PC1 上 D 盘 soft 文件夹中的《网络搭建及安全部署竞赛报告单》复制到 PC1 桌面的选手自建“比赛文档-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;
3. 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;

保存文档方式如下:

- 交换机、路由器、AC 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: RT-1 路由器文件命名为: RT-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；其他设备 CRT 软件字符编号为:GB2312。CRT 软件调整字符编号配置如

图：



一、 网络布线与基础连接（本部分 50 分）

右侧布线面板立面示意图　　左侧布线面板立面示意图

【说明】

1. 机柜左侧布线面板编号 101；机柜右侧布线面板编号 102。
2. 面对信息底盒方向左侧为 1 端口、右侧为 2 端口。所有配线架、模块按照 568B 标准端接。
3. 主配线区配线点与工作区配线点连线对应关系如下表所示。

PC1、PC2 配线点连线对应关系表

序号	信息点编号	配线架编号	底盒编号	信息点编号	配线架端口编号
1	W1-02-101-1	W1	101	1	02
2	W1-06-102-1	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（本部分 132 分）

(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。

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(实例 10)，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(实例 20)，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，Internet 路由表位于 VPN 实例名称 Internet 内。

(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，分别连接在两台核心交换机 E1/0/10-E1/0/11 接口测试，VLAN300 作为远程端口镜像 VLAN，Ethernet1/0/12 作为反射端口，将核心交换机与接入交换机、路由器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（本部分 168 分）

(一) 、尽可能加大集团路由器与分公司路由器之间专线链路带宽，配置 Mutlilink PPP 捆绑;

(二) 、规划集团与分公司、成都办事处之间使用 OSPF 协议进行互连互通，进程号为 1，具体要求如下:

1. 集团路由器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、集团路由器与分公司路由器之间均属于骨干区域，集团业务网段属于 Area1，分公司业务网段属于 Area2；集团路由器与成都办事处防火墙之间、成都办事处防火墙与分公司路由器之间、成都办事处业务网段属于 Area3;

2. 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;

3. 要求集团业务网段 Area、分公司业务网段 Area 禁止学习 LSA3、LSA4、LSA5、LSA7 类路由，要求集团业务网段、AP&交换机管理网段中不发送协议报文;

4. 集团路由器将访问郑州办事处业务网段的静态路由引入 OSPF，要求分公司禁止学习到郑州办事处业务网段路由。

(三)、实现集团销售&产品&信息技术&无线业务、分公司业务网段、成都办事处业务网段统一通过集团路由器访问 Internet，轮询使用 NAT 地址为：202.99.192.4/30(标准 IP 访问列表和地址池名称都命名为 1)，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)、集团路由器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_RT1 间链路转发，DCWS_SW-2_RT1 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、分公司、办事处互访流量优先通过 SW-1_RT1 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_RT1 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（本部分 44 分）

（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 SW-2 配置使用 DHCP 进行 AP 管理地址分配，利用 DHCP 方式让 AP 发现 AC 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）、配置所有 Radio 接口: AP 在收到错误帧时，将不再发送 ACK 帧; 打开 AP 组播广播突发限制功能; 开启 Radio 的自动信道调整，每天上午 10:00 触发信道调整功能。

五、 安全策略配置（本部分 50 分）

（一）、根据题目要求配置成都办事处防火墙、郑州办事处防火墙相应的业务安全域、业务接口；限制成都办事处业务网段只可以与集团销售、产品、财务业务网段 http&https 业务和 Internet 业务互访；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成都办事处业务网段、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）、集团计划在成都办事处进行 https 认证试点，对成都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 上下行最大 4Mbps 带宽，限制 http 流量最大上下行带宽为 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（本部分 56 分）

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，路由器公告的生存期为 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。

服务器配置及应用项目（480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v1.2》;

名称	用户名	密码	ssh	rdp
Windows10	administrator	Qwer1234	否	是
WindowsServer2012	administrator	Qwer1234	否	是
CentOS7-mini-V2	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，centos 主机实例可以通过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为“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 桌面上选手自建的“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（150 分）

