**2017年全国职业院校技能大赛中职组**

**“网络搭建与应用”赛项规程**

**一、赛项名称**

赛项编号：ZZ－2017023

赛项名称：网络搭建与应用

英语翻译：Network Establishment and Application

赛项组别：中职组

赛项归属产业：电子信息产业

**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，引导教师在教学模式和学生评价模式的改革，引导院校、教师、企业教产互动、校企合作，提升中职信息技术类专业学生能力素质与企业用人标准的吻合度,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。

**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服务(Windows/Linux)、数据库安装配置、服务器系统管理、虚拟化技术，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 |
| 9 | 服务器虚拟化  服务器集群 | 掌握虚拟化技术，使用服务器集群技术 |
| 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。 |
| 9 | 服务器虚拟化  服务器集群 | 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 |
| 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，可配2名指导教师。

可邀请国际团队观摩。

**五、竞赛流程**

（一）比赛场次

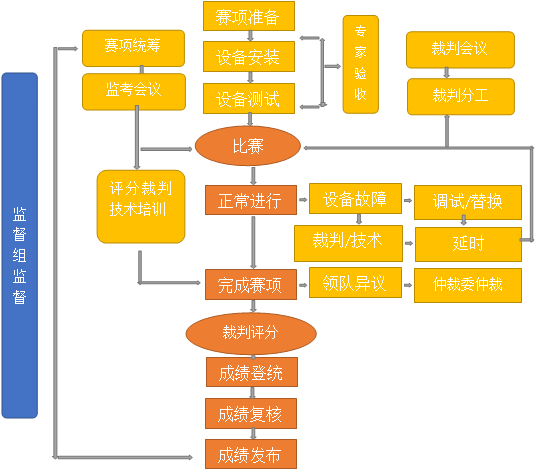
本赛项为单场次团体赛项目

（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 |
| 08:28 | 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 |
| 竞赛  后1日 | 13：30-14：00 | 闭赛式 | 领导、嘉宾、裁判、各参赛队、专家组 |  |

（三）比赛流程



赛前准备：选手抽签入场，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在答题纸上规划IP地址并填写，配置网络设备和服务器操作系统等，完成网络搭建及应用，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。

（二）本赛项公开试题和主要网络环境。比赛完成后，试题进行封闭回收。

（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)。

样题详见附件1：2017年全国职业院校技能大赛网络搭建与应用竞赛样题

**七、竞赛规则**

（一）选手报名

参赛选手2名，须为2017年度全日制在籍学生；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（当年），即1996年5月1日后出生。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。选手必须佩带参赛证提前30分钟进入大赛场地，比赛场地通过抽签决定，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．现场裁判核对参赛选手资格，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。

6．参赛选手在比赛过程中不得擅自离开赛场，如有特殊情况，须经现场裁判同意后作特殊处理。

7．当听到比赛结束命令时，参赛选手应立即停止所有操作，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。

8．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80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

可设置成果展示区、体验区，视赛项承办单位实际承接条件设置是否进行现场观摩。

**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](javascript:XPE.bus.occurred('bookDetails',%7bisPublished:'yes',uuid:'8a2c44cc-14a2-1000-9630-3fafc67de19c'%7d))

（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  （神州数码） | 数量 | 备注 |
| 1 | 路由器 | DCR-2655 | 2 | 沿用16年比赛设备 |
| 2 | 路由器线缆 | CR-V35MT-V35FC | 2 | 沿用16年比赛设备 |
| 3 | 三层交换机 | CS6200-28X-EI | 2 | 每台标配：  M6200-AC-A 交流电源模块  DAC-SFPX-3M VSF虚拟化连接套件 |
| 4 | 二层交换机 | S4600-28P-SI | 1 | 设备型号升级 |
| 5 | 多核防火墙 | DCFW-1800E-N3002 | 2 | 设备型号升级  标配：  USG-N3002-LIC 特征库升级许可 |
| 6 | 无线交换机 | DCWS-6028 | 1 | 沿用16年比赛设备 |
| 7 | 无线接入点 | WL8200-I2 | 1 | 沿用16年比赛设备 |
| 8 | POE模块 | DCWL-PoEINJ-G+ | 1 | 沿用16年比赛设备 |
| 9 | 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 | 4 | 承办校提供 |
| 10 | 网络设备机柜 | JZ-ONPTC-1.8M | 1 | 开放机柜，配线架等 |
| 11 | 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 2010(中文版)。

具体软件参数如下所示:

1. 微软 Windows 7 (64位中文版) 试用版；

2. Centos 6.5（64位）；

3. WINRAR 5.21(中文版) 试用版；

4. 微软 Microsoft Office 2010(中文版) 试用版；

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

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

7. VMware workstation 12免费版；

8. SecureCRT；

9.VMware vSphere 5.5 60天试用版；

10.存储模拟软件 openfileresa-2.99.1 开源软件;

11. Apache Tomcat 7.0.27；

12.JDK（Java Development Kit）1.7及以上；

13.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，满分为3分 |
| 2 | IP地址划分实施 | 完成子网划分、IP规划实施，满分为2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10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，满分为20分 |
| 6 | 服务器虚拟化  服务器集群 | 掌握虚拟化技术，使用服务器集群技术，满分为10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 | 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。裁判组遵照大赛执委会要求成立，需要裁判19名，裁判长1人，加密裁判2人，现场裁判4人，评分裁判12人分为6组评判，每组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。

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.成绩复核与公布

监督组按照全国职业院校技能大赛制度将对成绩进行复核，保证评判透明、准确。

竞赛成绩复核无误后，经裁判长、监督人员审核签字后公布，保证成绩公开。

**十二、奖项设定**

（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)。

（二）优秀指导教师奖励

本赛项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）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。

