

网络管理与运维赛项·样题（学生卷）

淮安市状元大赛 · 学生组 · 个人赛 · 2026 年

一、赛项信息

项目	内容
赛项名称	网络管理与运维
组别	学生组（个人赛，每位选手独立完成全部任务）
竞赛时长	180 分钟
满分	100 分（百分制）
竞赛形式	只考核技能，不单设理论考试

1.1 设备与平台清单（单工位）

类别	设备/软件	数量	备注
交换设备	三层交换机（DCN CS6200 级）	2 台	核心交换机 SW-1、SW-2
交换设备	二层接入交换机（DCN S4600 级）	2 台	接入交换机 SW-3、SW-4
无线设备	无线控制器（DCN AC）	1 台	接入 SW-2
无线设备	无线接入点（DCN AP，含供电模块）	2 台	AP-1、AP-2，由 AC 纳管
安全设备	边界防火墙（DCN DCFW-1800 级）	1 台	FW-1
虚拟化平台	虚拟化主机（不低于 8 核 16GB）	1 台	承载两台服务器虚拟机
终端	客户端计算机	2 台	PC-1（运维测试）、PC-2
软件	KVM / VMware 等虚拟化软件	1 套	赛前由赛场统一安装授权
软件	SecureCRT、Wireshark、抓包工具	各 1 套	放置于选手机 D 盘 soft

说明一：本赛项不单独配置物理服务器，Linux 与 Windows 服务器均以虚拟机形式部署在虚拟化平台，桥接接入业务 VLAN。

说明二：AP 数量以实际套件配置为准。AP-1 接 SW-3、AP-2 接 SW-4 的 GE0/0/11 端口（POE 供电），由 AC 通过 CAPWAP 无线方式纳管。

1.2 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. 请根据比赛环境清单，检查硬件设备、软件与耗材是否齐全、设备能否正常工作。
- 3. 选手须按题目要求独立完成全部任务，不得相互交流、传递资料或协作操作。
- 4. 操作过程中须及时保存设备配置；比赛结束后所有设备保持运行状态。
- 5. 赛场内不得接入互联网，不得使用自带存储介质与电子资料。
- 6. 提交的文件须严格按题目规定的命名规则与路径保存，未按要求提交的内容不予评分。
- 7. 竞赛结束信号发出后，选手须立即停止操作，双手离开键盘鼠标，原地等待裁判确认。

1.3 结果文档提交要求

选手须在 PC-1 桌面 比赛文档_XX 文件夹（XX 为赛位号）内提交以下材料，命名规则为设备名称.txt：

序号	提交内容	文件名示例
1	交换机 SW-1~SW-4 当前配置文件	SW-1.txt
2	防火墙 FW-1 当前配置文件	FW-1.txt
3	无线控制器 AC 当前配置文件	AC.txt
4	Linux 虚拟机 VM-1 关键配置文件（网络、DHCP、DNS、Nginx、FTP、共享）	VM-1.txt
5	Windows 虚拟机 VM-2 配置记录（导出为文本或截图汇编）	VM-2.txt
6	运维文档（见任务 3.4）	运维文档_XX.docx

二、竞赛拓扑与地址规划

2.1 设备互联关系

见下图（正式卷随卷发放纸质图）。图 3-1 竞赛网络拓扑与设备互联关系图：

2.2 端口分配表

设备	端口	对端设备/终端	用途
FW-1	GE1/0/1	PC-1	Internet 出口（untrust）
FW-1	GE1/0/2	SW-1 E1/0/8	内网网关（trust）
FW-1	GE1/0/3	SW-2 E1/0/9	DMZ 区（dmz）
SW-1	E1/0/1	SW-2 E1/0/1	三层互联 10.0.12.0/24