一、在云实训平台上完成如下操作（150 分）

（一）云平台基础设置（50 分）

1.按照“表 4：云平台网络信息表”要求创建三个外部网络，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”（30 分）;

2.创建 5 块云硬盘，卷命名为 hd1-hd5，其中 hd1-hd3 大小为 10G，h4-h5 大小自定（20 分）;

（二）创建虚拟主机（100 分）

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”（80 分）;

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（20 分）;

Windows 操作系统（165 分）

一、在云实训平台上完成如下操作（125 分）

（一）完成虚拟主机加入域

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

（二）在云主机 1 中完成域控制器及 DNS 服务器的部署

1.将云主机 1 的服务器配置成域控制器,域名为 netskills.net，设置域和林的功能级别为 Windows Server 2012;

2.将此服务器配置为主 DNS 服务器，要求正确配置 netskills.net 域名的正向及反向解析区域，创建对应服务器主机记录，正确解析 netskills.net 域中的所有服务器;

3.创建 3 个组织单位、采用对应部门名称的中文全拼命名，每个部门创建 2 个用户，行政部用户：adm1¯ adm2、营销部用户：sale1¯sale2、技术部用户：sys1¯sys2，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);

4.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 10 位、密码最长存留 34 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;

5.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”;

6.配置相关策略，实现所有营销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!”;

（三）在云主机 1 中完成 CA 服务器的部署（5 分）

1.将云主机 1 的服务器配置成 CA 服务器，安装证书服务，设置为企业根，颁发机构有效期为 7years，通过相应配置使从属证书颁发机构颁发的证书有效期为 4 年;

（四）在云主机 2 中完成从属证书及网络打印服务的部署（15 分）

1.将云主机 2 的服务器升级成 netskills.net 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，安装证书服务，设置为企业从属 CA，负责整个 netskills.net 域的证书发放工作，颁发的证书有效期年份为 4years;

3.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“HB-Print”;

（2）将“HB-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.netskills.net”查看打印机，证书由本机进行签署颁发;

（五）在云主机 3 中完成 DHCP 及 WDS 服务的部署（10 分）

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 dhcpserv，地址池为 210-215，仅允许

“服务器 2”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 2012 R2 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;

（六）在云主机 3 中完成磁盘管理及文件服务器的部署（10 分）

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、更改权限给 everyone 用户;

3.在 FilesWeb 文件夹内建立三个子文件夹:

（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;

（3）子文件夹为 “WWWLogFile”，用来存储日志文件;

（七）在云主机 4 中完成 WEB 服务器 1 的部署（15 分）

1.添加一块网卡，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.netskills.net 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.netskills.net 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，日志文件存储到“\\WDF\FilesWeb\WWWLogFile”目录中，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;

5.创建证书申请时，证书必需信息为:

（1）通用名称=“www.netskills.net”;

（2）组织=“netskills”;

（3）组织单位=“sales”;

（4）城市/地点 =“Shenzhen”;

（5）省/市/自治区=“Shenzhen”;

（6）国家/地区=“CN”;

（八）在云主机 4 中完成 NLB 群集服务器的部署（6 分）

1.安装 NLB 负载平衡服务,其群集 IPv4 地址为 10.30.30.150/24，新建群集优先级为 6，群集名称为 www.netskills.net，采用多播方式;

2.在访问 www.netskills.net 站点时，要求只允许使用域名通过 SSL 加密访问;

（九）在云主机 5 中完成 WEB 服务器 2 的部署（10 分）

1.添加一块网卡，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.netskills.net 站点的共享配置，启动 www.netskills.net 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.证书采用证书导入的方式，将云主机 4 为 www.netskills.net 站点申请的证书进行导入，并保证能在本服务器上正常使用；

（十）在云主机 5 中完成 NLB 群集服务器的部署（6 分）

1.安装 NLB 负载平衡服务，添加到“云主机 4”新建的群集中，优先级为 11，采用多播方式；

2.在访问 www.netskills.net 站点时，要求只允许使用域名通过 SSL 加密访问；

（十一）在云主机 6 中完成相关功能（2 分）

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 skills2019；

二、在 PC1 上完成如下操作（40 分）

（一）完成虚拟主机的创建（22 分）

1.安装虚拟机“服务器 1”，其内存为 1.5G，硬盘 50G；

2.安装虚拟机“服务器 2”，其内存为 2G，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 1”中完域控制器及域信任的部署（11分）