（二）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。

1. 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。

（四）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项执委会，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。

1. 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.各参赛代表队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2.各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料，正式比赛着统一参赛服装入场，除指定参赛证件外，任何无关东西不能带入比赛场地。

3.竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4.参赛代表队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5.对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或处理意见不服而停止竞赛，否则以弃权处理。

6.参赛队领队应对本队参赛队员和指导教师的参赛期间安全负责，参赛学校须为参赛选手和指导教师购买意外保险。

（二）指导教师须知

1.各参赛代表队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2.各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3.竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4.参赛代表队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5.对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服而停止竞赛，否则以弃权处理。

6.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。

（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。

（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**

本赛项在比赛过程中若出现有失公正或有关人员违规等现象，参赛队领队可在比赛结束后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。

**十六、竞赛观摩**

本赛项允许进行公开观摩，但需视承办校场地情况具体执行。

竞赛环境依据竞赛需求和职业特点设计，在竞赛不被干扰的前提下预先设计观摩方案、安全开放赛场。

欢迎各界人员沿指定路线、在指定时间和区域内到现场观赛。

**十七、竞赛直播**

赛项全程直播。

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、资源转化**

依照《全国职业院校技能大赛赛项资源转化工作办法》的有关要求，赛后向大赛执委会办公室提交资源转化方案，赛后6个月内完成资源转化工作。

第一类资源转化的内容是竞赛全过程的各类资源，包括：

（一）竞赛样题、试题。

（二）竞赛技能考核评分案例。

（三）考核环境描述。

（四）竞赛过程音视频记录。

（五）裁判、专家点评。

（六）优秀选手、指导教师访谈。

第二类资源转化的内容是计算机网络技术专业教学资源包。系统梳理计算机网络技术专业的培养目标、岗位需求、课程体系、核心知识点及历年竞赛考核内容与评分要点，并结合技术发展趋势对未来的竞赛内容设置进行了权威预测。

第三类资源转化的内容是计算机网络应用赛项案例集。将2010年—2016年国赛及各省赛的竞赛内容进行分析汇总，形成行业应用案例，从而使赛题中的行业应用成为日常教学内容的载体。

第四类资源转化的内容是计算机网络技术专业系列教材。依托大赛，开发一套融入大赛思想的，体现“新设备、新技术、新标准”的实用型系列教材。

第五类资源转化的内容是仿真实训微课的制作

根据教育部数字校园建设规范的要求“通过数字仿真、虚拟现实等信息化方式，在教学中普遍应用现代信息技术，多渠道系统优化教学过程，增强教学的实践性、针对性和实效性，提高教学质量”，DCN于2014年研发并搭建了“神州数码技云微课平台”，开发“在线交互式仿真实训课件”涵盖了网络技术、信息安全、计算机应用、软件测试、企业信息管理以及多媒体技术等多种职业类课程。提供课件定制开发服务，根据院校不同需要个性化定制实训课程。微课平台的网址是<http://dcn.skillcloud.cn>。

## 附件1：比赛样题

**2017年全国职业院校技能大赛中职组**

**“网络搭建与应用”赛项竞赛样题**

**（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。

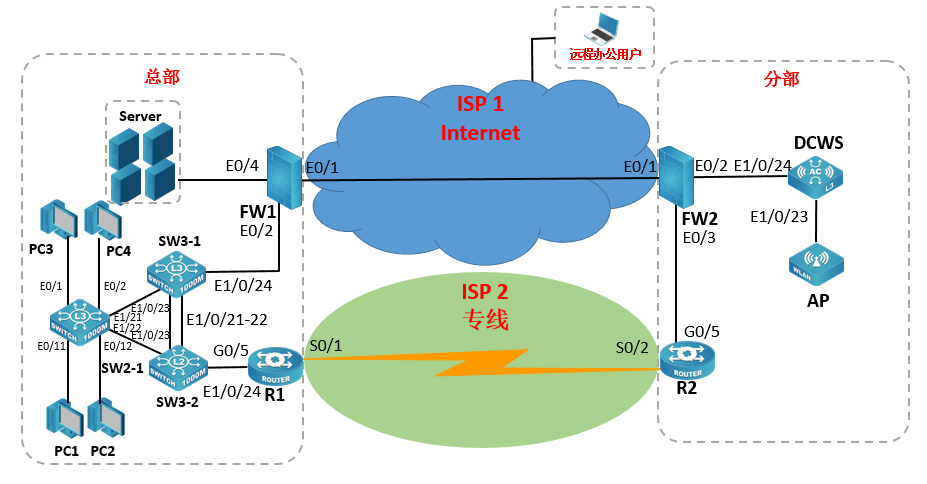
（7）与比赛相关的工具软件放置在D:\soft文件夹中。

项目简介:

某集团公司经过业务发展，总部在北京市，在上海设置了分部，为了实现快捷的信息交流和资源共享，需要构建统一网络，整合公司所有相关业务流程。采用单核心的网络架构模式，路由器接入城域网专用链路来传输业务数据流。总部为了安全管理每个部门的用户，使用VLAN技术将每个部门的用户划分到不同的VLAN中。分部采用防火墙接入互联网络，使用路由器连接城域网专用网络，分部的内网用户采用无线接入方式访问网络资源。为了保障总部与分部业务数据流传输的高可用性，使用防火墙VPN保证网络的可靠性。

