计算机网络实验实验报告

学院（系）名称：信息学院

姓名	高星杰	**学号**	2021307220712	**专业**	计算机科学与技术
班级	21 级计算机技术与科学 2 班	**实验项目**	Windows 和 Linux 环境下常用网络命令原理分析与 应用，以及使用交换机局域网组建及其扩展		
课程名称		计算机网络实验		**课程代码**	3103009336
实验时间		2023 年 9 月 28 日星期一		**实验地点**	逸夫楼 C207

考 核内 容	目的和原理 40	内容及过程分析 30	实验方案设计 10	实验结果（结论正确性以及分析合理性）20	**成绩**	
各项得分						
考核标准	○原理明确 ○原理较明确 ○原理不明确	○分析清晰 ○分析较清晰 ○分析不清晰	○设计可行 ○设计基本可行 ○设计不可行	○结论正确，分析合理 ○结论正确，分析不充分 ○结论不正确，分析不合理	**教师签字：**	

1. 实验目的：

（1） 熟悉 windows 下的一些网络命令的功能和使用方法。进而能用这些命令察看网络的状况并解决网络中的一些问题。掌握收发邮件的命令。

（2） 初步掌握使用命令排除错误的问题

2. 实验原理：

2.1 ARP 指令实验原理（链路层）

首先要了解 ARP 协议就要先了解 MAC 地址的概念

MAC 地址（Media Access Control address）又称为物理地址，是用于唯一标识网络设备（如网卡）的全球唯一地址。MAC 地址是一个由 12 个十六进制字符组成的地址，通常以冒号或破折号分隔为 6 个字节。

MAC 地址是在网络设备制造时固化在硬件中的，它与 IP 地址不同，**不会受到网络配置或路由变化的影响**。每个网络设备都有一个**唯一的 MAC 地址**，用于在局域网中进行数据帧的**传输和识别**。需要注意的是，MAC 地址是二层地址，**只在同一个局域网内部起作用，不跨越路由器传输**。而**在互联网上进行通信时，使用的是更高一层的 IP 地址来进行路由和寻址。**

ARP 协议：ARP（Address Resolution Protocol，地址解析协议）是一种用于将 IP 地址解析为 MAC 地址的协议。**它位于网络层（第三层）和数据链路层（第二层）之间。**在局域网（LAN,Local Area Network）中，通信设备使用 MAC 地址来标识自己，而 IP 地址用于进行网络通信。ARP 协议通过将 IP 地址映射到相应的 MAC 地址，实现了 IP 地址与 MAC 地址之间的转换。

它的实现包括以下几个步骤：

1. **发送 ARP 请求：**当一个主机需要知道目标 IP 地址对应的 MAC 地址时，它会发送一个 ARP 请求广播。该广播包含了源 IP 地址、源 MAC 地址、目标 IP 地址等信息。

2. **接收 ARP 请求：**所有在同一物理网络上的主机都会接收到这个 ARP 请求广播。
3. **目标主机响应：**只有目标主机（拥有目标 IP 地址的主机）会收到 ARP 请求后作出响应。目标主机会回复一个 ARP 响应，其中包含自己的 MAC 地址。
4. **更新 ARP 缓存：**发送 ARP 请求的主机收到目标主机的响应后，会将目标 IP 地址和 MAC 地址的映射关系记录在本地的 ARP 缓存中，以便以后重用。

ARP 的实现主要依赖于两个重要的表格：ARP 缓存表和 **ARP 请求表**。

ARP 缓存表：该表记录了已解析过的 IP 地址与对应的 MAC 地址的映射关系。当主机需要访问某个 IP 地址时，首先会查找 ARP 缓存表，如果找到相应的映射关系，则可以直接使用保存的 MAC 地址进行通信，避免发送 ARP 请求。

ARP 请求表：该表记录了待发送的 ARP 请求及其状态。主机发送 ARP 请求后会将目标 IP 地址和对应的请求放入 ARP 请求表中，并等待相应的 ARP 响应。

这样，当一个主机需要与另一个主机通信时，可以通过 ARP 协议先获取目标主机的 MAC 地址，然后使用 MAC 地址进行数据包的传输。ARP 的实现使得主机之间可以在局域网中进行高效的通信和数据交换。

