2023 年度湖南省“楚怡杯”职业院校技能竞赛

赛项规程

一、赛项名称

1.赛项名称：网络系统管理

2.赛项组别：高职高专组

3.赛项归属：电子信息大类

二、竞赛内容

1．竞赛任务

本赛项进行技能实操考核，需完成以下 3 个任务模块。

模块 A：网络构建模块（40%）

依据网络构建的服务需求，构建复杂的网络及服务，完成各类网络设备的配置与管理。根据行业认证要求，用户需求及设计要求，在各种网络设备上（路由器、数据中心交换机、出口网关、无线设备等）应用各种类型的服务配置，包括软件及硬件升级，设计并执行灾难恢复流程等。具体涉及到无线网络勘测与规划；设备基础信息配置；网络搭建与网络冗余备份方案部署；移动互联网搭建与网络优化；出口安全防护与远程接入等内容。

模块 B：Windows 环境模块（30%）

依据设计图纸要求，配置和管理 Windows 用户及应用服务器；在活动目录环境中实现用户、组和计算机账户统一管理，配置对共享文件夹的安全访问；为 Windows 远程管理安装和配置终端服务；创建控制用户桌面的设置等安全性的策略。

模块 C：Linux 环境模块（30%）

依据设计图纸配置系统网络连接，依据信息系统构建要求，完成基于 Linux 系统的企业信息化系统的构建；在符合 LPI2 技术水平规范要求的情况下，管理多台 Linux 服务的网络资源、存储资源、计算资源的分配与管理，提供安全有效的信息化系统平台的服务。

2．竞赛要求

（1）技术要求：参赛选手按照赛题要求，在设备上完成计算机网络搭建与调试、服务器配置与调试，并提交符合模板规范的有效 WORD 文件和对应的 PDF 文件。

（2）职业素养要求：注意赛场安全、有序组织和安排工作、规范操作、规范着装、尊重他人、爱护财物、保持环境整洁、遵守赛场纪律、严格自我管理。

三、竞赛方式

个人赛。

四、竞赛时量

比赛时量为 720 分钟。其中模块 A：网络构建为一场（240 分钟），模块 B：Windows 环境为一场（240 分钟） C：Linux 环境为一场（240 分钟）。

五、名次确定办法

比赛按照竞赛成绩（保留小数点后两位）从高到低排序确定名次，不设并列名次。如出现参赛队总分相同情况,按照 A、B、C 模块顺序的得分高低排序。即总成绩相同的情况下比较 A 模块的成绩，A 模块成绩高的排名优先；如果 A 模块成绩也相同，则按 B 模块的成绩进行排名；以此类推完成相同成绩的排序。如果 A、B、C 各模块分值均相同，则查看文档撰写规范的分值进行排序。

六、评分标准与评分细则

1．评分标准

竞赛满分为 1000 分。总成绩为网络构建（40%）、Windows 环境（30%）、Linux 环境（30%）得分之和。

各项评分均以参赛队伍提交的文档为准，选手提交文档错误（例如没按说明提交文档、文档内容粘贴错误等）将按照评分细则扣分。若在规定时间内，因选手原因未及时提交文档，则无相应分数。

2．评分细则

表 1　评分细则

考试模块	考查点	描述	权重
网络构建	无线网络勘测与设计	绘制平面图、AP 点位图、热图、设备清单、总价表、综合布线工程的水平布线图、机柜设备安装图、配线架标签、物料清单	40%
	设备基础信息配置与验证	根据拓扑规划，根据设备在实际案例中的位置，方位，配置设备命名规范；配置设备的远程访问，接口描述，规范密码标准等；网络设备密码恢复与重置；案例工程实施，根据软件版本发布规定升级到专属的软件版本；使用交换机配置安全技术实现网络安全性；网络联调测试验证。	
	网络搭建与网络冗余备份方案部署	使用交换机配置虚拟局域网技术，实现网络广播隔离与区域划分；使用交换机配置 DHCP 中继，实现用户动态获取地址；使用交换机配置生成树技术，实现网络冗余与备份；使用交换机配置路由技术，实现网络连通；根据需求描述及对功能的理解，完成赛题要求的路由器配置，包括静态路由、RIP、OSPF、BGP 等，实现网络连通；配置和应用常用的广域网技术；使用交换机配置高可靠性技术，实现链路快速收敛；使用交换机配置 VRRP 技术，实现网关冗余与备份；使用交换机配置 VSU 技术，实现数据中心虚拟化和高可靠。	
	移动互联网搭建与网优	使用无线控制器配置转发模式，实现用户数据本地或集中转发方式；使用无线控制器创建 SSID，实现无线用户关联 SSID；使用无线控制器配置热备功能，实现双 AC 负载均衡；实现无线认证，安全准入；使用无线控制器配置 AP 隔离，实现无线用户二层隔离；使用无线控制器针对 VIP 用户隐藏 SSID，禁用广播功能；使用无线控制器配置限制，实	

		现特性用户流量限速；使用无线控制器配置数据加密，实现用户通信安全。	
	出口安全防护与远程接入	使用出口网关配置 NAPT 及时间控制，实现用户访问互联网；使用出口网关 Web Portal 认证，实现用户身份认证；使用出口网关流量控制，实现特定业务速率限制；使用出口网关行为审计，实现内网用户数据安全审计；使用出口网关 VPN，基于行业应用场景，实现外网用户安全访问内网服务，实现隧道技术，包括不限于 SSL VPN，IPSEC VPN 等。	
	职业规范与文档	赛场安全、人身安全、环境保持、着装规范赛场纪律及其他；提交的文件有效、文件名称符合赛题要求、文件内容排版规范。	
Windows 环境	基础配置	正确按照需求在安装系统时进行分区设置，并成功安装系统； 按照要求正确设置桌面、控制面板、文件夹选项、网络连接和桌面管理参数； 按照要求正确创建本地用户账户、本地组，合理分配本地用户和组的权限； 正确设置文件和文件夹的权限，创建、使用和管理共享文件夹操作正确。	30%
	应用服务搭建	活动目录安装正确，主域控制器配置正确，辅助域控制器配置正确，域、组织单元规划合理，域策略配置正确； DNS 服务安装正确，正向解析域名正确，反向解析 IP 正确； DHCP 服务安装正确，客户机能获取正确的 IP、子网掩码、网关、DNS 地址，排除地址、保留地址设置正确； IIS 服务安装正确，正常发布基于 IIS 的各项服务； WEB 服务安装正确，同一服务器上多个网站运行正常，网站主目录路径设置正确，用户访问控制策略合理； WEB 服务器 SSL 安全证书配置，完成网站安全访问； FTP 服务安装正确，用户访问控制策略合理，正常上传/下载文件。	
	职业规范与文档	赛场安全、人身安全、环境保持、着装规范赛场纪律及其他；提交的文件有效、文件名称符合赛题要求、文件内容排版规范。	
Linux 环境	基础配置	能按照设计要求完成 Linux 操作系统的安装和部署，完成服务器网卡参数、磁盘分区等相关设置和配置，能用系统信息类命令查看系统时间、内存使用、硬盘分区及使用、目录硬盘占用等信息，确保系统正常可用。 能用命令方式创建、修改、删除、停用、启用、切换本地用户账户，能用命令方式创建、修改、删除本地组。	30%

		能用文件和目录类命令创建、修改、删除、查找、查看、复制、移动，压缩、解压文件和文件夹，查看、修改文件及文件夹权限，设置文件的拥有者，能用命令完成 Linux 下文件系统的创建、挂载与卸载；。 能用进程管理类命令查看和控制进程、挂起和回复进程等管理操作； 能用 RPM 和 YUM 方式安装、管理、卸载软件；能用命令对磁盘进行正确分区、配置磁盘配额，挂载光盘，建立和维护动态磁盘卷；定时执行命令；能用 LVM 创建、管理物理卷、卷组、逻辑卷； 能管理防火墙，设计并配置合理的防火墙放行策略，保障系统安全。	
	应用服务搭建	能安装 DNS 服务器，创建和管理正向和反向查找区域、DNS 资源记录，从而实现域名的正确解析。 能安装与配置 Samba 服务器，实现不同系统不同用户之间的文件共享。 能安装 DHCP 服务器，能正确配置 DHCP 服务器的地址池、排除地址、保留地址等 DHCP 选项，从而实现给网络中主机分配正确的 TCP/IP 参数。 能安装 Apache 服务器，能在一台服务器上建立多个网站，实现网站服务器用户访问控制、目录访问控制、日志记录等功能性和安全性配置与管理，从而实现网站的安全、稳定运行与可靠访问。 能安装 FTP 服务器，能实现文件传输服务器用户访问控制、目录访问控制等功能性和安全性配置与管理，从而实现文件传输服务器的安全、稳定运行与可靠访问。 能安装 MySQL 服务器，能实现数据库管理员密码的修改、数据库用户的添加与权限的修改、数据库的创建、数据表的创建、数据的增删查改、数据库的备份与还原，从而实现数据库服务器的安全、稳定运行与可靠访问。	
	职业规范与文档	赛场安全、人身安全、环境保持、着装规范赛场纪律及其他；提交的文件有效、文件名称符合赛题要求、文件内容排版规范。	
总计		合计	100 %

