全国职业院校技能大赛

赛项规程

赛项名称：网络建设与运维

英文名称：Network Construction and Operational Maintenance

赛项组别：中等职业教育

赛项编号：ZZ016

一、赛项信息

<table>
<tr><td colspan="4">赛项类别</td></tr>
<tr><td colspan="4">☑每年赛　　□隔年赛（□单数年/□双数年）</td></tr>
<tr><td colspan="4">赛项组别</td></tr>
<tr><td colspan="4">☑中等职业教育　□高等职业教育</td></tr>
<tr><td colspan="4">☑学生赛（□个人/☑团体）　□教师赛（试点）　□师生同赛（试点）</td></tr>
<tr><td colspan="4">涉及专业大类、专业类、专业及核心课程</td></tr>
<tr><td>专业大类</td><td>专业类</td><td>专业名称</td><td>核心课程
（对应每个专业，明确涉及的专业核心课程）</td></tr>
<tr><td rowspan="30">71 电子与信息</td><td rowspan="27">7102 计算机类</td><td rowspan="3">710201 计算机应用</td><td>数据库应用与数据分析</td></tr>
<tr><td>程序设计基础</td></tr>
<tr><td>信息技术设备组装与维护</td></tr>
<tr><td rowspan="9">710202 计算机网络技术</td><td>网络设备安装与调试</td></tr>
<tr><td>网络信息安全基础</td></tr>
<tr><td>路由交换技术</td></tr>
<tr><td>服务器配置与管理</td></tr>
<tr><td>综合布线设计与施工</td></tr>
<tr><td>Web 前端开发技术基础</td></tr>
<tr><td>Linux 操作系统应用基础</td></tr>
<tr><td>无线局域网技术</td></tr>
<tr><td rowspan="6">710207 网络信息安全</td><td>网络组建与安全维护</td></tr>
<tr><td>网站建设与安全管理</td></tr>
<tr><td>数据库管理与安全维护</td></tr>
<tr><td>网络安全产品部署与调试</td></tr>
<tr><td>系统安全加固</td></tr>
<tr><td rowspan="3">710208 网络安防系统安装与维护</td><td>综合布线设计与施工</td></tr>
<tr><td>网络服务器安装与配置</td></tr>
<tr><td>网络设备安装与调试</td></tr>
<tr><td rowspan="3">710209 网站建设与管理</td><td>网络服务器安装与配置</td></tr>
<tr><td>网站建设与管理</td></tr>
<tr><td>数据库应用与数据分析</td></tr>
<tr><td rowspan="3">7103 通信类</td><td rowspan="3">710301 现代通信技术应用</td><td>数据通信网络技术</td></tr>
<tr><td>云计算技术及应用</td></tr>
<tr><td>服务器管理与维护</td></tr>
<tr><td rowspan="2">710302 通信系统工程安装与维护</td><td>通信线路施工与维护</td></tr>
<tr><td>数据通信网络组建与维护</td></tr>
</table>

		710303 通信运营服务	信息通信运营管理
对接产业行业、对应岗位（群）及核心能力			
产业行业	岗位（群）	核心能力 （对应每个岗位（群），明确核心能力要求）	
新一代信息技术	计算机网络工程	具备应用计算机网络、操作系统、计算机硬件、程序设计、综合布线、网络信息安全等相关专业知识的能力	
		具备网络规划与设计、网络布线施工、网络设备安装及调试、 服务器配置的能力	
		具备网络工程建设、网络系统集成、网络管理和维护等能力	
		具备网络服务搭建、网站内容设计和管理的能力	
	网络部署与系统集成	具备应用计算机网络、操作系统、计算机硬件、程序设计、综合布线、网络信息安全相关专业知识的能力	
		具备数据库定义、修改、查询和 SQL 数据分析的能力	
		具备网络工程建设、网络系统集成、网络管理和维护等能力	
	计算机网络设备安装与调试	具备应用计算机网络、操作系统、计算机硬件、程序设计、综合布线、网络信息安全相关专业知识的能力	
		具备网络规划与设计、网络布线施工、网络设备安装及调试、 服务器配置的能力	
	网络管理与维护	具备网络规划与设计、网络布线施工、网络设备安装及调试、 服务器配置的能力	
		具备 Web 应用程序设计和网络管理的能力;	
		具备网站搭建和基础安全防护的能力	
		具备常用数据库系统搭建及基础安全防护的能力	
		具备网络安全防护软件和设备部署与配置的能力	
		具备使用工具对网络系统和应用服务进行初步渗透测试的能力	
		具备常见网站、主流互联网及云计算应用平台的基础技术支持与运维能力	
	网络产品服务与营销	具有快速学习新业务和新产品、为客户提供业务和产品技术咨询服务的能力	
		具有应用信息技术、数字技术等的能力	
		具有质量、环保、安全生产的意识和能力	

二、竞赛目标

本竞赛旨在贯彻党中央、国务院对职业教育工作的决策部署，响应党的二十大提出的“加快建设网络强国、数字中国”的国家战略，适应国产自主且安全可控的新诉求和信息技术应用创新产业的发展，通过产教协同发展，培养中职网络建设与运维方向高素质网络技术人才，促进数字化转型升级，服务信息基础建设和国家战略。以立德树人为根本任务，推进“三全育人”、深化“三教改革”，发挥树旗、导航、定标、催化作用，培养德智体美劳全面发展网络技术相关专业的高素质劳动者和技术技能人才。

竞赛内容紧跟网络信息技术产业的发展趋势和国际发展水平，选用源自企业真实项目和工作任务，围绕岗位要求，紧贴生产实际设计竞赛，考察学生综合能力，突出应变能力，强化职业素养，让教学、岗位、竞赛相互协同，提高网络建设与运维相关的核心专业能力，提高人才培养质量。通过竞赛，引导全社会尊重、重视、关心技能人才的培养和成长，营造崇尚技能的氛围，激励青年走技能成才、技能报国之路，培养更多能工巧匠、大国工匠。

三、竞赛内容

（一）竞赛主要内容

本赛项设置网络理论测试、网络建设与调试、服务搭建与运维三个模块，竞赛内容包括：职业规范与素养、网络布线与施工、网络设备配置与调试、安全策略配置、网络安全防护和应急响应、云平台网络连接、X86 与 ARM 架构计算机操作系统安装与管理、Windows 与

Linux 服务配置、网络运维等内容。各模块有机结合，比赛过程中，要求两名参赛选手按照题目独立完成理论测试，合理分工，安排工作流程、合作完成模块二和模块三等有关网络建设与运维职业典型工作任务，检验选手专业核心能力与职业综合能力。

（二）重点考查技能

重点考查参赛选手的网络理论的掌握以及灵活运用的实战能力，具体包括:

1. 能够全面正确理解网络基本知识理论，考查选手的专业可持续发展能力。

2. 能够根据提供的竞赛要求，读懂文档需求，理解业务架构，实现项目应用，检验网络实施规划统筹的综合规划能力。

3. 能够完成线缆制作、合理划分网络地址，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，考核综合布线和设备安装调试专业实践能力。

4. 能够根据业务需求和应用环境，安装部署各类服务器、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，考核多样化环境下系统部署和数据库应用的专业实践能力。

5. 能够预判网络运行中所面临的安全威胁，防范并解决网络恶意攻击行为；考查选手防御不良信息及病毒、构建和维护绿色网络的专业实战能力。

6. 能够通过竞赛前发布的竞赛设备列表、配套技术文档、赛项

规程和公开赛题等信息，分析网络架构、查找技术资料；能够根据临场30%竞赛要求变化，结合技术原理，参考设备技术文档进行现场任务解决，检验了参赛团队整体的文档理解、项目执行、故障解决、网络运维等各项综合专业能力。

模块		主要内容	比赛时长	分值
模块一	网络理论测试	计算机应用、计算机网络技术、网络信息安全、网络安防系统安装与维护、网站建设与管理、现代通信技术应用、通信系统工程安装与维护和通信运营服务各专业基本知识理论 10%	0．5小时	10%
模块二	网络建设与调试	2-1 工程统筹 10% 2-2 交换配置 10% 2-3 路由调试 10% 2-4 无线部署 5% 2-5 安全维护 5%	6.5 小时	40%
模块三	服务搭建与运维	3-1 X86 架构计算机操作系统安装与管理 5% 3-2 ARM 架构计算机操作系统安装与管理 5% 3-3Windows 云服务配置 15% 3-4 Linux 云服务配置 15% 3-5 网络运维 10%		50%

四、竞赛方式

（一）竞赛形式

竞赛采取单场次，线下比赛方式进行。

模块一网络理论测试：两名参赛选手在比赛赛场独自在线进行。

模块二网络建设与调试和模块三服务搭建与运维：两名参赛选手在本队竞赛场地内团队合作开展项目实施，协作完成工程统筹规划、综合布线实施测试、交换机配置、路由器调试、无线设备部署、网络安全防护；X86 架构计算机操作系统安装与管理、ARM 架构计算机操作系统安装与管理、Windows 和 Linux 云服务配置、云主机系统部署、网络运维等，项目实施完毕，需保证施工现场整理整顿整洁，工具归位，整个施工过程需保证无安全事故发生。