ARP（Address Resolution Protocol）只能获取本地网络中设备的 IP 地址和对应的 MAC 地址，因为他的工作在网络层（OSI 模型的第二层）。

2.2 ftp 指令实验原理

FTP 协议：FTP（File Transfer Protocol，文件传输协议）是一种用于在网络上进行文件传输的标准协议。**FTP 协议工作在计算机网络的应用层。**它使用客户端-服务器模型，在计算机之间传输文件。FTP 通过两个不同的连接进行通信：控制连接和数据连接。控制连接用于发送命令和接收服务器的响应，而数据连接用于实际的文件传输。以下是 FTP 的基本工作流程：

1. **建立连接：**客户端通过控制连接与 FTP 服务器建立连接。客户端通过指定服务器的地址（域名或 IP 地址）来连接到服务器。
2. **登录认证：**客户端发送用户名和密码给服务器，以验证客户端的身份。一旦身份验证成功，客户端就可以执行文件传输操作。
3. **导航和目录操作：**客户端可以使用相关指令（如 ls、cd）查看服务器上的文件和目录，切换当前工作目录等。
4. **文件传输：**客户端可以使用指令（如 get、put）从服务器下载文件到本地系统，或将本地文件上传至服务器。
5. **断开连接：**当完成文件传输后，客户端可以通过 bye 指令断开与服务器的连接。

FTP 还支持被动模式和主动模式的数据连接。在被动模式下，服务器监听一个端口以接收数据连接；而在主动模式下，客户端监听一个端口以接收数据连接。 两者的区别只有数据连接的区别，一般情况下使用的是被动模式，因为被动模式避免了客户端在防火墙、NAT 或代理服务器后面时可能遇到的连接问题。由于数据连接是由服务器在一个随机端口上主动等待客户端的连接，所以被动模式更容易穿越网络设备的限制，确保数据传输的顺利进行。

2.3 Ipconfig 指令实验原理

ipconfig 命令的原理是通过查询和解析操作系统中存储的网络配置信息来获取计算机上的网络接口信息。具体来说，ipconfig 命令会向操作系统发出相关系统调用，并获取返回结果，进而将这些信息输出到命令行终端中。

ipconfig 命令主要用于获取和配置网络接口信息，提供了以下功能：

1. **查看 IP 地址和子网掩码：**ipconfig 命令可以显示计算机上网络接口的 IP 地址和子网掩码，帮助确认网络连接是否正常。
2. **显示默认网关：**ipconfig 命令可以显示计算机所连接网络的默认网关，即数据包在网络中转发时的下一跳地址。
3. **查看物理地址（MAC 地址）：**ipconfig 命令可以显示计算机网络接口的物理地址（MAC 地址），

用于唯一标识网络适配器。

4. **释放和更新 IP 地址**：通过 ipconfig /release 命令，可以释放当前网络接口的 IP 地址；而通过`ipconfig /renew`命令，可以更新当前网络接口的 IP 地址，从 DHCP 服务器获取新的 IP 地址。

5. **刷新 DNS 缓存**：ipconfig /flushdns 命令可以清除本地 DNS 缓存，以便刷新 DNS 记录，解决 DNS 解析问题或更新 DNS 记录。

6. **显示 DNS 服务器信息**：ipconfig 命令可以显示计算机所使用的 DNS 服务器地址，帮助诊断与 DNS 相关的问题。

7. **注册计算机的 DNS 记录**：通过 ipconfig /registerdns 命令，可以向 DNS 服务器注册计算机的 DNS 记录，确保 DNS 服务器具有最新的计算机信息。

这些功能使得 ipconfig 命令成为网络故障排除和网络配置调整的有用工具。它可以帮助了解和管理计算机的网络连接，并提供必要的信息来解决网络问题。

2.4 nbtstat 指令实验原理

了解 nbtstat 指令需要先了解 NetBIOS

NetBIOS（Network Basic Input/Output System）是一种早期的网络通信协议，用于支持局域网中的计算机之间进行通信和资源共享。它最初由 IBM 开发，后来被微软广泛采用在 Windows 操作系统中。NetBIOS 协议提供了一种简单的编程接口，使应用程序能够在本地局域网上进行通信和访问共享资源。它定义了一些基本概念和功能，如 NetBIOS 名称、会话、数据包格式等。

