

第十届“星光计划”职业院校技能大赛

“网络系统管理”项目

技术描述

上海市星光计划组委会竞赛办公室

二〇二三年四月

目录

1.项目简介	4
1.1 项目描述	4
1.2 竞赛目的	4
1.3 相关文件.....	4
2.选手应具备的能力	4
3.竞赛试题	8
3.1 试题模块.....	8
3.2 模块简述.....	8
3.2.1 模块 A：客户端与服务器环境	8
3.2.2 模块 B：网络环境.....	8
3.2.3 模块 C：网络自动化运维环境	9
3.3 命题方式	9
3.4 命题方案.....	9
4.评分规则	10
4.1 测量分（客观）	10
4.2 评分流程说明	10
4.3 成绩排名（并列处理）	10
5.项目特别规定.....	11
6.竞赛场地与相关设施设备.....	11
6.1 场地设备工具：	11
6.2 材料:.....	12
6.3 竞赛选手须自备的设备和工具：	13
6.4 竞赛场地禁止自带使用的设备和材料：	13
7.健康和安​​全.....	13
8.开放赛场	13
8.1 公众要求.....	13

8.2 对于赞助商和宣传的要求	14
9.绿色环保	14
10.附件.....	14

本项目技术描述是对本竞赛项目内容的框架性描述，正式竞赛内容及要求以竞赛当日公布的赛题为准。

1.项目简介

1.1 项目描述

网络系统管理技术人员旨在为大中小型商业组织及政府部门提供广泛的 IT 服务，有效地保证系统的连续和稳定运行。网络系统管理人员需在多种环境下，包括网络操作中心、互联网服务供应商、数据中心，提供广泛的服务，包括：技术支持、建议指导，对各类型网络项目进行分析、设计、连接、配置、调试、升级，对服务器和客户端进行相应配置并能实现各类服务的互联互通及保障网络安全。

1.2 竞赛目的

本次大赛借鉴世界大赛的先进理念，深化教学改革、推进校企合作，促进专业发展，展示师生风采。提高学生素养，培育工匠精神。发挥大赛社会效应，展示职业教育成果，增强职业教育影响力和吸引力，迎接下一届的世界技能大赛。

1.3 相关文件

本项目技术描述只包含项目技术工作的相关信息。除阅读本文件外，开展本技能项目竞赛还需配合其他相关文件一同使用：

上海市“星光计划”第十届职业院校职业技能大赛网络系统管理项目样题——中职组。

2.选手应具备的能力

模块	能力描述
A	客户端与服务器环境 个人需要知道和理解： <ul style="list-style-type: none">• 保证用户设备和信息完整及安全的重要性• 规划，调度及设置优先等级的技术

-
- 系统性地进行操作工作的重要性
 - 系统变更的速度以及保持信息流通的需求
 - 操作系统的工作原理，了解内存管理、进程管理、CPU 调度和进程间的通讯等，并能理解 linux /Windows 系统的机制
 - 操作系统及软件的许可、规范、授权等
 - 熟悉计算机安全理论知识，了解常见的攻防策略
 - 操作系统使用范围及满足用户特殊需求的能力，给予客户预算
 - 为客户提供知识渊博的/最好的建议及可能的解决方法以满足技术性 & 安全性需求
 - 把预算/资源限制与最佳客户解决方案相结合
 - 准确地把客户意愿转化为逻辑图
 - 在客户内部问责制内以适当的水平讨论操作系统和网络设备的技术设计要求

个人应能够：

- 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
 - 对多台 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
 - 熟练配置 Linux 操作系统
 - 熟练配置运行于 Linux 的各类网络管理软件
 - 熟练配置下列服务，包括但不限于 HTTP 服务、邮件服务、打印服务、目录访问服务、文件服务、数据库等，并能熟练安装、配置、优化和监控等应用
 - 测试并改正所有的问题，若有需要，进行重新测试
 - 依据设计图纸要求，配置和管理 Windows 用户及应用服务器
-

	<ul style="list-style-type: none"> • 在活动目录环境中实现用户、组和计算机账户统一管理，配置共享文件夹 • 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 • 选择操作系统/服务器系统的角色及/或特性例如：活动目录域服务（角色）及 Windows 服务器备份（特性） • 包括但不限于 DNS、DHCP、FTP、IIS、RDS、Web-Server、VPN 等各类应用软件安装配置 • 测试并改正所有的问题，若有需要，进行重新测试
B	网络环境模块
	<p>个人需要知道和理解：</p> <ul style="list-style-type: none"> • 需使用个人防护装备的情况，例如：ESD（静电放电） • 健康与安全规程，义务，条例及文件 • 精确度，校验以及注意细节对所有实践工作的重要性 • 硬件的基础功能以及组装过程 • 根据客户要求完成网络服务。 • 构建网络的过程，以及如何配置能增加有效交流的网络设备的方法 • 网络设备的工作范围。例如：路由器，VoIP，IP 设备，打印机，无线接入口，内部网络连接 • 安全选项及它们的效果
	<p>个人应能够：</p> <ul style="list-style-type: none"> • 根据行业认证要求设计要求，解释用户需求及设计要求 • 根据所要求的流程进行工作，以完成成功的配置 • 为达到客户要求，选择合适的服务。 • 在所有有可能在网络环境出现的网络设备上，例如：路由器协议，网络安全，Wi-Fi，VoIP 等等设计并执行灾难恢复流程。 • 根据需求完成网络环境及拓扑结构

	<ul style="list-style-type: none"> • 根据需求完成逻辑图和功能图 • 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。 • 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。
C	网络自动化运维环境
	<p>个人需要知道和理解：</p> <ul style="list-style-type: none"> • Ansible 如何安装及主配置文件和主机清单 • 如何使用 ansible 管控主机以及主机清单的作用 • 常见模块的使用 • 常见模块的作用 • 常见模块的语法 • Playbook 的使用 • Hosts 执行的远程主机列表 • Tasks 任务集 • Tags 标签，指定某条任务执行，用于选择运行 playbook 中的部分代码 • Ansible 管理网络 • 管理网络的主配置文件 • 管理网络的方式，如何管理网络 • 编写多个 playbook 剧本去管理网络设备
	<p>个人应能够：</p> <ul style="list-style-type: none"> • 能够使用命令对一台主控端实现 ansible 的安装 • 能够知道主配置文件里的具体内容 • 能够在主机清单里面规划好被控端主机的 IP 地址以及分组 • 常见模块的用法 • 能够使用常见模块对主机进行一些基本配置 • 能够使用常见模块完成一些任务需求

	<ul style="list-style-type: none"> • 能够记住常见模块的使用以及一些语法 • 能够知道如何创建 <code>playbook</code> 并且进行编写 • 能够知道使用 <code>YAML</code> 语法使用方式 • 能够使用多种模块去编写 <code>playbook</code> • 能够对主配置文件的了解，知道管理了哪些网络设备 • 能够编写多个 <code>playbook</code> 剧本，并且解决不同的问题 • 能够对整个布局精准的了解和把控
--	---

3.竞赛试题

3.1 试题模块

模块编号	模块名称	竞赛时间 min	分数		
			评价分	测量分	合计
A	客户端与服务器环境	70	0	40	40
B	网络环境	70	0	40	40
C	网络自动化运维环境	40	0	20	20
总计		180	0	100	100

3.2 模块简述

3.2.1 模块 A：客户端与服务器环境

客户端与服务器环境模块比赛时间为 70 分钟。需要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、Windows 系统的企业信息化系统的构建；配置和管理系统用户及应用服务器；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；为操作系统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。在符合技术水平规范要求的情况下,管理多台服务器的网络资源、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。

3.2.2 模块 B：网络环境

网络环境模块比赛时间 70 分钟。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，在所有有可能在网络环境出现的网络设备上，例如：路由器，防火墙等等，应有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。