（二）组队方式

竞赛以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。

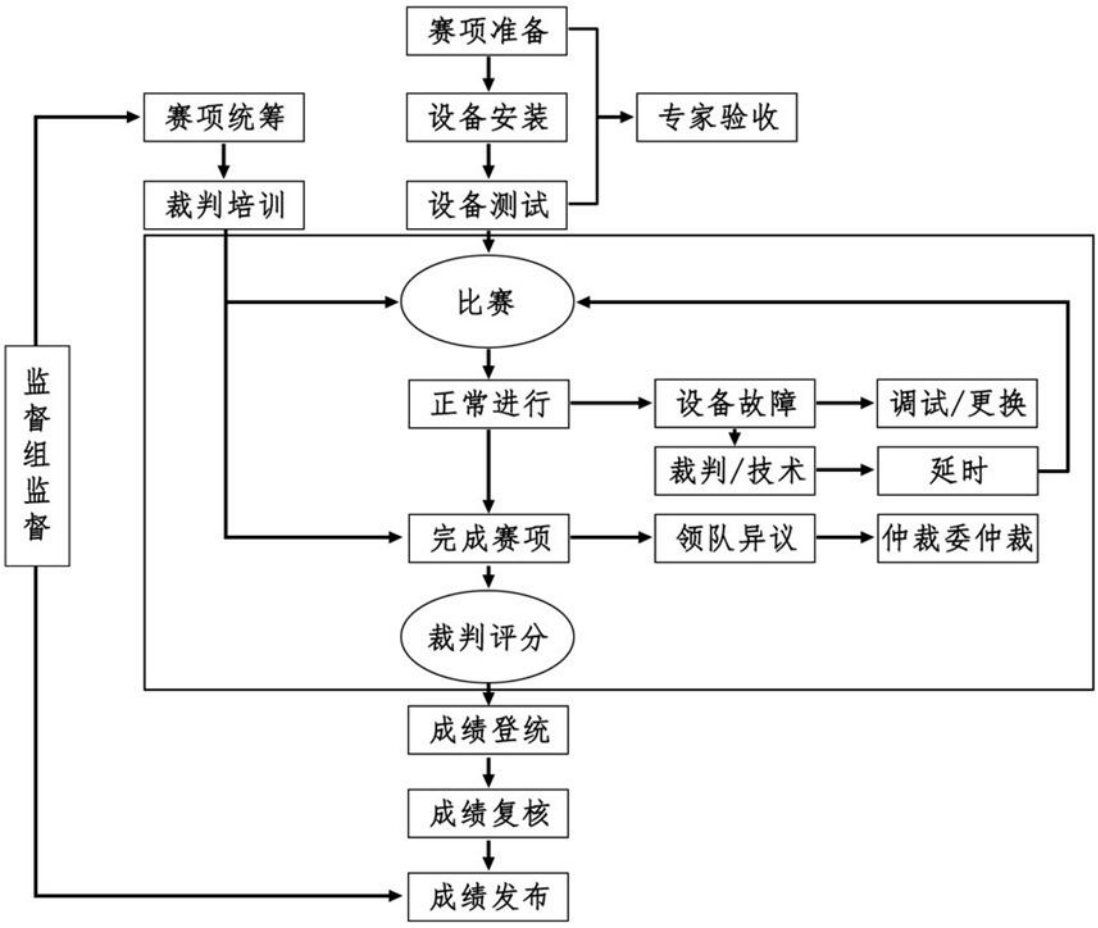
五、竞赛流程

（一）竞赛日程

日期	时间	事项	地点	工作组
比赛日前两天 12 点前		专家、裁判报到	分别入住酒店	承办校
		参赛队报到		
比赛日前一天	09:00-12:00	裁判工作会议	会议室	裁判组
	13:50-14:20	参赛队集体前往开赛式会议室	住宿酒店停车场	承办校
	15:00-15:30	开赛式	开幕式场地	承办校
	15:40-16:10	参观赛场	赛　场	专家组 裁判长 监督仲裁组
	16:10	封闭赛场		
	16:20	参赛队集体乘车回酒店	赛场停车场	承办校
	16:30-17:30	领队会议	会议室	承办校
	17:40	领队乘车回酒店	住宿酒店停车场	承办校
比赛日	6:50-7:20	参赛队集体乘车前往赛场	住宿酒店停车场	承办校
	7:20-7:40	选手签到、排队	赛场外空场	承办校
	07:40-08:20	检录 一次加密 二次加密	检录处加密处	裁判组
	08:20-08:30	裁判员宣读竞赛须知，竞赛选手就位并领取竞赛任务	赛　场	裁判组
	08:30-15:30	正式比赛	赛　场	裁判组
	15:30-21:30	三次加密 评分成绩汇总解密	赛场评分室	裁判组
	22:00-24:00	成绩公示	参赛队酒店大堂	裁判 监督仲裁组
	15:30-17:30	赛项申诉与仲裁	监督仲裁室	监督仲裁组
	15:30-16:00	参赛队集体乘车回酒店	停车场	承办校
比赛日后一天	9:30-9:40	参赛队集体 乘车前往闭赛式场地	住宿酒店停车场	承办校
	10:00-11:30	闭赛式	闭幕式场地	承办校
	11:30-12:00	参赛队集体乘车回酒店	停车场	承办校

日期	时间	事项	地点	工作组
比赛日后两天		竞赛结束安全返程	住宿酒店	承办校

（二）比赛流程



（三）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独自完成网络理论测试，团队配合完成 IP 地址规划、综合布线、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、网络运维等网络建设与运维整体工作项目实施。操作顺序和分工，由参赛队自行商定。

六、竞赛规则

（一）选手报名资格

每参赛队由2名参赛选手组成，须为参赛当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学生可参加比赛。参赛选手不得跨校组队，同一学校报名参赛队不超过1支；凡在往届全国职业院校技能大赛中获一等奖的选手，不能再参加今年同一专业类赛项的比赛。

参赛队可设指导教师，指导教师须为本校专兼职教师，每队限报2名指导教师。

（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。竞赛场上不得以任何方式泄露应该保密信息。选手必须佩带参赛证参赛，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. 参赛队在赛前领取比赛任务并进入竞赛工位，比赛正式开始后方可打开显示器，进行与比赛任务相关的操作。

3. 现场裁判引导参赛选手检查比赛环境，宣读《竞赛须知》。

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，并接受裁判员的指示，如遇问题须举手提问。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，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。比赛结束后，裁判员与参赛队队长要确认已成功提交竞赛要求的配置文件及保存位置，确认后离场。

7. 竞赛所需硬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，离场时，不得将与比赛有关的物品带离现场。

（三）赛事规定

1. 领队代表负责管理选手和指导教师，遵守赛项规程和相关要求，遵守申诉与仲裁程序。

2. 专家、裁判、监督仲裁按制度规定履行职责，严格保密，遵守竞赛规程，切实做到公平公正。

3. 赛事工作人员严格遵守规章制度，按照岗位职责，履职尽责。

七、技术规范

（一）教学标准

中等职业学校电子与信息大类相关专业国家教学标准。

（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）职业技能等级标准

对接“1+X 证书”等国家职业技能等级证书初中高的技能要求。

（四）主要竞赛知识点和技能点

序号	内容模块	子模块	具体内容
1-1	模块一：网络理论测试	理论考核	计算机类网络和通信相关专业和课程的基本知识理论
2-1	模块二：网络建设与调试	综合布线和IP地址划	网络布线、设备连接、端口标识、物理连通性检测、链路检测、端口检测
			VLSM、CIDR 等地址划分并实施网络配置
2-2		交换配置	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
2-3		路由调试	E1 链路捆绑、PPP 或者 HDLC 协议、静态、RIP 、 RIPng 、 OSPF 、 OSPFV3 、 BGP 、 MBGP4+、ISIS 等单播路由协议、PIM、IGMP 等组播协议、NTP、DHCP、TELNET、策略路由、IPV6、NAT、QOS 等
2-4		无线部署	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
2-5		安全维护	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 、 L2TP VPN 或 MPLS_VPN 等