设备	端口	对端设备/终端	用途
SW-1	E1/0/6、E1/0/7	SW-2 E1/0/6、E1/0/7	Eth-Trunk1 跨设备聚合
SW-1	E1/0/2	SW-3 GE0/0/1	Hybrid
SW-1	E1/0/3	SW-4 GE0/0/2	Hybrid
SW-2	E1/0/2	SW-3 GE0/0/2	Hybrid
SW-2	E1/0/3	SW-4 GE0/0/1	Hybrid
SW-2	E1/0/5	AC	AC 管理 10.10.50.60/24
SW-3	GE0/0/11	AP-1	无线接入点（POE 供电），纳管于 AC
SW-4	GE0/0/11	AP-2	无线接入点（POE 供电），纳管于 AC
SW-3	GE0/0/3~6	销售终端	VLAN10 业务端口
SW-3	GE0/0/7~8	产品终端	VLAN20 业务端口
SW-3	GE0/0/10~12	信息技术终端、VM-1、VM-2	VLAN50 业务端口
SW-4	GE0/0/3~4	法务终端	VLAN30 业务端口
SW-4	GE0/0/5~6	财务终端	VLAN40 业务端口

2.3 IP 地址与 VLAN 规划表

序号	网段名称	网段地址	网关/虚地址	SW-1 地址	SW-2 地址	备注
1	销售业务	10.10.10.0/24	10.10.10.254	10.10.10.252	10.10.10.253	VRRP
2	产品业务	10.10.20.0/24	10.10.20.254	10.10.20.252	10.10.20.253	VRRP
3	法务业务	10.10.30.0/24	10.10.30.254	10.10.30.253	10.10.30.252	VRRP
4	财务业务	10.10.40.0/24	10.10.40.254	10.10.40.253	10.10.40.252	VRRP
5	信息技术业务	10.10.50.0/24	10.10.50.254	10.10.50.252	10.10.50.253	VRRP
6	无线业务	10.10.130.0/24	10.10.130.254			VLAN300，AC 上创建业务网关
7	AP&设备管理	10.10.200.0/24	10.10.200.254	10.10.200.253	10.10.200.252	AP（接二层，POE）、AC 管理地址
8	内网—防火墙互联	10.0.1.0/30	—	10.0.1.2	—	SW-1 E1/0/8
9	DMZ—防火墙互联	10.0.2.0/30	—	—	10.0.2.2	SW-2 E1/0/9
10	核心互联	10.0.12.0/24	—	10.0.12.1	10.0.12.2	OSPF 骨干
11	NAT 地址池	100.99.99.8/30	—	—	—	100.99.99.10~20
12	FW-1	100.99.99.2/30	—	—	—	PC-1:

序号	网段名称	网段地址	网关/虚地址	SW-1 地址	SW-2 地址	备注
	Internet 接口					100.99.99.1
13	VM-1 CentOS	10.10.50.30/24	10.10.50.254	—	—	VLAN50
14	VM-2 WinSvr	10.10.50.40/24	10.10.50.254	—	—	VLAN50
15	SW3 交换机管理地址	10.10.200.30/24	10.10.200.254			
16	SW4 交换机管理地址	10.10.200.40/24	10.10.200.254			

2.4 VLAN 规划表

设备	VLAN 编号	VLAN 名称	端口	说明
SW-3	VLAN10	XS	GE0/0/3~6	销售
SW-3	VLAN20	CP	GE0/0/7~8	产品
SW-3	VLAN50	XXJS	GE0/0/10~12	信息技术（含两台服务器）
SW-4	VLAN30	FW	GE0/0/3~4	法务
SW-4	VLAN40	CW	GE0/0/5~6	财务
SW-1 / SW-2	VLAN200	GL	三层接口	AP&设备管理
SW-1 / SW-2	VLAN300	WLAN	三层接口（业务网关在 AC）	无线业务
AC	VLAN300	WLAN	AP 业务 VLAN	SSID 绑定 VLAN300

2.5 服务器与网络参数

项目	VM-1（Linux）	VM-2（Windows）
部署形式	虚拟化平台虚拟机（VM-1）	虚拟化平台虚拟机（VM-2）
操作系统	CentOS 7.x 最小化安装	Windows Server 2012 R2
主机名	srv1.lab.local	DC01.lab.local
IP 地址	10.10.50.30/24	10.10.50.40/24
网关	10.10.50.254	10.10.50.254
DNS	10.10.50.40	127.0.0.1
初始账号	root / Dcn@2019	Administrator / Dcn@2019
初始状态	网络未配置	加入工作组 worklab
附加资源	提供一块 20GB 未分配磁盘	C 盘剩余 ≥ 30GB

