实验报告三

|  |  |  |
| --- | --- | --- |
| **姓名：彭彦杰** | **时间：2025.05.29** | **评分：** |

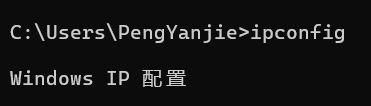
# Windows常用命令练习

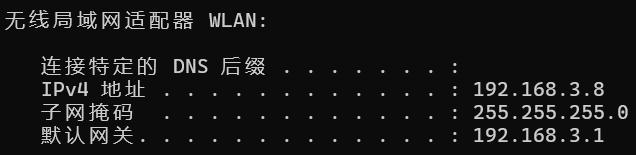
## Ping网关及域名

**1. 打开命令提示符（CMD）：**

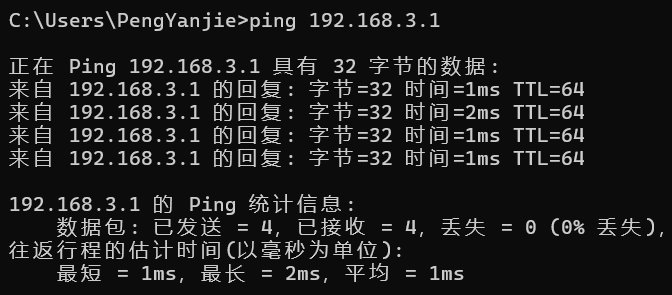
按下Win + R打开运行窗口 → 输入cmd → 回车。

**2. 查找网关地址**

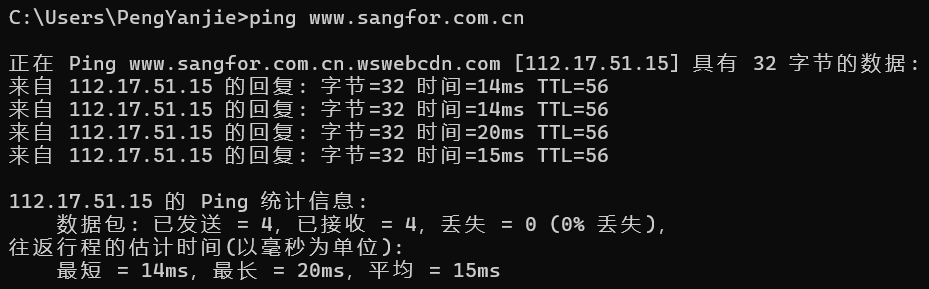




**3. Ping网关地址**



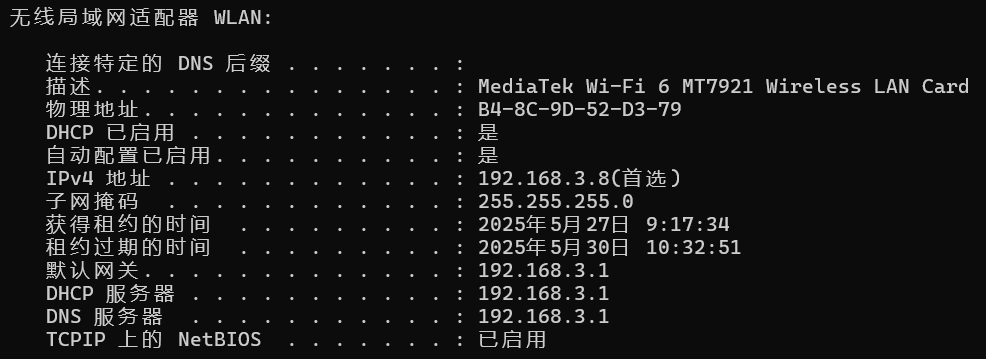
**4. Ping域名**



## 检查IP、MAC地址及直连路由

**1. 查看IP和MAC地址**





**2. 查看直连路由**







## 查看并删除ARP条目

**1. 查看ARP表**

arp -a

**2. 删除网关ARP条目**

arp -d 192.168.3.1

**3. 观察网络问题**

短暂无法访问互联网（浏览器打不开网页）。

原因：删除ARP条目后，PC需重新通过ARP请求获取网关MAC地址。

恢复：等待几秒后，ARP表自动重建，网络恢复正常。

## Tracert追踪访问路径

**1. 输入命令：**

tracert www.sangfor.com.cn

**2. 结果：**



显示数据包经过的每一跳（路由器或服务器）IP及延迟。

\* 表示节点未响应（可能防火墙阻止ICMP）。

# LDAP实验

## LDAP协议

**1. 需求背景**

核心痛点：

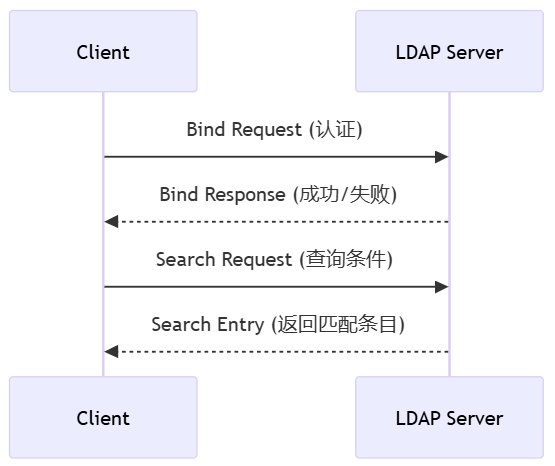
* 企业存在多套系统（邮箱/VPN/文件服务器），用户需记忆多组账号密码
* 员工离职后权限回收不全，存在安全风险

LDAP解决方案：

集中存储用户/组织架构信息（树形目录）

提供标准化接口供各系统查询认证（如cn=user1,ou=IT,dc=company,dc=com）

**2. 工作原理**



**3.** **报文结构解析**

LDAP协议报文结构

|  |  |  |
| --- | --- | --- |