序号	内容模块	子模块	具体内容
3-1	模块三：服务搭建与运维	X86 架构计算机操作系统安装与管理	安装配置开源 ubuntu 等桌面系统；安装 remmina 远程连接虚拟主机并配置相应服务；Linux 环境下开启虚拟化安装 Windows 服务，并导出系统配置结果
3-2		ARM 架构计算机操作系统安装与管理	安装配置国产开源麒麟系统；安装配置 minicom，连接并调试网络设备，并导出设备配置文件
3-3		Windows 云服务配置	能根据企业需求，在云平台创建实例规格、创建网络、创建卷、创建虚拟机等; 能根据任务要求，根据企业的应用需求，熟练安装和配置 AD、组策略、DNS、WEB、ASP、E-MAIL、DHCP、DFS、NTP、NIS、KDC、MariaDB、Apache、Nginx、NFS、Samba、Tomcat、CA 证书、iSCSI、文件共享、NLB、故障转移、多路径、BitLocker、打印服务、PowerShell 脚本、Linux Shell 脚本、python3 脚本、Redis、mysql、mariadb、mongodb、postgresql、数据库备份、PXE、WDS、ftp、FTPd、VPN、ansible、apache2、tomcat、mail、samba、nfs、haproxy、keepalived 、pacemaker、zabbix、ceph、etcd、openldap、docker、podman、kubernetes、containerd、redis、RAID、磁盘加密、WordPress、UFW 等开展系统服务和数据库配置、群集管理、Docker、podman、containerd、mysql、etcd、ceph、zabbix、mongodb、openstack 等应用; 能够完成开发环境搭建、操作系统系统更新、Linux 系统内核升级和故障排除
3-4		Linux 云服务配置	
3-5		网络运维	虚拟仿真主流操作系统、主流网络和安全设备实现互联互通，服务器搭建模拟，网络安全模拟演练等实现网络排错、电子取证、应急响应等技能

八、技术环境

（一）技术平台

竞赛场地每赛位需配备“网络及云服务设备”技术平台一套

序号	设备名称	数量	备注
1	路由器 (含路由线缆)	2	厂家提供
2	三层交换机 （需含虚拟化连接套件）	3	厂家提供
3	多核防火墙 （需含特征库升级许可）	2	厂家提供
4	无线控制器	1	厂家提供
5	无线接入点	1	厂家提供
6	云实训平台	1	厂家提供
7	ARM 架构服务器 CPU：主频>=2.6GHZ, >=三十二核 内存>=64G 硬盘>=1TB	1	厂家提供
8	POE 模块	1	厂家提供
9	ARM PC 机 1 台 CPU：主频>=2.3GHZ, >=八核 内存>=8G 硬盘>=256G nvme 支持硬件虚拟化 显示器：23.8 寸及以上 USB 键盘鼠标 X86 PC 机 1 台 CPU：主频>=3.5GHZ, >=八核心十六线程 内存>=16G 硬盘>=1T nvme UEFI 启动 支持硬件虚拟化 显示器：23.8 寸及以上 USB 键盘鼠标	2	承办校提供
10	网络设备机柜 （需包括开放机柜，配套配线架、布线管槽、底盒和模	1	厂家提供

序号	设备名称	数量	备注
	块）		
11	网络布线工具箱 （综合布线常用工具，含压线钳，打线钳，测线仪，美工刀等）	1	厂家提供

（二）技术环境

1. 理论题在线测试技术环境

理论在线测试平台满足自动组卷，现场评分功能。

序号	设备名称	数量	备注
1	服务器 CPU>=六核十二线程 内存>=16GB 硬盘>=300GB 网卡>=1Gb 以太网	2	承办校提供
2	PC 机 学生终端能连接局域网	每参赛队 2 台	承办校提供

2. 免费开源软件清单

Windows 系统平台由服务器版和桌面版组成，桌面版采用 kylin 和 ubuntu(英文版)，服务器版主要采用 Windows Server 2022(中文版)和 Rocky9。

每赛位具体软件参数如下所示:

序号	软件参数	备注
1	Ubuntu23 英文版	承办校电脑自带
2	Kylin 桌面版	赛场提供
3	Rocky9	云实训平台镜像
4	Windows Server 2022 中文数据中心版	云实训平台镜像
5	linux 服务配置需要的 deb 和 rpm 软件包	赛场提供
6	理论在线测试软件	厂家提供

九、竞赛样题

见附件 1

十、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。

（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。

2. 与地方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。

（三）比赛环境

1. 承办单位赛前须按照执委会要求排除安全隐患。

2. 裁判员要严防选手出现具有危险性的操作。

3. 承办单位制定安全制度和应急预案，并配备急救人员与设施。

4. 易燃易爆以及各类危险品严格禁止进入比赛场地。

5. 大赛现场需对赛场进行网络安全控制。

6. 制定人员疏导方案。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. 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）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。

十一、成绩评定

（一）评分标准

本赛项模块一网络理论测试：两名参赛选手独自完成，竞赛结果取两名参赛选手平均成绩计为参赛队该部分成绩。模块二网络建设与调试和模块三服务搭建与运维：两名参赛选手合作开展项目实施，模块任务评价标准中记分方式为千分制保留一位小数，竞赛结果取项目实施总成绩。三项模块总和核算为百分制，保留两位小数，为最终竞赛成绩。

序号	分类	评分细则与知识点、技能点	比例	评分方式
模块一	类型一	网络理论测试	10%	机考评分
1-1	单选题	考查学生对应网络建设与运维方面专业课程的基本知识、基本技能和基本素养		
1-2	判断题			
模块二	类型二	网络建设与调试	40%	机评为主
2-1	工程统筹	1. IP 地址规划正确 2. 整理赛位，工具、设备归位，保持赛后整洁有序 3. 无因选手原因导致设备损坏 4. 恢复调试现场，保证网络和系统安全运行 5. 综合布线符合工程标准，保证线路通畅	10%	结果评分
2-2	交换配置	能根据任务要求，正确完成交换机配置，并测试成功	10%	机考评分
2-3	路由调试	能根据任务要求，正确完成路由配置，并测试成功	10%	机考评分
2-4	无线部署	能根据任务要求，正确完成无线配置，并测试成功	5%	机考评分

2-5	安全维护	能根据任务要求，正确配置设备安全技术，并测试成功	5%	机考评分
模块三	类型三	服务搭建与运维	50%	机考评分
3-1	X86 计算机操作系统安装与管理	安装配置开源 ubuntu 等桌面系统；安装 remmina 远程连接虚拟主机并配置相应服务；Linux 环境下开启虚拟化安装 Windows 服务，并导出系统配置结果	5%	机考评分
3-2	ARM 计算机操作系统安装与管理	安装配置国产开源麒麟系统; 安装配置 minicom，连接并调试网络设备，并导出设备配置文件	5%	机考评分
3-3	Windows 云服务配置	能根据任务要求，正确在云平台创建虚拟机等; 能根据任务要求，正确根据企业的应用需求，熟练安装和配置各种系统服务，进行数据库、群集、Docker 等部署，并能测试成功; 能够正确完成开发环境搭建、操作系统更新、Linux 系统内核升级和常见故障排除	15%	机考评分
3-4	Linux 云服务配置		15%	机考评分
3-5	网络运维	能够通过虚拟仿真的主流操作系统、主流网络和安全设备完成网络排错、电子取证、应急响应等	10%	机考评分

（二）评分方式

1. 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知识能力水平:

（1）网络搭建与安全部署、系统配置与应用的正确性、规范性和合理性。

（2）网络理论的理解性。

（3）团队风貌、职业素养、协作与沟通、组织与管理能力。

2. 具体评分方法

（1）参赛队成绩评定采用结果评分。模块一为机考评分、模块二中“2-1 工程统筹”为人工客观评判由五名评分裁判依据评分标准独立评分取均值，其余模块由专家组决定为人工或系统客观评分。

（2）裁判组遵照大赛执委会要求成立，需要安排具备中高级职称（高级职业资格证书/技能等级）熟悉网络或操作系统技术的裁判 44 名，包括裁判长、现场裁判、评分裁判、加密裁判。

序号	专业技术方向	知识能力要求	执裁、教学、工作经历	专业技术职称（职业资格等级）	人数
1	网络技术方向（裁判长）	全面掌握网络布线、网络调试、操作系统和虚拟化方面知识和技能	省级以上执裁和组织执裁经验 具有领导能力，组织协调能力 5 年以上相关专业教学经验或相关行业工作经验	专业相关高级职称（高级职业资格证书/技能等级）	1
2	网络调试	能熟练应用网络知识理论题，完成网络布线和网络设备的安装调试工作	省级以上执裁经验 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）	20
3	操作系统	能熟练应用网络知识理论题，完成 Windows/Linux 服务器网络系统部署方面工作	省级以上执裁经验 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）	20
4	理工类专业（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	无，有责任心，与参赛队无利益关系	中级以上职称	3
裁判总人数		44			

（3）整体评分工作中模块一网络理论题在线测试提交赛卷后，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；第二模块 2-5 和第三模块竞赛环节可采取系统评判或人工核对，成绩

采用分步得分、累计总分的积分方式，按照网络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；三部分分数合计为参赛队总分。

（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，监督仲裁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%。监督仲裁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布。成绩公示 2 小时内无异议，在闭赛式上予以宣布。

（7）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。

（8）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、技术点的掌握程度，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。

（9）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仲裁组人员和裁判长签字后装袋密封留档，赛项承办院校封存，委派专人妥善保管。

十二、奖项设置

（一）选手奖励

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)。本赛项按照获奖比例设置奖项，评分为百分制保留 2 位小数，极小概率产生成绩并列。如因成绩并列而突破获奖比例，按流程逐级报大赛执委会办公室批准。