通过与客户沟通，项目交给小明负责。但小明一不小心误操作，把R1,R1路由器的NOS删除了。现场网络未完善。不能上网，无法下载第三方TFTP或者FTP软件，请根据现有情况帮助小明恢复路由器的NOS系统。相关操作手册在D:\soft文件夹中。

### 拓扑结构图



### 表1网络设备连接表

|  |  |  |  |
| --- | --- | --- | --- |
| **A设备连接至B设备** | | | |
| **设备名称** | **接口** | **设备名称** | **接口** |
| R1 | G0/5 | SW3-2 | E1/0/24 |
| R1 | S0/1 | R2 | S0/2 |
| R2 | G0/5 | FW2 | E0/3 |
| FW1 | E0/2 | SW3-1 | E1/0/24 |
| FW1 | E0/1 | FW2 | E0/1 |
| DCWS | E1/0/24 | FW2 | E0/2 |
| DCWS | E1/0/23 | AP |  |
| SW3-1 | E1/0/21-22 | SW3-2 | E1/0/21-22 |
| SW3-1 | E1/0/23 | SW2-1 | E1/21 |
| SW3-2 | E1/0/23 | SW2-1 | E1/22 |
| SW2-1 | E1/1 | PC3 | 模拟 |
| SW2-1 | E1/2 | PC4 | 模拟 |
| SW2-1 | E1/11 | PC1 | 模拟 |
| SW2-1 | E1/12 | PC2 | 模拟 |
| FW1 | E0/4 | Server1-4 | 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 | R1 | G 0/5 | 192.168.12.254/24 |
| S 0/1 | 202.1.1.1/30 |
| R2 | G 0/5 | 192.168.13.2/24 |
| S 0/2 | 202.1.1.2/30 |
| 三层交换机 | SW3-1 | VLAN10 SVI |  |
| VLAN20 SVI |  |
| VLAN30 SVI |  |
| VLAN40 SVI |  |
| VLAN11 SVI | 192.168.11.2/24 |
| VLAN1 SVI | 10.1.1.1/24 |
| SW3-2 | VLAN10 SVI |  |
| VLAN20 SVI |  |
| VLAN30 SVI |  |
| VLAN40 SVI |  |
| VLAN12 SVI | 192.168.12.1/24 |
| VLAN1 SVI | 10.1.1.2/24 |
| 防火墙1 | FW-1 | Eth0/1 | 200.1.1.1/30 |
| Eth0/2 | 192.168.11.254/24 |
| Eth0/4 | 100.10.10.254/24 |
| Loopback 1 | 172.16.100.254/24 |
| 防火墙2 | FW-2 | Eth0/1 | 200.1.1.2/30 |
| Eth0/2 | 192.168.100.254/24 |
| Eth0/3 | 192.168.13.1/24 |
| Loopback 1 | 172.16.200.254/24 |

**表3：服务器IP地址分配表**

| **宿主机** | **虚拟主机名称** | **域名信息** | **服务角色** | **系统及**  **版本信息** | **IPv4**  **地址信息** |
| --- | --- | --- | --- | --- | --- |
| **Server1** | Vsphere-A1 | Vsphere1 | 虚拟化 | ESXI5.5 | 100.10.10.223/24 |
| Win2012-A1 | ftp.chinaskills.com | DHCP服务器  FTP服务器 | Windows Server 2012R2 | 100.10.10.170/24 |
| Centos-A1 | mail.jnds.net | DHCP服务器  TFTP服务器  MAIL服务器 | Centos 6.5 | 100.10.10.213/24 |
| **Server2** | Vsphere-B1 | Vsphere2 | 虚拟化 | ESXI5.5 | 100.10.10.224/24 |
| Centos-B1 | ftp.jnds.net | 逻辑卷磁盘  容量服务  FTP服务器 | Centos 6.5 | 100.10.10.169/24 |
| Centos-B2 | backups.jdns.net | 冗余备份  NFS服务器 | Centos 6.5 | 100.10.10.210/24 |
| **Server3**  （VCENTER服务器）  IP：100.10.10.244 | Win2012-C1 | FQDN：www2.chinaskills.com | WEB服务器  故障转移集群服务 | Windows Server 2012R2 | 100.10.10.161/24 |
| Openfiler-C1 |  | 存储服务器 | OpenfileR2.99 | 100.10.10.245/24 |
| Centos-C1 | www.jnds.net | WEB服务器  数据库服务器 | Centos 6.5 | 100.10.10.212/24 |
| WIN7-C1 | Win7-C1.chinaskills.com | Client | Windows 7 | 100.10.10.117/24 |
| **Server4** | Win2012-D1 | dc.chinaskills.com | 域控制器  DNS服务器  CA证书服务器  存储服务器 | Windows Server 2012R2 | 100.10.10.186/24 |
| Win2012-D2 | FQDN：www1.chinaskills.com | WEB服务器  故障转移集群服务 | Windows Server 2012R2 | 100.10.10.160/24 |
| Win2008-D1 |  | Tomcat服务器 | Windows Server 2008 R2 | 100.10.10.196/24 |
| Centos-D1 | dns.jnds.net | BIND  域名服务器  Squid  代理服务器 | Centos 6.5 | 100.10.10.211/24 |

**表4：布线要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **项目** | **明细** |
| 1 | 跳线制作与连接 | 跳线长度预留合理、捆扎美观。 |
| 线标正确，粘贴合理。 |
| 2 | 施工过程 | 施工过程安全、文明施工、耗材与工具使用正确。 |

**网络配置项目**

**（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，注意保存配置。在D:\soft文件夹中有名为“答案.doc”的word文档，根据word中要求进行截图； SW2-1 ,SW3-1,SW3-2,DCWS四台设备需要保存show running-config 命令的结果，以”设备名称.doc”格式进行保存。

