2021年兰州市中等职业学校技能大赛
网络搭建与应用赛项
竞赛规程

一、赛项名称

赛项名称：网络搭建及应用

赛项组别：中职学生组

赛项归属专业:信息技术类

二、竞赛目的

通过竞赛，检验参赛选手的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。引导中职院校关注绿色、安全、智能的计算机网络技术发展趋势和产业应用方向，引导院校、教师、企业产教融合、校企合作，引领中职信息技术类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,提升专业学生能力素质与企业用人标准的吻合度,以适应新一轮科技革命和产业变革及新经济发展,展示职业教育改革成果及广大院校师生良好的精神风貌，扩大职业教育社会影响力，促进在全社会通过职业教育弘扬工匠精神,为在新形势下全面提高信息技术类专业教学质量、扩大就业创业、推进经济转型升级、培育经济发展新动能做出新贡献。

三、竞赛内容

根据行业企业的业务背景进行网络业务需求、技术应用环境和实际的工程应用与业务架构分析，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五个岗位，

竞赛内容即岗位工作主要内容。

（一）竞赛主要内容

主要分为三部分：

1.网络组建：利用本届赛项执委会提供的计算机、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。

（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比赛试题，读懂实际的项目文档，理解实际项目的应用与业务架构。

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，实现设备的正常运行。

3. 参赛学生能够根据业务需求和实际的应用环境，实现安装配置服务器操作系统，调试服务器、数据库和存储，并根据网络业务需求配置各种策略，以达到网络互联互通，网络服务适应业务需求。

4. 参赛学生能够根据网络实际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. 大赛设计与国际接轨，在竞赛前即会发布竞赛设备、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，技能水平迅速提高；在实际竞赛中，基于已经发布的网络环境，选手可对竞赛试题中具体的技术问题借助设备技术文档进行设计和解决，通过开放的形式可以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，最终可以充分考察学生整体运用知识的能力。

（三）比赛时间

本赛项为团体赛项目，竞赛时间 3 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	完成设备连接，保证和测试物理连通性
2		IP 地址划分实施	完成子网划分、IP 规划实施
3		网络调试	完成指定的交换路由、广域网和无线的配置
4		硬件防火墙配置	完成企业网的相关策略配置
5		网络配置优化	完成网络优化配置,交换虚拟化配置
6		设备安全技术	通过网络设备配置安全防护
7	系统配置管理 50%	操作系统安装(Windows/Linux)	完成操作系统的安装和配置
8		配置常用服务(Windows/Linux)	能够熟练安装配置各类应用服务、系统管理和数据库安装调试 在服务器、数据库、网络部署完成后,安装部署真实的移动 web 应用,可达到最终访问;掌握虚拟化技术，使用服务器集群技术

9		云平台部署	掌握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
10		操作系统安全技术	掌握操作系统方面安全技术配置

附：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 GB50312-2007）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	VLAN、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 等
4		路由基本配置	静态、RIP、OSPF、BGP 等路由协议、NTP、DHCP、TELNET、策略路由等
5		无线配置	设置、分配、接入、开通等
6		广域网配置	PPP、NAT、NAPT 等
7	服务器配置与管理	操作系统安装(Windows/Linux)	能够熟练安装操作系统，并能对操作系统进行安全配置和应用管理
8		配置常用服务(Windows/Linux)	能够根据企业的应用需求，熟练安装和配置 AD、DNS、WEB、FTP、E-MAIL、DHCP、代理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；使用服务器集群技术来实现网络的负载均衡
9		云平台部署	在云平台配置资源模板、创建网络、创建卷、利用平台内置系统生成实例，使运行后实例可以接入网络工作
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
11	网络安全与网络优化	防火墙	能够在企业网络中部署防火墙，使用防火墙规则保护内网服务安全，在防火墙上实现路由、NAT 转换、防 DDOS 攻击；实现包过滤、URL 过滤、P2P 流量控制等
12		网络优化	利用 ACL、QOS、交换机虚拟化等配置，实现网络优化

13		VPN 技术	利用 VPN 实现远程安全接入和站点到站点的 IPSEC VPN 等
14		无线网络	配置无线网络 WEP 加密、MAC 认证接入控制等；配置二层漫游、三层漫游、无线桥接（点对点）、负载均衡、无线桥接（点对多点），信道自动调整等

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，须为同校二、三年级在籍学生，其中队长 1 名，可配 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