（二）优秀指导教师奖励

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、赛项预案

（一）竞赛过程出现非选手原因设备掉电、故障等意外时，裁判需及时确认情况，安排技术人员处理，登记详细情况，填写补时登记表，报裁判长批准后，可安排延长补足比赛时间。

（二）预留 5%以上备用机位和充足备用 PC 及外部设备，出现非选手原因故障时，经现场裁判和裁判长确认，予以及时更换。

（三）模块一为网络理论题在线测试，从题库按照题目难易程度和技术方向抽取部分赛题组成统一赛卷，题目顺序随机排列，采用主备双服务器保障比赛顺利。如遇个体意外，可以延时更换测试电脑继续比赛；如遇大面积意外，可以中止比赛，重新抽取赛题开始比赛。模块二和三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情况不会影响其它赛位正常比赛，不会由此对成绩产生影响。

（四）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。

（五）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、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时完成赛项评价工作。

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各自参赛队参加各项赛事活动。

8. 参赛队领队应积极做好各自参赛队的服务工作，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

赛项监督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. 参赛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. 参赛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，如果违规行为：诸如打开显示器、制作线缆等任何操作，经裁判警告后仍无效，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，经裁判警告后仍无效，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，致使操作无法继续的，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. 竞赛结束，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。

十五、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，可向赛项监督仲裁组提出申诉。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小时之内向监督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。

赛项监督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。

十六、竞赛观摩

本赛项提供公开观摩区进行线下公开观摩，同时提供赛场外全程直播。

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。

十七、竞赛直播

本赛项除抽签加密外，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。

十八、赛项成果

（一）赛项成果转化清单

成果名称	成果形式	主要内容	方法途径	目标数量	完成时间
竞赛规程和公开赛题	大赛网公开	赛项技术文件	办赛过程中产生	1 套	开赛前
专家点评和技术分析报告	音频、视频、文本	赛项技术文件	比赛结果分析	1 套	赛后 1 个月内

优秀选手和指导教师访谈	10分钟左右的获奖代表队（选手）的风采展示片	体会，宣传推广	访谈	1 套	赛后 1 个月内
宣传报道	报刊，媒体	宣传推广	采访	1 套	比赛同步
风采展示宣传片	15分钟赛项宣传片	宣传推广	全程录制 后期剪辑	1 套	赛后 1 个月内
赛课融通教材	教材	赛题讲解	赛题解读	1 本	教材
在线课程资源	视频	赛题讲解	视频整理	各种讲解视频	赛后

（二）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/图像素材等形式数字化资源等。

（三）资源成果展现

赛项资源转化成果的开放共享。

（四）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。

附件 1

全国职业院校技能大赛
网络建设与运维

样题

赛题说明

一、竞赛项目简介

“网络建设与运维”竞赛共分 A. 网络理论测试（从公布赛题模块一中随机抽取选择题 70 道，判断题 30 道）；B. 网络建设与调试；C. 服务搭建与运维等三个模块。竞赛时间安排和分值权重见表 1

表 1 竞赛时间安排与分值权

模块		比赛时长	分值
模块一	网络理论测试	0.5 小时	10%
模块二	网络建设与调试	6.5 小时	40%
模块三	服务搭建与运维		50%
合计		7 小时	100%

二、竞赛注意事项

1. 竞赛期间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竞赛环境，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. 在进行任何操作之前，请阅读每个部分的所有任务。各任务之间可能存在一定关联。

4. 操作过程中需要及时按照答题要求保存相关结果。竞赛结束后，所有设备保持运行状态，评判以最后提交的成果为最终依据。

5. 竞赛完成后，竞赛设备、软件和赛题请保留在座位上，禁止将竞赛所用的所有物品（包括试卷等）带离赛场。

6. 禁止在提交资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

模块一：网络理论测试

一、单选题

1. 下面哪个路由协议是外部网关路由协议？（ ）

A. 直连路由协议　　B. 静态路由协议

C. OSPF 路由协议　　D. BGP 协议

2. 在 Linux 中，下列哪个不是主流的电子邮件服务器软件（ ）。

A. Sendmail 服务器　　B. Postfix 服务器

C. Qmail 服务器　　D. Pop3 服务器

3. 网络管理希望能够有效利用 192.168.176.0/25 网段的 IP 地址现公司市场部门有 20 个主机,则最好分配下面哪个地址段给市场部。（ ）

A. 192.168.176.0/25　　B. 192.168.176.160/27

C. 192.168.176.48/29　　D. 192.168.176.96/27

4. STP 交换机缺省的优先级为( )。

A. 0　　B. 1　　C. 32767　　D. 32768

5. telnet 远程管理时数据的源端口号和目的端口号可能为( )。

A. 1025,21　　B. 1024,23　　C. 23,1025　　D. 211022,0

二、判断题

1. 云平台中可以直接删除原有卷。（ ）

2. 使用 traceroute 命令可以检验目标网路是否在路由表中。( )

3. 在短时间内同时产生大量的请求消息冲击某 Web 服务器,无法正常响应其他合法用户的请求,这属于 DDoS 攻击。（ ）

4. 通过发送包含不同 TTL 的 ICMP 报文并监听回应报文,来探测到达目的计算机的路径的命令是 ping。（ ）

5. 建筑物综合布线系统中的园区子系统是指连接各个建筑物的通信系统。（ ）

模块二：网络建设与调试

任务描述:

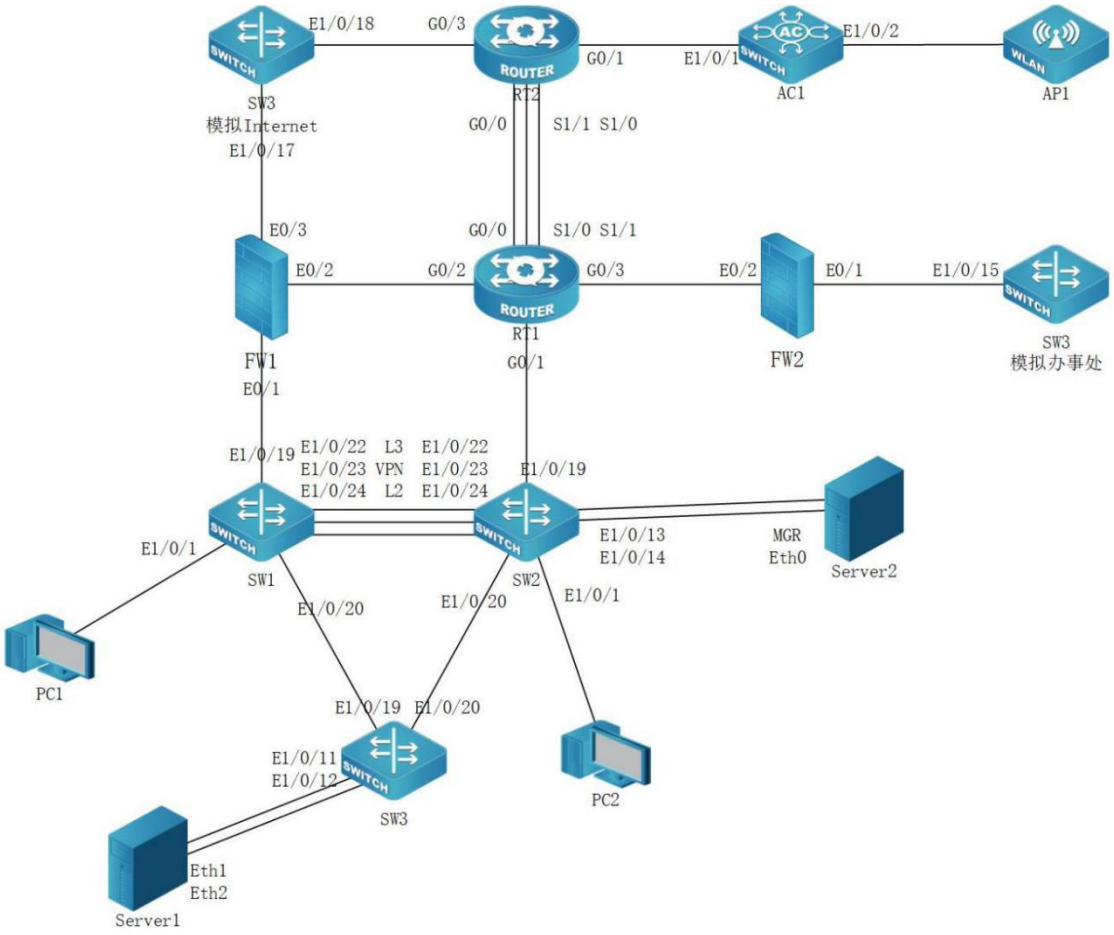
某集团公司原在北京建立了总公司，后在成都建立了分公司，又在广东设立了办事处。集团设有产品、营销、法务、财务、人力 5 个部门，统一进行 IP 及业务资源的规划和分配，全网采用 OSPF、RIP、ISIS、BGP 路由协议进行互联互通。