3.上述文档完成后，请存放在PC1桌面的“比赛结果”文件夹中。

4.裁判以各参赛队的文档为主要评分依据。无文档相关环节视为0分。

**一、物理连接与IP地址划分**

1.按照网络拓扑图制作以太网网线，并连接设备。要求符合T568A和T568B的标准，其线缆长度适中。

2.根据“拓扑结构图”和“表2:网络设备IP地址分配表”所示，给网络中的所有设备接口配置IP地址。分配地址时做到节省IP资源，合理分配(先划分大的地址块，再划分小的地址块，可以节省IP资源)。总部除服务器区外所有主机规划使用10.62.11.0/11地址所在地址段。财务部（vlan10）有10台主机、生产部（vlan20）有60台主机、销售部（vlan30）和技术部（vlan40）两个部门都有300台主机，服务器的网段为100.10.10.0/24。分部与所有设备互联地址使用表中分配地址，把算出的IP地址填入上面“表2.网络设备IP地址分配表”中的空白处。网关使用每个网段的最后一个IP地址。

**二、交换机配置**

1.在两台三层交换设备上开启telnet管理功能，登陆后即可查看和修改配置，本地认证用户名:2017DCN,密码：pwd@dcn；

2.总部的交换网络中，有4个VLAN；财务部使用VLAN10，名字为CW，生产部使用VLAN20，名字为SC，销售部使用VLAN30，名字为XS，技术部使用VLAN40，名字JS；

3.按下表要求将端口加入VLAN并做相应配置：

|  |  |  |
| --- | --- | --- |
| **设备名称** | **VLAN** | **端口** |
| **SW2-1** | 10 | E 1/1-5 |
| 20 | E 1/6-10 |
| 30 | E 1/11-15 |
| 40 | E 1/16-20 |

4.SW2-1为接入交换机，为防止终端产生mac地址防洪攻击，请配置端口安全，除E1/1接口外每个已划分vlan的端口最多学习到5个mac地址，发生违规，阻止后续违规流量通过，不影响已有流量并产生LOG日志；E1/1为专用接口，限定mac地址00-11-11-11-11-11可以连接；

5.SW3-1,SW3-2配置防止PC端发出网关欺骗报文；

6.使用端口汇聚技术，在SW3-1、 SW3-2之间的链路启用端口汇聚，汇聚接口为动态方式；

7.配置生成树协议，要求启用MSTP协议，name 为 2017DCN，revision-level 1，实例1中包括VLAN10、20、30；实例2中包括VLAN40；要求SW3-1为实例1的主根，SW3-2为实例2 的主根，并互为备份根；通过在SW2-1修改cost值保证实例1中SW2-1 E1/22阻断，实例2中E1/21阻断；在三层交换机上保护根桥在有更高优先级交换机接入E1/0/1-20口时不得抢占为根桥；

8.在三层交换之间启用VRRP协议，为VLAN、10、20、30、40实现网关备份，vrrp组中的虚拟IP为vlan中最后一个IP地址,SW3-1为VLAN10、20、30的master； SW3-2为40的master，且互为备份，开启抢占功能；配置监视接口以实现上联接口断开时自动降低优先级以实现master,slave自动切换保证冗余性；

9.SW3-1将访问Internet的双向流量镜像到E1/0/20口；

10.SW3-1，SW3-2配置VSF，VSF成员编号1，其中SW3-1为VSF成员Master，SW3-2为Standby Master，SW3-1向SW3-2同步配置信息，当SW3-1设备出现故障后SW3-2可以无缝接替其工作；

**三、路由器配置与调试**

由于历史原因，总部、分部各有一部分Area 0，但总部的用户需要通过FW1连接互联网，分部需通过FW2连接互联网；

1.总部内部，FW1、SW3-1、SW3-2、R1之间连接使用OSPF,Area 0；

2.分部内部，FW2、R2之间连接使用OSPF Area 0；

3.R1、R2之间使用RIPv2路由协议,关闭自动汇总；

4.FW1、FW2通过默认路由连接至ISP1；并向内部传播默认路由；

5.总部VLAN40是管理员所在VLAN，管理员通过专线telnet管理分部网络设备，使用路由策略在R1路由重发布时只允许总部的服务器、VLAN40管理员网段与分部进行通信；总部FW1 loopback1与分部 FW2 loopback1口正常情况下也使用专线传输。

**四、广域网配置**

1.总部FW1允许VLAN10、VLAN20、VLAN30、VLAN40的用户通过源NAT访问外网，VLAN10使用200.1.1.4，VLAN20使用200.1.1.5，VLAN30使用200.1.1.6，VLAN40使用200.1.1.7；

2.在FW1上，外网通过200.1.1.8可以访问Server 100.10.10.212；

3.FW2上使用出接口配置PAT，实现内网访问外网；

4.R1与R2采用专线连接方式，采用PPP封装，CHAP认证方式，双方使用自己的hostname做用户名，密码为123456；

**五、无线配置**

1.使用无线控制器提供DHCP服务，动态分配IP地址和网关：

DCWS配置VLAN100为管理和通信VLAN, DHCP下发192.168.100.0/24地址，DNS:8.8.8.8，需要排除网关，地址租约为2天；网关使用最后一个可用IP地址，DCWS使用第一个地址作为管理地址,AC使用DHCP功能下发管理地址；