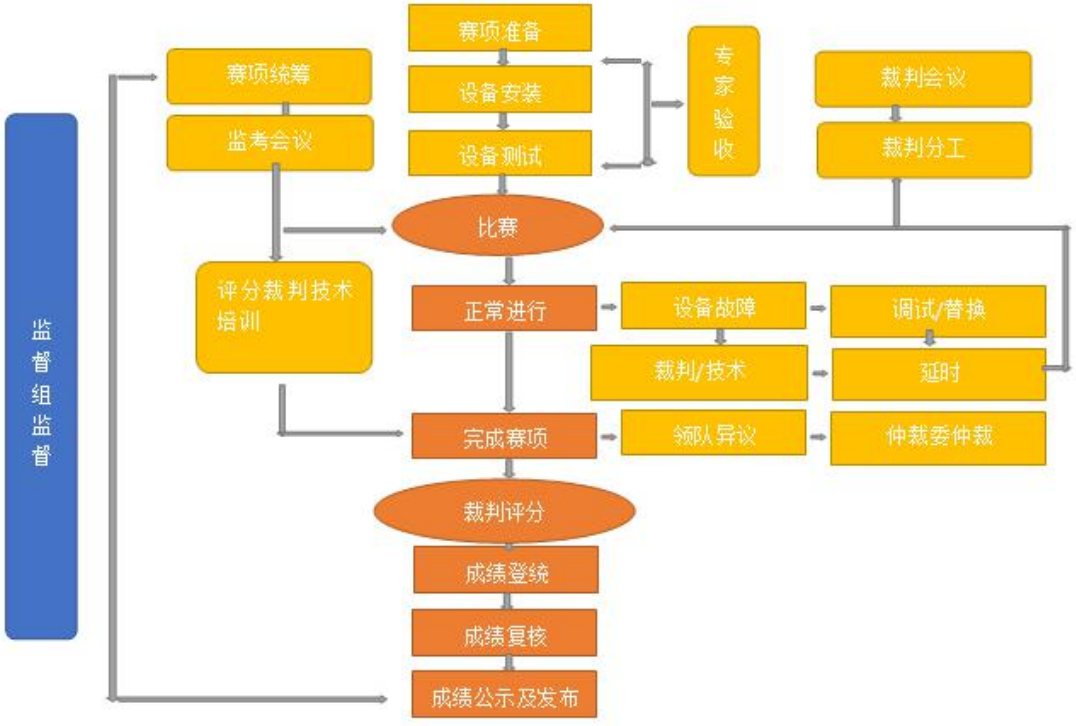
（二）日程安排

竞赛时间 3 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
	13:00-14:30	领队会	各参赛队领队、裁判长	会议室
	15:00-16:00	参观赛场	各参赛队领队	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	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，裁判员宣读竞赛须知	参赛选手、现场裁判、裁判长、监督	竞赛场地
	08:30-11:30	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	参赛选手、裁判、仲裁、监督、专家组、指导教师、领队	承办校安排
	12:30	回酒店	参赛选手、指导教师、领队	住宿酒店
	12:30-评判完毕	评判（含晚餐、夜宵）	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，成绩公示	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 闭赛式	领导、嘉宾、裁判组、各参赛队、专家组、监督组	礼堂

（三）比赛流程



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，配置网络设备、安装调试操作系统，配置安全策略等，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。

六、竞赛试题

（一）赛项执委会下设的专家工作组负责本赛项命题工作。

七、竞赛规则

按照《全国职业院校技能大赛制度汇编》中的相关制度执行。

（一）选手报名

1.每校选手不超过 6 队，每支参赛队由 2 名同一院校 2020 年二、三年级在籍学生组成，并从中指定队长 1 名。年龄不超过 21 周岁，不得跨校组队。

2.每个参赛队可配指导教师 2 名，每个参赛院校指派领队 1 名。指导教师须为本校专兼职教师。

3.已获得省赛一、二、三等奖的选手不得参加本次竞赛。

（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。选手必须佩带参赛证提前 30 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 10 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《大赛规则》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予以解决，故障中断时间不计时；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。

八、竞赛环境

（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。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 6 支参赛队的竞赛场地。竞赛工位标明工位号，并配备竞赛平台和技术工作要求的软、硬件，配有与比赛要求一致的布线线缆及相应水晶头。环境标准要求保证赛场采光(大于 500lux)、照明和通风良好；每支参赛队提供一个垃圾箱。

（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。

（三）其他区域

可设置观摩区、成果展示区、体验区，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	GB50311-2007	综合布线系统工程设计规范
2	GB50312-2007	综合布线系统工程验收规范
3	GB50174-2008	电子信息系统机房设计规范
4	GB21671-2008	基于以太网技术的局域网系统验收测评规范
5	GB/T22239-2008	信息系统安全等级保护基本要求

（三）职业技术标准

达到并超过中级计算机网络技术人员（国家职业资格四级)），接近高级计算机网络技术人员（国家职业资格三级)。

十、技术平台

（一）硬件平台

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
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，>=四核心四线程 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 Microsoft 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 7(中文版)，服务器版主要采用 Windows 2008 Server(中文版)、Windows 2012 Server(中文版)；Linux 系统平台主要采用 Centos 6.5 服务器版本；办公软件的版本为 Microsoft Office（中文版)。

具体软件参数如下所示：

1. 微软 Windows 7/10(64 位中文版) 试用版；
2. Centos 6.5（64 位)；
3. Centos 7.0（64 位）
4. WINRAR 5.21(中文版) 试用版；
5. 微软 Microsoft Office（中文版） 试用版；
6. 微软 Windows Server 2008 R2(中文版) 试用版；

7. 微软 Windows Server 2012 R2(中文版) 试用版；

8. VMware workstation 12 免费版；

9. SecureCRT；

10. Apache Tomcat 7.0.27；

11.JDK（Java Development Kit）1.7 及以上；

12.谷歌浏览器(Google Chrome)官方正式版。

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、团队协作与沟通、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
3	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
4	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
5	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
6	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
7	硬件防火墙配置	完成企业网的相关策略配置，满分为 5 分
8	网络配置优化	完成网络优化配置，满分为 10 分
9	VPN 技术	完成 VPN 配置，满分为 4 分
10	无线网络安全技术	完成无线网络安全配置，满分为 1 分
11	操作系统安全技术 系统	掌握操作系统方面安全技术配置，满分为 10 分

（三）具体评分方法

1. 参赛队成绩由裁判组统一评定，裁判完成评判规定模块全部参赛队评分，保证评判公平。

2. 在监督人员监督下，每组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。

3. 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。

4. 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。

5. 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。

6. 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示。

7. 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.命题期间，对所有命题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。在竞赛一次加密前30分钟，由竞赛执委会工作人员收缴裁判所有通信设备，直至竞赛成绩发布后再归还裁判。

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。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。

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。

（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）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执委会，同时采取措施避免事态扩大。赛项执委会应立即启动预案予以解决并报告赛区执委会。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。

（七）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。

十四、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《全国职业院校技能大赛奖惩办法》给予警告、取消比赛成绩、通报批评等处理。

（二）带队教师须知

1.带队教师应按时参加赛前会议，不得无故缺席。

2.带队教师负责组织本校参赛队参加项赛事活动。

3.参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，须由带队教师

向赛项仲裁组提交书面申诉材料。各参赛队带队教师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。

（三）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。

（四）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，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。

（五）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。

十五、申诉与仲裁

按照《全国职业院校技能大赛制度汇编》中的相关制度执行。

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。

2020 年全国职业院校技能大赛中职组
“网络搭建与应用”赛项省赛竞赛样题
（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络配置项目

第二部分：系统配置与管理项目

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）本试卷共有两个部分。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。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为最终结果。

（5）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。

（6）禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）与比赛相关的工具软件放置在D:\soft文件夹中。

项目简介：

某集团公司建立了总公司，后建立了分公司一、分公司二。总公司设有研发、人事、财务、市场等4个部门，统一进行IP及业务资源的规划和分配，网络采用OSPF和RIP等路由协议。

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，集团决定采购云服务实训平台并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，以及增强业务部署弹性的目的。