3.2.3 模块 C：网络自动化运维环境

网络自动化运维环境比赛时间 40 分钟。为促进参赛选手更好地掌握自动化运维基本知识，熟练掌握计算机的操作技能，引入企业先进的自动化编排工具，Ansible 是近年十分流行的一款运维自动化工具，其主要功能是帮忙运维实现 IT 工作的自动化、降低人为操作失误、提高业务自动化率、提升运维工作效率，常用于软件部署自动化、配置自动化、管理自动化、系统化系统任务、持续集成、零宕机平滑升级等。该模块需要选手根据试题要求采用所对应的功能模块进行自动化运维工作。

3.3 命题方式

本项目赛题的命题方式为第三方专家命题。

本项目为提前公布部分试题的项目，由专家组长根据本《技术描述》文件的技术要求、竞赛模块命制样题，并于赛前 30 天公布（包括试题、评分表）。

决赛试题由专家组长主持裁判组在赛前对试题进行修订，修订比例一般不超过 30%。对于公布赛题后各参赛代表队普遍反映的问题或合理的意见建议，将由专家组长进行最终修正和调整，并对最终比赛试题签字确认，比赛试题于赛前执裁专家组培训时公布。

3.4 命题方案

试题设计要求：

本项目依据世界技能职业标准（WSOS）命题，命制中参考融合了世赛特别赛真题、世赛上海选拔赛真题。

- 每一份试题都含有一份详细的物理拓扑图及/或一份详细的逻辑图；
- 模块 A/B/C 的评分点的设计上，每个模块评分点在 30—80 个之间，单个评分点分值不低于 0.1 分，不要高于 2.0 分；

4.评分规则

本次评分规则参照世界技能大赛评分规则执行。本项目评分标准为可采用客观数据表述的测量分（**客观**）方式评判。

4.1 测量分（客观）

测量分（**Measurement**）打分方式：按模块设置若干个评分组，每组由 2 名及以上裁判构成。每个组所有裁判一起商议，在对该选手在该项中的实际得分达成一致后最终只给出一个分值。测量分以测试功能或查看配置情况来评分，测量分只有两种结果，即得分和不得分。

测量分评分准则样列表：

类型	示例	最高分值	正确分值	不正确分值
满分或零分	正确设置 IP 地址	0.20	0.20	0
满分或零分	各评分点全对满分，错一点不得分	1.00	1.00	0

4.2 评分流程说明

竞赛开始的前 1 天（**C-1**），各参赛队裁判按照裁判长的安排进行裁判分组，裁判长根据裁判员人数和评分工作量将裁判员分成若干小组。

本项目采用事后结果评分，不计算时间分。裁判长不参与评分。每个小组的裁判只对裁判长分配的指定模块及指定的评分项进行评分，评判的过程中完全按照评分标准进行测量分评分。

为确保评分过程的公平性和公正性，评分过程采取回避制度，裁判执裁过程中不能与所在参赛队选手进行任何交流（中午休息时间除外），评分过程中不得参与自己选手的评分。

无相应模块（评分项）执裁任务的裁判不得进入选手工位，不得干扰和影响其他裁判的执裁工作。

4.3 成绩排名（并列处理）

本次大赛仅有决赛部分。如选手成绩出现同分情况的，按照模块 C、模块 B、模块 A 的

顺序计算排名顺序。

5.项目特别规定

(1) 禁止携带和使用如下电子设备：手机、智能手表等通信工具、多媒体播放设备、摄像录音设备、笔记本电脑或平板电脑等电子产品、U 盘、移动硬盘等存储设备、计算器及参考资料。

(2) 赛场内与一切比赛相关事项听从裁判长指挥，任何人不得干预裁判长的独立决策。

(3) 参赛选手在竞赛过程中，禁止与其他人员沟通。若遇到竞赛相关问题（试题问题、技术问题等），可举手向裁判员询问。

(4) 选手的所有操作必须全部按照赛题的规定要求，所有的软件、资源都需按设备环境和试题说明进行使用。

(5) 比赛过程中，需要及时保存配置以防止意外断电导致丢失操作结果。比赛结束后，请保持比赛设备、环境处于正常运行状态，不要拆、动硬件连接，确保设备正常运行，裁判可以正常评分。

(6) 对于赛题错误、设备故障、系统故障等疑难事项，选手可以举手示意，由裁判裁定、处理。

(7) 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（包括试卷和草稿纸）带离赛场。

(8) 竞赛过程中赛题使用中文描述。

6.竞赛场地与相关设施设备

6.1 场地设备工具：

(以每一个选手必须配备)

序号	主体设备名称	型号	单位	数量
1	High Performance PC	CPU: E5-2670 以上 12 核 24 线程 *2	台	1

		内存：64G 网卡：双口千兆 以太网卡 电源：600w 90% 高效电源		
2	显示器	23 寸 宽屏	台	1
3	UPS	后备式 ups 不间断电源 备用电脑 1000VA/600W	台	2
4	SSD HardDisk	1TB SSD SATA 接口	块	1

6.2 材料:

(以每一个选手必须配备)

序号	设备名称	型号	单位	数量
1	ESXI	7.0U2a	套	1
2	Debian	11.6	套	1
3	Windows Server 2019	17763	套	1
4	Windows 10	15063	套	1
5	firewalld	0.93	套	1
6	isc-dhcp-server	4.4.1	套	1
7	bind9	9.16	套	1
8	samba	4.13	套	1
9	mdadm	4.1	套	1
10	zabbix server	6.0	套	1
11	zabbix agent2	6.0	套	1
12	filezilla	3.63	套	1
13	firefox	111.0.1	套	1
14	putty	0.78	套	1
15	openssl	1.1.1	套	1
16	Ubuntu Desktop	Ubuntu 18.04 LTS	套	1
17	GNS3 网络仿真环境 (Ubuntu)	2.2.31	套	1
18	CiscoSecure ACS 4.0 for Windows Server	4.0	套	1

19	Ansible	2.9.27	套	1
20	Csr1000	12.4	套	1

6.3 竞赛选手须自备的设备和工具：

无

6.4 竞赛场地禁止自带使用的设备和材料：

序号	设备和材料名称
1	电子设备，包括但不限于手机、智能手包、平板电脑、笔记本电脑、多媒体播放社别、录音录像设备等。
2	存储设备，包括但不限于移动硬盘、U 盘、SD 卡、TF 卡等。
3	影响赛事公平性的其他工具。

7.健康和安

- 1.参赛选手应严格遵守设备安全操作规程。
- 2.参赛选手停止操作时，应保证设备的正常运行，比赛结束后，所有设备保持运行状态，不要拆、动硬件连接，确保设备正常运行和正常评分。
- 3.参赛选手应遵从安全规范操作，例如：ESD(静电放电)，静电放电无害环境下的设备用途，安全使用及储存。
- 4.参赛选手应保证设备和信息完整及安全。
- 5.禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。
- 6.赛场必须留有安全通道，必须配备灭火设备。赛场应具备良好的通风、照明和操作空间的条件。做好竞赛安全、健康和公共卫生及突发事件预防与应急处理等工作。

8.开放赛场

8.1 公众要求

1. 赛场内除指定的执裁专家、工作人员外，其他与会人员须经组委会同意或在组委会负责人陪同下，佩带相应的标志方可进入赛场内。
2. 允许进入赛场的人员，只可在安全区内观摩竞赛，不得使用录像设备长时间拍摄选