2.设置协议802.11n 2.4G频段；

3.设置SSID DCN，加密模式为wpa-personal,其口令为：chinaskill

4.设置SSID GUEST 不进行认证加密；

5.配置所有无线接入用户相互隔离；

6.GUEST最多接入10个用户，并对GUEST网络进行流控，每用户上行1M，下行2M；

7.考虑到无线网络会进一步部署，增加更多的AP，设置已有AP信道和发射功率每隔1小时自动调节；

8.配置AP在脱离AC管理时依然可以正常工作；

**六、安全策略部分**

1.FW1，FW2配置trust,untrust,dmz区域和相应策略

2.FW1，FW2攻击防护

**开启以下Flood防护：**

ICMP洪水攻击防护，警戒值1000，动作丢弃；

UDP洪水攻击防护，警戒值1000，动作丢弃；

SYN洪水攻击防护，警戒值1000，动作丢弃；

**开启以下DOS防护：**

Ping of Death攻击防护；

Teardrop攻击防护；

IP选项，动作丢弃；

ICMP大包攻击防护，动作丢弃；

1.FW1为了保证带宽的正常使用，通过流量管理功能将P2P软件的影响降到最低；

2.FW1为了防止垃圾邮件， 配置邮箱过滤，过滤可能含有“发票”字样的邮件；

3.FW1加强访问Internet安全性，禁止从HTTP下载可执行文件和批处理文件；

4.总部FW1 loopback1与分部 FW2 loopback1之间正常情况下使用专线同步数据，配置FW1、FW2之间的IPSec链路为两台FW loopback1间的同步数据备份链路。通过更改防火墙上路由优先级，使FW上专线路由丢失时，自动使用FW1、FW2间IPSec 链路同步数据；数据ESP封装，加密算法采用3DES、认证算法采用SHA；

5.FW1配置SSL VPN，允许远程办公用户访问FW1 loopback1，起始地址为172.16.1.10，结束地址为172.16.1.100 ，用户名user1,密码dcn001；

**系统配置与管理项目**

**（500分）**

【说 明】

1.题目中所涉及的所有系统的管理员以及其他普通用户密码均为2017Netw@rk（注意区分大小写），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属性设置请按照网络拓扑结构图以及“表3：服务器IP地址分配表”的要求设定。

3.除非作特殊说明，在同一主机下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.所有系统镜像文件及试题所需的其它软件均存放在每台主机的D:\soft文件夹中，并将题目要求的截图内容以.jpg格式存储于各物理机桌面BACKUP\_X（X为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为0分。

5.题目要求的虚拟机均安装于每台主机的D：\virtualPC目录，即路径为D：\virtualPC\虚拟主机名称。

6.所有服务要求虚拟机系统重新启动后，均能正常启动和使用，否则扣除该服务功能一半分数。

**虚拟化和存储部分**

**一、在Server 1上完成如下操作:**

**（一）完成虚拟化系统ESXI Server的创建**

1.在VMware Workstation上安装名为“Vsphere-A1”的虚拟化系统，具体要求内存为4G，硬盘80G；

2.开启Vsphere-A1的shell和ssh功能；

**二、在Server 2上完成如下操作:**

**（一）完成虚拟化系统ESXI Server的创建**

在VMware Workstation上安装名为“Vsphere-B1”的虚拟化系统，具体要求内存为4G，硬盘80G；

**三、在Server 3上完成如下操作:**

**（一）完成存储系统的虚拟机创建**

在VMware Workstation上安装名为“Openfiler-C1”的存储系统，具体要求为内存为1G，硬盘10G；

**（二）完成VMware Vcenter Server和VMware vSphere Client的安装**

将Server3的IP地址配置为100.10.10.244/24，并完成VMware Vcenter Server和VMware vSphere Client的安装；

**（三 ）完成存储系统中磁盘的配置**

1.在Openfiler-C1存储系统上添加三块SATA磁盘，每块磁盘大小为30G；

2.将三块硬盘配置成RAID5格式的卷组，卷组名称为：iSCSI-1；

3.将卷组iSCSI-1配置成iSCSI格式的逻辑卷，逻辑卷名称为：iSCSI-2，大小为全部空间可用，逻辑卷描述为：openfiler-iSCSI，将配置结果截图保存为filer.jpg；

4.开启iSCSI target server的服务，截图保存为on.jpg；

5.添加new iSCSI target，并对其iSCSI-2进行映射，读写模式为：write-thru，配置Network ALL允许同网段的计算机可以访问；

**（四）完成Vcenter Server数据中心的创建和主机的添加**

1.使用VMware vSphere Client登录Vcenter Server，并创建数据中心，名称为：DataCenter，截图保存为dvs-1.jpg；

2.在DataCenter中添加虚拟主机Vsphere1和Vsphere2，截图保存为dvs-2.jpg；

**（五）完成ESXI Server中使用iSCSI磁盘的配置**

1.在Vsphere-A1和Vsphere-B1上，要求通过动态发现的方式，配置iSCSI存储适配器；

2.在Vsphere-A1和Vsphere-B1上，完成主机挂载数据存储，文件系统版本为：VMFS-5，共享存储名称为：iSCSI-disk，容量为：最大可用空间，使服务器进行正常存储，将最终结果截图保存为iSCSI-disk.jpg；

**（六）完成ESXI Server中虚拟系统的创建**

1.在Vsphere-A1上，上传windows7的镜像文件，保存在iSCSI-disk中；

2.在Vsphere-B1上，上传Centos6.5的镜像文件，保存在iSCSI-disk中；

3.在Vsphere-A1上创建windows7的虚拟机操作系统，名称为win7-C1，内存为512M，硬盘大小为10G，并加入到chinaskills.com域中，成功加域后截图保存为dcc.jpg；