集团总公司及分公司的网络拓扑结构如下图所示。

其中云服务实训平台编号为CS，用于各类服务架设；一台S4600交换机编号为SWC，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，作为总公司的核心交换机；一台DCFW-1800编号为FWA,作为总公司的内网防火墙;另一台DCFW-1800编号为FWB,作为分公司二网防火墙；一台DCR-2600路由器编号为RTB，作为分公司一路由器；另一台DCR-2600路由器编号为RTA；一台DCWS-6028作为分公司一机构的有线无线智能一体化控制器，编号为AC，通过与WL8200-I2高性能企业级AP配合实现分公司无线覆盖。

拓补结构图

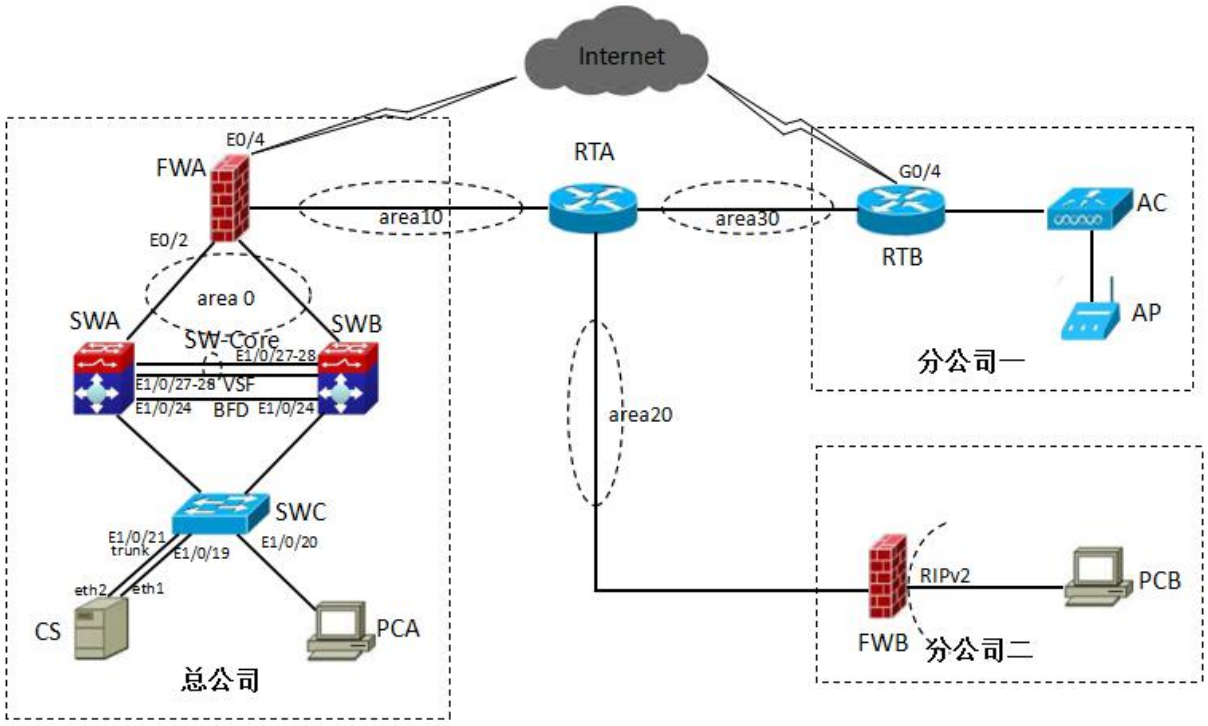

Internet
E0/4
FWA
E0/2
area10
RTA
area30
G0/4
RTB
AC
AP
分公司一
area 0
SWA
SW-Core
SWB
E1/0/27-28
E1/0/27-28 VSF
E1/0/24
BFD
E1/0/24
area20
SWC
E1/0/21
trunk
E1/0/19
E1/0/20
eth2
eth1
CS
PCA
总公司
RIPv2
PCB
FWB
分公司二

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
RTA	G0/3	FWA	E0/1
RTA	G0/4	FWB	E0/1
RTA	S0/1	RTB	S0/2
SWA	E1/0/28	SWB	E1/0/28
SWA	E1/0/27	SWB	E1/0/27
SWA	E1/0/24	SWB	E1/0/24
SWA	E1/0/23	SWC	E1/0/23
SWB	E1/0/23	SWC	E1/0/24
SWA	E1/0/22	FWA	E0/2
SWB	E1/0/22	FWA	E0/3
RTB	G0/3	AC	E1/0/20
RTB	G0/4	FWA	E0/4
AC	E1/0/1	AP	
SWC	E1/0/19	CS	eth1
SWC	E1/0/21	CS	eth2
SWC	E1/0/20	PCA	NIC
FWB	E0/2	PCB	NIC

表 2：网络地址规划表：

设备	设备名称	设备接口	IP 地址	备注
路由器	RTA	G0/3	206.210.18.6/28	
		G0/4	215.160.185.33/30	
		S0/1	214.16.187.45/30	
		L0	1.1.1.1/32	
	RTB	G0/3	10.10.2.1/26	
		G0/4	202.101.13.2/28	
		S0/2	214.16.187.46/30	
		L0	2.2.2.2/32	
防火墙	FWA	E0/1	206.210.18.5/28	
		E0/2	192.168.101.6/30	
		E0/3	192.168.101.2/30	
		E0/4	202.101.13.1/28	
		L1	3.3.3.3/32	
	FWB	E0/1	215.160.185.34/30	
		E0/2	10.10.10.1/24	
		L1	4.4.4.4/32	
无线控制	AC	Vlan130	10.10.2.2/26	20 端口所在 VLAN