手工位、屏幕。

3. 允许进入赛场的人员，应遵守赛场规则，不得与选手交谈，不得妨碍、干扰选手竞赛。

4. 允许进入赛场的人员，不得在场内吸烟、喧哗。

5. 进入现场的人员一切听从执裁专家指挥。

8.2 对于赞助商和宣传的要求

经组委会允许的赞助商和负责宣传的媒体记者，按竞赛规则的要求进入赛场相关区域。上述相关人员不得妨碍、干扰选手竞赛，不得有任何影响竞赛公平、公正的行为。

9.绿色环保

1. 赛场严格遵守我国环境保护法。

2. 比赛过程中尽量减少纸张的使用并杜绝浪费。

3. 大赛任何工作都不应该破坏赛场周边环境。

10.附件

（一）试题（公开项目）

另见附件一。

（二）评分表（公开项目）

另见附件二。

上海市“星光计划”
第十届职业院校技能大赛

网络系统管理赛项
(中职杯)
(样题)

客户端与服务器环境

目 录

一、竞赛说明.....	3
(一) 竞赛简介.....	3
(二) 竞赛成果物提交要求.....	3
(三) 竞赛注意事项.....	3
二、初始化环境.....	3
(一) 默认账号及默认密码.....	3
(二) 操作系统配置.....	4
(三) 软件环境.....	4
三、项目任务描述.....	4
(一) 拓扑图.....	5
(二) 网络地址规划.....	5
四、项目任务清单.....	6
(一) ROUTER 上的工作任务.....	6
(二) DC 上的工作任务.....	6
(三) WEB 上的工作任务.....	6
(四) NAS 上的工作任务.....	6
(五) MONITOR 上的工作任务.....	7
(六) 全局工作任务.....	7

一、竞赛说明

（一）竞赛简介

竞赛模块：（客户端与服务器环境）

（二）竞赛成果物提交要求

请在 U 盘中建立“竞赛成果物”文件夹，文件夹中包含以下内容：

- 系统服务-答题卡.docx

（三）竞赛注意事项

1. **竞赛环境确认：**选手入场后请根据竞赛所提供的《竞赛环境确认单》，依次检查所列的硬件设备、软件、材料、U 盘内竞赛答题卡等是否齐全，软硬件设备是否能正常使用，检查完毕后在《竞赛环境确认单》上签字并上交。
2. **试卷确认：**竞赛分发试题后请检查试题名称是否与当前考核模块相符，试题内容无缺页、模糊问题。
3. **安全操作：**竞赛过程安全操作，注意赛位电源线位置，操作时不要碰到，及时进行设备配置保存，以防误碰电缆导致设备断电配置丢失情况。
4. **竞赛成果物提交确认：**评分将以各参赛队提交的竞赛提交物为主要评分依据。请按照 U 盘中答题卡要求创建和编辑竞赛成果物，确保答题卡截图信息清晰完整，并在竞赛结束时提交，所有提交的内容必须按照“竞赛成果物提交要求”进行命名并签署《竞赛成果提交确认单》。
5. **离场要求：**竞赛结束时，所有设备保持运行状态，不要拆掉网络连接。禁止将竞赛用的所有物品（包括试卷和草纸）带离赛场。

二、初始化环境

（一）默认账号及默认密码

Windows 登录信息	
用户名	Administrator
密码	ChinaSkills123

Linux 登录信息	
用户名	root
密码	ChinaSkills123

注：若非特别指定，所有账号的密码均为 ChinaSkills123

（二）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。

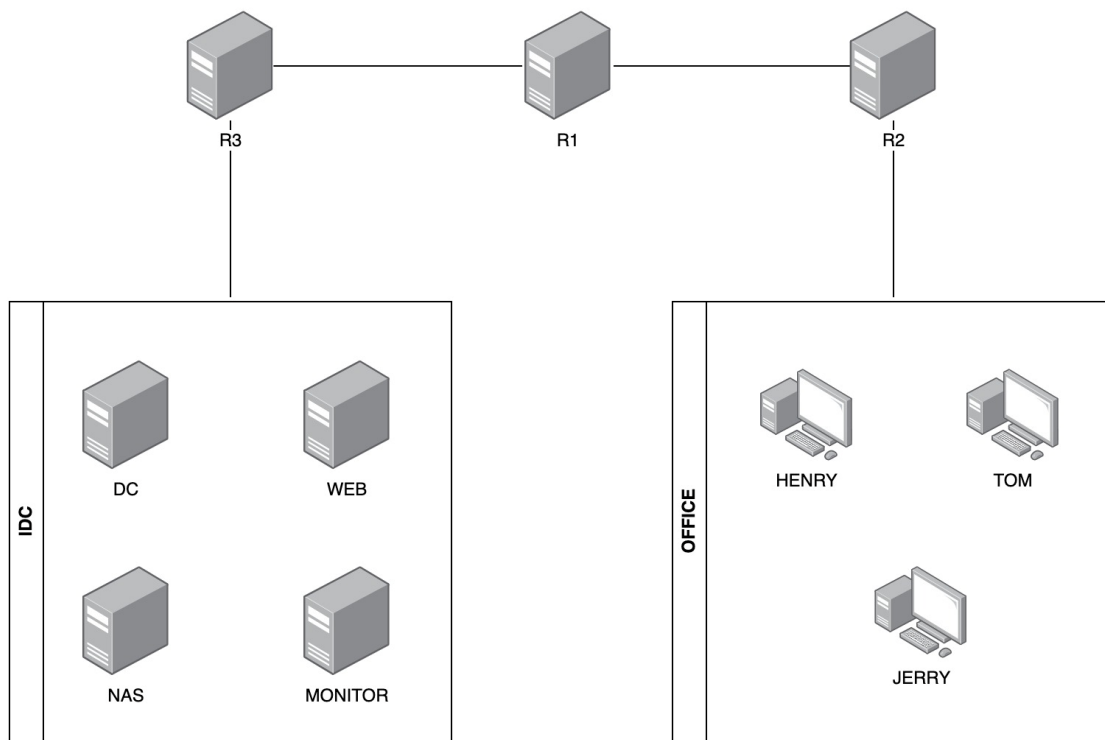
（三）软件环境

选手机上安装的软件都存放在 C:\APPS 目录下。

三、项目任务描述

你作为技术工程师，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 和 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：

(一) 拓扑图



(二) 网络地址规划

服务器和客户端基本配置如下表，各虚拟机已预装系统。

主机名	所在域	网络地址	DNS	网关	系统
R1	/	10.10.0.1/24 10.20.0.1/24	/	/	Debian 11
R2	/	10.10.0.254/24 192.168.1.1/24	/	10.10.0.1	Debian 11
R3	/	10.20.0.254/24 172.16.1.1/24	/	10.20.0.1	Debian 11
DC	dc.skills-sh.xg	172.16.1.10/24	172.16.1.10	172.16.1.1	Windows Server 2019
NAS	Nas.skills-sh.xg	172.16.1.20/24	172.16.1.10	172.16.1.1	Debian 11
WEB	Web.skills-sh.xg	172.16.1.30/24	172.16.1.10	172.16.1.1	Debian 11

MONITOR	Monitor.skills-sh.xg	172.16.1.40/24	172.16.1.10	172.16.1.1	Debian 11
JERRY	Jerry.skills-sh.xg	DHCP	172.16.1.10	192.168.1.1	Windows 10
TOM	Tom.skills-sh.xg	DHCP	172.16.1.10	192.168.1.1	Windows 10
HENRY	Henry.skills-sh.xg	DHCP	172.16.1.10	192.168.1.1	Windows 10

四、项目任务清单

（一）ROUTER 上的工作任务

1. 在路由间配置路由，可以实现 IDC 和 OFFICE 之间相互访问
2. 在 R2 上配置 DHCP 服务
3. HENRY, TOM, JERRY 的 IP 地址、网关、DNS 信息从 R2 上获取
4. R2 上地址池的范围设置为 192.168.1.101-192.168.1.199