基于 TCP/IP 的 NetBIOS 协议的主要特点包括：

端口号：基于 TCP/IP 的 NetBIOS 协议使用特定的端口号来标识 NetBIOS 会话和连接。通常使用的端口号是 139（NetBIOS 会话服务）和 445（直接主机间通信服务）。

名称解析：基于 TCP/IP 的 NetBIOS 协议使用 WINS（Windows Internet Name Service）服务器来进行 NetBIOS 名称解析。WINS 服务器负责将 NetBIOS 名称转换为 IP 地址，以便进行通信。

广域网支持：由于基于 TCP/IP 的 NetBIOS 协议使用 TCP/IP 作为底层传输协议，因此可以在广域网中进行通信。它可以通过路由器或 VPN 连接连接不同的局域网和子网。

兼容性：基于 TCP/IP 的 NetBIOS 协议可以与旧版的 NetBIOS 协议（如基于 NetBEUI 和 IPX/SPX 的 NetBIOS）进行互操作。这使得在网络环境中使用不同的 NetBIOS 协议栈的计算机之间进行通信成为可能。

nbtstat 是 Windows 操作系统中的一个命令行工具，用于查看和管理 NetBIOS（Network Basic Input/Output System）名称缓存以及与 NetBIOS 相关的网络连接信息。

nbtstat 命令的原理是通过查询和解析 NetBIOS 相关的网络信息来获取计算机上的 NetBIOS 名称缓存、会话表和连接表等信息。具体来说，nbtstat 命令会向操作系统发出相关**系统调用**，并获取返回结果，进而将这些信息输出到命令行终端中。

2.5 net 指令实验原理

Net 命令有很多函数用于实用和核查计算机之间的 NetBIOS 连接，可以查看我们的管理网络环境、服务、用户、登陆等信息内容

Net 指令合集：

Net User

作用：添加或更改用户帐号或显示用户帐号信息。

命令格式：Net user [username [password | *] [options]] [/domain]

有关参数说明：

- 键入不带参数的 Net user 查看计算机上的用户帐号列表
- username 添加、删除、更改或查看用户帐号名
- password 为用户帐号分配或更改密码
- 提示输入密码
- /domain 在计算机主域的主域控制器中执行操作。该参数仅在 Windows NT Server 域成员的

Windows NT Workstation 计算机上可用。默认情况下，Windows NT Server 计算机在主域控制器中执行操作。注意：在计算机主域的主域控制器发生该动作。它可能不是登录域。

例如：Net user ghq123 查看用户 GHQ123 的信息。

2.6 netstat 指令实验原理

用于显示网络连接、路由表和网络接口等网络相关信息。它通过读取操作系统的网络协议栈的信息，包括当前的网络连接、端口状态等。这些信息通常被操作系统用于管理网络连接和数据传输。

1. 访问网络协议栈：

当在命令行中输入 netstat 指令时，操作系统会**调用相应的网络 API** 来获取当前系统上的网络连接信息。这些信息存储在操作系统的网络协议栈中，包括已建立的网络连接、监听中的端口、路由表等。

2. 获取网络连接信息：

netstat 通过操作系统提供的系统调用（system calls）来获取网络连接信息。这些信息通常保存在内核的数据结构中，如 TCP 连接表和 UDP 套接字表。netstat 会读取这些数据结构，以获得有关网络连接的详细信息，例如本地地址和端口、远程地址和端口、连接状态等。

3. 显示网络连接：

netstat 将从操作系统获取的网络连接信息格式化并显示在命令行界面上。用户可以看到本地计算机上的所有活动网络连接，包括 TCP 和 UDP 连接，以及监听中的端口。这个信息可以帮助用户监视网络活动、查找网络问题和进行网络分析。

总的来说，netstat 的原理是通过操作系统提供的**系统调用**，访问网络协议栈中的**数据结构**，然后将获取的**网络连接信**息以用户友好的方式呈现给用户。这使得用户可以在命令行界面上查看当前系统的**网络状态**和**活动连接。**

2.7 ping 指令实验原理

ping 是一个常用的网络诊断工具，用于测试主机之间的网络连接。它的原理基于 ICMP（Internet Control Message Protocol，互联网控制消息协议）协议，该协议是在网络层（OSI 模型中的第三层）上工作的。下面是 ping 指令的实验原理：