器		Vlan110	10.10.2.65/26	5-10 端口所在 VLAN
		Vlan120	10.10.2.129/26	11-15 端口所在 VLAN
		Vlan200	10.10.2.193/26	
三层交换机	SW-Core	Vlan100	192.168.100.1/24	
		Vlan101	192.168.101.5/30	E1/0/22 端口所在 VLAN
		Vlan102	192.168.101.1/30	E2/0//22 端口所在 VLAN
		Vlan10	192.168.10.1/24	研发部
		Vlan20	192.168.20.1/24	人事部
		Vlan30	192.168.30.1/24	财务部
		Vlan40	192.168.40.1/24	市场部
		Vlan1	172.16.10.1/24	
二层交换机	SWC	Vlan10		1-4 端口所在 VLAN
		Vlan20		5-8 端口所在 VLAN
		Vlan30		9-12 端口所在 VLAN
		Vlan40		13-18 端口所在 VLAN
		Vlan100		19-20 端口所在 VLAN
		Vlan1	172.16.10.2/24	
云服务实训平台	CS	eth1	192.168.100.100/24	已设置
	PCA		192.168.100.101/24	
	PCB		10.10.10.2/24	

表 3：服务器 IP 地址分配表：

虚拟机名称	域名信息	服务角色	系统及 版本信息	IPv4 地址信息(由云平台提供)
Win2012-A1	dc.2018skills.com.	域控制器 域名服务器 分布式文件系统服务器	Windows Server 2012 R2	范围: 192.168.10.100 /24 至 192.168.10.200/24
Win2012-A2	sdc.win.2018skills.com.	域控制器 CA 证书服务器 域名服务器 分布式文件系统服务器	Windows Server 2012 R2	
Centos-A3	dns.lin.2018skills.com.	域名服务器	Centos 6.5	
Centos-A4	www.lin.2018skills.com.	网站服务器	Centos 6.5	
Win2012-B1	iis.win.2018skills.com.	网站服务器	Windows Server 2012 R2	范围: 192.168.20.100 /24 至 192.168.20.200/24
Win2008-B2	ftp.win.2018skills.com.	文件传输服务器 磁盘阵列	Windows Server 2008 R2	
Win2012-B3	jdk.2018skills.com.	Tomcat 服务器 集群服务器	Windows Server 2012 R2	
Win2012-B4	cs.2018skills.com.	磁盘阵列 集群服务器	Windows Server 2012 R2	
Centos-C1	ftp.lin.2018skills.com.	文件传输服务器	Centos 6.5	范围: 192.168.30.100 /24 至 192.168.30.200/24

网络搭建及安全部署项目

（500 分）

【说明】

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

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

保存文档方式分为两种：

- 交换机、路由器、AC 要把 show running-config 的配置保存在 PCA 桌面的相应文档中，文档命名规则为：设备名称.docx，例如：RTA 路由器文件命　名为：RTA.docx，然后放入到 PCA 桌面上“比赛文档_X”文件夹中；
- 交换机、路由器、AC 除收集 show running-config 的配置外，还需收集其他命令一同保存在相关设备的“设备名称.docx”文档中，每个设备收集的 命令有所差异，详见表 4：设备收集命令表；

表 4：设备收集命令表

设备名称	收集命令
SWC	show ip int brief show vlan
SW-Core	show ip int brief show vsfconfig show vsf show mad config show vlan show port-group detail

	show ip route show ip route ospf show route map
RTA	show ip int brief show ip route show ip route ospf
RTB	show ip int brief show queueing priority show ip route show route-map
AC	show ip int brief show wireless show wireless ap status

- 防火墙设备的截图方式：把截图放到同一 word 文档中，文档命名规则为：设备名称.docx，例如：防火墙 FWA 文件命名为：FWA.docx，保存后放入到 PCA 桌面上“比赛文档_X”文件夹中；

一、线缆制作与基础配置

1.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，制作网络线缆，根据题目要求，插入相应设备的相关端口；

2.根据网络拓扑要求及网络地址规划表，对网络设备进行地址设置。

3.对每个三层网络设备互联端口进行描述，例如对 RTA 与 RTB 连接的 RTA 的端口描述为：“RTA to RTB”+RTB 端口号。

二、交换机配置

4.总公司两台三层交换机通过 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 1，每个 vsf port-group 绑定两个千兆光端口，VSF 逻辑域为 5，SWA 的成员编号为 1，SWB 的成员编号为 2，正常情况下 SW-1 负责管理整个 VSF，采用 BFD MAD 分裂检测，使能 VSF 自动合并功能采用 BFD MAD 分裂检测，SWA BFD MAD IP 地址为：192.168.101.253/30，SWB BFD MAD 接口 IP 地址为：

192.168.101.254/30，使能 VSF 自动合并功能；

5.根据“表 5:vlan 信息表”所示,在每个交换机上创建相应的 VLAN,并将交换机的相应端口加入对应的 VLAN;

表 5：vlan 信息表

设备	VLAN 编号	VLAN 名称	端口	说明
SWC	VLAN10	YFB	E1/0/1 至 E1/0/4	研发部
	VLAN20	RSB	E1/0/5 至 E1/0/8	人事部
	VLAN30	CWB	E1/0/9 至 E1/0/12	财务部
	VLAN40	SCB	E1/0/13 至 E1/0/18	市场部
	VLAN100	FWQ	E1/0/19、E1/0/20	服务器连接
	VLAN1			管理
SW-Core	VLAN1000		E1/0/24、E2/0/24	BFD MAD
	VLAN10	YFB		研发部
	VLAN20	RSB		人事部
	VLAN30	CWB		财务部
	VLAN40	SCB		市场部
	VLAN100	FWQ		服务器连接
	VLAN1			管理

6.根据网络拓扑图及 IP 地址规划表所示，根据网络地址规划表对所有网络设备使用的环回接口、VLAN 接口进行 IP 地址配置；

7.交换机互联接口和云服务实训平台连接端口开通“Trunk”;

8.SW-Core、SWC 上配置 telnet 服务,telnet 登录密码为 ds2018,enable 登录密码为 mn2018，要求设置为明文；

9.总公司的 VLAN 40 网段内用户通过 SW-Core 上的 DHCP 获得 IP 地址， DHCP 地址池名字为 SC40，租期为 7 天，配置默认网关为 192.168.40.254，排除地址为 192.168.40.1-10 和 250-254，其中 192.168.40.200 保留给 0050.0ea0.bcd1 机器使用；

10.在交换机 SW-Core 上配置 MSTP 防止二层环路;创建 instance30,关联 VLAN10、VLAN30、VLAN20、VLAN40，以 SW-Core 为根。