七、赛项相关设施设备技术参数

1．赛项软件平台

赛点提供已经安装好操作系统的 PC 计算机，用以组建竞赛所需网络，并安装好常用的工具应用软件。

表 2　软件

序号	软件名称	说明	单位	数量
1	Windows Server 2019	Data center中文版	套	1
2	Windows 10	Enterprise中文版	套	1
3	CentOS Linux	Version 7 以上	套	1
4	国产操作系统UOS	uniontechos-server-20	套	1
5	SDN控制器	OpenDaylight	套	1
6	虚拟化云平台	VMware Workstation Pro 16 以上	套	1
7	VPNClient	OPENVPN 2.4 以上	套	1
8	Zabbix-Agent	Zabbix-Agent 3.4 以上	套	1
9	Office	Version 2013 以上	套	1
10	Putty	Version 0.7 以上	套	1
11	无线地勘系统	无线地勘系统	套	1
12	解压缩软件	RAR4.0 以上	套	1
13	PDF 阅读器	Adobe Reader X1 11以上	套	1
14	网络调试工具	SercureCRT8.1以上	套	1
15	截图工具	FScapture6.5以上	套	1
16	FTP 客户端	FlashFXP5.4 以上	套	1
17	Firefox Browser	Firefox 85 以上	套	1

2．赛项相关设备与器材

（1）个人计算机

表 3　个人电脑配置

序号	类别	设备	厂商	配置要求	数量
1	硬件	个人计算机	国产	操作系统：Windows 10 或更新版本 处理器：I7 及以上 内存：16G 或 32GB 硬盘：500GB 或以上 外设：U 口不少于 4 个，自带串口用于连接调试线缆 网卡：有限千兆以太网 1 个，无线网络适配器 1 个 显示器：分辨率 1024x768 像素或以上	2 台

（2）网络设备

表 4　网络设备清单

序号	设备名称	型号	单位	数量
1	路由器	多功能路由器	台	3
2	交换机（1）	数据中心交换机（带电源）	台	2
3	交换机（2）	三层可控交换机（带电源）	台	3
4	交换机（3）	二层可控交换机（带电源）	台	2
5	网关	安全设备（含防火墙功能）（带电源）	台	2
6	无线控制器	无线控制器（带电源）	台	2
7	无线接入设备	胖、瘦一体 AP（带电源）	台	3
8	配件（1）	串口接口模块	块	6
	配件（2）	串口线缆对	对	3
	配件（3）	万兆模块及配对线缆	块	2
	配件（4）	配置线缆	条	1

备注：具体设备由赛点提供。

八、选手须知

1．选手自带工具清单

所有工具由举办方提供，选手无需自带工具。

2．主要技术规程及要求

表 5　技术规范统计表

序号	标准号	中文标准名称
1	教育部职业教育与成人教育司	高等职业学校专业教学标准（试行）—电子信息大类
2	GB50174-2008	电子信息系统机房设计规范
3	GB21671-2008	基于以太网技术的局域网系统验收测评规范
4	GB/T22239-2008	信息系统安全等级保护基本要求

3．选手注意事项

（1）参赛选手不得穿戴有学校标志的工作服或校服进入赛场，也不得以任何方式透露参赛学校和个人信息，如有违反则取消参赛资格。

（2）参赛选手不允许携带任何书籍和其他纸质资料（相关技术资料的电子文档由组委会提供），不允许携带通讯工具和存储设备（如 U 盘）。

（3）比赛期间，不允许参赛选手接受指导教师的指导。

（4）参赛选手入场后，应与赛场工作人员共同确认操作条件及设备状况，确认材料、工具等。竞赛期间参赛选手原则上不得离开比赛场地。凡在竞赛期间提前离开的选手，不得返回赛场。

（5）竞赛时，各参赛队自行决定分工、工作程序和时间安排。选手在接到开赛信号后才能启动操作设备。在指定工位上完成竞赛项目，严禁作弊行为。

（6）竞赛期间，选手饮水等由赛场统一提供，不得自带。选手休息、饮食或如厕时间均计算在比赛时间内。

（7）参赛选手应严格遵守赛场规章、操作规程和工艺准则，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛。

（8）竞赛过程中，因操作失误或安全事故不能进行比赛的（例如因线缆连接发生短路导致赛场断电、造成设备不能正常工作），现场裁判员有权中止该队比赛。由于选手错误操作造成的设备损坏故障，需要承担赔偿。

（9）在竞赛中如遇非人为因素造成的设备故障，经裁判员、裁判长确认后，补足排除故障的时间。

（10）参赛队如欲提前结束比赛，应向现场裁判员举手示意，由裁判员记录竞赛终止时间。竞赛终止后，不得再进行任何与竞赛有关的操作。

（11）竞赛时间到，参赛队选手应立即结束操作，按照竞赛要求和赛题要求提交竞赛成果，禁止在竞赛成果上做任何与竞赛无关的记号。

（12）竞赛操作结束后，参赛队要确认成功提交竞赛要求的文件，裁判员在竞赛结果的规定位置做标记，并与参赛队一起签字确认。

（13）在竞赛过程中，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，由裁判按照规定扣减相应分数并且给予警告，情节严重的取消竞赛资格，竞赛成绩记 0 分，选手退出比赛现场。

（14）在竞赛期间，未经组委会批准，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。

4．竞赛直播

1.赛点提供全程无盲点录像。

2.可在赛点指定区域通过网络监控观摩比赛。

九、样题（附）

2023 年度“楚怡杯”湖南省职业院校技能竞赛

高职高专组电子与信息类网络系统管理赛项

[时量：720 分钟，试卷号：　]

（样卷）

竞

赛

任

务

书

场次号：_____　机位号（工位号、顺序号）：_____。

2022 年 12 月　日

模块 A：网络构建模块（40%）

一、考试说明

本模块比赛时间为 4 小时。请合理分配竞赛时间。请仔细阅读以下要求。

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。

2. 操作过程中，需要及时保存配置。比赛结束后，所有设备、计算机保持运行状态，不要拆动硬件连接。

3. 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。

4.严格按照“网络构建答题卡.docx”文档格式要求，制作输出竞赛结果文件。同时，另存一份“PDF 格式文档”。

5.在每台设备上使用 show running-config 命令，将该命令下显示的结果，分别保存为独立的“*.txt”文件中。其中，文件名要以设备的编号命名。并把所有的“*.txt”文件，集中存放在新建的“设备配置”文件夹下。

6.考生所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。

二、任务描述

随着业务的发展，现在要对星城银行进行全网改造，为其它区域的网络提供高效的保障服务。同时，星城银行还针对各个分支行、网点的网络进行升级、改造和优化。你做为火星公司网络工程师前往并完成网络规划与建设任务。

三、任务清单

（一）基础配置

1.根据附录 1 拓扑图及附录 2 地址规划表，配置设备接口信息。

2.需要在所有的网络设备上，都需要开启 SSH 服务，以保障网络设备的安全。其中，用户名密码分别为 admin、admin1234。特权密码为 admin1234。

3.网络管理员计划增设网管平台，网管平台的 IP 规划为 192.2.90.25/24。配置所有网络设备的 SNMP 消息报告机制。其中，向主机 192.2.90.25/24 发送 Trap 消息版本采用 V2C。读写的 Community 为“admin”。只读的 Community 为“public”。开启 Trap 消息通告。