2023 年随着企业数字化转型工作进一步推进，为持续优化运营创新，充分激活数据要素潜能，为社会创造更多价值，集团决定在北京建立两个数据中心，在贵州建立异地灾备数据中心，以达到快速、可靠交换数据，增强业务部署弹性的目的，完成向两地三中心整体战略架构演进，更好的服务于公司客户。

集团、分公司及办事处的网络结构详见拓扑图。编号为 SW1 的设备作为集团北京 1#DC 核心交换机，编号为 SW2 的设备作为集团北京 2#DC 核心交换机；编号为 SW3 的设备作为贵州 DC 核心交换机；编号 FW1 的设备作为集团互联网出口防火墙；编号为 FW2 的设备作为办事处防火墙；编号为 RT1 的设备作为集团核心路由器；编号为 RT2 的设备作为分公司路由器；编号为 AC1 的设备作为分公司的有线无线智能一体化控制器，通过与 AP1 配合实现所属区域无线覆盖。

网络拓扑图及 IP 地址表:

1. 网络拓扑图



2. 网络设备 IP 地址分配表

设备名称	设备接口	IP 地址
SW1	loopback1 ospfv2 ospfv3 bgp	10.13.1.1/32 2001:10:13:1::1/128
	loopback2	10.13.1.2/32 2001:10:13:1::2/128
	vlan10	10.13.11.1/24 2001:10:13:11::1/64
	vlan20	10.13.12.1/24 2001:10:13:12::1/64
	vlan30	10.13.13.1/24 2001:10:13:13::1/64
	vlan40	10.13.14.1/24 2001:10:13:14::1/64
	vlan50	10.13.15.1/24 2001:10:13:15::1/64
	vlan1019	10.13.255.14/30
	vlan1020	10.13.255.5/30

设备名称	设备接口	IP 地址
	vlan1022	10.13.255.1/30
	vlan1023 vpn	10.13.255.1/30
SW2	loopback1 ospfv2 ospfv3 bgp	10.13.2.1/32 2001:10:13:2::1/128
	loopback2	10.13.2.2/32 2001:10:13:2::2/128
	vlan10	10.13.21.1/24 2001:10:13:21::1/64
	vlan20	10.13.22.1/24 2001:10:13:22::1/64
	vlan30	10.13.23.1/24 2001:10:13:23::1/64
	vlan40	10.13.24.1/24 2001:10:13:24::1/64
	vlan50	10.13.25.1/24 2001:10:13:25::1/64
	vlan1019	10.13.255.22/30
	vlan1020	10.13.255.9/30
	vlan1022	10.13.255.2/30
	vlan1023 vpn	10.13.255.2/30
SW3	loopback1 ospfv2 ospfv3 bgp	10.13.3.1/32 2001:10:13:3::1/128
	vlan10	10.13.31.1/24 2001:10:13:31::1/64
	vlan20	10.13.32.1/24 2001:10:13:32::1/64
	vlan30	10.13.33.1/24 2001:10:13:33::1/64
	vlan50	10.13.35.1/24 2001:10:13:35::1/64
	vlan1019	10.13.255.6/30
	vlan1020	10.13.255.10/30
W3 模拟办事处	loopback2	10.13.3.2/32 2001:10:13:3::2/128
	vlan110	10.13.110.1/24 2001:10:13:110::1/64
	vlan120	10.13.120.1/24 2001:10:13:120::1/64

设备名称	设备接口	IP 地址
	vlan1015	10.13.255.46/30
SW3 模拟 Internet	loopback3	200.200.3.3/32 2001:200:200:3::3/128
	vlan1017	200.200.200.1/30
	vlan1018	200.200.200.5/30
AC1	loopback1 ospfv2 ospfv3	10.13.4.1/32 2001:10:13:4::1/128
	loopback2 rip ripng	10.13.4.2/32 2001:10:13:4::2/128
	loopback3	10.13.4.3/32 2001:10:13:4::3/128
	vlan1001	10.13.255.42/30
	vlan130 无线管理	10.13.130.1/24 2001:10:13:130::1/64
	vlan140 无线 2.4G 产品	10.13.140.1/24 2001:10:13:140::1/64
	vlan150 无线 5G 营销	10.13.150.1/24 2001:10:13:150::1/64
RT1	loopback1 ospfv2 ospfv3 bgp mpls	10.13.5.1/32 2001:10:13:5::1/128
	loopback2 rip ripng	10.13.5.2/32 2001:10:13:5::2/128
	loopback3 isis	10.13.5.3/32 2001:10:13:5::3/128
	loopback4 集团与办事处互联	10.13.5.4/32 2001:10:13:5::4/128
	loopback5 vpn 财务	10.13.5.5/32 2001:10:13:5::5/128
	g0/0	10.13.255.29/30
	g0/1	10.13.255.21/30
	g0/2	10.13.255.18/30
	g0/3	10.13.255.25/30
	s1/0	10.13.255.33/30
	s1/1	10.13.255.37/30
RT2	loopback1 ospfv2 ospfv3 bgp mpls	10.13.6.1/32 2001:10:13:6::1/128

设备名称	设备接口	IP 地址
	loopback2 rip ripng	10.13.6.2/32 2001:10:13:6::2/128
	loopback3 isis	10.13.6.3/32 2001:10:13:6::3/128
	loopback4 ipsecvpn	10.13.6.4/32 2001:10:13:6::4/128
	tunnel4 ipsecvpn	10.13.255.50/30
	loopback5 vpn 财务	10.13.6.5/32 2001:10:13:6::5/128
	g0/0	10.13.255.30/30
	g0/1	10.13.255.41/30
	g0/3	200.200.200.6/30
	s1/0	10.13.255.38/30
	s1/1	10.13.255.34/30
FW1	loopback1 ospfv2 ospfv3 trust	10.13.7.1/32 2001:10:13:7::1/128
	loopback2 rip ripng trust	10.13.7.2/32 2001:10:13:7::2/128
	loopback4 ipsecvpn trust	10.13.7.4/32 2001:10:13:7::4/128
	tunnel4 ipsecvpn VPNHUB	10.13.255.49/30
	e0/1 trust	10.13.255.13/30
	e0/2 trust	10.13.255.17/30
	e0/3 untrust	200.200.200.2/30
FW2	loopback1 ospfv2 ospfv3 trust	10.13.8.1/32 2001:10:13:8::1/128
	e0/1 trust	10.13.255.45/30
	e0/2 dmz	10.13.255.26/30

一、 工程统筹

1. 职业素养

(1)整理赛位，工具、设备归位，保持赛后整洁有序。

(2)无因选手原因导致设备损坏。

(3)恢复调试现场，保证网络和系统安全运行。

2. 网络布线

左侧布线面板立面示意图

右侧布线面板立面示意图

(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:

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	2	06

(4)铺设线缆并端接。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。将 2 根双绞线的一端，端接在配线架相应端口，另一端端接上 RJ45 模块，并且安装上信息点面板，并标注标签。

(5)跳线制作与测试。截取 2 根当长度的双绞线，端接水晶头，所有网络跳线要求按 568B 标准制作，两端制作标签，连接网络信息点和相应计算机。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，插入相应设备的相关端口上，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）。

3．IP 规划

为了不断壮大集团业务经营范围，集团计划在上海成立办事处。通过调研，计划在上海办事处设立与 Internet 连接的 4 个业务部门，每个业务部门的最大所需主机数如下表所示，要求从 10.13.10.100/19 主机地址所在网络第一个网段开始进行 IP 地址规划，IP 地址按照下表依次往后顺延规划，网关地址取每个网段最后一个可用地址，请完成下表 IP 地址规划。

部门名称	最大主机数	网络地址 （表示形式 X.X.X.X/N）	网关地址 （表示形式 X.X.X.X）
营销	110		
产品	600		
法务	126		
财务	14		

二、交换配置

1．配置 vlan，SW1、SW2、SW3、AC1 的二层链路只允许相应 vlan 通过。

设备	vlan 编号	端口	说明
SW1	vlan10	E1/0/1	产品 1 段
	vlan20	E1/0/2	营销 1 段
	vlan30	E1/0/3	法务 1 段
	vlan40	E1/0/4	财务 1 段
	vlan50	E1/0/5	人力 1 段
SW2	vlan10	E1/0/1	产品 2 段
	vlan20	E1/0/2	营销 2 段
	vlan30	E1/0/3	法务 2 段
	vlan40	E1/0/4	财务 2 段

设备	vlan 编号	端口	说明
	vlan50	E1/0/5	人力 2 段
SW3	vlan10	E1/0/1	产品 3 段
	vlan20	E1/0/2	营销 3 段
	vlan30	E1/0/3	法务 3 段
	vlan50	E1/0/5	人力 3 段