三、路由器配置与调试

11.路由器开启远程登录功能，RTA,RTB 上配置 telnet 管理功能，其中 RTA 只允许 192.168.100.0/24 的主机对路由器进行管理，RTB 只允许 10.10.10.0/24 网段的主机对路由器进行管理，同时要求每台路由器只允许 3 个线路管理网络设备，用户分别为 user1、user2、user3，口令都为 ds2018，所有设备的特权口令均为 jnds2018；

12.分公司一的 vlan110 和 vlan120 网段用户通过 RTB 上的 DHCP 来获取 IP 地址，DHCP 地址池名字分别为 SC110、SC120，租期为 7 天，其中 SC110 配置默认网关为 10.10.2.65/26,地址池范围为 10.10.2.70-120/26；SC120 配置默认网关为 10.10.2.129/26,地址池范围为 10.10.2.130-180/26；

13.为了保障专用线路的链路安全，在 RA 与 RB 之间连接的链路上配置 PPP 协议，采用双向先 PAP 后 chap 的验证方式，用户名分别为 RA 和 RB，验证口令都为 54321；

14.SW-Core 与 FWA、FWA 与 RTA、RTA 与 FWB、RTA 与 RTB 之间使用 OSPF 路由协议，分公司二使用 RIP 路由协议，分公司一使用静态路由协议，防火墙开启相关策略，确保公司内部之间互联互通；

15.为保障路由协议安全，在路由更新时采用基于接口的 MD5 认证，其口令为“ZZMOP”；打开 SW-Core 记录 OSPF 邻居状态变化日志功能；

16.分公司二规划使用 RIP 协议，版本为 RIPv2；FWB 上设置路由重发布，将 RIPv2 路由信息发布到 OSPF 路由协议时，设置其类型为 E1，其开销为 80；将 OSPF 路由信息发布到 RIPv2 路由协议时，设置其开销为 3；

17.分公司一网络采用了静态路由协议；RTB 上设置路由重发布，将静态路由信息发布到 OSPF 路由协议时，设置其类型为 E1，其开销为 50。

四、广域网配置

18.FWA 上配置 NAT，要求总公司内网的 VLAN20、VLAN30、VLAN40 用户均可经地址转换后而访问公网，使用的地址池为 202.101.13.1-4/28，要求用户只能在工作日的上班时间（周一至周五 9:00-17:00）访问互联网；

19.分公司一内网用户使用相应设备外部接口的 IP 地址访问公网，并且要求只允许网络用户周一至周四 8:00-17:00 才能访问互联网；分公司二通过总公司访问公网；

20. 在 FWA 和 FWB 上配置 L2TP 远程接入 VPN，允许远程办公用户 10.10.20.10-20/26 可以访问内网资源,其使用的合法用户名为 name1、name2、name3，其共同口令为 vp2018；

21.为了提高网络可靠性，使用互联网作为业务数据传输的备份链路。考虑到安全性，FWA 与 RB 之间使用 IPSec VPN 技术对数据进行加密。VPN 传输需要采用隧道模式，预共享密码为 180224，IKE 阶段 1 采用 DH 组 1、DES 和 MD5 加密方式，IKE 阶段 2 采用 ESP-DES。

五、无线配置

22.分公司一的 vlan110 和 vlan120 网段内网用户，分别通过 RTB 上的 DHCP 设置中的地址池 SC110、SC120 获取 IP 地址；

23.分公司一内网使用无线方式搭建网络，通过无线交换机和瘦 AP 来实现,创建两个无线信号,WS 配置 VLAN200 为 AP 管理 VLAN,VLAN110、120 为业务 VLAN，需要排除相关地址；WS 使用管理 VLAN 最后一个地址作为管理地址，采用序列号认证，SSID 分别为“DCFI”+组号和“DSSE”+组号，“DCFI”对应于 VLAN110，用户接入无线网络时需要采用基于 WPA2 加密方式，其口令为“dswx2018”；“DSSE”对应于 VLAN120，用户接入无线网络时不需要认证；开启所有无线用户的二层隔离，设定

每个无线用户的限速为 2Mb/S；为 AP 配置管理地址及路由。

六、安全策略配置

24.防火墙内网接口开启 telnet、ssh 和 http 的管理功能；25.分公司一 RTB 实施 QoS 策略，使得 VLAN110 的服务器能够得到高优先级的带宽使用优先权，VLAN120 配置成低优先级；

26.总公司 FWB 上配置安全策略，只允许 VLAN 20 用户才可以访问 PCB 服务器的 TCP3389 端口；

27.总公司 FWA 上配置安全策略，VLAN30 用户每天只允许在 8:00-17:00 时间段才可以访问 PCB 服务器的 FTP 服务（TCP21 端口）和 WEB 服务（TCP80 端口）；

28.总公司 FWB 上配置安全策略，只允许 PCA 可以去 ping 通 PCB，反之拒绝；

29.开启 FWA、FWB 的 SNMP 服务，配置只读共同体为“SMGL”，配置读写共同体为“SMRWGL”；

30.监测 PCA 的网络入流量，连接的交换机接口镜像到以太口 22。

服务器配置及应用项目

（500 分）

【说 明】

（1）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其他信息如“表 6：镜像信息表”所示；

表 6：镜像信息表

名称	硬盘	VCPU	用户名	密码	ssh	rdp
win7	30G	1	admin	Qwer1234	否	是
win2008	40G	1	administrator	Qwer1234	否	是
win2012	40G	1	administrator	Qwer1234	否	是
centos6.5-desktop	30G	1	root	dcncloud	是	是
centos6.5-mini	30G	1	root	dcncloud	是	是

Centos7-mini	30G	1	root	000000	是	否

（2）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，centos6.5 可以通过 CRT 软件连接进行操作，centos6.5-desktop 也可以通过远程桌面连接进行操作，所有 linux 主机都默认开启了 ssh 功能。

（3）虚拟主机按照“服务器 IP 地址分配表”的要求分配网络，同时虚拟主机使用云服务实训平台获取的 IP 地址。

（4）云服务实训平台中生成的 Windows 系统 SID 相同，根据实际需求做相应设置,注意重置 SID 的虚拟主机密码必须改回为“Qwer1234”，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。