（二）有线网络配置

1.在全网 Trunk 链路上做 VLAN 修剪。

2.在 S5、S6 的 Gi0/10-Gi0/15 端口上启用端口保护。

3.在搭建完成的虚拟交换机 S5-S6 的 Gi1/0/10-Gi1/0/15 端口上启用端口保护。

4.在连接 PC 机端口上开启 Portfast 和 BPDUguard 防护功能。

5.端口被检测异常进入 Err-Disabled 状态，再过 240 秒后会自动恢复（基于接口部署策略），重新检测是否有环路。交换机端口检测到环路，处理的方试为 shutdown-Port。

6.省行 DHCP 服务器安装在 S2 交换机上,分配以下 3 个网段地址：省行办公有线用户（192.3.10.0/24）、省行办公区 AP（192.3.50.0/24）、省行办公区无线（192.3.60.0/24）。交换机 S5-S6 上，部署 DHCP 安全防护功能，使用“Snooping +IP Source Guard+ARP-CHECK”技术。按照要求为无线用户和 AP 分配地址和管理地址，其

中无线 AP 租约为永久，无线用户租约设为 0.5 天。
7.ZR 金融公司 DHCP 服务器搭建于 AP3 上，按照地址规划表规划地址。
8.在交换机 S3、S4、AC1、AC2 上配置 MSTP。要求来自 VLAN90 中的数据流经过 S3 交换机转发，一旦 S3 交换机失效时经过 S4 交换机转发。要求来自 VLAN60 和 VLAN 100 数据流经过 S4 交换机转发，S4 失效时经过 S3 交换机转发。配置 MSTP 参数要求：region-name 为 test。revision 版本为 1。实例 1 包含 VLAN90。实例 2 包含 VLAN60,VLAN100。
9.配置 S3 交换机作为实例 1 的主根、实例 2 的从根。配置 S4 交换机作为实例 2 的主根、实例 1 的从根。其中，主根交换机的优先级为 4096。从根交换机的优先级为 8192。
10.在交换机 S3、S4 连接连接 AC1 和 AC2 的接口上，启用“TC-IGNORE”功能。
11.在交换机 S3 和 S4 上配置 VRRP，实现网络中的主机的网关冗余，所配置的参数要求如表 1 所示。其中，在交换机 S3、S4 上设置各 VRRP 组中的高优先级设置为 150，低优先级设置为 120。

表 1　S3 和 S4 的 VRRP 参数表

VLAN	VRRP 备份组号（VRID）	VRRP 虚拟 IP
VLAN60	60	192.3.60.254
VLAN90	90	192.2.90.254
VLAN100	100	192.2.100.254

12.在交换机 S3 与 S4 之间部署 2 条互联链路（Gi0/21、Gi0/22），采取 LACP 动态聚合模式配置二层链路聚合。
13.部署交换机 S5 和 S6 之间的 Te0/27-28 端口作为 VSL 链路，使用网络虚拟化技术，实现核心网络的虚拟化。其中：设置 S5 交换机为主交换机。设置 S6 交换机为备用交换机。规划交换机 S5 和 S6 之间的 Gi0/22 端口，作为双主机检测链路，配置基于 BFD 的双主机检测。需要配置主交换机参数信息为：Domain id：1。Switch id:1;priority 150; description:Access-Switch-Virtual-Switch1
需要配置备交换机设备参数信息为：Domain id：1。Switch id:2。priority 120。description:Access-Switch-Virtual-Switch2。
14.省行核心区与服务器区（S1、S2、S3、S4）部署 OSPF 100，使用单区域（区域 0）部署，省行核心区与外联区（S1、S2、EG1）部署 OSPF 100，规划区域为 10，重发布路由进 OSPF 中使用类型 1。
15.核心区（S1、S2）使用自治域号为 64520，互联区及超辰支行（R1、R2、R3）自治域号为 64521，省行核心区与互联区（S1、S2、R1、R2）使用互联接口地址部署 EBGP，省行及各支行/网点（R1、R2、R3）使用 LOOPBACK 0 地址部署 IBGP，其底层 IGP 协议使用静态路由协议。
16.省行核心区与办公区（S1、S2）部署静态路由协议，省行服务器区中无线控制器 AC1 和 AC2 设备，与两台交换机 S3 和 S4 之间部署静态路由协议，Internet 区域（EG1、EG2、R3）均使用静态路由协议。
17.使得生产性业务的传输主路径为 R3-R1-S1-S3。办公性业务的传输主路径为 R3-R2-S2-S4, 并且要求来回路径保持一致，主链路或主设备故障时，可无缝切换到备用链路或设备上，在使用 BGP 路由通告网络中，交换机 S1、S2 和路由器 R3 通过 Network 引入明细路由。禁止将 IGP 路由以重发布形式导入 BGP 自制系统中。
18.使用 BGP 选路策略中，要求只能在省行核心区 S1、S2 交换机上部署。其中，凡涉及 MED 值调整，要求其值必须是 10、15、20。凡涉及 LP 值调整，要求值必须是 200、300。此外，省行生产流量定义为 ACL1。省行办公流量定义为 ACL2。

支行生产流量定义为 ACL11。支行办公流量定义为 ACL12，在部署 OSPF 各路由图以及各接口中，凡涉及 COST 值的调整，要求其值必须为 5 或 10。

（三）无线网络配置

现在对星城银行进行无线网络优化项目拟投入 18 万元(网络设备采购部分）平面布局如图 1 所示。

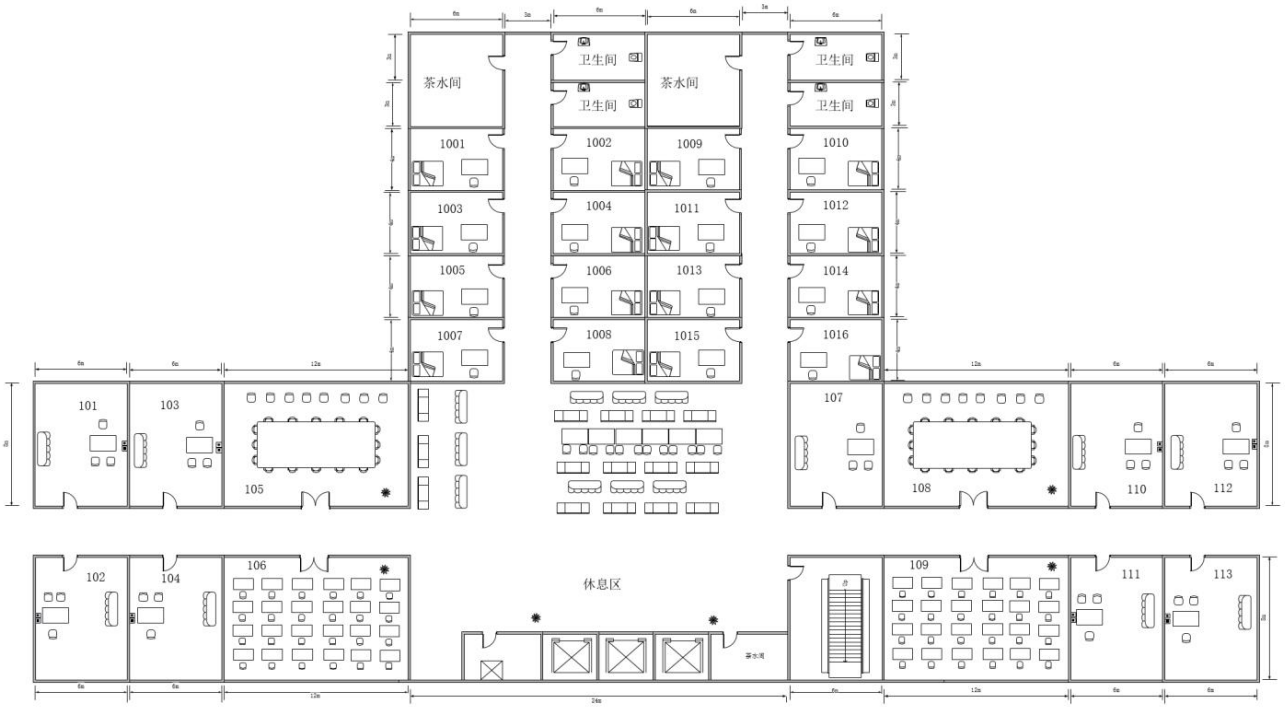


图 1 平面布局图

1.绘制 AP 点位图（包括：AP 型号、编号、信道等信息，其中信道采用 2.4G 的 1、6、11 三个信道进行规划，洗手间、茶水间无须覆盖）。

2.使用无线地勘软件，输出 AP 点位图的 2.4G 频道的信号仿真热图（仿真信号强度要求大于-65db）。

3.输出该无线网络工程项目设备的预算表，网络设备型号和价格依据表 2。

表 2 无线产品价格表

产品型号	产品特征	传输速率（2.4G/最大）	推荐/最大带点数	功率	价格（元）
AP1	双频双流	300M/1.167G	32/256	100mw	6000
AP2	双频双流	300M/600M	32/256	100mw	11000
AP3	单频单流	150M	12/32	60mw	2500
线缆 1	10 米馈线	N/A	N/A	N/A	1600
线缆 2	15 米馈线	N/A	N/A	N/A	2400
天线	双频单流/单频单流	N/A	N/A	N/A	500
Switch	24 口 POE 交换机	N/A	N/A	240w	15000
AC	无线控制器	6*1000M	32/200	40w	50000