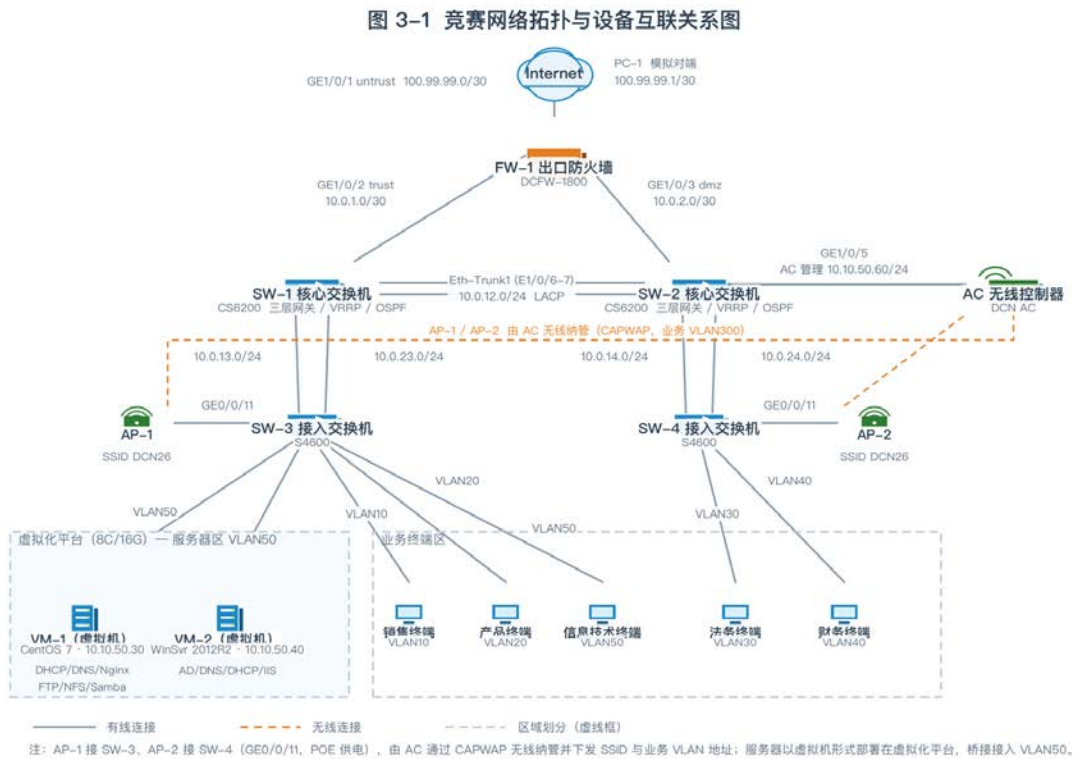
2.6 统一参数

项目	值
设备管理密码	Dcn@2019（全部设备统一，密文保存）
管理员账号	admin，权限级别 15
OSPF 进程号 / 区域	进程 1，业务网段 area 1
OSPF / VRRP 认证密钥	DCN2019
无线 SSID	DCN26
无线认证方式	WPA2-PSK，密钥 Dcn@2019
Web 网站首页关键字	Welcome to DCN Lab

模块一 网络规划与设备配置（45 分）

任务 1.1 布线与基础连接（4 分）

按



- 2.2 端口分配表完成全部设备间及设备与终端的跳线连接，共 10 根跳线。
- 双绞线按 T568B 标准端接，压接后进行通断测试。
- 跳线两端制作标签，标明本端与对端设备名及端口号。
- 机柜内线缆经理线架与扎带整理固定，不得缠绕、悬垂。
- 完成设备加电，确认指示灯正常、无告警；console 管理链路可正常登录。

任务 1.2 VLAN 与端口划分（7 分）

1. 按 2.4 规划表在四台交换机与 AC 上创建 VLAN，名称须与表格一致。
2. 业务端口配置为 **Access** 端口，只允许所属 VLAN 流量通过。
3. 接入交换机上行口配置为 **Hybrid** 类型，透传所属业务 VLAN 与管理 VLAN（VLAN200）。
4. 核心交换机间 Eth-Trunk 链路放通全部业务 VLAN 与管理 VLAN，**禁止 VLAN 1 数据流通过**。
5. 业务端口配置**端口隔离**，同 VLAN 内终端之间二层隔离，仅允许访问网关。