（5）云服务实训平台中生成的 Linux 系统提供镜像文件，可用来配置 yum 源，镜像文件存储于/opt 目录下。

（6）在 PCA 桌面，选手自己建立 BACKUP_X（X 为工位号）文件夹，在该文件夹中建立 windows 和 linux 两个文件夹，将竞赛题目要求的截图和文档内容分别以.jpg 和.docx 格式,按系统分别存储于 windows 和 linux 文件夹中，文件名和存放位置错误，涉及到的所有操作分值记为 0 分。

（7）在云服务实训平台中保留竞赛生成的所有虚拟主机，同时要求虚拟机系统重新启动后，所有服务均能正常启动和使用，否则扣除该服务功能一半分数。

云实训平台安装与运用

一、在云实训平台上完成如下操作

（一）完成云平台基础设置

在浏览器中使用 http://192.168.100.100/dashboard 地址登录云服务实训平台进行设置，用户名 admin，密码 dncloud 要求如下：

1.如“表 7：云平台网络信息表”要求创建三个外部网络，详细操作过程请参照“云服务实训平台用户操作手册 v1.0”中第 4 节；

表 7：云平台网络信息表

网络名称	所属 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	192.168.10.0/24	192.168.10.1	是	192.168.10.100-192.168.10.200
vlan20	20	是	vlan20-subnet	192.168.20.0/24	192.168.20.1	是	192.168.20.100-192.168.20.200
vlan30	30	是	vlan30-subnet	192.168.30.0/24	192.168.30.1	是	192.168.30.100-192.168.30.200

2.设置 10 块卷，卷命名为 hd1~hd10，其中 hd1~hd5、hd8、hd10 大小为 4G，hd6、hd7、hd9 大小为 2G；选择项目→计算→卷→创建卷。

（二）完成虚拟主机的创建

3.如“表 8：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 v1.0”中第 6.1 节。

表 8：虚拟主机信息表

虚拟主机名称（Instance Name）	镜像模板(源)	云主机类型(flavor)	网络(与表 7 关联)	备注
Win2012-A1	win2012	window-large	vlan10	

Win2012-A2	win2012	window-large	vlan10	
Win2012-B1	win2012	window-large	vlan20	
Win2008-B2	win2008	window-small	vlan20	连接卷 hd1、hd2、hd3
Win2012-B3	win2012	window-large	vlan20	
Win2012-B4	win2012	window-large	vlan20	连接卷 hd4、hd5
Centos-A3	centos6.5-desktop	linux-small	vlan10	
Centos-A4	centos6.5-desktop	linux-small	vlan10	
Centos-C1	centos6.5-mini	linux-small	vlan30	简版界面
Centos-C2	centos6.5-desktop	linux-small	vlan30	
Centos-C3	centos6.5-desktop	linux-small	vlan30	连接卷 hd6、hd7、hd8
Centos-C4	centos6.5-desktop	linux-small	vlan30	连接卷 hd9、hd10

Windows 操作系统

一、在 win2012-A1 上完成如下操作：

（一）完成主域控制器服务器的部署

1.将其升级为 2018skills.com 的主域控制器，其完全域名为 dc.2018skills.com;

2.按照“表 9：域用户和组信息表”所示，创建域用户、域用户组等;

表 9：域用户和组信息表

域用户名	密码	登陆时间	域用户组	组作用域	组类型
adm1	2018skills.com	周一至周五 8 点至 17 点	adm	全局	安全组
adm2	2018skills.com	周一至周五 8 点至 17 点			
sale1	2018skills.com	周一至周五 8 点至 17 点	sale	全局	通讯组
sale2	2018skills.com	周一至周五 8 点至 17 点			
sys1	2018skills.com	周一至周六 8 点至 20 点	sys	本地域	安全组
sys2	2018skills.com	周一至周六 8 点至 20 点			

3.设置所有域用户账户策略，密码长度至少 3 位，最长使用期限 60 天，密码最短使用 0 天，账户锁定阈值 7 次，账户锁定时间 30 分钟，复位账户锁定计数器 30 分钟，将设置截图保存为 1-1-1.jpg;

4.创建组织单元，名称为：研发部，该组织单元包含 sys 组、adm1 用户、Win2012-A1 电脑和 Win2012-A2 电脑；设置该组织单元组策略，命名为“研发部 GPO”，要求关闭 windows 自动更新，并禁止修改 IE 浏览器的主页,将设置截图保存为 1-1-2.jpg。

（二）完成域名服务器的部署

5.将此服务器配置为主 DNS 服务器，正确配置 2018skills.com 域名的正向及反向解析区域，按照“表 10：域名信息表 1”创建对应服务器主机记录，并关闭网络掩码排序功能。设置 DNS 服务正向区域和反向区域与活动目录集成，启用 Active Directory 的回收站功能；

表 10：域名信息表 1

虚拟机名称	完全限定域名
Win2012-A1	dc.2018skills.com.
Win2012-B3	jdk.2018skills.com.
Win2012-B4	cs.2018skills.com.
Centos-C2	mail.2018skills.com.

（三）完成分布式文件系统服务器部署

6.配置 DFS 服务，与 sdc.win.2018skills.com 做文件夹同步，在 C 盘创建文件夹 dfs-root 作为复制对象，复制组为 dfs-backup，在每天 0 点复制,将设置截图保存为 1-3-1.jpg。

二、在 win2012-A2 上完成如下操作：

（一）子域控制器服务器的部署

7.升级为子域控制器，域名为 win.2018skills.com，其完全域名为 sdc.win.2018skills.com。

（二）完成 CA 证书服务器的部署

8.安装证书服务，设置为企业根，有效期为 5 年，为企业内部自动回复证书申请，将证书服务安装配置过程的主要步骤，截图保存在名字为 2-2-1.docx 的文档中。

（三）完成域名服务器的部署

9.配置 DNS 服务，正确配置 win.2018skills.com 域名的正向及反向解析区域，如“表 11：域名信息表 2”创建对应服务器主机记录，将创建好的记录截图为 2-3-1.jpg。

表 11：域名信息表 2

虚拟机名称	完全限定域名
Win2012-A2	sdc.win.2018skills.com
Win2012-B1	iis.win.2018skills.com
	web.win.2018skills.com
	www.win.2018skills.com
	sec.win.2018skills.com
Win2008-B2	ftp.win.2018skills.com
	ftp1.win.2018skills.com