（二）DC 上的工作任务

1. DC 是 IDC 的域控服务器，OFFICE 中所有的设备登录用户都必须是域用户
2. TOM 和 JERRY 目录设置为漫游模式，双方互换设备也可以使用
3. 在 DC 服务器上部署证书颁发机构，配置 DC 为 DNS 服务器，DC 上配置根域名为 skills-sh.xg
4. 批量创建域名 nas01-100.skills-sh.xg，地址指向 172.16.1.20

（三）WEB 上的工作任务

1. 在 WEB 上配置 APACHE 服务器，Web 服务器启用 https 服务，使用 Win10 客户端浏览 WEB 网站时不会出现证书告警
2. 在 Web 服务器上部署 FTP 服务，根目录指向 web 服务器的网页根目录
3. 将 TOM 桌面上的 WEB 目录里的文件，通过 Filezilla 上传到 Web 服务器的网页目录下，并覆盖原有文件

（四）NAS 上的工作任务

1. 在 NAS 服务器上部署 RAID5 磁盘阵列
2. 在挂载的 RAID5 磁盘上设置 SAMBA 共享

3. 创建 HENRY、TOM 和 JERRY 用户，每个用户的共享空间保持独立
4. 将各用户的 SAMBA 空间挂载到 WIN10 客户端中

(五) MONITOR 上的工作任务

1. 在 Monitor 服务器上安装 zabbix 服务
2. 在 zabbix 设备中监控 IDC 内的所有设备
3. 监控每台设备上的 CPU，内存，网络和磁盘的情况

(六) 全局工作任务

1. 在 R1, R2, R3 上已经安装 firewalld 防火墙软件，放行 icmp 流量和需要对外访问的服务端口，默认其他均为禁止
2. 开启所有 Windows 系统的防火墙，仅放行对外服务端口和 ICMP 协议
3. R1 上部署 NTP 服务，作为时间服务器，将所有时间全部调整为中国时区
4. 所有设备上开启时间同步，与 R1 的时间同步

测量分评分表

2023上海市星光杯（中职组） 上海市选拔赛

项目名称 网络系统管理

项目编号 _____

竞赛日 _____

子配分说明 客户端与服务器环境

选手号 _____
子模块号 A

评分细则编号	最大分值	评分细则描述	规定或标称值	结果或实际值	实际得分
M1	0.50	R1: 网络地址/掩码			
M2	0.50	R2: 网络地址/掩码/网关			
M3	0.50	R3: 网络地址/掩码/网关			
M4	1.00	DC: 域名; 网络地址/掩码/网关			
M5	0.50	NAS: 网络地址/掩码/网关			
M6	0.50	WEB: 网络地址/掩码/网关			
M7	0.50	MONITOR: 网络地址/掩码/网关			
M8	2.00	路由功能: 开启路由转发; 配置网络地址转换, 实现内网访外网, 实现外网访内网资源; 配置静态			
M9	1.50	DHCP: 启用DHCP服务器; 客户端成功获取地址。			
M10	1.00	正确安装域控, 域名为skills-sh.xg			
M11	2.00	将Windows系统加入DC域中			
M12	1.00	创建必要的正向和反向区域, 并添加对应的 A 记录和 PRT 记录			
M13	2.00	nas01.skills-sh.xg - nas100.skills-sh-xg 的域名解析			
M14	2.00	TOM设置为漫游模式			
M15	2.00	给WEB服务器配置证书, 可以正常访问https://www.skills-sh.xg			
M16	2.00	IE浏览器信任根证书			
M17	1.00	JERRY使用SSH公私钥加密登录远程服务器			
M18	1.00	在NAS服务器上设置raid5磁盘阵列			
M19	1.00	在NAS上设置SAMBA共享空间			
M20	1.00	存在SAMBA用户: henry, tom, jerry			
M21	1.00	SAMBA可以正常挂载到Windows10中, 并可以使用SAMBA用户登录			
M22	1.00	可以在SAMBA共享空间上存储文件			
M23	1.00	在dc服务器上安装了zabbix agent			
M24	1.00	在web服务器上安装了zabbix agent			
M25	1.00	在nas服务器上安装了zabbix agent			
M26	1.00	在monitor服务器上安装了zabbix agent			
M27	2.00	正确设置mysql数据库			
M28	2.00	可以访问http://monitor.skills-sh.xg			
M29	2.00	各设备的CPU、内存、网络、磁盘截图			
M30	0.50	查看R1、R2、R3防火墙是否开启混杂模式			
M31	0.50	查看DC上是否开启445/tcp, 445/udp			
M32	0.50	查看dc上是否开启53/tcp, 53/udp			
M33	1.00	时区是否是中国时区			
M34	1.00	Linux系统与R1时间同步			
M35	1.00	Windows系统与R1时间同步			

40.00 子模块分值

实际得分 _____

上海市“星光计划”第十届职业院校技能大赛 (中职组, 样题)

网络系统管理

模块 B
网络环境模块

上海市职业技能竞赛组织委员会

二〇二三年四月





引言

竞赛模块 B 网络环境部分，比赛时间总长为 1 小时。假定你作为某一个互联网企业的网络管理员，在这个模块中，你需要按照任务要求，在给定的企业网络架构中，配置 Cisco 路由器、交换机等网络设备，完成公网及内部网络互联，实现配套的服务器网络服务。

选手须知

首先阅读整个测试项目非常重要。你有责任有效地管理你的时间和决定完成任务的顺序。如上所述，如果你遇到一些较难的任务，请不要浪费太多的时间。你可以使用临时解决方案并继续处理其他任务，如果还有时间的话，你可以事后返回并修复那些无法正常运行的问题。另外，我们建议你在完成以下模块时，检查你之前的所有工作。

比赛结束前，选手需将拓扑图中的交换机、路由器相关设备的配置导出，每个设备配置单独保存成一个文本文件，文件取名分别为“设备名称.txt”，如 HQ-SW1.txt, HQ-SW2.txt, HQ-ASW1.txt, HQ-ASW2.txt, …。具体配置导出可参考使用 show run 命令，将结果复制后粘贴到各自 GNS3.VM 操作机的桌面“比赛设备配置保存”文件夹中的对应文件中（如 HQ-SW1.txt, HQ-SW2.txt, HQ-ASW1.txt, HQ-ASW2.txt, …）。另外，检查命令输出结果，可能要求选手截屏粘贴到答题卡中。这些都是比赛评分配置检查的主要依据。

注意：不要改变网络拓扑图中交换机、路由器等设备的接口标识，不得改变拓扑结构及网络连接关系。网络路由规划与配置，请参考附件路由示意图及 L3 部分的任务要求。操作中，建议经常保存设备配置，防止意外情况发生。未特别说明的，一般为默认配置。

如果题目没有提供详细信息，请使用默认配置。

GNS3.VM 的本地账户为 gns3/Skills39

WinServer (Win2003.ACS) 虚拟机的本地账户为 administrator/ Skills39

除非特别说明，服务器、终端默认网关的 IP 地址，是其所在子网的最后一个可用 IP

安装软件位于所在虚拟机桌面的相关目录下备用

其它默认密码：Skills39

任务描述

任务主要分为以下几部分配置：

- 基础配置
- L2 配置
- L3 配置
- VPN 及安全配置



- 服务器配置
- 终端（客户端）配置

环境说明

在比赛网络拓扑图环境中，由 ISP 模拟互联网（公网）环境。由 HQR、HQ-SW1、HQ-SW2、HQ-ASW1、HQ-ASW2 等组成企业总部网络。企业的两个分支结构，分别由 SH-SW 和 SH-R1、GZ-R1 和 GZ-R2 等组成。分支机构网络和总部网络之间通过专线和 VPN 实现互联。服务器和终端的配置任务要求，见后。