任务 1.3 生成树与链路聚合（7 分）

1. 四台交换机运行 **MSTP** 协议，域名为 **DCN26**，生成树路径开销取值范围为 **1—65535**，BPDU 最大跳数 **7 跳**，拓扑改变刷新次数限制为 **5 次**。
2. 指定 **SW-1** 为（vlan10、20、30）**根桥**（根桥优先级 设置为 0），SW-2 为（vlan 40、vlan50、vlan200）根桥；SW-3、SW-4 不得成为任何 VLAN 的根桥或备份根桥。
3. 所有业务端口配置为**边缘端口**，并启用 BPDU 保护：接口收到 BPDU 时丢弃并关闭端口，**5 分钟**内未收到 BPDU 则自动恢复。
4. SW-1 与 SW-2 之间使用 **E1/0/6、E1/0/7** 组成 **Eth-Trunk1**，采用 **LACP active** 模式，成员口物理 UP 后加入，并在 Eth-Trunk1 上配置三层地址 **10.0.12.1/24**。

任务 1.4 网关冗余 VRRP（5 分）

1. 在 SW-1、SW-2 上为 VLAN10、VLAN20、VLAN30、VLAN 40、VLAN 50、VLAN 200、配置 **VRRP**，实现网关冗余。vlan10、vlan 20、vlan 30 在 SW1 上为 master，vlan 40、VLAN50、VLAN 200、VLAN 300 在 SW2 上为 master。
2. 虚地址使用该 VLAN 中**最后一个可用 IP**；SW-1 使用**倒数第三个可用 IP**（Master 优先级 120，Backup 优先级 60）SW-2 使用**倒数第二个可用 IP**（Master 优先级 120，Backup 优先级 60）。
3. 配置 **Preempt 抢占**，使原 Master 恢复后可重新接管转发。
4. VRRP 认证字符串为 **DCN2019**。

任务 1.5 静态路由与 OSPF 动态路由（8 分）

1. 防火墙需要配置**默认路由**，下一跳 **100.99.99.1**，需要在 OSPF 中引入默认路由。
2. 规划集团使用 **OSPF** 协议（**进程号 1**）实现互联互通：
 - 10.0.12.0 互联网段与防火墙互联段属于**骨干区域 area 0**；
 - 各业务网段（三层接口网段）属于 **area 1**，配置为 **stub no-summary** 区域；
 - 骨干区域启用 **MD5 认证**，密钥 **DCN2019**。
3. 将 SW-1、SW-2 互联的以太网接口网络类型调整为 **P2P**，加快邻居收敛。
4. 业务网段三层接口配置 **silent-interface**，不发送 OSPF 协议报文。
5. 配置**手工汇总路由 10.10.0.0 16** 并引入 OSPF，减少骨干区域 LSA 数量。
6. SW-2 上配置指向无线业务网段汇的静态路由，AC 上配置默认路由下一条地址为 10.10.50.254。

任务 1.6 IPv6 地址与无状态配置（4 分）

1. 在 SW-1 上配置 VLAN10 的 IPv6 地址 2001:10:10::254/64，开启 ND 邻居发现。
2. 在 SW-2 上配置 VLAN20 的 IPv6 地址 2001:10:20::254/64，开启路由公告（RA）功能，RA 生存期为 7200 秒。
3. RA 前缀通告配置：前缀 2001:10:20::/64，有效生存期 2592000 秒，首选生存期 604800 秒，托管标志设置为非托管（无状态）。
4. 在 VLAN20 三层接口上强制发送 RA，确保无线/有线终端一定能获取地址。