（四）完成分布式文件系统服务器部署

10.配置 DFS 服务，与 dc.2018skills.com 做文件夹同步，在 C 盘创建文件夹 dfs-root 作为复制对象，复制组为 dfs-backup，在每天 0 点复制。

三、在 win2012-B1 上完成如下操作：

（一）完成网站服务器部署

11.将此服务器加入 win.2018skills.com 域，其完全域名为 iis.win.2018skills.com;

12.创建 web.win.2018skills.com 站点，主目录为 C:\web_root，默认文档：index.htm，主页显示内容为“热烈庆祝 2018 年职业技能竞赛开幕”,同时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，将设置截图为 3-1-1，并将网页测试截图为 3-1-2.jpg；

13.创建 www.win.2018skills.com 站点，主目录为 C:\www_root，默认文档：auto.htm，主页显示内容为“传承技术技能、促进就业创业”；设置该网站虚拟目录为 vdir，虚拟目录内容为“劳动光荣，技能宝贵”；访问端口为 1080，编辑匿名用户身份验证凭据：用户名为 webuser，密码为 2018skills.com，将匿名用户设置截图为 3-1-3，并将网页测试截图为 3-1-4.jpg；

14.配置 web 服务器，创建 sec.win.2018skills.com 站点，主目录为 C:\sec_root，默认文档：sec.htm，主页显示内容为“人人皆可成才、人人尽展其才”，通过加密认证方式访问该网站，其中 CA 证书从 win2012-A2 获取，将网页测试截图为 3-1-5.jpg。

四、在 win2008-B2 上完成如下操作：

（一）完成文件传输服务器部署

15.将此服务器加入 win.2018skills.com 域，其完全域名为 ftp.win.2018skills.com;

16.建立 ftp 站点 ftp1.win.2018skills.com，站点主目录为 C:\ftp_root,不允许匿名登录,所有用户只具有读取和写入文件权限，FTP 站点欢迎消息为：“欢迎访问网络搭建 FTP 服务器!”，并且用命令浏览文件时使用 UNIX 方式显示，日志文件记录到 C:\ftp_root\LogFiles 目录下;

17.为 ftp1.win.2018skills.com 设置域用户隔离，在域控制器中创建域用户 ftpuser1 和 ftpuser2，密码为 2018skills.com，设置两个用户主目录分别为网络文件夹 \\ftp_root\ftpuser1 、\\ftp_root\ftpuser2。

（二）完成磁盘阵列部署

18、利用已添加的三块虚拟硬盘 hd1、hd2、hd3 进行设置，完成磁盘阵列 RAID5 并对应盘符为 E,将设置截图保存为 4-2-1.jpg。

五、在 win2012-B3 上完成如下操作：

（一）完成 Tomcat 服务器部署

19.将此服务器加入 2018skills.com 域，其完全限定域名为 jdk.2018skills.com;

20.安装 jdk 和 jre，安装完成后，配置 JAVA 环境变量，配置完成

后，测试 JAVA 运行环境是否已安装成功，将测试 JAVA 运行环境安装成功截图保存为 5-1-1.jpg；

21. 安装 tomcat 服务并启动，在浏览器输入 http://jdk.2018skills:8080，测试结果截图保存为 5-1-2.jpg。

（二）完成故障转移集群服务器部署

22.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 C:\；虚拟磁盘名称分别为 Quorum 和 Files，大小分别为 512M 和 3G，访问服务器为 Win2012-B2,将设置截图保存为 5-2-1.jpg；

六、在 win2012-B4 上完成如下操作：

（一）完成故障转移集群服务器部署

23.将此服务器加入 2018skills.com 域，其完全限定域名为 cs.2018skills.com；

24.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，将添加成功后的界面截图保存为 6-1-1.jpg；

25.使用 iSCSI 发起程序连接 Win2012-B1 的 iSCSI 虚拟磁盘 Quorum 和 Files,实现对 iSCSI 虚拟磁盘 Quorum 和 Files 的存储多路径功能，并对 Quorum 和 Files 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,将设置截图保存为 6-1-2.jpg，6-1-3.jpg；

26.创建故障转移群集，群集名称为：cluster，IP 地址为：192.168.20.21./24，在故障转移群集功能中，添加 Win2012-B3 和 Win2012-B4 服务器，并生成故障转移群集验证报告验证结果，6-1-4.jpg。

（二）完成磁盘阵列部署

27.利用已添加的两块虚拟硬盘 hd4、hd5 进行设置，完成磁盘阵列

RAID1，对应磁盘盘符为 F,将设置截图保存为 6-2-1.jpg。

Linux 操作系统部分

一、在 Centos-A3 上完成如下操作：

（一）完成域名服务器部署

1．在此服务器中配置 yum 源，安装相关服务，实现域名服务器部署，设置开机自动加载服务；

2.配置该服务器为 2018skills.com 的子域名服务器，解析区域为 lin.2018skills.com；按照“表 12：域名信息表 3”完成正反向解析，禁止 192.168.70.0/24 网段的主机访问此 DNS 服务器；利用 nslookup 命令完成验证,正向解析截图为 1-1-1.jpg,反向解析截图为 1-1-2.jpg。

表 12：域名信息表 3

虚拟机名称	完全限定域名
Centos-A3	dns.lin.2018skills.com.
Centos-A4	www.lin.2018skills.com
Centos-C1	ftp.lin.2018skills.com.
Centos-C2	mail.lin.2018skills.com.
Centos-C3	smb.lin.2018skills.com.
Centos-C4	data.lin.2018skills.com。

（二）配置远程登陆服务器

3.在此服务器中安装相关服务，实现远程登陆服务器部署，设置开机自动加载服务，只允许 IP 地址以 192.168 开头的主机使用 telnet 命令远程登录该服务器，将配置内容截图为 1-2-1.jpg；

4.在主机 Centos-C4 上使用 telnet 命令登录本服务器，将成功登陆的内容截图为 1-2-2.jpg。

二、在 Centos-A4 上完成如下操作：

（一）完成网站服务器部属

5.在此服务器中配置 yum 源,安装相关服务,实现网站服务器部署,设置开机自动加载服务；

6.创建网站 http://www.lin.2018skills.com:8080,其网站主目录为/www/8080，主页名为 skills8080.html，首页内容为“Welcome chinaskills’s website: 8080”，被访问端口为 8080，虚拟目录名为 vdir，将网页测试截图为 2-1-1.jpg;