| **操作类型** | **请求报文关键字段** | **响应报文关键字段** |
| Bind | version, name, simpleAuth | resultCode (0=成功) |
| Search | baseObject, filter, scope | objectName, attributeList |
| Modify | object, modification | resultCode |

## AD域

**1. 需求背景**

企业痛点：

* 200台电脑需统一设置密码策略（如长度+复杂度）
* 销售部员工需自动映射网络驱动器

AD域价值：

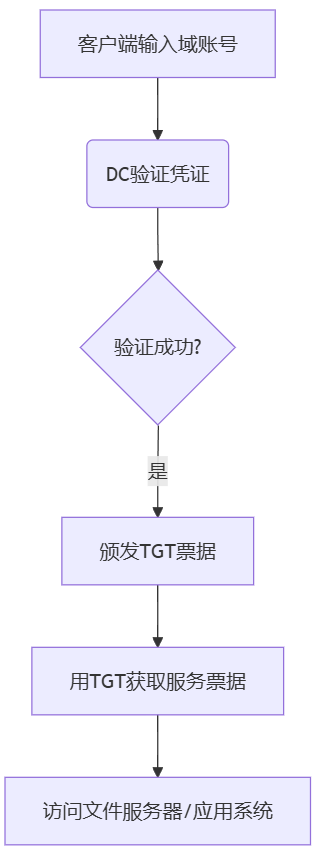
* 集中管理用户/计算机/策略
* 单点登录访问所有域资源

**2.** **核心组件**

AD域核心组件

|  |  |  |
| --- | --- | --- |
| **组件** | **作用** | **关键文件/命令** |
| 域控制器(DC) | 存储目录数据库，处理认证请求 | NTDS.dit (数据库文件) |
| DNS服务器 | 解析域内资源名称 | \_ldap.\_tcp.dc.\_msdcs SRV记录 |
| 组策略对象(GPO) | 统一配置用户/计算机策略 | gpmc.msc (管理控制台) |
| Kerberos协议 | 实现安全票据认证 | klist (查看票据) |

**3. 认证流程**



## AD域的搭建和组策略

**1. 搭建AD域（Windows Server）**

# 安装AD域服务

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

# 提升为域控制器

Install-ADDSForest -DomainName "corp.company.com" -InstallDNS

**2.** **组策略经典应用**

组策略经典应用

|  |  |
| --- | --- |
| **场景** | **GPO配置路径** |
| 禁用USB存储 | 计算机配置→策略→管理模板→系统→可移动存储访问 |
| 强制密码复杂度 | 计算机配置→策略→Windows设置→安全设置→账户策略→密码策略 |
| 开机自动映射网络驱动器 | 用户配置→首选项→Windows设置→驱动器映射→新建→操作=更新，位置=\\filesrv\share |