任务 1.7 出口安全与地址转换（6 分）

1. 在 FW-1 上划分 4 个安全域：trust、untrust、dmz、local，并将 GE1/0/1 划入 untrust、GE1/0/2 划入 trust、GE1/0/3 划入 dmz。
2. 配置安全策略，实现下列访问控制：
 - 销售、产品、信息技术业务网段（10.10.10.0/24、10.10.20.0/24、10.10.50.0/24）允许访问 Internet，源地址转换；
 - 财务业务网段（10.10.40.0/24）仅允许访问外网 DNS 53、TCP 80、443；
 - 法务业务网段（10.10.30.0/24）只在上班时间可以访问 Internet，（周一到周五 上午 9 点到下午 5 点）；
 - AP&设备管理网段（10.10.200.0/24）禁止任何 Internet 访问，仅允许外网通过 SSH（TCP 22）管理访问 AC 管理地址；
 - 无线业务网段（10.10.130.0/24）允许访问 Internet。
3. 配置 NAT 地址池 100.99.99.10 ~ 100.99.99.20，网关地址 100.99.99.1；业务网段出向 Internet 时做源地址转换。
4. 配置目的地址转换（服务器映射）：Internet 侧 100.99.99.1 访问 100.99.99.10:8080 时，映射到 VM-2（10.10.50.40）的 TCP 8080 服务。

任务 1.8 无线网络配置（4 分）

1. AC 通过 10.10.50.60/24 地址接入 SW-2，完成 AC 的默认网关（10.10.50.254）配置。
2. 在 AC 上创建 SSID DCN26，业务 VLAN 300，地址由 AC 下发（网关 10.10.130.254）。
3. 配置 SSID 认证方式为 WPA2-PSK，密钥 Dcn@2019。
4. AP-1、AP-2 分别接在 SW-3、SW-4 的 GE0/0/11 端口，在 SW-3、SW-4 上将对应端口配置为 trunk，native VLAN200 并开启 POE 供电。
5. 将 AP-1、AP-2 纳管到 AC（CAPWAP），使其状态显示为在线；验证无线终端能获取 10.10.130.0/24 地址段地址并访问 Internet。

模块二 网络服务部署与运维（40 分）

任务 2.1 Linux 网络服务（VM-1: CentOS 7）（20 分）

2.1.1 系统基础配置（5 分）

1. 设置主机名 `srv1.lab.local`，配置 `/etc/hosts` 使 `srv1.lab.local`、`www.lab.local`、`files.lab.local` 解析到 `10.10.50.30`。
2. 为 `ens33` 配置静态地址 `10.10.50.30/24`、网关 `10.10.50.254`、DNS `10.10.50.40`，配置开机自动生效。
3. 关闭 `firewalld` 并设置开机不启动，SELinux 置为 `disabled`。
4. 配置完成后重启服务器，验证网络配置仍然有效。

2.1.2 磁盘配额与虚拟化运维（5 分）

1. 对提供的 20GB 未分配磁盘 `/dev/sdb` 分区：创建 2 个主分区，类型均为 LVM。
2. 创建卷组 `vgdata` 与两个逻辑卷：`lvdata`（2GB）、`lvbackup`（1GB）。
3. `lvdata` 格式化 `ext4` 挂载至 `/data`，`lvbackup` 挂载至 `/backup`，使用 `UUID` 配置 `/etc/fstab` 开机自动挂载。
4. 在 `/data` 下创建目录 `/data/quota`，配置磁盘配额：限制 `fin01` 用户（若不存在可用 `quotouser` 用户）可用空间不超过 **100MB**（软限制 80MB）。
5. 在虚拟化平台对 VM-1 创建快照（命名 `srv1-init`），并演示克隆一台 VM 验证服务可迁移。

2.1.3 DHCP 与 DNS 服务（5 分）

1. 安装并设置 `dhcp` 服务开机自启动，配置地址池 `finance`：网段 `10.10.40.0/24`，地址范围 `10.10.40.100 ~ 10.10.40.200`，网关 `10.10.40.254`，DNS `10.10.50.40`，租期 4 小时，排除网关地址 `10.10.40.254` 1。
2. 在 SW-1 的 `Vlanif40` 接口配置 DHCP 中继，指向服务器 `10.10.50.30`，使财务网段终端可获取地址。
3. 安装并设置 `bind` 服务开机自启动，配置 `lab.local` 正向区域，将 `srv1`、`www`、`files` 指向 `10.10.50.30`，`dc01` 指向 `10.10.50.40`，SOA 序列号为 `20261008`。
4. 使用 `dig` 验证正向前进解析正确。