2. SW1 和 SW2 之间利用三条裸光缆实现互通，其中一条裸光缆承载三层 IP 业务、一条裸光缆承载 VPN 业务、一条裸光缆承载二层业务。用相关技术分别实现财务 1 段、财务 2 段业务路由表与其它业务路由表隔离，财务业务 VPN 实例名称为 Finance。承载二层业务的只有一条裸光缆通道，配置相关技术，方便后续链路扩容与冗余备份，编号为 1，用 LACP 协议，SW1 为 active，SW2 为 passive；采用源、目的 IP 进行实现流量负载分担。

3. SW3 针对每个业务 VLAN 的第一个接口配置 Loopback 命令，模拟接口 UP，方便后续业务验证与测试。

4. 将 SW3 模拟为 Internet 交换机，实现与集团其它业务路由表隔离，Internet 路由表 VPN 实例名称为 Internet。将 SW3 模拟办事处交换机，实现与集团其它业务路由表隔离，办事处路由表 VPN 实例名称为 Office。

5. SW1 法务物理接口限制收、发数据占用的带宽分别为 100Mbps、90Mbps，禁止采用访问控制列表，只允许 IP 主机位为 20-30 的数据包进行转发；禁止配置访问控制列表，实现端口间二层流量无法互通，组名称 FW。

6. 配置 SW1 相关特性实现报文上送设备 CPU 的前端整体上对攻击报文进行拦截，开启日志记录功能，采样周期 10s 一次，恢复周

期为 120s，从而保障 CPU 稳定运行。

7. 对 SW1 与 FW1 互连流量镜像到 SW1 E1/0/1，会话列表为 1。

三、路由调试

1. 配置接口 ipv4 地址和 ipv6 地址，互联接口 ipv6 地址用本地链路地址。

2. SW2 配置 DHCPv4 和 DHCPv6，分别为总公司产品 1 段、总公司产品 2 段、分公司 Vlan130、分公司 Vlan140 和分公司 Vlan150 分配地址。IPv4 地址池名称分别为 Poolv4-Vlan11、Poolv4-Vlan21、Poolv4-Vlan130、Poolv4-Vlan140、Poolv4-Vlan150，排除网关，DNS 为 10.13.210.101 和 10.13.220.101 。 IPv6 地址池名称分别为 Poolv6-Vlan11、Poolv6-Vlan21、Poolv6-Vlan130、Poolv6-Vlan140、Poolv6-Vlan150，IPv6 地址池用网络前缀表示,排除网关，DNS 为 2400:3200::1。PC1 保留地址 10.13.11.9 和 2001:10:13:11::9，PC2 保留地址 10.13.21.9 和 2001:10:13:21::9，AP1 保留地址 10.13.130.9 和 2001:10:13:130::9。SW1、AC1 中继地址为 SW2 Loopback1 地址，SW1 启用 DHCPv4 和 DHCPv6 snooping，如果 E1/0/1 连接 dhcpv4 服务器，则关闭该端口，恢复时间为 10 分钟。

3. SW1、SW2、SW3、RT1 以太链路、RT2 以太链路、FW1、FW2、AC1 之间运行 OSPFv2 和 OSPFv3 协议（路由模式发布网络用接口地址，BGP 协议除外）。

(1)SW1、SW2、SW3、RT1、RT2、FW1 之间 OSPFv2 和 OSPFv3 协议，进程 1，区域 0，分别发布 loopback1 地址路由和产品路由，FW1 通告 type1 默认路由。

(2)RT2 与 AC1 之间运行 OSPFv2 协议，进程 1，nssa no-summary 区域 1; AC1 发布 loopback1 地址路由、产品和营销路由，用 prefix-list

重发布 loopback3。

(3)RT2 与 AC1 之间运行 OSPFv3 协议，进程 1，stub no-summary 区域 1；AC1 发布 loopback1 地址路由、产品和营销。

(4)SW3 模拟办事处产品和营销接口配置为 loopback，模拟接口 up。SW3 模拟办事处与 FW2 之间运行 OSPFv2 协议，进程 2，区域 2，SW3 模拟办事处发布 loopback2、产品和营销。SW3 模拟办事处配置 ipv6 默认路由；FW2 分别配置到 SW3 模拟办事处 loopback2、产品和营销的 ipv6 明细静态路由，FW2 重发布静态路由到 OSPFv3 协议。

(5)RT1、FW2 之间 OSPFv2 和 OSPFv3 协议，进程 2，区域 2；RT1 发布 loopback4 路由，向该区域通告 type1 默认路由；FW2 发布 loopback1 路由，FW2 禁止学习到集团和分公司的所有路由。RT1 用 prefix-list 匹配 FW2 loopback1 路由、SW3 模拟办事处 loopback2 和产品路由、RT1 与 FW2 直连 ipv4 路由，将这些路由重发布到区域 0。

(6)修改 ospf cost 为 100，实现 SW1 分别与 RT2、FW2 之间 ipv4 和 ipv6 互访流量优先通过 SW1_SW2_RT1 链路转发，SW2 访问 Internet ipv4 和 ipv6 流量优先通过 SW2_SW1_FW1 链路转发。

4. RT1 串行链路、RT2 串行链路、FW1、AC1 之间分别运行 RIP 和 RIPng 协议，FW1、RT1、RT2 的 RIP 和 RIPng 发布 loopback2 地址路由，AC1 RIP 发布 loopback2 地址路由，AC1 RIPng 采用 route-map 匹配 prefix-list 重发布 loopback2 地址路由。RT1 配置 offset 值为 3 的路由策略，实现 RT1-S1/0_RT2-S1/1 为主链路，RT1-S1/1_RT2-S1/0 为备份链路，ipv4 的 ACL 名称为 AclRIP，ipv6 的 ACL 名称为 AclRIPng。RT1 的 S1/0 与 RT2 的 S1/1 之间采用 chap 双向认证，用户名为对端设备名称，密码为 Key-1122。

5. RT1 以太链路、RT2 以太链路之间运行 ISIS 协议，进程 1，

分别实现 loopback3 之间 ipv4 互通和 ipv6 互通。RT1、RT2 的 NET 分别为 10.0000.0000.0001.00、10.0000.0000.0002.00，路由器类型是 Level-2，接口网络类型为点到点。配置域 md5 认证和接口 md5 认证，密码均为 Key-1122。

6. RT2 配置 ipv4 nat，实现 AC1 ipv4 产品用 RT2 外网接口 ipv4 地址访问 Internet。RT2 配置 nat64，实现 AC1 ipv6 产品用 RT2 外网接口 ipv4 地址访问 Internet，ipv4 地址转 ipv6 地址前缀为 64:ff9b::/96。

7. SW1、SW2、SW3、RT1、RT2 之间运行 BGP 协议，SW1、SW2、RT1 AS 号 65001、RT2 AS 号 65002、SW3 AS 号 65003。

(1)SW1、SW2、SW3、RT1、RT2 之间通过 loopback1 建立 ipv4 和 ipv6 BGP 邻居。SW1 和 SW2 之间财务通过 loopback2 建立 ipv4 BGP 邻居，SW1 和 SW2 的 loopback2 互通采用静态路由。

(2)SW1、SW2、SW3、RT2 分别只发布营销、法务、财务、人力等 ipv4 和 ipv6 路由；RT1 发布办事处营销 ipv4 和 ipv6 路由到 BGP。

(3)SW3 营销分别与 SW1 和 SW2 营销 ipv4 和 ipv6 互访优先在 SW3_SW1 链路转发; SW3 法务及人力分别与 SW1 和 SW2 法务及人力 ipv4 和 ipv6 互访优先在 SW3_SW2 链路转发，主备链路相互备份；用 prefix-list、route-map 和 BGP 路径属性进行选路，新增 AS 65000。

8. 利用 BGP MPLS VPN 技术，RT1 与 RT2 以太链路间运行多协议标签交换、标签分发协议。RT1 与 RT2 间创建财务 VPN 实例，名称为 Finance，RT1 的 RD 值为 1:1，export rt 值为 1:2，import rt 值为 2:1；RT2 的 RD 值为 2:2。通过两端 loopback1 建立 VPN 邻居，分别实现两端 loopback5 ipv4 互通和 ipv6 互通。

四、无线部署

1. AC1 loopback1 ipv4 和 ipv6 地址分别作为 AC1 的 ipv4 和 ipv6

管理地址。AP 二层自动注册，AP 采用 MAC 地址认证。配置 2 个 ssid，分别为 skills-2.4G 和 skills-5G。skills-2.4G 对应 vlan140，用 network 140 和 radio1（模式为 n-only-g）,用户接入无线网络时需要采用基于 WPA-personal 加密方式，密码为 Key-1122。skills-5G 对应 vlan150，用 network 150 和 radio2（模式为 n-only-a），不需要认证，隐藏 ssid，skills-5G 用倒数第一个可用 VAP 发送 5G 信号。

2. 当 AP 上线，如果 AC 中储存的 Image 版本和 AP 的 Image 版本号不同时，会触发 AP 自动升级。AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时。