4.在省行办公区的无线部署中，无线 AP 采用 FIT AP 架构，所有 AP（AP1）关联到省行服务器区 AC，在省行办公区无线部署中，使用 S2 交换机作为无线用户

（VLAN 60）和无线 FIT AP（VLAN 50）的 DHCP 服务器，在省行的业务区部署无线网络，创建省行业务区中内网的 SSID 为：Admin_SHBGQ_XX(XX 现场提供)。WLANID 为 1。AP-GROUP 为 Admin_SHBGQ。其中，内网无线用户关联 SSID 后，可自动获取 VLAN60 地址，在省行办公区无线部署中，配置省行办公区 AP 采用集中式转发。

5.超辰支行无线网络架构采用 FIT AP+AC 的方案，区域内所有 AP（AP2）都关联到 VAC 进行管理，超辰支行使用 R3 路由器作为无线生产用户（VLAN 10）、办公用户（VLAN 60）和无线 FIT AP（VLAN 50）的 DHCP 服务器，超辰支行无线网络部署中，创建生产用户 SSID 为：Admin_CCZH_SS_XX(XX 现场提供)。WLANID 为 2。AP-GROUP 为 Admin_CCZH。生产用户关联 SSID 后，可自动获取 VLAN10 地址。创建超辰支行办公用户 SSID 为：Admin_CCZH_BG_XX(XX 现场提供)。WLANID 为 3。AP-GROUP 为 Admin_CCZH。生产用户关联 SSID 后可自动获取 VLAN60 地址，超辰支行无线网络部署中，超辰支行 AP 采用本地转发。

6.在无线网络中部署 AC 冗余，实现备份。两台 AC 采用主备形式。其中，AC1 为省行办公区 AP 主设备。AC2 为超辰支行 AP 主设备，两 AC 互为备份。

7.在 ZR 金融公司部署胖 AP 设备，用户网关及 DHCP 服务器均部署在 AP3 上。AP3 与 EG2 之间使用静态路由协议实现连通，配置 AP3 设备，在 AP3 上配置 SSID(WLAN-ID 4)为 Admin-Fat_XX(XX 现场提供)，内网无线用户关联 SSID 后，可自动获取 195.1.60.0/24 网段地址。

8.5.8G 频段的 Coverage-area-control 功率调整为 17db。2.4G 频段的 Coverage-area-control 功率调整为 10db，关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入，调整 2.4G 频段射频卡 powerlocal 功率数值为 20。调整 5.8G 频段射频卡 powerlocal 功率数值为 100，调整 5.8G 频段的射频卡无线频率带宽至 40MHz。

9.限制 3 台 AP 的每个射频卡最大带点人数为 15 人，通过 Fit AP 方式接入无线网络时，采用 WPA2 加密方式，加密密码为 XX(现场提供)，通过 Fat AP 方式接入无线网络时，采用 WEB 认证方式，认证用户名、密码为 XX(现场提供)。

（四）出口网络配置

1.省行的外联区出口网关 EG1 上进行 NAT 配置，实现省行业务区办公网络（VLAN 60、VLAN 110）通过 NAPT 方式，将内网 IP 地址转换到互联网接口上。其中，NAT 地址池的地址为 201.1.1.3/29-201.1.1.5/29。生产网络及其他地址均不允许访问互联网，转换 ACL 定义为 ACL 120。

2.省行外联区出口网关 EG1 上配置，使省行的核心交换机 S1 的 HTTP 服务器（IP 为 11.1.0.1）的 HTTP 服务（TCP 80）将其地址映射至运营商线路上，映射地址为 201.1.1.6，映射端口 58888。

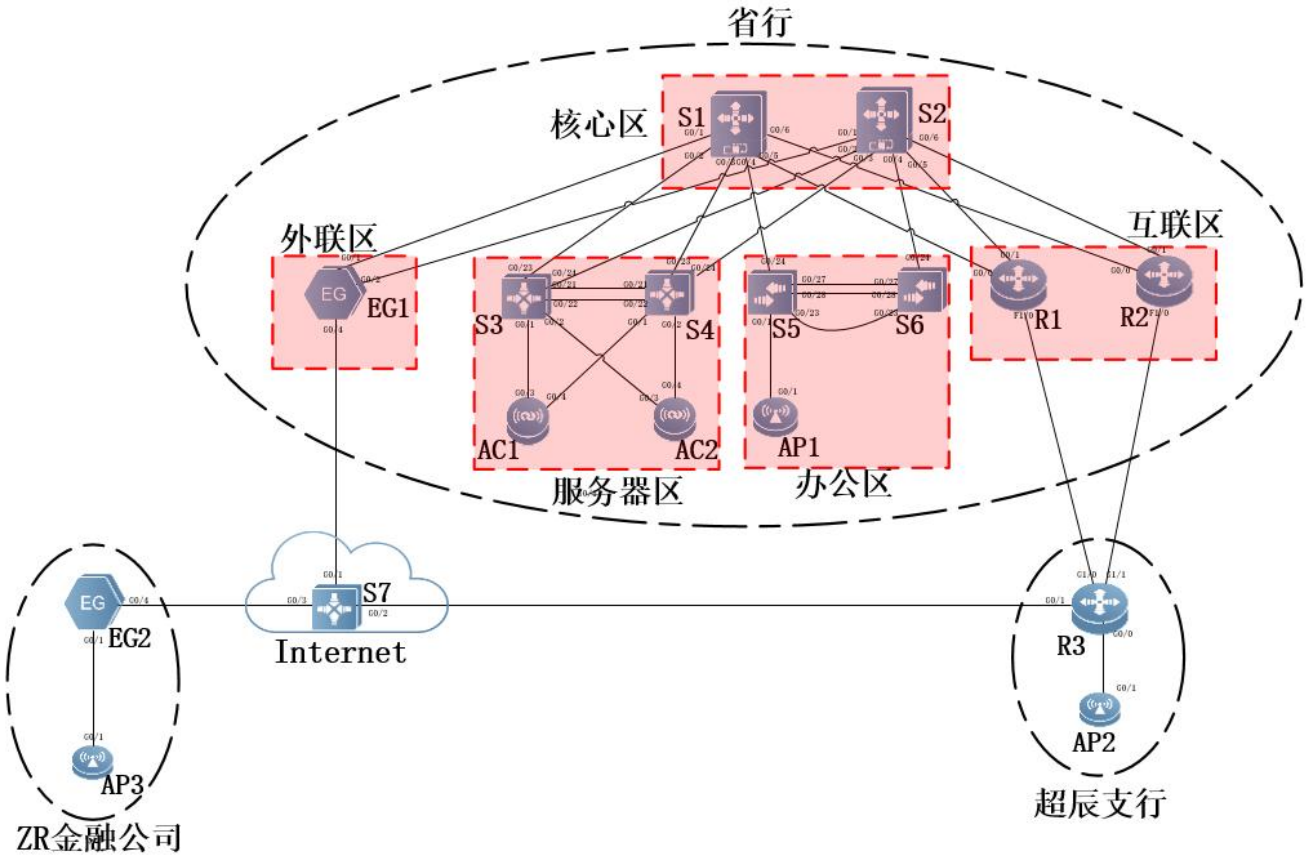
3.超辰支行部署了一条 Internet 出口，实现支行办公用户访问 Internet。正常情况下，生产用户不允许访问 Internet,ALC 编号为 101。其中：超辰支行出口路由器 R3 上 NAT 地址池的地址为 202.1.1.3/29-201.1.1.4/29。