4.在Vsphere-B1上创建Cenots6.5的虚拟机操作系统，名称为Centos-C1，内存大小为512M，硬盘大小为10G，存储位置为iSCSI-disk中；

**（七）在主机Win7-C1中完成相关测试功能**

访问<https://www.chinaskills.com>网站，显示内容截图为index.jpg；

**（八）在主机Centos-C1中完成Apache服务器及MySQL数据库服务器的部署**

1.在此服务器中安装httpd服务，建立站点[www.jnds.net](http://www.jnds.net)，其网站主目录为/var/www/html，首页内容为“chinaskills’s website”，将显示结果截图保存为cw.jpg；

2.使用openssl申请证书，创建自签名证书server.crt和私钥server.key，要求只允许使用域名通过SSL加密访问；

3.将此服务器配置为MYSQL服务器，升级服务器版本为5.6.24，通过适当命令查询MySQL服务器版本截图保存为bb.jpg；创建数据库为userdatabase，在库中创建表为username，在表中创建2个用户，分别为（myuser1，1995-7-1，男），（myuseR1，1995-9-1，女），口令与用户名相同，要求Password字段以密文显示，需要对登录网站的用户进行身份验证，表结构如下，通过适当命令显示表结构内容截图保存为str.jpg；

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **数据类型** | **主键** | **自增** |
| ID | Int | 是 | 是 |
| Name | varchar(10) | 否 | 否 |
| birthday | Datetime | 否 | 否 |
| sex | char(5) | 否 | 否 |
| Password | char（200） | 否 | 否 |

4.在username表格中，查询性别为男的用户记录，修改用户myuseR1的出生日期为1996-10-25，截图保存为da.jpg；

5.每周五凌晨1:00备份数据库userdatabase到／var/databak/userdatabase.sql，截图保存为back.jpg；

**Windows操作系统**

**一、在Server 1上完成如下操作:**

**（一）完成虚拟主机的创建**

1.安装虚拟机“Win2012-A1”，具体要求为内存为1.5G，硬盘60G，并将服务器加入到Windows域环境；

2.在虚拟机“Win2012-A1”中添加二块SCSI虚拟硬盘，其每块硬盘的大小为10G；并创建以SCSI-two为名字的存储池，利用存储池技术添加一块虚拟简单卷盘符为E盘，在E盘开启数据删除重复功能，排除扩展名为.doc,.txt的文件；

**（二）在主机Win2012-A1中完成DHCP服务的部署**

1.安装DHCP服务，为内网财务部、生产部、销售部和技术部的用户主机动态分配IPv4地址，建立作用域，作用域的名称采用对应部门名称的全拼，超级作用域的名称为DHCPSERVER，为用户分配网关、DNS服务器及域名；此后将DHCP服务管理器有关超级作用域内容展开并截图存储为dhcp.jpg；

2.当DHCP服务出现故障时，转移到win2012-C1服务器上，设置模式为热备用服务器，伙伴服务器角色为“待机”，启用消息验证功能，密码为“135790”；

**（三）在主机Win2012-A1中完成FTP服务的部署**

安装FTP服务，新建一个FTP站点，主目录为E:\ftproot，通过适当技术实现匿名用户登录FTP站点时，只能浏览到“Public”子目录中的内容，若使用个人用户soft1与soft2登录FTP站点时，则只能访问自己的子文件夹；

**二、Server 3上完成如下操作:**

**（一）完成虚拟主机的创建**

安装虚拟机“Win2012-C1”，其内存为2G，硬盘60G，并将服务器加入到Windows域环境；

**（二）在主机Win2012-C1中完成故障转移群集服务器的部署**

1.在VMwareWorkstation上添加安装两块网卡，一块网卡提供网络服务，其IPv4地址为100.10.10.161/24,，另一块网卡为心跳线网卡，其IPv4地址为11.11.11.11；

2.使用iSCSI发起程序连接Win2012-D1的iSCSI虚拟磁盘M和N，并能正常访问；

3.安装故障转移群集功能和文件服务器功能；

**（三）在主机Win2012-C1中完成WEB服务器2的部署**

1.安装IIS组件，创建www.chinaskills.com站点，在N:\MyShare文件夹内中创建名称为chinaskills.html的主页，主页显示内容“热烈庆祝2017年全国职业技能竞赛开幕”，同时只允许使用SSL且只能采用域名方式进行访问；

2.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，使用W3C记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；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、服务器端口号和方法；

**三、在Server 4上完成如下操作:**

**（一）完成虚拟主机的创建**

1.安装虚拟机“Win2012-D1”，其内存为2G，硬盘70G；

2.在虚拟机“Win2012-D1”中添加3块SCSI虚拟硬盘，其每块硬盘的大小为5G，将三块硬盘配置为RAID5，对应磁盘盘符为E:\，截图保存为raid.jpg；

3.使用VMwareWorkstation自带的克隆功能，克隆一个虚拟机名称为“Win2012-D2”，并将服务器加入到Windows域环境，将体现克隆过程的界面截图为ghost.jpg；

4.安装虚拟机“Win2008-D1”，其内存为1G，硬盘40G；

**（二）在主机Win2012-D1中完成域控制器的部署**

1.创建4个用户组，组名采用对应部门名称的全拼命名，每个部门都创建4个用户，财务部用户：fin1~fin4、生产部用户：eng1~eng4、销售部用户：soft1~soft4、技术部用户：sys1~sys4，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（每周工作日 9:00~18:00）；