发送 ICMP Echo 请求：

当在命令行中输入 ping 命令，操作系统会创建一个 ICMP Echo 请求消息（也称为 ping 请求）。这个消息包含了目标主机的 IP 地址，以及一些其他的控制信息。这个消息的目的是要求目标主机响应，以确认目标主机是否可达并且能够正常回应请求。

发送 ICMP Echo 请求消息：

操作系统将 ICMP Echo 请求消息发送到指定的目标主机。这个消息经过计算机网络中的路由器和交换机等设备，沿着网络路径传输到达目标主机。

目标主机响应：

如果目标主机是可达的并且能够正常工作，它将接收到的 ICMP Echo 请求消息视为一种请求，并会生成一个 ICMP Echo 回应消息（ping 回应）。这个回应消息包含了相同的数据，表明目标主机已经收到了请求。

接收 ICMP Echo 回应消息：

源主机（发起 ping 请求的计算机）接收到目标主机发送的 ICMP Echo 回应消息。通过分析回应消息的时间戳等信息，源主机可以计算出往返时间（Round-Trip Time，RTT），即从发送请求到接收回应所经历的时间。

显示结果：

操作系统将往返时间（RTT）、丢包率（如果有的话）等信息显示在命令行界面上，供用户查看。如果目标主机不可达或者网络连接有问题,ping 命令会显示相应的错误信息,帮助用户进行网络故障排除。

总的来说,ping 命令的实验原理基于发送 ICMP Echo 请求消息,接收并分析目标主机的 ICMP Echo 回应消息，以及计算往返时间和显示结果。这样的操作帮助用户确定网络连接的状态，发现潜在的网络问题。

2.8 route 指令实验原理

route 命令是一个用于**查看或配置操作系统的路由表的命令**。路由表是一个记录了网络数据包应该被发送到哪个网络接口的数据结构。下面是 route 指令的实验原理：

1. 查看路由表：

当在命令行中输入 route print（在 Windows 系统中）或者 route -n（在 Linux/Unix 系统中），操作系统会显示当前计算机的路由表。这个路由表包含了到达各个网络的路由信息，包括目标网络的 IP 地址、子网掩码、网关地址、以及数据包应该被发送到哪个网络接口。

2. 添加路由规则：

如果使用 route add 命令添加一条路由规则，操作系统会根据你提供的信息，将新的路由规则添加到路由表中。这个信息包括目标网络的 IP 地址、子网掩码、网关地址和网络接口。当你添加一条路由规则后，操作系统会将这个规则应用到路由表，确保将数据包发送到正确的网络接口。

3. 删除路由规则：

使用 route delete 命令可以删除路由表中的一条路由规则。这样，操作系统会将这条规则从路由表中移除，不再使用它来决定数据包的路由路径。

4. 修改路由规则：

使用 route change 命令可以修改路由表中现有规则的属性。你可以修改目标网络的 IP 地址、子网掩码、网关地址和网络接口等信息。这个命令允许你调整现有的路由规则，以满足网络配置的需求。

5. 原理：route 命令的原理是通过操作系统提供的系统调用（system calls）来访问和修改路由表。当你使用 route 命令时，操作系统会根据你提供的参数执行相应的系统调用，以便更新路由表。这些路由表的变化会影响到操作系统处理数据包的方式，确保数据包被正确地路由到目标网络。

总的来说，route 命令的实验原理是通过系统调用访问和修改操作系统的路由表，以实现网络数据包的正确路由。

2.9 Telneth 指令实验原理

"Telnet" 是一种用于在远程计算机上执行命令和管理网络设备的协议和工具。在命令行界面中，telnet 命令允许用户连接到远程主机并与其进行文本通信。以下是 telnet 命令的工作原理：

建立连接：当你在命令行中输入 telnet 命令，你需要指定目标主机的 IP 地址或域名以及连接的端口号（默认端口为 23）。操作系统会尝试与目标主机建立网络连接。

发起连接：一旦连接建立，telnet 客户端会发送一个连接请求到目标主机。这个请求包括通信协议、终端类型、终端大小等信息。

接受连接：目标主机上的 Telnet 服务器会接受连接请求，验证客户端的身份（如果需要的话），并建立一个 Telnet 会话。这个会话允许客户端与远程主机进行双向文本通信。