基础配置

1. 根据拓扑所示，在所有路由器、交换机设备上配置主机名。
2. 除非有特殊说明，要求配置密码/口令的，都采用“Skills39”。
3. 在所有设备上激活并配置在用接口，配置要求参考附件。
4. 为了验证网络连通性，需全网放行 icmp、traceroute 相关协议流量。

L2 配置

1. 根据网络拓扑图，结合附表要求，完成网络设备基本配置。
2. 在 HQ-SW1、HQ-SW2、HQ-ASW1、HQ-ASW2 上配置 VTP 协议，版本为 2，使用“Skills39”作为 VTP 的域名及密码，交换机的 VLAN 数据库上必须包含以下 VLANs：
 - a. VLAN 10 名字为 "client"
 - b. VLAN 20 名字为 "server"
 - c. VLAN 30 名字为 "interconn"
3. 在 HQ-SW1、HQ-SW2、HQ-ASW1、HQ-ASW2 交换机互联链路上，按以下要求，配置 IEEE 802.1q trunking。
 - a. (HQ-SW1、HQ-SW2) -- (HQ-ASW1、HQ-ASW2) 之间互联链路是 Trunk，只允许 VLAN 10、20 通过
 - b. HQ-SW1--HQ-SW2 之间互联链路是 Trunk，允许上述创建的 3 个 VLAN 通过
4. 在 HQ-SW1 and HQ-SW2 之间配置接口绑定技术。
 - a. 使用 port-channel 号码为 12
 - b. HQ-SW1 交换机负责开启端口通道的协商
5. 在 HQ-SW1、HQ-SW2、HQ-ASW1、HQ-ASW2 上配置多实例生成树协议（MSTP）。
 - a. 使用 starsh.edu 作为域名
 - b. 将 VLAN 10 映射到 MST 1，VLAN20 映射到 MST 2
 - c. 正常情况下，HQ-SW1 是 MST 1 的根，而 HQ-SW2 是 MST 2 的根
 - d. 如果 HQ-SW1 发生故障，则 HQ-SW2 应成为 MST 1 的根



- e. 如果 HQ-SW2 发生故障，则 HQ-SW1 应成为 MST 2 的根
- 6. HQ-ASW1、HQ-ASW2 交换机上在用的，连接到终端、服务器的端口，要求是使它允许立即连接到网络，而不是等待端口从侦听、学习状态再转移到转发状态。

L3 配置

1. 按下列要求，配置 DHCP 服务：
 - a. GZ-PC 通过 GZ-R1 上的 DHCP 服务获取 IP 地址。
 - b. 在 DHCP 地址池中排除前 50 个(即 10.3.0.1-50)可用的地址。
 - c. DNS 服务器 10.1.20.2
2. 在HQ-SW1和HQ-SW2上配置网关负载平衡协议，实现网络中的主机网关冗余，启用抢占模式，所配置的参数要求如下表所示。其中，在交换机HQ-SW1和HQ-SW2上分别设置为各组中的高优先级（设置为200）、低优先级（设置为100）：

HQ-SW1 和 HQ-SW2 的 GLBP 参数表

VLAN SVI	组号 (VRID)	GLBP 虚拟 IP	其它要求
10	10	10.1.10.254/24	
20	20	10.1.20.254/24	

3. 根据附件中的路由示意图，配置 OSPF 路由协议。
 - a. 进程号统一为：1
 - b. Router-id 为设备的 Loopback0 IP（若有）
 - c. 接口区域划分参见路由示意图
 - d. HQR 的 Tunnel 100 接口为 DR，SH-R1 和 GZ-R1 的 Tunnel 100 接口不参与 DR 选举
4. 根据附件中的路由示意图，配置 EIGRP 路由协议。
 - a. Router-id 为设备的 Loopback0 IP（若有）
 - b. 自治系统号为：100
5. 配置网络地址（端口）转换 NAT 或 PAT
 - a. SH-PC1 终端所在的子网（定义 access-list 10 匹配感兴趣流量），去访问外部互联网时，需将其源 IP 地址转换为 SH-R1 路由器的 eth0/0 出接口 IP
 - b. SH-PC2 所在的子网，不能访问互联网
6. 对于SH-R1与HQR之间互联链路，链路层封装协议采用PPP，采用PPP CHAP 单向认证方式
7. 对于GZ-R1与HQR之间互联链路，链路层封装协议采用HDLC。
8. 相关服务器及终端 IP 地址：
 - a. WebServer IP 地址为 10.1.20.1，WinServer（Win2003.ACS）IP 地址为“10.1.20.2
 - b. “GZ-PC” IP 地址为 DHCP 方式自动获取
 - c. 其余终端、服务器 IP 地址配置参考拓扑图和附表



VPN 及安全配置

1. 在 HQR、SH-R1、GZ-R1 之间配置 DMVPN 连接，使得 SH-R1、GZ-R1 各自所在分支机构，均可通过安全加密的 VPN 通道访问企业总部内网服务。相关配置要求如下：
 - a. 传输流量启用 IPSec 加密
 - b. 为所有路由器使用 Tunnel 100 作为 VTI（虚拟隧道接口）
 - c. 配置所有 VTIs 上的 MTU 值设置为 1400
 - d. 使用 Ethernet0/0 接口作为每一台路由器上的隧道源接口
 - e. HQR、SH-R1、GZ-R1 上 Tunnel 100 接口的 IP 地址分别为：172.16.123.1/24、172.16.123.2/24、172.16.123.3/24
 - f. NHRP 配置：
 - i. 隧道 ID—100；
 - ii. NHRP 认证密钥 “Skills39”
 - iii. tunnel key 为 “123”；
 - iv. 使用 HQR 路由器作为 DMVPN hub NHS 服务器
 - g. 传输流量启用 IPSec 加密
 - h. IKE 第一阶段（参考）配置：
 - i. Hash - MD5
 - ii. Encryption - 3DES
 - iii. DH group - 2
 - iv. Authentication - pre-shared key
 - i. IPSec 第二阶段（参考）配置：
 - i. Hash- MD5
 - ii. Encryption - 3DES
 - iii. Protocol - ESP
2. SH、GZ 分支机构访问 HQ 企业总部内部网络时，路由优选 DMVPN。在 DMVPN 故障情况下，网络路由能自动切换到 Serial 专线。
3. 分别在 SH-R1、GZ-R1 路由器上，通过访问控制列表 ACL，实现以下互访安全限制要求：
 - a. 限制 SH 分部的终端不能访问 WebServer（TCP 23）
 - b. 限制 GZ 分部的终端不能访问 WebServer（TCP 8080）
 - c. 两分支机构对网络其它部分访问不限制
4. 配置总部 HQ-SW1 远程管理，要求如下：
 - a. 按照下面图表创建网络管理员用户名与密码：

用户名	密码	所在
User1	Us1Pass	Win2003. ACS (AAA)
Mgmt	MgmtPass	Local



- b. HQ-SW1 只允许 10.1.20.0/24 网段的网管终端 TELNET 远程接入，通过 TACACS+实现集中的身份认证
- c. AAA 服务器如果没响应，身份认证则次选本地认证
- d. 设置 TELNET 连接尝试的安全策略，在 1 分钟内认证失败次数达 3 次时，将禁止访问 TELNET 服务连接 5 分钟
- e. Console 口登录免认证，权限级别为 15

服务器配置

1. 需在 WinServer (Win2003.ACS) 上安装 Cisco ACS4.0 软件，需根据上下文要求做好配置，提供 AAA 服务。
2. WebServer 是由路由器模拟的，需提供基于 TCP 8080 端口的 web 访问服务，已预先完成相关网络、WEB 服务等必要配置，以便提供访问测试。