4.ZR 金融公司出口网关 EG2 上进行 NAT 配置，实现其无线用户能访问 Internet，NAT 地址池与 EG2 的 Gi0/4 接口 IP 相同。

5.在网关 EG1 上启用 Web Portal 认证服务。创建两个认证用户，其用户名/密码分别为：user1/user1、user2/user2，在省行的无线办公用户（VLAN 60）上，需进行 WEB 认证方式访问互联网，在省行有线办公用户（VLAN 110），不需在 EG 上进行 WEB 认证，即可访问互联网，在出口网关 EG2 上，实施基于网站访问、邮件收发、IM 聊天、论坛发帖、搜索引擎等多应用，启用审计功能，配置 EG2 设备安

全防护，要求从周一到周六的工作时间 09：00—17:00（命名为 work）内，阻断并审计 P2P 应用软件使用,审计策略名称定义为 P2P。
6.在网络安全出口设备 EG2 与 R3 出口网关之间，启用 IPSec VPNOver GRE.配置 IPSec 使用静态点对点模式，esp 隧道模式封装协议，isakmp 策略定义加密算法采用 3des，散列算法采用 md5，预共享密码为 admin，DH 使用组 2。转换集 myset 定义加密验证方式为 esp-3des esp-md5-hmac，感兴趣流 ACL 编号为 103，加密图定义为 mymap。

附录 1：拓扑图


省行
核心区
S1
S2
外联区
EG
EG1
S3
S4
S5
S6
互联区
R1
R2
AC1
AC2
AP1
服务器区
办公区
EG
EG2
S7
Internet
R3
AP2
AP3
ZR金融公司
超辰支行

附录 2：地址规划表

设备	接口或 VLAN	VLAN 名称	二层或三层规划	说明
S1	Gi0/1	\	10.1.1.1/30	互联地址
	Gi0/2	\	10.1.2.1/30	互联地址
	Gi0/3	\	10.1.2.5/30	互联地址
	Gi0/4	\	10.1.3.1/30	互联地址
	Gi0/5	\	10.1.4.1/30	互联地址
	Gi0/6	\	10.1.4.5/30	互联地址
	Loopback 0	\	11.1.0.1/32	——
S2	Gi0/1	\	10.1.1.5/30	互联地址
	Gi0/2	\	10.1.2.9/30	互联地址
	Gi0/3	\	10.1.2.13/30	互联地址
	Gi0/4	\	10.1.3.5/30	互联地址
	Gi0/5	\	10.1.4.9/30	互联地址
	Gi0/6	\	10.1.4.13/30	互联地址
	Loopback 0	\	11.1.0.2/32	——
EG1	Gi0/1	\	10.1.1.2/30	互联地址
	Gi0/2	\	10.1.1.6/30	互联地址
	Gi0/4	\	201.1.1.2/29	ISP 地址
	Loopback 0	\	11.1.0.10/32	——
S3	VLAN 90	Server	192.2.90.252/24	生产服务器地址 Gi0/5-15
	VLAN 60	Wireless	192.3.60.252/24	办公区无线用户地址
	VLAN 100	Manage	192.2.100.252/24	设备管理地址
	Gi0/23	\	10.1.2.2/30	互联地址
	Gi0/24	\	10.1.2.10/30	互联地址
	Loopback 0	\	11.1.0.3/32	——
S4	VLAN 90	Server	192.2.90.253/24	生产服务器地址 Gi0/5-15
	VLAN 60	Wireless	192.3.60.253/24	办公区无线用户地址
	VLAN 100	Manage	192.2.100.253/24	设备管理地址
	Gi0/23	\	10.1.2.6/30	互联地址
	Gi0/24	\	10.1.2.14/30	互联地址
	Loopback 0	\	11.1.0.4/32	——
AC1	VLAN 100	Manage	192.2.100.1/24	设备管理地址
	Loopback 0	\	11.1.0.5/32	——
AC2	VLAN 100	Manage	192.2.100.2/24	设备管理地址
	Loopback 0	\	11.1.0.6/32	——
S5-S6 (VSU)	VLAN 110	Office-Wire	192.3.10.254/24	办公/有线用户地址 Gi1/0/6 至 Gi1/0/20, Gi2/0/6 至 Gi2/0/20
	VLAN 150	APManage_BGQ	192.3.50.254/24	业务区 AP 管理地址 Gi1/0/1 至 Gi1/0/5, Gi2/0/1 至 Gi2/0/5
	VLAN 1301	Connect-S1	10.1.3.2/30	互联地址 Gi1/0/24
	VLAN 1302	Connect-S2	10.1.3.6/30	互联地址 Gi2/0/24
R1	Gi0/0	\	10.1.4.2/30	互联地址
	Gi0/1	\	10.1.4.10/30	互联地址

	VLAN101	\	10.2.1.1/30	Fa1/0 成员口
	Loopback 0	\	11.1.0.7/32	——
R2	Gi0/0	\	10.1.4.6/30	互联地址
	Gi0/1	\	10.1.4.14/30	互联地址
	VLAN201	\	10.2.1.5/30	Fa1/0 成员口
	Loopback 0	\	11.1.0.8/32	——
R3	VLAN101	\	10.2.1.2/30	Gi1/0 成员口
	VLAN201	\	10.2.1.6/30	Gi1/1 成员口
	Gi0/0.10	Production	194.2.10.254/24	超辰支行生产用户
	Gi0/0	APManage_CCZH	194.3.50.254/24	超辰支行 AP 管理
	Gi0/0.60	Office	194.3.60.254/24	超辰支行办公用户
	Gi0/1	\	202.1.1.2/29	ISP 地址
	Loopback 0	\	11.1.0.9/32	——
EG2	G0/1	\	10.6.1.1/30	互联
	Gi0/4	\	203.1.1.2/29	互联地址
	Loopback 0	\	11.1.0.11/32	——
AP3	VLAN60	\	195.1.60.254/24	用户地址
	Gi0/1	\	10.6.1.2/30	互联
S7	Gi0/1	\	201.1.1.1/29	ISP 地址
	Gi0/2	\	202.1.1.1/29	ISP 地址
	Gi0/3	\	203.1.1.1/29	ISP 地址

模块 B：Windows 环境

一、竞赛简介

1. 请认真阅读以下指引！
2. 比赛共 4 个小时，你必须自行决定如何分配你的时间。
3. 当比赛结束时，离开时请不要关机您的虚拟机。
4. 如果没有明确要求，请使用“Chinaskill23”作为默认密码。

二、竞赛注意事项

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。
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. 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，不要拆动硬件连接。
4. 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。
5. 裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，不得以任何形式体现参赛院校、工位号等信息。

三、竞赛结果文件的提交

按照题目要求，提交符合模板的 WORD 文件以及对应的 PDF 文件（利用 Office Word 另存为 pdf 文件方式生成 pdf 文件），所有截图建议除了配置文件截图外，还需要截功能测试的图，能在终端上测试的就一定要在终端上测试并截图，否则功能测试部分不得分。

四、初始化环境

1.默认账号及默认密码

Username: Administrator
Password: Chinaskill23!
Username: demo
Password: Chinaskill23!
注：若非特别指定，所有账号的密码均为 Chinaskill23!