文本通信：一旦 Telnet 会话建立，你可以在本地命令行上键入命令，然后这些命令会通过 Telnet 会话发送到远程主机。远程主机会执行这些命令，并将结果返回给你的本地终端。这使你能够在远程主机上执行操作，就好像你直接在那台主机上工作一样。

终止连接：当你完成与远程主机的操作后，你可以关闭 Telnet 会话，并断开与远程主机的连接。通常，你可以在 Telnet 会话中键入特定的命令来退出会话。

telnet 命令的原理是建立一个虚拟终端连接，使本地终端与远程主机之间可以进行文本通信。这种通信通过 Telnet 协议实现，通常是明文传输，因此在公共网络上使用时需要注意安全性，最好使用加密通信（如 SSH）以保护敏感信息。

2.10 Tracert 指令实验原理

tracert（在 Windows 系统中称为 tracert，在 Unix/Linux 系统中称为 traceroute）是一个用于诊断网络问题和跟踪数据包在网络上的路径的命令行工具。它的原理基于 ICMP 协议（Internet Control Message Protocol，互联网控制消息协议）。

以下是 tracert 指令的实验原理：

发送 ICMP 探测数据包：当你在命令行中输入 tracert 命令，操作系统会创建一系列的 ICMP 探测数据

包，每个数据包的 TTL（Time-To-Live，生存时间）字段被设置为逐跳递增的值。ICMP 数据包中包含了目标主机的 IP 地址。

发送第一个数据包：tracert 命令会将第一个 ICMP 数据包发送到目标主机。这个数据包的 TTL 值通常设置为 1。当第一个路由器（或者目标主机本身）收到这个数据包时，TTL 值变为 0，路由器将数据包丢弃，并向发送者发送 ICMP 时间超时消息。

逐跳跟踪：每当一个中间路由器（或者目标主机）收到一个 ICMP 数据包，它会将 TTL 减 1。如果 TTL 减为 0，路由器会丢弃数据包并发送 ICMP 时间超时消息。tracert 通过检测这些 ICMP 时间超时消息，确定数据包在网络上的路径。

收集响应：tracert 会收集每个中间路由器返回的 ICMP 时间超时消息。这些消息中包含了路由器的 IP 地址和往返时间（RTT）。通过这些信息，tracert 可以确定数据包的路径，并估计每一跳的延迟。

显示结果：tracert 命令将收集到的路由信息和往返时间显示在命令行界面上，供用户查看。这些信息帮助用户了解数据包在网络上的路径，以及诊断网络中的潜在问题，例如延迟、丢包或路由循环等。

总的来说，tracert 指令的实验原理是通过发送逐跳递增 TTL 的 ICMP 数据包，检测每个路由器的响应（ICMP 时间超时消息），从而确定数据包在网络上的路径和延迟。

3. 实验分析：

实验内容是首先是要了解每个指令的功能，其次按照指令的格式来完成要求，并且能够清楚每个指令的使用场景，了解指令的基本原理。

1. ARP 指令

它原理就是 ARP 协议（Address Resolution Protocol，地址解析协议），用来将 IP 地址解析为 MAC 地址的协议（是在计网中的网络层-链路层中），通过 ARP 协议可以获取到 MAC 地址和对应的 IP 地址，所以 ARP 指令的主要功能就是这个协议的应用。

然后他的格式有

```
arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>]                <-显示 ARP 缓存
 arp [-v]  [-i <if>] -d  <host> [pub]  <- 删除 ARP 记录
 arp [-vnD] [<HW>] [-i <if>] -f  [<filename>]      <- 从文件添加记录
 arp [-v]   [<HW>] [-i <if>] -s  <host> <hwaddr> [temp]   <-添加记录
 arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub
```

具体的功能就是查看 MAC 与 IP 的对应表，并且能够增加或删除这个记录。

2. ftp 指令

同样的 ftp 指令的原理也是一个协议，与 ARP 不同的是协议工作的层是在应用层，对应的协议是 FTP 也就 ftp 指令来实现 FTP 协议中文件传输等功能。

连接 ftp 服务器

格式：ftp [hostname| ip-address]