终端（客户端）配置

1. 按照拓扑图和附表要求，根据网络连接需要，完成主机网络配置



附录：拓扑设备端口及 IP 地址信息表（补充）

所属区域	设备名称	端口(接口)信息	IP/子网掩码	用途
HQ	HQ-SW1	eth0/1	10.1.40.1/30	连接 HQR eth0/1
		eth3/0		链路聚合
		eth3/1		
		Vlan10	10.1.10.252/24	
		Vlan20	10.1.20.252/24	
		Vlan30	10.1.30.1/30	
	HQ-SW2	eth0/1	10.1.50.1/30	连接 HQR eth1/0
		eth3/0		链路聚合
		eth3/1		
		Vlan10	10.1.10.253/24	
		Vlan20	10.1.20.253/24	
		Vlan30	10.1.30.2/30	
	HQR	eth0/0	192.16.12.2/24	连接 ISP
		eth0/1	10.1.40.2/29	连接 HQ-SW1
		eth1/0	10.1.50.2/29	连接 HQ-SW2
		S2/0	172.16.12.1/30	连 SH-R1
		S2/1	172.16.13.1/30	连 GZ-R1
		Loopback0	1.1.1.1/32	
Tunnel 100		172.16.123.1/24		
公网	ISP	eth0/1	192.16.12.1/24	连接 HQR
		eth0/2	192.16.22.1/24	连接 SH-R1
		eth0/3	192.16.32.1/24	连接 GZ-R1
		Loopback0	4.4.4.4/32	
SH	SH-R1	eth0/0	192.16.22.2/24	连接 ISP
		eth0/1	10.2.0.254/24	



所属区域	设备名称	端口(接口)信息	IP/子网掩码	用途
		eth0/1.2	10.2.1.254/24	Dot1q 200
		S2/0	172.16.12.2/30	连 HQR
		Loopback0	2.2.2.2/32	
		Tunnel 100	172.16.123.2/24	
	SH-SW	eth0/0		连接 SH-R1
GZ	GZ-R1	eth0/0	192.16.32.2/24	连接 ISP
		eth0/1	10.3.1.1/24	连接 GZ-R2
		S2/0	172.16.13.2/30	连 HQR
		Loopback0	3.3.3.3/32	
		Tunnel 100	172.16.123.3/24	
	GZ-R2	eth0/0	10.3.0.254/24	
		eth0/1	10.3.1.2/24	

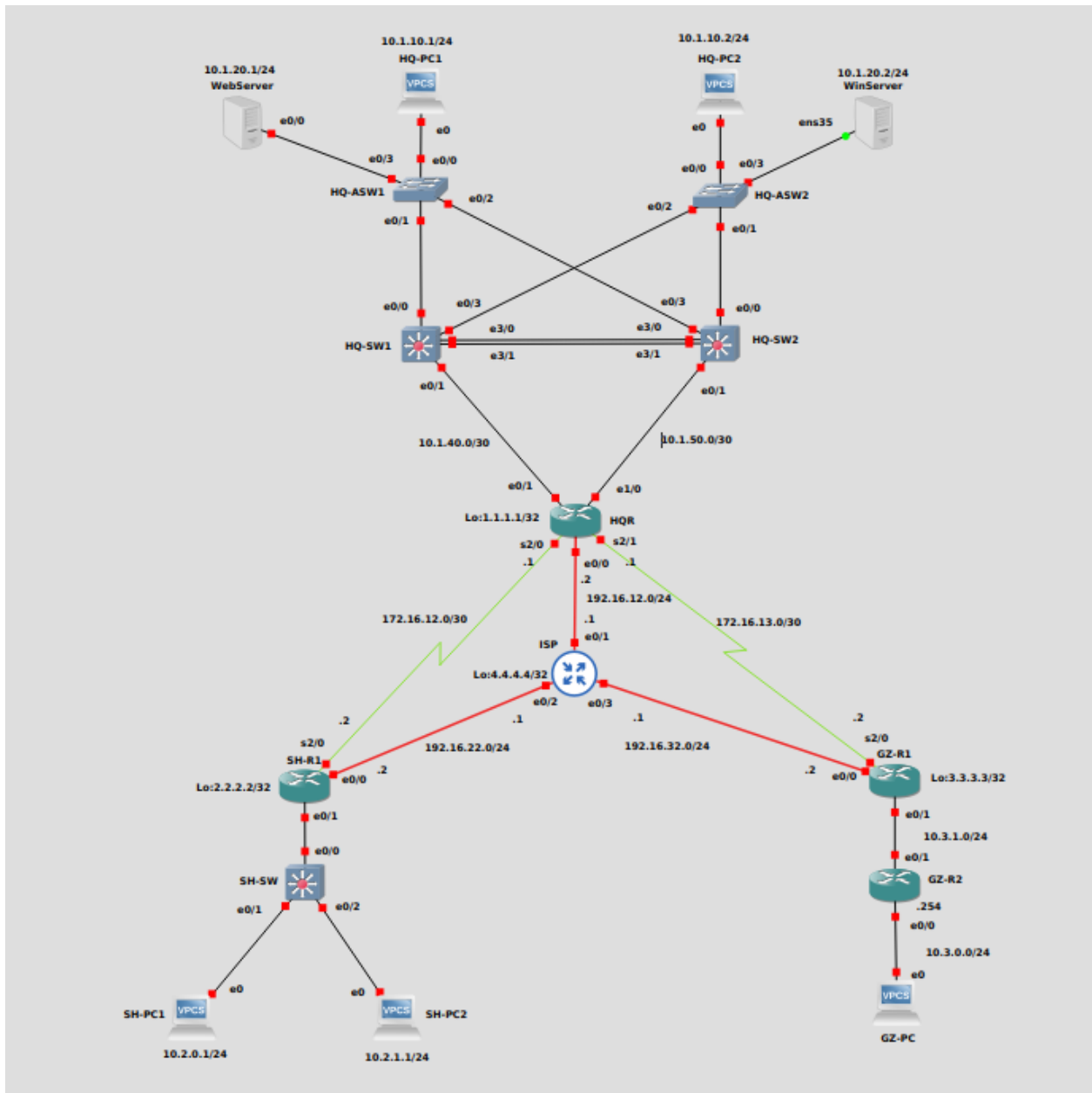


附表：终端（客户端）网络配置

设备名称	设备接口	IP 地址	网关	备注
HQ-PC1	e0	10.1.10.1/24	10.1.10.254	VPC
HQ-PC2	e0	10.1.10.2/24	10.1.10.254	VPC
WebServer	e0/0	10.1.20.1/24	10.1.20.254	路由器模拟
WinServer	本地连接	10.1.20.2/24	10.1.20.254	Win2003.ACS
SH-PC1	e0	10.2.0.1/24	10.2.0.254	VPC
SH-PC2	e0	10.2.1.1/24	10.2.1.254	VPC
GZ-PC	e0	DHCP 获取		VPC