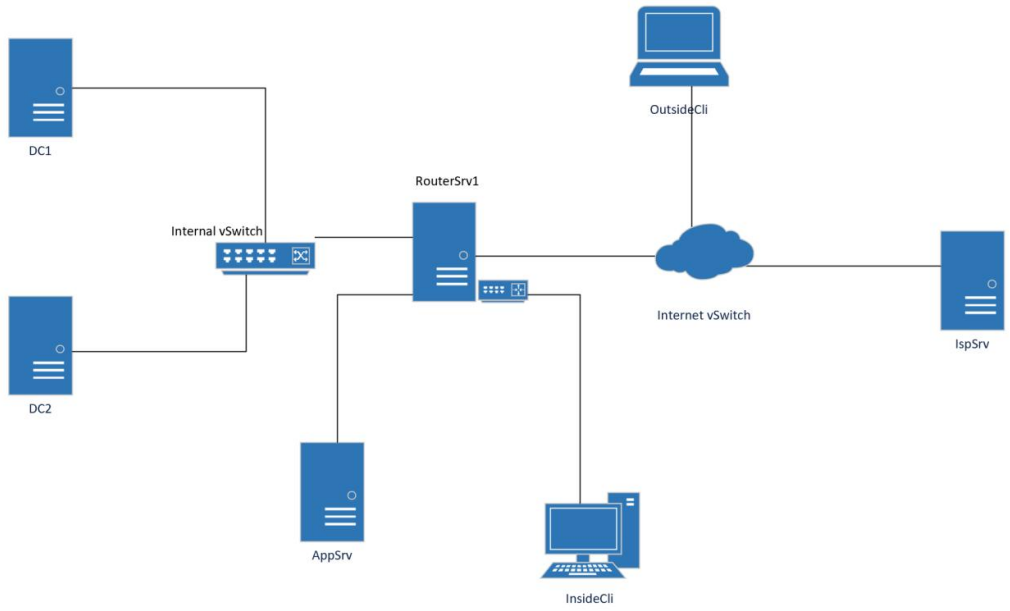
2.操作系统配置

Region: China
Locale: English US (UTF-8)
Key Map: English US
注意：当任务是配置 TLS，请把根证书或者自签名证书添加到受信任区。

五、项目任务描述

你作为一个微软高级认证的技术工程师，被指派去构建一个公司的内部网络，要为员工提供便捷、安全稳定内外网络服务。你必须在规定的时间内完成要求的任务，并进行充分的测试，确保设备和应用正常运行。任务所有规划都基于 Windows 操作系统，请根据网络拓扑、基本配置信息和服务需求完成网络服务安装与测试，网络拓扑图和基本配置信息如下：

1.拓扑图



2.网络地址规划

服务器和客户端基本配置如下表：

主机名	域名	IP 地址	DNS	网关
DC1	chinaskills.com	192.168.100.100/24	127.0.0.1	192.168.100.254
DC2	chinaskills.com	192.168.100.200/24	127.0.0.1	192.168.100.254
AppSrv	chinaskills.com	192.168.200.100/24	192.168.100.100 192.168.100.200	192.168.200.254
RouterSrv1	chinaskills.com	192.168.100.254/24 192.168.0.254/24 192.168.200.254/24 100.100.100.251/24	192.168.100.100	100.100.100.254
IspSrv	保持工作组状态	100.100.100.100/24	127.0.0.1	无
InsideCli	chinaskills.com	192.168.0.0/24(dhcp)	192.168.100.100 192.168.100.200	192.168.0.254
OutsideCli	保持工作组状态	100.100.100.10/24	100.100.100.100	100.100.100.254

六、项目任务清单

（一）服务器 IspSrv 上的工作任务

1. 互联网访问检测服务器

- 为了模拟 Internet 访问测试，请搭建网卡互联网检测服务。

2. Web Print

- 添加一台虚拟打印机，名称为“CS-Print”，发布到 AD 域。
- 客户端们都能够通过访问“https://print.worldskills2023.cn/”查看打印机，证书由 WORLDSKILLS2023-ROOTCA 进行签署颁发。

（二）服务器 RouterSrv1 上的工作任务

1. 路由功能

- 安装 Remote Access 服务开启路由转发，为当前实验环境提供路由功能。
- 启用网络地址转换功能，实现内部客户端访问互联网资源。
- 配置网络地址转换，允许互联网区域客户端访问 AppSrv 上的 HTTP 资源。

2. 动态地址分配中继服务

- 安装和配置 dhcp relay 服务，为办公区域网络提供地址上网。
- DHCP 服务器位于 AppSrv 服务器上。

3. 虚拟专用网络

- 设置 L2TP/IPSec，IKE 通道采用证书进行验证。
- L2TP 通道使用 chinaskills.com 域内用户进行身份验证，仅允许 manager 组内用户通过身份证验证。
- 对于 vpn 客户端，请使用范围 192.168.1.200-192.168.1.220/24。

（三）服务器 AppSrv 上的工作任务

1. 万维网服务

- 在 RouterSrv1 上搭建网站服务器。
- 将访问 http://www.chinaskills.com 的 http 的请求重定向到 https://www.chinaskills.com 站点。
- 网站内容设置为“该页面为 www.chinaskills.com 测试页！”。
- 将当前 web 根目录的设置为 d:\wwwroot 目录。
- 启用 windows 身份验证，只有通过身份验证的用户才能访问到该站点，manager 用户组成员使用 IE 浏览器打开不提示认证，直接访问。
- 设置“http://www.chinaskills.com/”网站的最大连接数为 1000，网站连接超时为 60sl；
- 使用 W3C 记录日志；每天创建一个新的日志文件，文件名格式:
- 日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号；
- 日志文件存储到“C:\WWWLogFile”目录中；
- IIS（FTP）：
- 匿名用户上传的文件都将映射为 ftp2 用户
- ftp 在登录前显示 Banner 消息：
- “Hello, unauthorized login is prohibited!”

2. 动态地址分配服务

- 安装和配置 dhcp 服务，为办公区域网络提供地址上网。
- 地址池范围：192.168.0.100-192.168.0.200。

3. DFS

- 在 ppSrv 上安装及配置 DFS 服务。
- 目录设置在 F：\DFSsharedir。
- 配置 DFS 复制，使用 Server03 作为次要服务器，复制方式配置为交错拓扑。
- 在 F：\DFSsharedir 文件夹内新建所有部门的文件夹。
- 所有部门的用户之可以访问部门内的文件，不可以跨部门访问别的部门文件夹内容。
- Management 用户组用户可以访问全局的文件夹。

4. 磁盘管理

- 安装及配置软 RAID5。
- 在安装好的 **AppSrv** 虚拟机中添加三块 10G 虚拟磁盘。
- 组成 RAID5，磁盘分区命名为卷标 F 盘：Raid5。
- 手动测试破坏一块磁盘，做 RAID 磁盘修复；确认 RAID5 配置完毕。

5. DNS

- 安装 DNS 服务器，根据题目创建必要的 DNS 解析。

- 把当前机器作为互联网根域服务器。

（四）服务器 DC1&DC2 上的工作任务

1. 活动目录域服务

- 在 DC1 和 DC2 服务器上安装活动目录域服务，DC1 作为主域控，DC2 作为备份域控，活动目录域名为：chinaskills.com。
- 域用户能够使用[username]@csk.cn 进行登录。
- 创建一个名为“CSK”的 OU，并新建以下域用户和组：
  - sa01-sa20，请将该用户添加到 sales 用户组。
  - it01-it20，请将该用户添加到 IT 用户组。
  - ma01-ma10，请将该用户添加到 manager 用户组。
    - 许除 manager 组和 IT 组，所有用户隐藏 C 盘。
    - 除 manager 组和 IT 组，所有普通给用户禁止使用 cmd。
- 禁止客户端电脑显示用户首次登录动画。
- 所有用户的 IE 浏览器首页设置为“https://www.chinaskills.com”。
- 所有用户都应该收到登录提示信息：标题“登录安全提示：”，内容“禁止非法用户登录使用本计算机。”。
- 设置所有主机的登录 Banner：
  - 标题为“CHINASKILLS-DOMAIN”；
  - 内容为“Hello, unauthorized login is prohibited!”。
- 域内的所有计算机（除 dc 外），当 dc 服务器不可用时，禁止使用缓存登录。
- 启用 AD 回收站功能。

2. NPS（网络策略服务）

- 在 DC1 上安装网络策略服务作为 VPN 用户登录验证。
- 仅允许 L2TP/IPSEC VPN 进行 VPN 连接访问验证。
- 认证、授权日志将存储到 DC1 上的“C:\NPS\”目录下。

3. DNS（域名解析服务）

- 拓扑中所有主机的 DNS 查询请求都应由 IspSrv 进行解析。

4. 证书颁发机构

- 在 DC1 服务器上安装证书办法机构。
- 定义名称：CSK2023-ROOTCA。
- 证书颁发机构有效期：3 years。
- 为 chinaskills.com 域内的 web 站点颁发 web 证书。
- 当前拓扑内所有机器必须信任该证书颁发机构。
- 所域内所有计算机自动颁发一张计算机证书。

5. 文件共享

- 创建用户主目录共享文件夹：
  - 本地目录为 F:\share\users\，允许所有域用户可读可写。在本目录下为所有用户添加一个以名称命名的文件夹，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, *.bat, *.sh”文件。
- 创建 manager 组共享文件夹：
  - 本地目录为 F:\ share\managers，仅允许 manager 用户组成员拥有写入权限，该共享文件对其他组成员不可见。