1.将“服务器 1”服务器升级为域服务器，域名为 netjnds.com;

2.通过使用单向信任关系，实现 netskills.net 域的员工（不包括域管理员账户）可以访问 netjnds.com 域的共享资源,反之不可以;

（三）在主机“服务器 2”中完成子域控制器的部署（7分）

1. 将“服务器 2”的服务器，升级为子域 hm.netskills.net;

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 skills2019;

Linux 操作系统部分（165 分）

一、在云实训平台上完成如下操作（95 分）

（一）在云主机 7 中完成域名服务器及证书服务器的部署（20 分）

1.在此服务器中安装配置 DNS 服务,负责区域“chinaskills.net”内主机解析，七台主机分别为 dns.chinaskills.net、mail.chinaskills.net、www1.chinaskills.net、www2.chinaskills.net、ssm.chinaskills.net 、www3. chinaskils.net 、www.chinaskils.net,做好正反向 DNS 服务解析;

2.将此服务器配置成 CA 证书服务器(CA 认证中心),负责 HAProxy、Mail 服务器和 Squid 服务器的证书发放工作,HAProxy、Mail 和 Squid 服务器的证书通用名称均为 msh.chinaskills.net;

（1）CA 证书路径为/etc/pki/CA/cacert.pem;

（2）签发数字证书，颁发者主要信息如下:

①Country Name=CN;

②State or Province Name =Shenzhen;

③Organization Name=DCN;

④Organizational Unit Name= chinaskills;

⑤Common Name=chinaskills.net;

（二）在云主机 8 中完成 Apache 服务器的部署（5 分）

1.在此服务器中安装 Apache 服务，建立虚拟主机站点

www1.chinaskills.net:

（1）配置网站主目录为/www/netdj，将 D:\Soft\Apache 中的主页存放该主目录中;

（2）配置访问日志路径和名称为/var/log/httpd/www1.chinaskills.net-access_log，日志记录格式为普通型;

（三）在云主机 8 中完成 E-MAIL 服务器的部署（15 分）

1.在此服务器上安装配置 Postfix 邮件服务，具体要求为:

（1）创建二个邮箱用户 mail1 和 mail2，用户密码为 321，不允许本地登录;

（2）邮件服务器的域名后缀为 chinaskills.net;

（3）邮件服务器要在所有 IP 地址上进行侦听;

（4）设置邮件服务器仅支持 smtps 和 pop3s 协议连接;

（四）在云主机 9 中完成 Apache 服务器的部署（5 分）

1.在此服务器中安装 Apache 服务，建立虚拟主机站点 www2.chinaskills.net:

（1）配置网站主目录为/www/netdj，将 D:\Soft\Apache 中的主页存放该主目录中;

（2）配置访问日志路径和名称为/var/log/httpd/www2.chinaskills.net-access_log，日志记录格式为复合型;

（五）在云主机 9 中完成数据库服务器的部署（15 分）

1.将此服务器配置为数据库服务器，创建数据库为 School，在库中创建表为 Score，在表中创建 2 个用户，分别为（1，suser1，1999-6-1，female），（2，suser2，2000-9-1，male），口令与用户名相同，表结构如下;

字段名	数据类型	主键
ID	Int	是
Name	varchar(20)	否
Birthday	Datetime	否
Sex	char(10)	否
Password	char（64）	否

2. 开启数据库的查询日志，路径为/var/log/mariadb/mariadb.log;

（六）在云主机 10 中完成 JSP+Tomcat 运行环境的部署（15 分）

1.安装 jdk 和 jre（软件包在 D:\Soft 下），安装完成后，配置 JAVA 环境变量;

2.安装 tomcat（软件包在 D:\Soft 下）服务并启动，保证用户可使用浏览器浏览 tomcat 默认主页;