2.1.4 Web、FTP 与文件共享服务（5 分）

1. 安装并设置 `nginx` 开机自启动，默认站点监听 `8080` 端口，首页 `/usr/share/nginx/html/index.html` 内容包含 `Welcome to DCN Lab`。
2. 配置虚拟主机 `www.lab.local`：监听 `80` 端口，根目录 `/data/quota`，开启目录索引 `autoindex on`。
3. 配置虚拟主机 `files.lab.local`：仅允许 `10.10.50.0/24` 网段访问，其余返回 403（`allow/deny`）。

4. 安装并设置 **vsftpd** 开机自启动，配置匿名用户可读、禁止上传，服务端口 21。
5. 配置 **samba** 开机自启动，共享目录 **/data/quota**，共享名 **share**，只读，创建用户 **cw**（密码 **Dcn@2019**）。
6. 编写 Shell 脚本 **/backup/backup.sh**（赋予执行权限），实现每日 **02:00** 将 **/data/quota** 打包为 **/backup/quota_\$(date +%Y%m%d).tar.gz**，并配置 **crontab** 定时执行。

任务 2.2 Windows 网络服务（VM-2: Windows Server 2012 R2）（20 分）

2.2.1 系统基础配置（4 分）

1. 将计算机名改为 **DC01**，设置 **DNS 后缀 lab.local**，重启后生效。
2. 配置静态 IPv4 地址 **10.10.50.40/24**，网关 **10.10.50.254**，首选 DNS **127.0.0.1**。
3. 重启服务器，验证网络配置仍然有效。

2.2.2 活动目录域服务（6 分）

1. 将 VM-2 安装为域控制器，域名 **lab.local**，功能级别 Windows Server 2012 R2，配置 DSRM 密码 **Dcn@2019**，安装完成后重启。
2. 创建组织单位（OU）：**Sales**、**Product**、**Finance**。
3. 创建用户 **sales01**、**sales02**（Sales OU）与 **fin01**（Finance OU），密码均为 **Dcn@2019**，勾选密码永不过期。
4. 创建全局组 **SalesTeam**、**FinTeam**，并将 **sales01**、**sales02** 加入 **SalesTeam**，**fin01** 加入 **FinTeam**。
5. 配置一条组策略：对域内所有计算机禁用页面文件管理器（**gpedit.msc** 或组策略管理），或为 Finance OU 内用户设置登录脚本。

2.2.3 DNS、DHCP 与 IIS 服务（5 分）

1. 在 VM-2 上添加 **DNS 主要区域 lab.local**，添加记录：**srv1** → **10.10.50.30**、**www** → **10.10.50.40**、**dc01** → **10.10.50.40**、**MX** → **mail.lab.local**。
2. 安装 **DHCP 服务器**，创建作用域 **DHCP-XXJS**，地址范围 **10.10.50.60 ~ 10.10.50.79**，掩码 **255.255.255.0**，网关 **10.10.50.254**，DNS **10.10.50.40**，租期 **2 天**，排除地址 **10.10.50.40**。
3. 验证 DHCP 服务已启动（DNS 客户端可获取地址）。
4. 安装 **IIS**，默认站点绑定 **TCP 443** 端口并启用 **HTTPS**（自签名证书）。
5. 在 **C:\inetpub\wwwroot** 创建 **index.html**，内容包含 **Welcome to DCN Lab**，验证 **https://10.10.50.40** 可正常访问。

2.2.4 文件共享、权限与配额（5 分）

1. 创建并共享文件夹 **Share**。
2. 配置共享权限：**SalesTeam** 读取、**FinTeam** 修改。

3. 配置 NTFS 权限: SalesTeam 读取与写入、FinTeam 完全控制; 说明并验证实际生效权限为共享权限与 NTFS 权限的交集。
4. 为共享文件夹配置磁盘配额: SalesTeam 组可用空间上限 50MB。
5. 通过 net share、icacls、fsutil quota query c: 等命令验证配置结果。