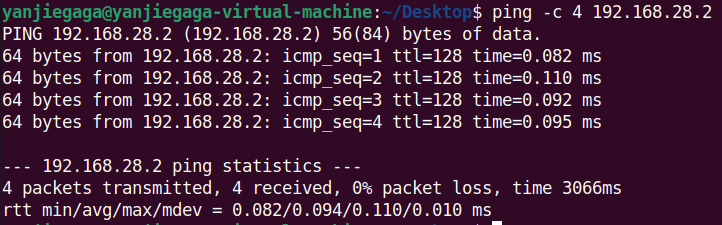
# Linux常用命令

## Ping网关及域名

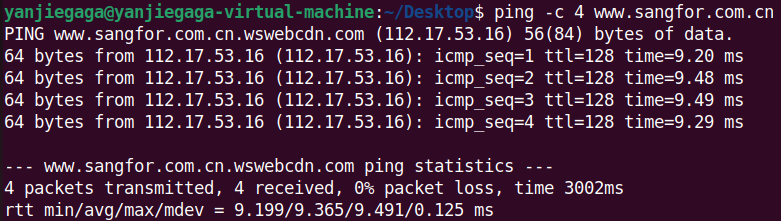
**1. 查找网关地址**



**2. Ping网关**



**3. Ping域名**

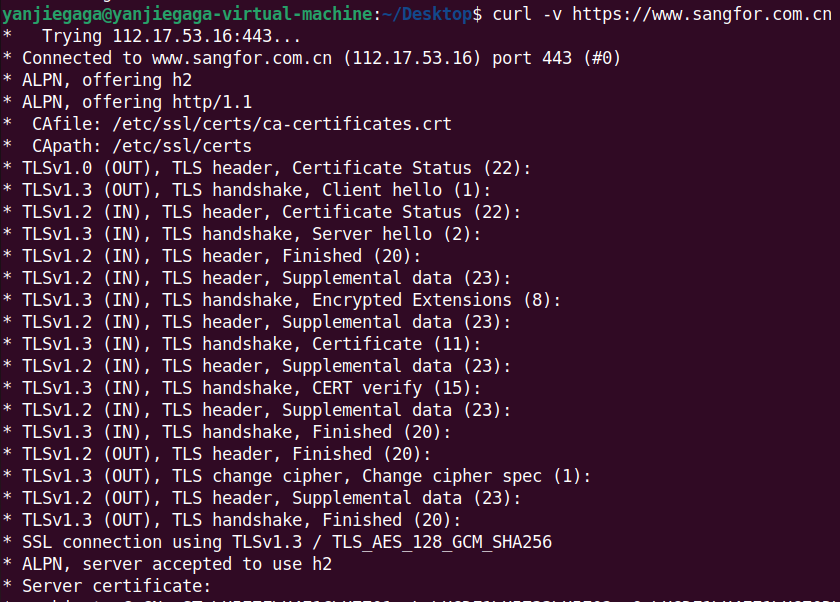


## 访问域名（使用curl）

**1. 访问域名：**

curl -v <https://www.sangfor.com.cn>

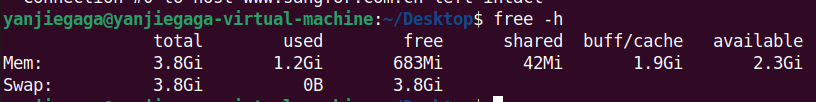
-v参数显示详细连接过程（含SSL握手信息）



## 系统信息检查

**1. 内存占用（free）**

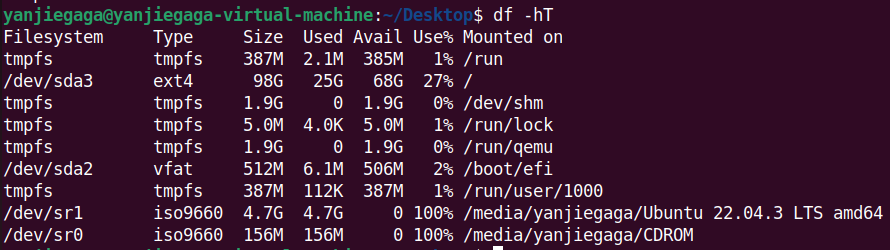
free -h # -h参数人性化显示单位



* total：总内存
* used：已用内存
* free：空闲内存
* buff/cache：缓存占用

**2. 磁盘分区（df）**

df -hT # -h人性化显示，-T显示文件系统类型



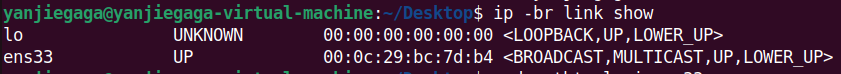
**3. 网口驱动（ethtool）**

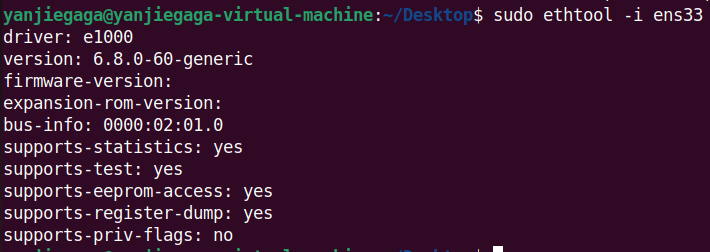
# 先确认网卡名称

ip -br link show

# 查看驱动信息

sudo ethtool -i ens33





driver：驱动名称

version：驱动版本

## tcpdump抓包分析

**1. 开始抓包**

sudo tcpdump -i any -n host www.sangfor.com.cn -w sangfor.pcap

-i any：监听所有网卡

-n：禁用主机名解析

host www.sangfor.com.cn：过滤该域名流量

-w：保存为pcap文件

**2. 触发访问**

curl https://www.sangfor.com.cn > /dev/null

**3. 停止抓包**

按Ctrl+C停止捕获

**4. 分析抓包文件**

wireshark sangfor.pcap

## 常用命令应用场景及用法

### 系统监控与资源管理

**1. top - 实时系统监控**

top -d 2 -p 1234,5678 # 2秒刷新，监控特定PID

应用场景：

* 服务器性能突降时快速定位高负载进程
* 监控关键进程的CPU/内存使用率