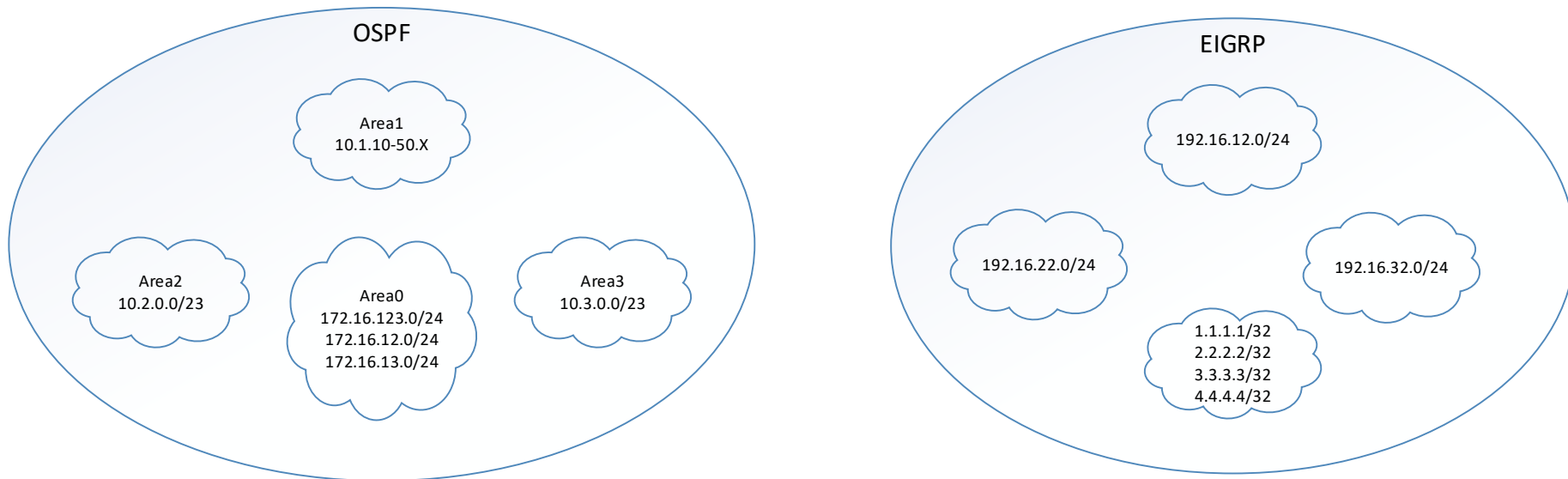


拓扑图





路由示意图



测量分评分表

2023上海市星光杯（中职组）

上海市选拔赛

项目名称 网络系统管理

竞赛日

选手号

子配分说明 网络环境

子模块号

B

评分细则编号	最大分值	评分细则描述	规定或标称值	结果或实际值	实际得分
M1	0.40	HQ-SW1主机名、VTP协议配置正确，结果符合要求			
M2	0.40	HQ-SW2主机名、VTP协议配置正确，结果符合要求			
M3	0.60	HQ-SW1接口Trunk配置符合要求			
M4	0.60	HQ-SW1 VLAN配置符合要求			
M5	0.60	HQ-SW2接口Trunk配置符合要求			
M6	0.80	HQ-SW1-HQ-SW2链路聚合配置符合要求			
M7	0.80	HQ-SW1、HQ-SW2上STP协议配置符合要求			
M8	0.50	HQ-ASW1、HQ-ASW2主机名、VTP协议配置符合要求			
M9	0.50	HQ-ASW1、HQ-ASW2的STP协议配置符合要求			
M10	0.30	HQ-ASW1、HQ-ASW2接口Trunk配置符合要求			
M11	0.30	HQ-ASW1、HQ-ASW2接口其他配置符合要求			
M12	0.80	SH-SW主机名、VLAN、trunking配置符合要求			
M13	0.30	SH-SW 端口安全配置正确			
M14	0.80	HQ-SW1接口IP、掩码、状态配置符合要求			
M15	0.80	HQ-SW2接口IP、掩码、状态配置符合要求			
M16	1.00	HQR主机名、接口IP、掩码、状态配置符合要求			
M17	0.80	SH-R1主机名、接口IP、掩码、状态配置符合要求			
M18	0.80	GZ-R1主机名、接口IP、掩码、状态配置符合要求			
M19	0.50	GZ-R2主机名、接口IP、掩码、状态配置符合要求			
M20	0.80	ISP主机名、接口IP、掩码、状态配置符合要求			
M21	1.00	GZ-PC通过DHCP获取IP符合要求			
M22	1.00	GZ-R1、GZ-R2的DHCP配置正确，结果符合要求			
M23	1.50	HQ-SW1和HQ-SW2上网关高可用性配置正确，结果符合要求			
M24	0.60	HQ-SW1的OSPF配置正确，结果符合要求			
M25	0.60	HQ-SW2的OSPF配置正确，结果符合要求			
M26	0.80	HQR的OSPF配置正确，结果符合要求			
M27	1.00	SH-R1的OSPF配置正确，结果符合要求 EIGRP邻居状态正常			
M28	0.80	GZ-R1的OSPF配置正确，结果符合要求 EIGRP邻居状态正常			
M29	0.40	GZ-R2的OSPF配置正确，结果符合要求 EIGRP邻居状态正常			
M30	1.50	ISP、HQR、SH-R1、GZ-R1 的EIGRP配置正确，结果符合要求 OSPF邻居状态正常			
M31	1.00	HQR与SH-R1之间PPP协议配置符合要求，且连接正常			
M32	1.20	SH-R1公网访问相关配置正确，符合要求			
M33	1.20	HQR的DMVPN配置正确，结果符合要求			
M34	1.00	SH-R1的DMVPN配置正确，结果符合要求			
M35	1.00	GZ-R1的DMVPN配置正确，结果符合要求			
M36	2.00	HQR、SH-R1、GZ-R1之间DMVPN连接IPSec配置正确，结果符合要求			
M37	1.50	分支机构与企业总部内部网络时，选路结果符合要求 DMVPN故障情况下，网络路由能自动切换到Serial专线			
M38	1.50	SH分部-总部之间网络端到端连通性测试结果符合要求			
M39	1.50	GZ分部-总部之间网络端到端连通性测试结果符合要求			
M40	1.00	针对SH分部的终端相关安全访问策略配置正确，结果符合要求			
M41	1.00	针对GZ分部的终端相关安全访问策略配置正确，结果符合要求			
M42	1.50	Win2003.ACS AAA服务器安装、配置符合要求			
M43	1.50	HQ-SW1远程管理配置符合要求，且运作正常			
M44	1.00	对HQ-SW1的远程接入（TELNET）安全策略1设置符合要求			
M45	0.50	对HQ-SW1的远程接入（TELNET）安全策略2设置符合要求			

40.00 子模块分值

实际得分

上海市“星光计划”第十届职业院校技能大赛
(中职组, 样题)
网络系统管理

模块 C

网络自动化运维

DevOps & Programmability Environment

引言

Ansible 是近年越来越火的一款运维自动化工具，其主要功能是帮忙运维实现 IT 工作的自动化、降低人为操作失误、提高业务自动化率、提升运维工作效率，常用于软件部署自动化、配置自动化、管理自动化、系统化系统任务、持续集成、零宕机平滑升级等。它丰富的内置模块（如 acl、command、shell、cron、yum、copy、file、user 等，多达 569 个）和开放的 API 接口，同时任何遵循 GPL 协议的企业或个人都可以随意修改和发布自己的版本。ansible 是一个由 Python 编写的强大的配置管理解决方案。尽管市面上已经有很多可供选择的配置管理解决方案，但他们各有优劣，而 ansible 的特点就在于它的简洁。让 ansible 在主流的配置管理系统中与众不同的一点便是，它并不需要你在想要配置的每个节点上安装自己的组件。

选手须知

首先阅读整个测试项目非常重要。选手需有效地管理时间和决定完成任务的顺序。如上所述，如果遇到一些较难的任务，请不要浪费太多的时间。考生可以使用临时解决方案并继续处理其他任务，如果还有时间的话，可以事后返回并修复那些无法正常运行的问题，在考试中并不排除前后关联性问题，即如果不能解决基础问题则后续问题可能无法继续完成。另外，我们建议在完成后续模块时，检查您之前的是否完成了对应工作。