模块三 网络安全管理与运维 (15 分)

任务 3.1 交换机安全防护 (5 分)

1. 在 SW-3、SW-4 上配置端口安全: 业务端口最大 MAC 地址数为 2, 超出则丢弃并记录日志。
2. 在 SW-3、SW-4 上启用 ARP 检查 (ARP 源地址检测), 防止 ARP 欺骗。
3. 在 SW-3 上启用 DHCP 监听 (DHCP Snooping), 绑定可信 DHCP 服务器地址 10.10.50.30。
4. 在接入交换机上配置 IP 与 MAC 地址绑定, 将 VLAN50 中服务器地址与 MAC 静态绑定。

任务 3.2 设备管理安全 (3 分)

1. 为全部网络设备配置 SSH 远程登录 (端口 22), 认证方式 AAA, 关闭 HTTP 服务。
2. 配置登录失败防护: 连续失败 3 次锁定 15 分钟。
3. 配置 ACL 限制管理访问源, 仅允许管理网段 10.10.200.0/24 访问设备的 SSH 服务。
4. 将 VLAN200 配置为管理 VLAN, 管理 VLAN 与业务 VLAN 之间二层隔离 (禁止业务 VLAN 访问 VLAN200)。

任务 3.3 日志采集与分析 (2 分)

1. 配置 SNMPv2c, 团体字串 dcnet2019, Trap 主机 10.10.200.10, 开启 LinkDown、LinkUp、OSPF 邻居变化三类 Trap。
2. 配置 Syslog 日志服务器 10.10.200.30, 日志级别 information。
3. 配置 NTP: SW-1 作为 NTP Server (时钟源 10.10.200.20), 其余设备同步 SW-1。
4. 在 PC-1 上通过 Wireshark 抓取并分析一次 SNMP Trap 或 Syslog 日志报文, 写明关键字段。

任务 3.4 故障排查与运维文档 (5 分)

3.4.1 故障排查 (3 分)

按下列故障现象定位并排除, 写出排查命令、定位过程、原因与解决措施:

1. VLAN50 终端能 ping 通 10.10.50.254, 但无法访问 VM-1 (10.10.50.30) 的 Web 服务。
2. SW-1 与 SW-2 的 OSPF 邻居长时间停留在 ExStart 状态。

3.4.2 运维文档（2 分）

提交 运维文档_XX.docx，须包含：

- 1. 拓扑说明：网络拓扑图与设备连接关系描述（可截图手绘）。
- 2. 地址规划表：VLAN、网段、网关、设备互联地址与服务器地址。
- 3. 关键配置说明：核心交换机、无线控制器、防火墙的关键配置片段及用途注释。
- 4. 测试记录：关键连通性测试结果（VLAN 间互通、服务器服务访问、无线接入、Internet 访问）截图或记录。

三、时间分配建议（180 分钟）

阶段	建议用时	内容
第一阶段	0~15 分钟	布线、设备登录、连通性确认
第二阶段	15~45 分钟	模块一（VLAN/MSTP/聚合/VRRP/路由/IPv6/安全/无线）
第三阶段	45~100 分钟	模块二（Linux 4 题 + Windows 4 题）
第四阶段	100~130 分钟	模块二补齐与模块三安全配置
第五阶段	130~165 分钟	模块三故障排查与运维文档
第六阶段	165~180 分钟	全面验证、保存配置、整理提交文档

提示：虚拟机部署耗时较长，建议在第一阶段布线完成后立即启动虚拟化平台创建两台服务器，与网络配置并行推进。

四、竞赛素养要求（不单独计分，违反将按规则扣分）

- 1. 遵循企业生产 6S 管理规范：整理、整顿、清扫、清洁、素养、安全。
 - 2. 工位整洁有序，工具、线缆、设备规范摆放。
 - 3. 提交文档整洁规范，截图清晰、有序、可辨识，按题目要求命名与归位。
 - 4. 遵守赛场纪律，服从裁判与工作人员安排，不得进行与竞赛无关的操作。
- 本样题依据《淮南市状元大赛网络管理与运维赛项技术文件》编写，题量与分值可依据赛前样题评审结果在 30% 范围内调整。