7.创建网站 http://www.lin.2018skills.com，其网站主目录为/www/jnds，主页为 skills.html，首页内容为“Welcome chinaskills’s website”；创建用户 webuser1 和 webuser2，密码同用户名，实现网站的认证访问，只有这两个用户可以通过认证访问 http://www.lin.2018skills.com 网站,将网页测试截图为 2-1-2.jpg，将用户认证配置截图为 2-1-3.jpg;

8.创建网站 https://www.lin.2018skills.com，其网站主目录为/www/ssl，主页名字为 skillsssl.html，首页内容为“Welcome chinaskills’s website: ssl”，使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求实现加密访问，将网页测试截图为 2-1-4.jpg，将申请证书代码截图为 2-1-5.jpg。

三、在 Centos-C1 上完成如下操作：

（一）完成文件传输服务器部署

9.在此服务器中配置 yum 源，安装相关服务，实现文件传输服务器部署，设置开机自动加载服务;

10.创设域名为 ftp.lin.2018skills.com 的站点,，根目录为/var/ftp，最大上线人数为 50 人，同一 IP 来源最大连接数量为 5 人，不允许匿名用户访问，开启 ftp 支持被动数据传输模式;

11.建立虚拟用户 ftpuser1 及 ftpuser2，密码同用户名，用户的宿主目录为/home/vsftpd，用户的权限配置文件目录为/etc/vsftpd_user_conf，实现 ftpuser1 用户具有浏览目录、上传和

下载文件、创建和删除目录的权限，ftpuser2 用户可以下载，但不能上传文件。

（二）完成防火墙服务器部署

12.开启防火墙，并仅允许客户机对本机文件传输服务的访问；

13.禁止本机利用 ping 命令访问主机 Win2012-A1；

14.本机基于默认端口访问网站，均强制转为 Centos-A4 上的 http://web.lin.2018skills.com:8080 网站页面；

15.使用命令将防火墙所有设置保存到/var/iptables 文件中；设置立即生效且开机自启。

四、在 Centos-C2 上完成如下操作：

（一）完成邮件服务器部署

16.在此服务器中配置 yum 源，安装 sendmail 服务，实现邮件服务器部署；

17.该服务器满足 2018skills.com，lin.2018skills.com 两个区域邮件服务；创建两个用户 winmail、linmail；每个用户的邮箱空间为 30MB，显示两个用户邮箱大小截图保存分别为 4-1-1.jpg；限定用户发邮件时，附件最大为 5MB，附件大小截图保存为 4-1-2.jpgh 和 4-1-3.jpg；

18.为 winmail 和 linmail 两员工创建邮箱账户，实现不同用户之间的正常通讯，密码同用户名，邮件服务器的域名后缀分别为 2018skills.com、lin.2018skills.com，邮件服务器要在所有 IP 地址上进行侦听；

19.安装 office outlook 2010 软件发送邮件；创建名称为 everyone 的邮件列表，发给 everyone@2018skills.com 、everyone@lin.2018skills.com 的邮件，所在区域员工均可收到，将配

置截图为 4-1-4.jpg；winmail、linmail 两员工分别利用 winmail@2018skills.com 和 linmail@lin.2018skills.com 实现邮件互发，主题为“你好”，内容为“欢迎大家”,邮件发送成功截图保存为 4-1-5.jpg 和 4-1-6.jpg。

（二）完成 NTP 服务器部署

20.在此服务器上实现网络时间服务(NTP)的配置，使得 CentOS-C2 所在网络中的其它计算机通过此服务器进行网络校时，将服务成功启动截图为 4-2-1.jpg;在 Centos-C3 虚拟机系统上成功校对时间截图为 4-2-2.jpg。

五、在 Centos-C3 上完成如下操作:

（一）完成 samba 服务器部署

21.在此服务器中配置 yum 源，安装相关服务，实现 samba 服务器部署，设置开机自动加载服务;

22.此服务不允许 172.16.0.0/16 网段的电脑访问，并创建四个用户 tom、jerry、jack、man，密码同用户名，其中 tom 和 jerry 属于 administration 组,jerry 和 jack 属于 sales 组;man 用户属于 manager 组;

23. 建立共享目录 /var/administration_share 和 /var/sales_share，administration 组的用户对目录 administration_share 共享有读写权限，sales 组的用户对目录 administration_share 共享有只读权限；sales 组的用户对目录 sales_share 共享有读写权限;manager 用户对所有目录均有读写权限;

24、建立共享目录/var/public_share，共享名为 share，允许匿名用户访问 public_share，具有读取权限。

（二）完成磁盘阵列部署

25.利用已添加的三块虚拟硬盘 hd6、hd7、hd8 进行设置，hd6、hd7 对应硬盘均设置为一个主分区，hd8 对应硬盘设置为两个 2G 大小的逻辑分区，并完成磁盘阵列 RAID10 的操作；

26.将 RAID10 的/dev/md10 分区，分出一个大小为 1G 的空间，格式化为 swap 分区，设为开机生效。

六、在 Centos-C4 上完成如下操作：

（一）完成数据库服务器部署

27.在此服务器中配置 yum 源，安装相关服务，实现数据库服务器部署，开机自启动数据库服务；

28.修改 mysql 的 root 用户的密码为 687145；创建一个名为 myDB 的数据库，在该数据库中创建一个名称为 baseinfo 的表，其结构“表 13：baseinfo 结构表”所示；并自行插入 5 条记录，记录内容需满足表中字段的要求即可，查看表结构并截图为 6-1-1.jpg；

表 13：baseinfo 结构表

Field	Type	Null	Key	Default
studentID	varchar(10)	NO	PRI	NULL
name	varchar(10)	NO		NULL
sex	char(1)	YES		M
birthday	date	YES		NULL
school	char(20)	YES		NULL

29.将表 mytable 中的记录导出，存放到/root/mysql.sql 文件中。

（二）完成磁盘阵列部署

30、利用已添加的两块虚拟硬盘 hd9、hd10 进行设置，hd9 对应硬盘设置为一个主分区，hd10 对应硬盘设置为两个 2G 大小的逻辑分区，并完成磁盘阵列 RAID5 的操作。