2.将此服务器配置为主DNS服务器，正确配置chinaskills.com域名的正向及反向解析区域，能够正确解析chinaskills.com域中的所有服务器；创建对应服务器主机记录，需要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；要求动态更新设置为非安全，启用Active Directory的回收站功能；

3.将此服务器设置为域控制器，设置域和林的功能级别为Windows Server 2012，将此功能级别截图保存为jb.jpg；此外，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；

4.制订备份计划，每天的0点对“系统状态”进行备份，并采用VSS完整备份，备份至E:\；

**（三）在主机Win2012-D1中完成磁盘配额的部署**

1.将Win2012-D1系统的C盘磁盘空间划出10G，对应磁盘盘符为F:\，将能体现划出磁盘空间的界面截图为disk.jpg；

2.在F盘上新建Share文件夹，利用磁盘配额管理功能，完成对Share文件夹500M大小的限制，对文件夹限制大小界面截图保存为pe.jpg；

3.限制对Share文件夹内不可以保存\*.xlsx和\*.pptx文档，截图保存为xp.jpg；

**（四）在主机Win2012-D1中完成iSCSI存储的部署**

安装iSCSI目标服务器，并新建iSCSI虚拟磁盘，存储位置为F:\；虚拟磁盘名称分别为Quorum和Files，大小分别为512M和5G，访问服务器为Win2012-D2和Win2012-C1；

**（五）在主机Win2012-D2中完成故障转移群集服务器的部署**

1.在VMwareWorkstation上添加安装两块网卡，一块网卡提供网络服务，其IPv4地址为100.10.10.160/24,，另一块网卡为心跳线网卡，其IPv4地址为11.11.11.12；

2.使用iSCSI发起程序连接Win2012-D1的iSCSI虚拟磁盘Quorum和Files，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；

3.安装故障转移群集功能，添加Win2012-D2和Win2012-C1服务器，并生成故障转移群集验证报告验证结果，截图为baogao.jpg；

4.创建故障转移群集，群集名称为：webcluster，IP地址为：100.10.10.166/24;

5.添加文件服务器功能和配置文件服务器角色，名称为：MyCluserFiles，IP地址为：100.10.10.165/24，为MyClusterFiles添加文件共享，配置文件采用“SMB共享-快速”，共享名称为MyShare，存储位置为N:\，启用连续可用性和允许共享缓存，权限采用默认；

**（六）在主机Win2012-D2中完成WEB服务器1的部署**

1.安装IIS组件，创建www.chinaskills.com站点，在N:\MyShare文件夹内中创建名称为chinaskills.html的主页，主页显示内容“热烈庆祝2017年全国职业技能竞赛开幕”，同时只允许使用SSL且只能采用域名方式进行访问；

2.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，使用W3C记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；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、服务器端口号和方法；

**（七）在主机Win2008-D1中完成JSP+Tomcat运行环境的部署**

1.安装jdk，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，在DOS命令提示符下查看jdk版本并将显示的页面截图保存为jdk.jpg；

2.安装tomcat服务并启动，在浏览器输入[http:// 100.10.10.196:8080，将显示的页面截图保存为tomcat.jpg](http://x.x.x.x:8080，将显示的页面截图保存为tomcat.jpg)；

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，可以实现通过http:// 100.10.10.196显示指定的网页内容，打开chrome浏览器，按F12点击“移动设备模式”将浏览模式切换到手机模拟器，将微网站链接复制的链接粘贴在谷歌浏览器地址栏中，在谷歌浏览器页面显示的截图保存为mweb.jpg；

**Linux操作系统部分**

**一、在Server 1上完成如下操作:**

**（一）完成虚拟主机的创建**

安装虚拟机“Centos-A1”,具体要求为内存512MB，硬盘10GB；

**（二）在主机Centos-A1中完成DHCP和TFTP服务器的部署**

1.在此服务器上以YUM方式安装DHCP服务，创建超级作用域，名称为：mydhcpdomain，网段分别为100.10.10.0/24和100.10.11.0/24，地址池分别为100.10.10.2-100.10.10.5和100.10.11.2-100.10.11.10。指定DNS服务域名为dns.jnds.net，指定DNS服务器以及网关的IP地址信息，设置租约时间172800s，最大租约时间为259200s；

2.在此服务器上以YUM方式安装TFTP服务，并将服务根目录设置为/tftpboot；

**（三）在主机Centos-A1中完成E-MAIL服务器的部署**

1.在此服务器上安装配置sendmail服务，创建二个用户mail1,mail2；每个用户的邮箱大小为20MB，显示二个用户邮箱大小截图保存为quota.jpg，限定用户发邮件时，附件大小为5MB，附件大小截图保存为[ament](http://www.baidu.com/link?url=DwP6WPLzg8EdvAIUD_yWtGQkawfWSEbN7V5Jokfzhe9yo2IsuPw5YEhlxntordh-MGBqGvXONqC-p_uW7ZaoNg7xM4pCxoqc4fhcYKd8WAO&wd=&eqid=9c6ed544000849390000000657296f9e).jpg；

2.为每个员工创建邮箱账户，实现不同用户之间的正常通讯，用户密码为123，邮件服务器的域名后缀为jnds.net，邮件服务器要在所有IP地址上进行侦听；

3.创建名称为everyone的邮件列表，发给everyone@jnds.net的邮件，每个员工均可收到；

4.开启SMTP的SASL验证,允许通过身份验证的用户转发邮件；

5.使用Server1上安装的office outlook 2010软件发送邮件，mail1用户发给mail2用户，主题为“你好”，内容为“欢迎大家”,截图保存为success.jpg；