**2. free - 内存分析**

free -m -t # 以MB显示，包含总计行

**3. df - 磁盘空间**

df -hT -x tmpfs # 人性化显示，排除临时文件系统

**4. du - 目录空间分析**

du -sh /var/log/\* | sort -hr # 按大小排序

### 网络诊断与操作

**1. ping - 连通性测试**

ping -c 5 -i 0.2 -W 1 www.sangfor.com.cn

**2. netstat - 网络连接分析**

netstat -tulnp # 查看监听端口及进程

**3. tcpdump - 网络抓包**

tcpdump -i eth0 -n 'port 80 and host 192.168.1.100' -w web.pcap

**4. ifconfig/ip - 网络配置**

ip addr show eth0 # 查看IP配置

ip route add 10.0.0.0/24 via 192.168.1.1 # 添加路由

**5. ethtool - 网卡诊断**

ethtool eth0 # 查看基础信息

ethtool -S eth0 # 统计信息（错包/丢包）

### 文件与进程管理

**1. ls - 文件查看**

ls -lath --time-style=full-iso # 完整时间格式

**2. find - 文件搜索**

find /var/log -name "\*.log" -mtime -7 -size +10M

**3. ps - 进程查看**

ps -ef --forest # 树形显示进程关系

**4. kill - 进程控制**

kill -9 $(pgrep -f "java.\*backend") # 强制终止Java进程

### 系统操作与维护

**1. wget/curl - 网络下载**

wget -c --limit-rate=1M https://example.com/large.iso # 限速续传

curl -O -x http://proxy:8080 https://files.example.com # 代理下载

**2. iptables - 防火墙配置**

iptables -A INPUT -p tcp --dport 22 -s 192.168.1.0/24 -j ACCEPT

iptables -L -v -n # 详细规则查看

**3. telnet - 端口测试**

telnet smtp.example.com 25 # SMTP服务测试