列出文件列表以及切换目录，就是使用 ls 和 cd 和 Linux 下的指令没有区别

然后就是使用下载文件和上传文件

下载文件：下载文件通常用 get 和 mget 这两条命令。

a) get

格式：get [remote-file] [local-file]

将文件从远端主机中传送至本地主机中。

如要获取远程服务器上/usr/your/1.htm，则

ftp> get /usr/your/1.htm 1.htm

b) mget

格式：mget [remote-files]

从远端主机接收一批文件至本地主机。

如要获取服务器上/usr/your/下的所有文件，则
ftp> cd /usr/your/
ftp> mget *.*
c) 显示下载进度
默认情况下，下载是没有进度的，也就是说，只能瞎等着，啥也看不见。
ftp> hash
再进行传输，就能够显示下载进度了，以#号显示
上传文件：
a) put
格式：put local-file [remote-file]
将本地一个文件传送至远端主机中。
如要把本地的 1.htm 传送到远端主机/usr/your,并改名为 2.htm
ftp> put 1.htm /usr/your/2.htm
b) mput
格式：mput local-files
将本地主机中一批文件传送至远端主机。
如要把本地当前目录下所有 html 文件上传到服务器/usr/your/ 下
ftp> cd /usr/your
ftp> mput *.htm
注意：上传文件都来自于主机的当前目录下。比如，在 /usr/my 下运行的 ftp 命令，则只有在/usr/my 下的文件 linux 才会上传到服务器/usr/your 下。
断开连接：
bye：中断与服务器的连接。
ftp> bye
改变传输模式：ftp 的传输模式有 ascii 模式和二进制模式
直接输入 ascii 则设置传输模式为 ascii 模式
ftp> ascii
直接输入 binary 则设置传输模式为 binary 模式
ftp> binary
ftp 指令还有其他好多的可选参数和指令，在此由于篇幅和深度的问题就不分析了
3. Ipconfig 指令
这个指令就是调用系统调用来显示各种本机的网络相关的信息，当我们想知道本地的 ip 地址或者网卡的信息时就可以使用这个指令
用法：ipconfig [选项] [适配器]
ipconfig 显示网卡配置信息
ipconfig /all 显示网卡配置详细信息
ipconfig /renew 本地连接，更新本地连接网卡配置
是否匹配适配器连接：ipconfig /release 本地连接* 会释放所有本地连接开头的网卡的连接，如果是 DHCP 获取地址的网卡则会清除 IP 地址配置，会出现断网。重新获取地址可以使用 ipconfig /renew 重新获取地址。
显示 DNS 缓存信息：ipconfig /displaydns 显示 DNS 缓存信息
4. nbtstat 指令
这个指令可以获取远程 NetBios 的信息，如用户名，所属工作组，网卡的 MAC 地址等
Nbtstat -a 如知道远程主机的名称或者 ip 地址既可以得到他的 NETBIOS 的信息
Nbtstat -n 列出本机的所有 NetBIOS 信息

基本上用得到的就这两个格式
使用场景：
网络故障排查：当网络连接或通信出现问题时，可以使用 NBTSTAT 命令来检查 NetBIOS 相关的配置和状态信息，以定位问题所在。例如，通过查看 NetBIOS 名称缓存和解析器统计信息，可以判断是否存在名称解析问题或冲突。
NetBIOS 名称管理：如果需要管理 NetBIOS 名称缓存，比如添加、删除或刷新名称记录，可以使用 NBTSTAT 命令来执行相应操作。例如，使用"nbtstat -R"命令可以刷新本地计算机的 NetBIOS 名称缓存。
远程计算机查询：NBTSTAT 命令还支持查询远程计算机的 NetBIOS 名称缓存和解析器统计信息。这对于远程故障排查和管理其他计算机的 NetBIOS 配置非常有用。
需要注意的是，在现代的网络环境中，使用更先进的网络协议和工具（如 TCP/IP 和 DNS）已经成为主流。因此，NBTSTAT 命令的实际使用场景相对较少，一般仅在特定需要时或与老旧的 NetBIOS 基础设施相关的情况下才会用到。