- 创建 public-share 公共共享文件夹：
  - 本地目录为 F:\ share\public-share，仅允许 manager 用户组成员拥有写入权限，其他认证用户只读权限。

（五）客户端 InsideCli 上的工作任务

- 按照要求将该主机加入到对应区域的域。
- 设置电源配置，以便客户端在通电的情况下，永不进入睡眠。
- 该客户端用于测试用户登录，Profiles，文件共享，安全策略和 RDS 等功能。

（六）客户端 OutsideCli 上的工作任务

- 该主机不允许加入域。
- 添加一个名为 Connect-CSK 的 VPN 拨号器，用于连接到 chinaskills.com 域网络，不记录用户名称密码信息。
- 设置电源配置，以便客户端在通电的情况下，永不进入睡眠。
- 该客户端用于测试用户登录，Profiles，文件共享，安全策略和 RDS 等功能。

模块 C：Linux 环境

一、竞赛简介

1. 请认真阅读以下指引！
2. 比赛共 4 个小时，你必须自行决定如何分配你的时间。
3. 当比赛结束时，离开时请不要关机您的虚拟机。
4. 如果没有明确要求，请使用“Chinaskill23”作为默认密码。
5. 本模块所有的系统为已经安装的最基本的系统状态，客户端带桌面。

二、竞赛注意事项

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。
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. 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，不要拆动硬件连接。
4. 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。
5. 裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，不得以任何形式体现参赛院校、工位号等信息。

三、竞赛结果文件的提交

按照题目要求，提交符合模板的 WORD 文件以及对应的 PDF 文件（利用 Office Word 另存为 pdf 文件方式生成 pdf 文件），所有截图建议除了配置文件截图外，还需要截功能测试的图，能在终端上测试的就一定要在终端上测试并截图，否则功能测试部分不得分。

四、初始化环境

1.默认账号及默认密码

Username: root
Password: Chinaskill23!
Username: skills
Password: Chinaskill23!
注：若非特别指定，所有账号的密码均为 Chinaskill23!

2.操作系统配置

所处区域：CST + 8
系统环境语言：English US (UTF-8)
键盘：English US
注意：当任务是配置 TLS，请把根证书或者自签名证书添加到受信任区。
控制台登陆后不管是网络登录还是本地登录 ，都按下方欢迎信息内容显示

****

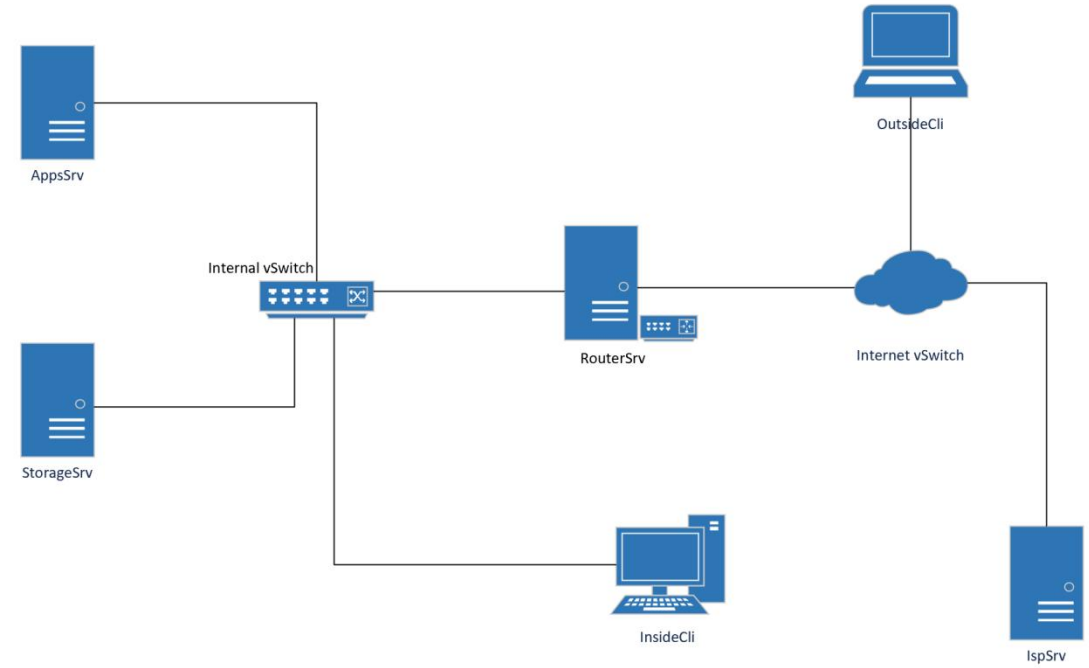
ChinaSkills 2023 – Hunan
Module A Linux
lnxserver1
选手姓名拼音全拼

>>hostname<<
>>Debian Version<<
>> TIME <<
****

五、项目任务描述

你作为一个 Linux 的技术工程师，被指派去构建一个公司的内部网络，要为员工提供便捷、安全稳定内外网络服务。你必须在规定的时间内完成要求的任务，并进行充分的测试，确保设备和应用正常运行。任务所有规划都基于 Linux 操作系统，请根据网络拓扑、基本配置信息和服务需求完成网络服务安装与测试，网络拓扑图和基本配置信息如下：

1.拓扑图



2.网络地址规划

服务器和客户端基本配置如下表：

ISPSRV

- 完全限定域名：ispsrv
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关：81.6.63.100/24/无

AppSrv

- 完全限定域名：appsrv.chinaskills.cn
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关：192.168.100.100/24/192.168.100.254

STORAGESRV

- 完全限定域名：storagesrv.chinaskills.cn
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关：192.168.100.200/24/192.168.100.254

ROUTERSRV

- 完全限定域名：routersrv.chinaskills.cn
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关： 192.168.100.254/24/无、192.168.0.254/24/无、81.6.63.254/24/无

INSIDECLI

- 完全限定域名：insidecli.chinaskills.cn
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关：DHCP From AppSrv

OUTSIDECLI

- 完全限定域名：outsidecli.chinaskills.cn
- 普通用户/登录密码：skills/Chinaskill23
- 超级管理员/登录密码：root/Chinaskill23
- 网络地址/掩码/网关：DHCP From IspSrv

六、项目任务清单

（一）服务器 IspSrv 工作任务

1. DHCP

- 为 OutsideCli 客户端网络分配地址，地址池范围：81.6.63.110-81.6.63.190/24；
- 域名解析服务器：按照实际需求配置 DNS 服务器地址选项；
- 网关：按照实际需求配置网关地址选项；

2. DNS

- 安装 BIND9；
- 配置为 DNS 根域服务器；
- 其他未知域名解析,统一解析为该本机 IP；
- 创建正向区域“chinaskills.cn”。
  - 类型为 Slave；
  - 主服务器为“AppSrv”。

3. CHRONY

- 安装 chrony，提供时间同步。
- 在 AppSrv 和 StorageSrv 创建 CRON 计划任务，每隔五分钟进行一次时间同步。

4. RAID5 & 磁盘加密

- 在虚拟机上，新建四块大小为 10GB 的虚拟硬盘，挂载到系统上；
- 创建 raid 5 md0 组，模式为三个磁盘，一个为热备；
- 挂载 md0 到系统中创建的/backup 文件夹下；
- 系统启动自动挂载 md0 RAID 磁盘；
- 创建一块新的磁盘，对该卷进行磁盘加密，解锁密码为“CSK2023!”，映射到/dev/mapper/crypt 分区上；格式化成 ext4 分区；挂载到/mut/crypt 目录；配置开机自动挂载；

5. WEB 服务

- 安装 nginx 软件包；
- 配置文件名为 ispweb.conf，放置在/etc/nginx/conf.d/目录下；
- 网站根目录为/mut/crypt（目录不存在需创建）；
- 启用 FastCGI 功能，让 nginx 能够解析 php 请求；
- index.php 内容使用 Welcome to 2020 Computer Network Application contest!