3. MAC 认证模式为黑名单，MAC 地址为 80-45-DD-77-CC-48 的无线终端采用全局配置 MAC 认证。

4. 防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC 10 分钟内建立连接 5 次就不再允许继续连接，2 小时后恢复正常。

5. 配置 vlan110 无线接入用户相互隔离，开启 ARP 抑制功能，限制每天早上 0 点到 4 点禁止终端接入。

6. 配置 vlan110 无线接入用户上下行最大带宽为 800Mbps，arp 上下行最大速率为 6packets/s。

7. 配置 vlan110 无线接入用户上班时间（工作日 09:00-17:00）访问 Internet https 上下行 CIR 为 1Mbps，CBS 为 20Mbps，PBS 为 30Mbps，exceed-action 和 violate-action 均为 drop。时间范围名称、控制列表名称、分类名称、策略名称均为 Skills。

8. AP 发射功率为 90%。

五、安全维护

说明：ip 地址按照题目给定的顺序用“ip/mask”表示，ipv4 any 地

址用 0.0.0.0/0，ipv6 any 地址用::/0，禁止用地址条目，否则按零分处理。

1. FW1 配置 ipv4 nat，实现集团产品 1 段 ipv4 访问 Internet ipv4，转换 ip/mask 为 200.200.200.16/28，保证每一个源 ip 产生的所有会话将被映射到同一个固定的 IP 地址；当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至 10.13.11.120 的 UDP 514 端口，记录主机名，用明文轮询方式分发日志；开启相关特性，实现扩展 nat 转换后的网络地址端口资源。

2. FW1 配置 nat64，实现集团产品 1 段 ipv6 访问 Internet ipv4，转换为出接口 IP，ipv4 转 ipv6 地址前缀为 64:ff9b::/96。

3. FW1 和 FW2 策略默认动作为拒绝，FW1 允许集团产品 1 段 ipv4 和 ipv6 访问 Internet 任意服务。

4. FW2 允许办事处产品 ipv4 访问集团产品 1 段 https 服务，允许集团产品 1 段访问办事处产品 ipv4、FW2 loopback1 ipv4、SW3 模拟办事处 loopback2 ipv4。

5. FW1 与 RT2 之间用 Internet 互联地址建立 GRE Over IPSec VPN，实现 loopback4 之间的加密访问。

6. FW1 要求内网每个 IP 限制会话数量为 300。

7. FW1 开启安全网关的 TCP SYN 包检查功能，只有检查收到的包为 TCP SYN 包后，才建立连接，否则丢弃包；配置对 TCP 三次握手建立的时间进行检查，如果 1 分钟内未完成三次握手，则断掉该连接；配置所有的 TCP 数据包和 TCP VPN 数据包每次能够传输的最大数据分段为 1460，尽力减少网络分片。

模块三：服务搭建与运维

任务描述:

随着信息技术的快速发展，集团计划把部分业务由原有的 X86 服务器上迁移到 ARM 架构服务器上，同时根据目前的部分业务需求进行了部分调整和优化。

一、X86 架构计算机操作系统安装与管理

1．PC1 系统为 ubuntu-desktop-amd64 系统（已安装，语言为英文），登录用户为 xiao，密码为 Key-1122。启用 root 用户，密码为 Key-1122。

2．安装 remmina，用该软件连接 Server1 上的虚拟机，并配置虚拟机上的相应服务。

3．安装 qemu 和 virtinst。

4．创建 Windows Server 2022 虚拟机，虚拟机信息如下:

虚拟机名称	vcpu	内存	硬盘	IPv4 地址	完全合格域名
windows8	2	4096MB	40GB	10.13.11.101/24	windows8.skills.lan
windows9	2	4096MB	40GB	10.13.11.102/24	windows9.skills.lan

5．安装 windows8，系统为 Windows Server 2022 Datacenter Desktop，网络模式为桥接模式，网卡、硬盘、显示驱动均为 virtio，安装网卡、硬盘、显示驱动并加入到 Windows AD 中。

6．安装 windows9，系统为 Windows Server 2022 Datacenter Desktop，网络模式为桥接模式，网卡、硬盘、显示驱动均为 virtio，安装网卡、硬盘、显示驱动并加入到 Windows AD 中。在 windows9 中添加 3 块 5GB 的硬盘（硬盘驱动为 virtio），初始化为 GPT，配置为 raid5。驱动器盘符为 D。

二、ARM 架构计算机操作系统安装与管理

1．从 U 盘启动 PC2，安装 kylin-desktop-arm64（安装语言为英文），安装时创建用户为 xiao，密码为 Key-1122。启用 root 用户，密码为 Key-1122。

2．配置 minicom，用该软件连接网络设备，并对网络设备进行配置。

三、Windows 云服务配置

1．创建实例

(1)网络信息表

网络名称	vlan	子网名称	网关	IPv4 地址池
network210	210	subnet210	10.13.210.1/24	10.13.210.100-10.13.210.109
network211	211	subnet211	10.13.211.1/24	10.13.211.100-10.13.211.109
network212	212	subnet212	10.13.212.1/24	10.13.212.100-10.13.212.109

(2)实例类型信息表

名称	id	vcpu	内存	硬盘	实例名称	镜像
skills	1	4	4GB	40GB	windows1-windows7	windows2022

(3)实例信息表

实例名称	IPv4 地址	完全合格域名
windows1	10.13.210.101	windows1.skills.lan
windows2	10.13.210.102	windows2.skills.lan
windows3	10.13.210.103	windows3.skills.lan
windows4	10.13.210.104	windows4.skills.lan
windows5	10.13.210.105 10.13.211.105	windows5.skills.lan

实例名称	IPv4 地址	完全合格域名
windows6	10.13.210.106 10.13.211.106 10.13.212.106	windows6.skills.lan
windows7	10.13.210.107 10.13.211.107 10.13.212.107	windows7.skills.lan

2. 域服务

任务描述：请采用域环境，管理企业网络资源。

(1)配置 windows2 为 skills.lan 域控制器；安装 dns 服务，dns 正反向区域在 active directory 中存储，负责该域的正反向域名解析。

(2)把 skills.lan 域服务迁移到 windows1；安装 dns 服务，dns 正反向区域在 active directory 中存储，负责该域的正反向域名解析。

(3)把其他 windows 主机加入到 skills.lan 域。所有 windows 主机（含域控制器）用 skills\Administrator 身份登陆。

(6)启用所有 windows 服务器的防火墙。

(7)在 windows1 上新建名称为 manager、dev、sale 的 3 个组织单元；每个组织单元内新建与组织单元同名的全局安全组；每个组内新建 20 个用户：行政部 manager00-manager19、开发部 dev00-dev19、营销部 sale00-sale19，不能修改其口令，密码永不过期。manager00 拥有域管理员权限。

3. 组策略

(1)添加防火墙入站规则，名称为 icmpv4，启用任意 IP 地址的 icmpv4 回显请求。

(4)允许 manager 组本地登录域控制器，允许 manager00 用户远程登录到域控制器；拒绝 dev 组从网络访问域控制器。

(5)登录时不显示上次登录，不显示用户名，无须按 ctrl+alt+del。

(6)登录计算机时，在桌面新建名称为 chinaskills 的快捷方式，目

标为 http://www.chinaskills-jsw.org，快捷键为 ctrl+shift+f6。

4. 文件共享

任务描述：请采用文件共享，实现共享资源的安全访问。

(1)在 windows1 的 C 分区划分 2GB 的空间，创建 NTFS 分区，驱动器号为 d; 创建用户主目录共享文件夹: 本地目录为 D:\share\home，共享名为 home，允许所有域用户完全控制。在本目录下为所有用户添加一个以用户名命名的文件夹，该文件夹将设置为所有域用户的 home 目录，用户登录计算机成功后，自动映射挂载到 h 卷。禁止用户在该共享文件中创建“*.exe”文件，文件组名和模板名为 my。

(2)创建目录 D:\share\work，共享名为 work，仅 manager 组和 Administrator 组有完全控制的安全权限和共享权限，其他认证用户有读取执行的安全权限和共享权限。在 AD DS 中发布该共享。

5. ASP 服务

任务描述：请采用 IIS 搭建 web 服务，创建安全动态网站，。

(1)把 windows3 配置为 ASP 网站，网站仅支持 dotnet clr v4.0，站点名称为 asp。

(2)http 绑定本机与外部通信的 IP 地址，仅允许使用域名访问。

(3)网站目录为 C:\iis\contents，默认文档 index.aspx 内容为 "Helloaspx"。

(4)使用 windows5 测试。

6. powershell 脚本

任务描述：请采用 powershell 脚本,实现快速批量的操作。

(1)在 windows7 上编写 C:\createfile.ps1 的 powershell 脚本,创建 20 个文件 C:\file\file00.txt 至 C:\file\file19.txt，如果文件存在，则删除后，再创建；每个文件的内容同主文件名，如 file00.txt 文件的内容为