比赛结束后，选手保存 python 项目中的脚本文件至个人姓名目录，并将目录上传至考场提供的 FTP 目录中。这将是比赛评分检查的主要依据。

第一部分 Linux

环境说明

在比赛网络拓扑图 1 中，选择 192.168.10.1/24 主机，已安装 ansible 做为主控端，其余三台主机为被控端，即 host，请通过一系列模块去管控三台被控端，以完成考试需求。

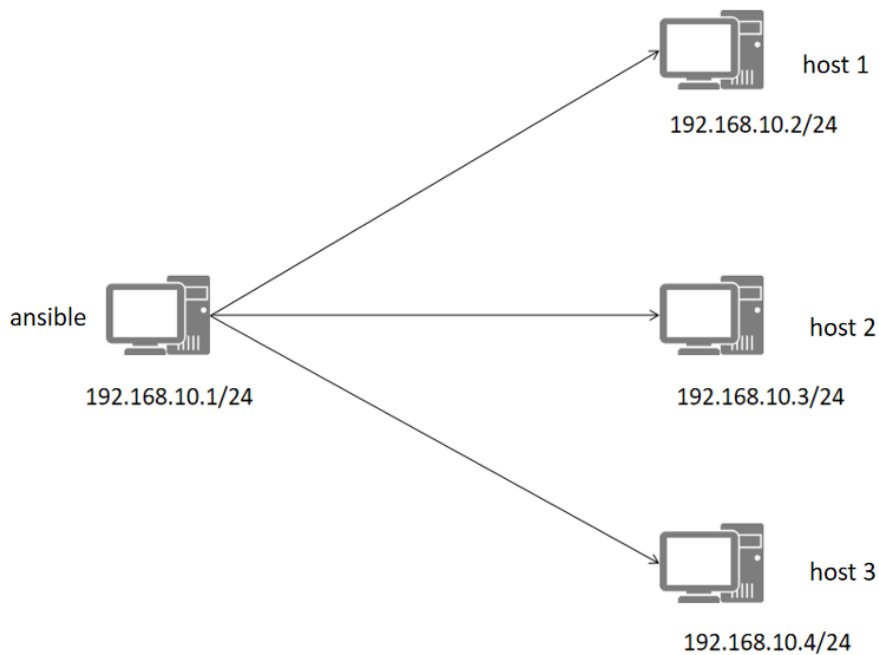


图 1

环境说明：

- 1) 三台被控制端设备名称为：host1、host2、host3；
- 2) 三台被控端系统 root 密码为 123456；
- 3) Ansible 主控端名称为 ansible；
- 4) 主控端系统 root 用户的密码为 123456；
- 5) 如有必要，可配置 SSH 协议远程登录被控系统

题目要求

1. Ansible 主机清单的配置

- 1) 在搭建好的比赛环境中 ansible 已经安装，请将被控端的主机 IP 地址写入主机清单，使得 ansible 得知被控主机数
- 2) 主机清单中，host1 和 host2 为 webservs 组，host2 和 host3 为 dbsrvs 组，host1 和 host3 为 appsrvs 组
- 3) 实施密钥认证，方便后期管理，端口号为 22，登录身份为 root，密码为 123456

2. Command 模块和 Shell 模块的使用（以下指定所有主机）

- 1) 用 command 模块创建一个 /xgb 目录；

2) 在/rgb 目录下用 shell 模块创建一个名为 xingguangbei2 的文件;

3. Copy 模块和 Fetch 模块的使用 (以下指定所有主机)

- 1) 用 copy 模块把源文件/etc/shadow 复制到目的/rgb 下;
- 2) 用 fetch 模块把源文件/var/log/messages 抓取到目的/rgb 下;

4. File 模块的使用 (以下指定所有主机)

- 1) 用 file 模块在/rgb 下创建一个 f2 文件
- 2) 用 file 模块在/rgb 下创建一个 dir2 文件夹

第二部分 网络

环境说明

如图 2 的网络拓环境中, 主控主机已安装 ansible, 其余三台路由器为思科路由器, 通过 ansible 管控这三台路由器

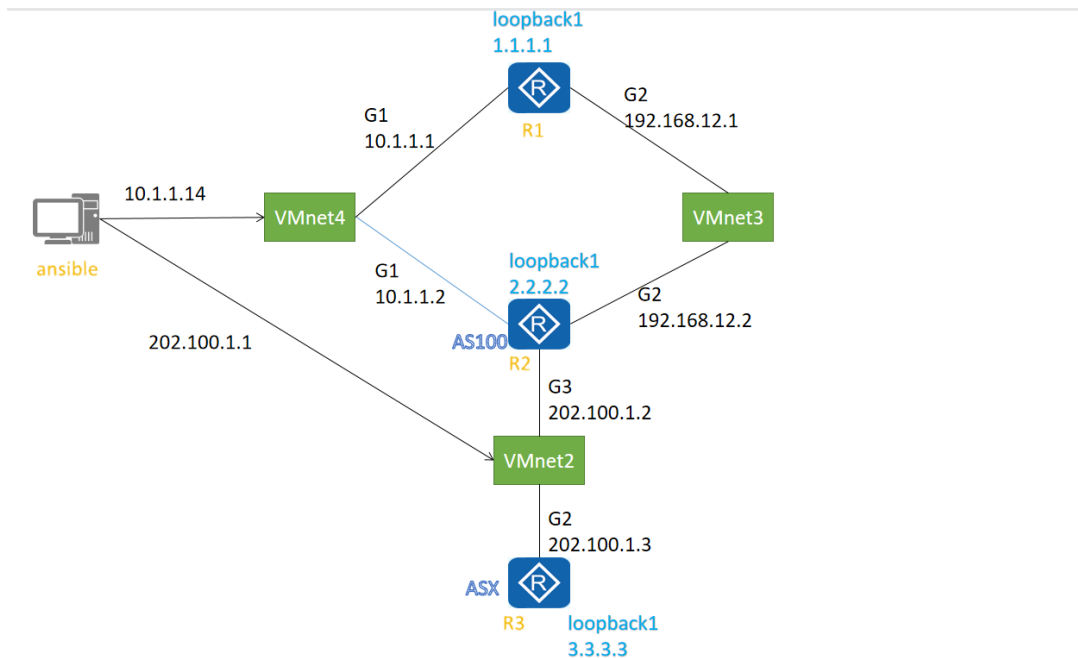


图 2

环境说明:

- 1) 被控制三台设备名称: cvr1000v-1、cvr1000v-2、cvr1000v-3;
- 2) 主控端设备名称为 ansible;

- 3) 主控端系统 root 用户密码为 123;
- 4) 如有必要, 可配置 SSH 协议远程登录被控系统

题目要求:

1. 主机清单和仓库的配置以及密钥认证

- 1) 在搭建好的比赛环境, 调试好网络适配器, 按照图 2 分别在 2 张网卡上配置 2 个 IP 地址, 用 ansible 的 ping 模块测试连通性, 并输出结果
- 2) 配置好主机清单 (hosts) 以及仓库 (inventory) 为了方便管理员后期管理, 请配置配置密钥认证, user 为 qyt, 密码为 qyt

2. 配置 R1/R2 G2 和 loopback 口并测试连通性

- 1) 编写一个名为 xgbSH 的脚本
- 2) R1 的 G2 口地址为 192.168.12.1/24, loopback 口地址为 1.1.1.1/32
- 3) R2 的 G2 口地址为 192.168.12.2/24, loopback 口地址为 2.2.2.2/32
- 4) 脚本中要求显示 R1 和 R2 的所有接口信息

3. 配置 R1 和 R2 的 OSPF

- 1) 编写一个名为 xgbOSPF 的脚本
- 2) 运行 OSPF 协议, 要求接口下开启 OSPF
- 3) 要求把 R1/R2 的 loopback 口地址也宣入 OSPF
- 4) 脚本中要求查看 R1/R2 的 OSPF 相关配置