3.将 D:\soft\jndsjs 中全部微网站应用程序，复制到 tomcat 的相关目录下，通过适当配置，让用户可以通过 https 的访问方式，正确显示指定的网页内容;

（七）在云主机 10 中使用系统存储管理器完成磁盘管理的部署（20 分）

1.添加两块 20G 的物理磁盘，分别为 vdb 和 vdc，分区的大小和多少个分区，根据后面任务的需求自己确定;

2.使用物理磁盘 vdb 来扩展存储池 centos 的容量，增加容量大小为 18G;

3.将系统设备卷/dev/centos/root 增加 15G 的容量，来达到扩展系统根分区容量的目的;

4.用物理磁盘 vdc 创建一个名为 vg1 的存储池，并在该存储池上创建一个名为 lv1 的 LVM 卷，该卷的大小为 500M，使用 xfs 文件系统格式化卷，并将它挂载到/soft 目录下;

5.发现 lv1 逻辑卷 500M 的容量不够，现需要将其再扩容 10G;

二、在 PC2 上完成如下操作（70 分）

（一）完成虚拟主机的创建（35 分）

1.安装虚拟机“**服务器 3**”，要求为内存 1G，硬盘 30GB，引导分区和根分区的文件系统采用 btrfs 格式;

2.安装虚拟机“**服务器 4**”，要求为内存 1G，硬盘 35GB;

3.安装虚拟机“**服务器 5**”，要求为内存 1G，硬盘 25GB;

（二）在主机“服务器 3”中完成 Apache 服务自签名证书的部署（5 分）

1.安装和配置 Apache 服务，其网站主目录为/skills/www，主页内容为“This is a reverse proxy!”，通过自签名证书完成该网站的 SSL 访问;

（三）在主机“服务器 3”中完成磁盘管理的部署（5 分）

1.添加四个 10G 磁盘，使用 btrfs 将四个磁盘创建一个 RAID6，并将它挂载到/share/raid6 目录下;

2.使用 btrfs 快照功能，对/share/raid6 创建快照，快照名称为“kuaizhao”（2 分）;

（四）在主机“服务器 3”中完成 firewall 服务器的部署（5 分）

1.配置系统防火墙 firewall,关闭除提供系统服务(22、80、443、25、110、53）以外的端口;

（五）在主机“服务器 4”中完成反向代理服务器的部署（10 分）

“服务器 3”为内网中的一台 WEB 服务器，现想让此 WEB 服务器作为公司的一台外网 WEB 服务器提供门户网站的作用，请您添加一块网卡连接内网的 WEB 服务器，通过“服务器 4”的反向代理功能将其实现。

1.安装 squid 代理服务器，允许所有人访问，外网监听端口为 443;

2.设置 squid 代理服务器采用 ufs 缓存机制，缓存目录设置为/cache,目录容量为 5GB，L1 及 L2 级目录数量分别为 16 及 256，定义高速缓存值为 512MB;

3.指定目标服务器地址为“服务器 3”的 IP 地址，后端端口为 443，别名为 nets，允许最大连接数为 35、权值为 5;

4.当用户请求 https://chinaskills.net 或 https://www3.chinaskills.net 时，转发到别名为 nets 的真实服务器上;

（六）在主机“服务器 5”中完成 HAProxy 服务器的部署（10 分）

1.在此服务器上安装HAProxy服务,配置HAProxy使用frontend、backend实现https代理，开启日志功能;

2.配置 HAProxy 的 frontend 的名称为 https_hap、监听端口为 80 和 443、模式为 http、默认后端为 server_http;

3.配置HAProxy的backend的名称为server_http、模式为http、负载均衡算法为 roundrobin、后端 server 为 www1 和 www2、权重值为 3、引入健康检查、连续 6 次检测结果失败标记为服务器不可用;

4.配置客户端在使用 http 访问时自动跳转到 https;

职业规范与素养

（本部分 20 分）

一、 整理赛位，工具、设备归位，保持赛后整洁有序;

二、 无因选手原因导致设备损坏。