“file00”。

四、Linux 云服务配置

1. 系统安装

(1)通过 PC1 web 连接 Server2，给 Server2 安装 rocky-arm64 CLI 系统（语言为英文）。

(2)配置 Server2 的 IPv4 地址为 10.13.220.100/24。

(3)安装 qemu 和 virt-install。

(4)创建 rocky-arm64 虚拟机，虚拟机硬盘文件保存在默认目录，名称为 linuxN.qcow2(N 表示虚拟机编号 1-9，如虚拟机 linux1 的硬盘文件为 linux1.qcow2,虚拟机 linux2 的硬盘文件为 linux2.qcow2),虚拟机信息如下:

虚拟机名称	vcpu	内存	硬盘	IPv4 地址	完全合格域名
linux1	2	4096MB	40GB	10.13.220.101/24	linux1.skills.lan
linux2	2	4096MB	40GB	10.13.220.102/24	linux2.skills.lan
linux3	2	4096MB	40GB	10.13.220.103/24	linux3.skills.lan
linux4	2	4096MB	40GB	10.13.220.104/24	linux4.skills.lan
linux5	2	4096MB	40GB	10.13.220.105/24	linux5.skills.lan
linux6	2	4096MB	40GB	10.13.220.106/24	linux6.skills.lan
linux7	2	4096MB	40GB	10.13.220.107/24	linux7.skills.lan
linux8	2	4096MB	40GB	10.13.220.108/24	linux8.skills.lan
linux9	2	4096MB	40GB	10.13.220.109/24	linux9.skills.lan

(5)安装 linux1，系统为 rocky-arm64 CLI，网卡、硬盘、显示驱动均为 virtio，网络模式为桥接模式。

(6)关闭 linux1，给 linux1 创建快照，快照名称为 linux-snapshot。

(7)根据 linux1 克隆虚拟机 linux2-linux9。

2．dns 服务

任务描述：创建 DNS 服务器，实现企业域名访问。

(1)所有 linux 主机启用防火墙，防火墙区域为 public，在防火墙中放行对应服务端口。

(2)利用 chrony，配置 linux1 为其他 linux 主机提供 NTP 服务。

(3)所有 linux 主机之间（包含本主机）root 用户实现密钥 ssh 认证，禁用密码认证。

(4)利用 bind，配置 linux1 为主 DNS 服务器，linux2 为备用 DNS 服务器。为所有 linux 主机提供冗余 DNS 正反向解析服务。

3．apache2 服务

任务描述：请采用 Apache 搭建企业网站。

配置 linux1 为 Apache2 服务器，使用 skills.lan 或 any.skills.lan(any 代表任意网址前缀，用 linux1.skills.lan 和 web.skills.lan 测试)访问时，自动跳转到 www.skills.lan。禁止使用 IP 地址访问，默认首页文档 /var/www/html/index.html 的内容为"apache"。

4．tomcat 服务

任务描述：采用 Tomcat 搭建动态网站。

(1)配置 linux2 为 nginx 服务器，默认文档 index.html 的内容为“hellonginx”；仅允许使用域名访问，http 访问自动跳转到 https。

(2)利用 nginx 反向代理，实现 linux3 和 linux4 的 tomcat 负载均衡，通过 https//tomcat.skills.lan 加密访问 Tomcat。

(3)配置 linux3 和 linux4 为 tomcat 服务器，网站默认首页内容分别为“tomcatA”和“tomcatB”，仅使用域名访问 80 端口 http。

5．samba 服务

任务描述：请采用 samba 服务，实现资源共享。

(1)在 linux3 上创建 user00-user19 等 20 个用户；user00 和 user01 添加到 manager 组，user02 和 user03 添加到 dev 组。把用户 user00-user03 添加到 samba 用户。

(2)配置 linux3 为 samba 服务器,建立共享目录/srv/sharesmb，共享名与目录名相同。manager 组用户对 sharesmb 共享有读写权限，dev 组对 sharesmb 共享有只读权限；用户对自己新建的文件有完全权限，对其他用户的文件只有读权限，且不能删除别人的文件。在本机用 smbclient 命令测试。

(3)在 linux4 修改/etc/fstab,使用用户 user00 实现自动挂载 linux3 的 sharesmb 共享到/sharesmb。

6．kubernetes 服务

任务描述：请采用 kubernetes 和 containerd，管理容器。

(1)在 linux5-linux7 上安装 containerd 和 kubernetes，linux6 作为 master node，linux6 和 linux7 作为 work node；使用 containerd.sock 作为容器 runtime-endpoint。导入 nginx 镜像，主页内容为“HelloKubernetes”。

(2)master 节点配置 calico，作为网络组件。

(3)创建一个 deployment，名称为 web，副本数为 2；创建一个服

务，类型为 nodeport，名称为 web，映射本机 80 端口和 443 端口分别到容器的 80 端口和 443 端口。

7. mysql 服务

任务描述：请安装 mysql 服务，建立数据表。

(1)配置 linux2 为 mysql 服务器，创建数据库用户 xiao，在任意机器上对所有数据库有完全权限。

(2)创建数据库 userdb；在库中创建表 userinfo，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	varchar(5)	否	否
password	varchar(200)	否	否

(3)在表中插入 2 条记录，分别为(1,user1，1999-07-01，男)，(2,user2，1999-07-02，女)，password 与 name 相同，password 字段用 password 函数加密。

(4)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。

(5)每周五凌晨 1:00 以 root 用户身份备份数据库 userdb 到 /var/databak/userdb.sql(含创建数据库命令)。

8. shell 脚本

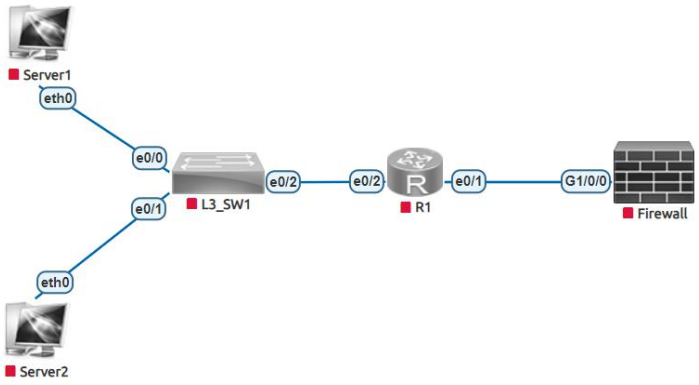
任务描述：请采用 shell 脚本,实现快速批量的操作。

在 linux4 上编写/root/createfile.sh 的 shell 脚本，创建 20 个文件 /root/shell/file00 至/root/shell/file19，如果文件存在，则删除再创建；每个文件的内容同文件名，如 file00 文件的内容为“file00”。用

/root/createfile.sh 命令测试。

五、网络运维

某单位网络拓扑架构如下，交换机连接两台服务器，其中Server1服务器是数据取证服务器，Server2服务器是应急响应服务器，通过交换设备相连，通过路由设备连接到安全设备防火墙，单位的网络拓扑结构如下图所示。



网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
服务器	Server1	Eth0	192.168.1.10/24
	Server2	Eth0	192.168.2.10/24
三层交换机	L3_SW1	e0/0	192.168.1.2/24
		e0/1	192.168.2.2/24
		e0/2	10.1.1.1/24
路由器	R1	e0/2	10.1.1.2/24
		e0/1	20.1.1.1/24
防火墙	Firewall	G1/0/0	20.1.1.2/24

1. 网络排错

网络按照表中要求已经搭建完成，现在有如下故障:

L3_SW1上交换机需要设置三层网络，现在三层直连路由无法ping通，但是查看接口的状态发现，接口物理状态都是up的，请分析原因并且故障排除。

拓扑中R1路由器与交换机所在的服务器网段通信异常，请分析故障排除。

Firewall防火墙日志收到了来自内网的ddos攻击，请分析日志将相关的攻击者/或者网络运维人员误操作引起的攻击流量找出，并设置黑名单策略，请分析日志并进行故障排除。

2. 数字取证

Server1服务器上出现了黑链，并且入侵者已经将服务器上的痕迹清除，无法在服务器上进行溯源，恰好在前端的防火墙的开启了数据包分析功能。请你在数据包中进行取证工作，找到入侵者的信息。

（1）通过对数据包的分析找到黑客的攻击机IP，并将他作为Flag提交；（格式：[192.168.1.1]）

（2）通过对数据包的分析找到黑客扫描服务器的命令，将服务器开放的端口作为Flag提交；端口从小到大排序提交（格式：[21,22,23,24]）

3. 应急响应

防火墙的日志中出现了webshell警告，Server2服务器上出现了webshell连接情况，管理员已经将服务器进行了安全隔离。请登陆到服务器上，对webshell情况进行排查。

（1）在服务器上找到webshell文件，并将webshell的文件名作为flag提交；（格式：[abc.xxx]）

（2）在服务器上找到上传webshell的上传方式和时间，将webshell上传的时间作为flag进行提交；（格式：[10/Apr/2020:09:35:41]）