（二）服务器 RouterSrv 上的工作任务

1. DHCP RELAY

- 安装 DHCP 中继；

- 允许客户端通过中继服务获取网络地址；

2. **ROUTING**
   - 开启路由转发，为当前实验环境提供路由功能。
   - 根据题目要求，配置单臂路由实现内部客户端和服务器之间的通信。
3. **SSH**
   - 工作端口为 2023；
   - 只允许用户 user01，密码 Chinaskill23 登录到 router。其他用户（包括 root）不能登录，创建一个新用户，新用户可以从本地登录，但不能从 ssh 远程登录。
   - 通过 ssh 登录尝试登录到 RouterSrv，一分钟内最多尝试登录的次数为 3 次，超过后禁止该客户端网络地址访问 ssh 服务。
   - 记录用户登录的日志到/var/log/ssh.log，日志内容要包含：源地址，目标地址，协议，源端口，目标端口。
4. **OPENVPN**
   - VPN 客户端只能与 InsideCli 客户端网段通信，以及允许访问 StorageSrv 主机上的 SAMBA 服务；
   - VPN 客户端可使用的地址范围是 172.16.0.100-172.16.0.120/24。
   - 允许在 OutsideCli 客户端上使用 systemctl start openvpn@csk 进行连接。
5. **IPTABLES**
   - 添加必要的网络地址转换规则，使外部客户端能够访问到内部服务器上的 DNS、MAIL、WEB 和 FTP 服务。
   - INPUT、OUTPUT 和 FOREARD 链默认拒绝（DROP）所有流量通行。
   - 配置源地址转换允许内部客户端能够访问互联网区域。

（三）服务器 AppSrv 上的工作任务

1. **SSH**
   - 安装 SSH，工作端口监听在 192101。
   - 仅允许 InsideCli 客户端进行 ssh 访问，其余所有主机的请求都应该拒绝。
   - 在 cskadmin 用户环境下可以免秘钥登录，并且拥有 root 控制权限。
2. **DHCP**
   - 为 InsideCli 客户端网络分配地址，地址池范围：192.168.0.110-192.168.0.190/24；
   - 域名解析服务器：按照实际需求配置 DNS 服务器地址选项；
   - 网关：按照实际需求配置网关地址选项；
   - 为 InsideCli 分配固定地址为 192.168.0.190/24。
3. **DNS（BIND）**
   - 为 chinaskills.cn 域提供域名解析。
   - 为 www.chinaskills.cn、download.chinaskills.cn 和 mail.chinaskills.cn 提供解析。
   - 添加邮件 MX 记录用于邮件服务器；配置 DNS 组件；
   - 启用内外网解析功能，当内网客户端请求解析的时候，解析到对应的内部服务器地址，当外部客户端请求解析的时候，请把解析结果解析到提供服务的公有地址。
   - 请将 IspSrv 作为上游 DNS 服务器，所有未知查询都由该服务器处理。
4. **APACHE2**
   - 安装 apache 服务；
     - 服务以用户 webuser 系统用户运行；
     - 限制 web 服务只能使用系统 500M 物理内存；
     - 全站点启用 TLS 访问，使用本机上的“CSK Global Root CA”颁发机构颁发，网站证书信息如下：

       C = CN
       ST = China
       L = BeiJing
       O = skills

OU = Operations Departments
CN = *.chinaskills.com

- 客户端访问 https 时应无浏览器（含终端）安全警告信息；
- 当用户使用 http 访问时自动跳转到 https 安全连接；

- 搭建 www.chinaskills.cn 站点；
  - 网页文件放在 StorgeSrv 服务器上；
  - 在 StorageSrv 上安装 MriaDB，在本机上安装 PHP，发布 WordPress 网站；
  - MariaDB 数据库管理员信息：User: root/ Password: Chinaskill23!。
- 创建网站 download.chinaskills.cn 站点;
  - 仅允许 ldsgp 用户组访问；
  - 网页文件存放在 StorageSrv 服务器上；
  - 在该站点的根目录下创建以下文件“test.mp3, test.mp4, test.pdf”，其中 test.mp4 文件的大小为 100M，页面访问成功后能够列出目录所有文件。
  - 作安全加固，在任何页面不会出现系统和 WEB 服务器版本信息。

5. MAIL（POSTFIX-SMTPS & DOVECOT-IMAPS）

- 安装配置 postfix 和 dovecot，启用 imaps 和 smtps，并创建测试用户 mailuser1 和 mailuser2。
- 使用 mailuser1@chinaskills.cn 的邮箱向 mailuser2@chinaskills.cn 的邮箱发送一封测试邮件，邮件标题为“just test mail from mailuser1”，邮件内容为“hello , mailuser2”。
- 使用 mailuser2@chinaskills.cn 的邮箱向 mailuser1@chinaskills.cn 的邮箱发送一封测试邮件，邮件标题为“just test mail from mailuser2”，邮件内容为“hello , mailuser1”。
- 添加广播邮箱地址 all@chinaskills.cn，当该邮箱收到邮件时，所有用户都能在自己的邮箱中查看。
- 使用 https://mail.chinaskills.cn 网站测试邮件发送与接收。

6. CA（证书颁发机构）

- CA 根证书路径/csk-rootca/csk-ca.pem；
- 签发数字证书，颁发者信息：(仅包含如下信息)

C = CN
ST = China
L = BeiJing
O = skills
OU = Operations Departments
CN = CSK Global Root CA

（四）服务器 StorageSrv 上的工作任务

1. SSH

- 安装 openssh 组件；
- 创建的 user01 、 user02 用户允许访问 ssh 服务；
- 服务器本地 root 用户不允许访问；
- 修改 SSH 服务默认端口，启用新端口 3358；
- 添加用户 user01 user02 到 sudo 组；用于远程接入，提权操作。

2. DISK

- 添加大小均为 10G 的虚拟磁盘，配置 raid-5 磁盘。
- 创建 LVM 命名为/dev/vg01/lv01，大小为 100G，格式化为 ext4，挂在到本地目录/webdata，在分区内建立测试空文件 disk.txt。

3. NFS

- 共享/webdata/目录；
- 用于存储 AppSrv 主机的 WEB 数据；
- 仅允许 AppSrv 主机访问该共享。

4. VSFTPD

- 禁止使用不安全的 FTP，请使用“CSK Global Root CA”证书颁发机构，颁发的证书，启用 FTPS 服务；
- 用户 webadmin，登录 ftp 服务器，根目录为/webdata/；
- 登录后限制在自己的根目录;
- 允许 WEB 管理员上传和下载文件，但是禁止上传后缀名为.doc .docx .xlsx 的文件；
- 上传的文件所有者均设置为 ftpusr。

5. AIDE

- 配置aide安全监控策略；
- 监控/webdata目录，当目录中文件发生变化时进行检查可以看到相关提示信息 ；

6. SAMBA

- 安装 Samba 组件
- 创建 Samba 共享目录为/var/skills，共享名为 csk-share；
- user01,user02,用户都能访问共享文件夹；
- user01 能够查看和删除所有人的文件；user02 能够查看所有人的文件，但不能删除别人的文件；
- 通过物理机访问共享目录，根据配置上传，下载文件进行测试操作；

7. ShellScript

- 编写添加用户的脚本,存储在/shells/userAdd.sh 目录；
- 当有新员工入职时，管理员运行脚本为其创建公司账号;
- 自动分配客户端账号、公司邮箱、samba 目录及权限、网站账号等;
- 以 user Add　lifei 的方式运行脚本，lifei 为举例的员工姓名。

（五）客户端 OutsideCli 和 InsideCli 工作任务

1. OutsideCli

- 作为 DNS 服务器域名解析测试的客户端，安装 nslookup、dig 命令行工具;
- 作为网站访问测试的客户端，安装 firefox 浏览器, curl 命令行测试工具;
- 作为 SSH 远程登录测试客户端，安装 ssh 命令行测试工具;
- 作为 SAMBA 测试的客户端，使用图形界面文件浏览器测试, 并安装 smbclient 工具;
- 作为 FTP 测试的客户端，安装 lftp 命令行工具；
- 作为防火墙规则效果测试客户端，安装 ping 命令行工具。
- 截图的时候请使用上述提到的工具进行功能测试。

2. InsideCli

- 作为 DNS 服务器域名解析测试的客户端，安装 nslookup、dig 命令行工具;
- 作为网站访问测试的客户端，安装 firefox 浏览器, curl 命令行测试工具;
- 作为 SSH 远程登录测试客户端，安装 ssh 命令行测试工具;
- 作为 SAMBA 测试的客户端，使用图形界面文件浏览器测试, 并安装 smbclient 工具;
- 作为 FTP 测试的客户端，安装 lftp 命令行工具；
- 作为防火墙规则效果测试客户端，安装 ping 命令行工具。
- 截图的时候请使用上述提到的工具进行功能测试。