**二、在Server 2上完成如下操作：**

**（一）完成虚拟主机的创建**

1.安装虚拟机“Centos-B1”,具体要求为内存512MB，硬盘10GB；

2.安装虚拟机“Centos-B2”,具体要求为内存512MB，硬盘10GB；

**（二）在主机Centos-B1中完成磁盘管理的部署**

1.在“Centos-B1”中手动再添加两块SCSI硬盘，容量均为8G，分别将两块硬盘设置为一个主分区（2G容量）和两个逻辑分区（分别2G容量），并完成PV物理卷的初始化操作；

2.将/dev/sdb1及/dev/sdc5加入到卷组VG1中，其显示的逻辑卷名称为LV1，格式化为ext3文件系统，对应挂载目录为/volume，并针对/volume目录实现开机自动挂载；

3.针对现有的逻辑卷/dev/vg1/lv1实现在线扩容，将/dev/sdb5分区加入到已有的逻辑卷LV1中，实现目录/volume在线扩容2G容量，总容量达到6G；

4.利用分区/dev/sdb6及/dev/sdc1完成条带卷的设置，条带容量为8KB，建立的条带卷容量为2G，卷组名称VG1，条带卷名称为stripe1；

5.利用分区/dev/sdc6、/dev/sdb6及/dev/sdc1完成条带卷的设置，条带容量为64KB，建立的条带卷容量为3G，卷组名称VG1，条带卷名称为stripe2；

6.借助命令hdparm完成磁盘读写速度的测试，具体命令语法为“hdparm -t逻辑卷名称”，并将截图放置到hdparm.jpg；

1. **在主机Centos-B1中完成FTP服务器的部署**

1.配置FTP服务，创设FTP服务站点，绑定ftp服务地址为100.10.10.169，域名为[ftp.jnds.net](ftp://ftp.jnds.net)，站点主目录为 /var/ftp1，不允许匿名用户访问，开启ftp支持被动数据传输模式；

2.建立虚拟用户ftpuser1及ftpuseR1，密码和用户相同，用户的宿主目录为/home/vsftpd，实现ftpuser1用户具有上传和下载的权限，但不能删除文件，ftpuseR1用户可以下载，但不能上传和对文件进行改名；

**（四）在主机Centos-B2中完成主服务器的冗余备份**

实现Win2012-D1中DNS服务器的冗余备份，同时提供本域内主机名与IP地址的解析，此域名服务器的地址数据库需要Win2012-D1中定期更新；

**（五）在主机Centos-B2中完成NFS服务的部署**

1.配置NFS服务，按下表要求共享目录：

|  |  |
| --- | --- |
| 共享目录 | 共享要求 |
| /var/test | 100.10.10.0这个网段的用户具有读写权限，其它只读 |
| /var/tmp | 所有人都可以存取，root写入的文件还具有root的权限 |

2.创建用户nfsuser，当nfsuser在终端登录时，自动mount 共享的/var/test目录到/home/nfsuser/t，退出时自动umount，登录自动运行脚本内容截屏保存为nfs2-1.jpg；退出自动运行脚本内容截屏保存为nfs2-2.jpg；

**三、在Server 4上完成如下操作：**

**（一）在主机Centos-D1中完成密码的清除**

注：如果由于不会破解密码而无法实现后续试题，可自行安装一个Centos-D2的虚拟机系统，但需要扣除5分。

1.将标识为“Server 4上”的计算机上的已有虚拟机Centos-D1启动，请破解root的密码，并将新密码设置为chinaskills，将能体现破解密码的界面截图为pj.jpg；

2.为了防止管理员之外的人员再次破解root密码，请配置BOOT启动密码为：2017network，截图为boot.jpg；

**（二）在主机Centos-D1中完成BIND域名服务器及代理服务器的部署**

1.在此服务器中安装配置bind服务，负责区域“jnds.net”内主机解析，五台主机分别为mail.jnds.net、dns.jnds.net 、[www.jnds.net](http://www.jnds.net)、ftp.jnds.net、backups.jnds.net,做好正反向DNS服务解析, 正向解析成功保存为[forward](http://www.baidu.com/link?url=akd4ppR1Gsm8_GmxekHvRg4JrAfOs26iSeLgy_H4vBrOBD9nhMrCK3Ko5PUt_tmoF15V8iHXOfwDIo0yqvoOVwpGs1W39hh_7zwCHh7uOXKB1uib985OkOdbso96cQc1&wd=&eqid=b84e4c8a0003251d0000000657296878).jpg，反向解析成功保存为[reverse](http://www.baidu.com/link?url=uDsCaHWyw_0QJcd4isEfcFpq3MUZjxYExyF0kA_mM3PfnW5AacT7RQHonMMY6JF_VXjsXGjWV7kDsEiaE5JB5odIaxMwe1KRxAtCrPFMLF3&wd=&eqid=aa28c3710002ad650000000657296887).jpg；

2.安装并完成代理服务器squid的初始配置，使用8080作为代理服务端口，指定DNS服务器IP地址信息，使得squid服务器能够解析域名；

3.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；

4.针对主机100.10.10.212/24提供代理服务，为缓解请求队列忙碌，设置重定向器池进程数为20，并将缓存日志存放于/var/squid/cache.log中；

**（三）在主机Centos-D1中完成iptables的部署**

1.开启服务器的路由转发功能；

2.管理员为了防止公司的Linux服务器遭受SYN的攻击，请您帮助管理员实现防止同步包洪水、防止各种端口扫描、防止Ping洪水攻击（Ping of Death），三种方式中涉及的时间均为每秒1次，并将其进行保存到/etc/iptables文件中。