5. net 指令

6. nestat 指令

nestat：打印网络连接、路由表、接口统计信息、伪装连接和多播成员，使用最多的是打印网络连接信息。
常见的参数：
-a (all)显示所有选项，默认不显示 LISTEN 相关
-t (tcp)仅显示 tcp 相关选项
-u (udp)仅显示 udp 相关选项
-n 拒绝显示别名，能显示数字的全部转化成数字。
-l 仅列出有在 Listen (监听) 的服務状态
-p 显示建立相关链接的程序名
-r 显示路由信息，路由表
-e 显示扩展信息，例如 uid 等
-s 按各个协议进行统计
-c 每隔一个固定时间，执行该 netstat 命令。

常用的 netstat 命令：

1. 查询进程号所占用的端口号： netstat -anp | grep 进程号
2. 查看端口号对应的进程，用于排查端口号是否被占用：netstat -tunlp | grep 端口
3. 查看端口号的使用情况：netstat -anp | grep 端口号
4. 显示 pid 和进程：netstat -pt
5. 列出所有处于监听状态的 Sockets：

```
netstat -l          #只显示监听端口
netstat -lt         #只列出所有监听 tcp 端口
netstat -lu         #只列出所有监听 udp 端口
netstat -lx         #只列出所有监听 UNIX 端口
```

7. ping 指令

指令格式：
-t ：Ping 指定的计算机直到中断。
-a ：将地址解析为计算机名。
-l size ：发送包含由 size 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是 65,527。
-f ：在数据包中发送"不要分段"标志。数据包就不会被路由上的网关分段。
-i ttl ：将"生存时间"字段设置为 ttl 指定的值。

-v tos :将"服务类型"字段设置为 tos 指定的值。
-r count :在"记录路由"字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。
-s count :指定 count 指定的跃点数的时间戳。
-j host-list :利用 host-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。
-k host-list :利用 host-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。
-w timeout :指定超时间隔，单位为毫秒。
destination-list :指定要 ping 的远程计算机。

使用 Ping 这命令来测试网络连通：

连通问题是由许多原因引起的，如本地配置错误、远程主机协议失效等，当然还包括设备等造成的故障。

使用 Ping 检查连通性有五个步骤：

A. 使用 ipconfig /all 观察本地网络设置是否正确

B. Ping 127.0.0.1，127.0.0.1 回送地址 Ping 回送地址是为了检查本地的 TCP/IP 协议有没有设置好

C. Ping 本机 IP 地址，这样是为了检查本机的 IP 地址是否设置有误；

D. Ping 本网网关或本网 IP 地址，这样的是为了检查硬件设备是否有问题，也可以检查本机与本地网络连接是否正常；（在非局域网中这一步骤可以忽略）

E. Ping 远程 IP 地址，这主要是检查本网或本机与外部的连接是否正常。

8. route 指令

功能 ： Route 命令是用于操作基于内核 ip 路由表，它的主要作用是创建一个静态路由让指定一个主机或者一个网络通过一个网络接口，如 eth0。

指令格式：

route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]]

指令参数：

-c 显示更多信息
-n 不解析名字
-v 显示详细的处理信息
-F 显示发送信息
-C 显示路由缓存
-f 清除所有网关入口的路由表。
-p 与 add 命令一起使用时使路由具有永久性。
add:添加一条新路由。
del:删除一条路由。
-net:目标地址是一个网络。
-host:目标地址是一个主机。
netmask:当添加一个网络路由时，需要使用网络掩码。
gw:路由数据包通过网关。
metric: 设置路由跳数。
Command 指定您想运行的命令 (Add/Change/Delete/Print)。
Destination 指定该路由的网络目标。

9. telnet 指令

功能： 执行 telnet 指令开启终端机阶段作业，并登入远端主机。telnet 命令通常用来远程登录。

但是，telnet 因为采用明文传送报文，安全性不好，很多 Linux 服务器都不开放 telnet 服务，而改用更安全的 ssh 方式了。但仍然有很多别的系统可能采用了 telnet 方式来提供远程登录，因此弄清楚 telnet 客户端的使用方式仍是很有必要的。

指令格式：

telnet　[参数]　[主机]

指令参数：

-8 允许使用 8 位字符资料，包括输入与输出。
-a 尝试自动登入远端系统。
-b<主机别名> 使用别名指定远端主机名称。
-c 不读取用户专属目录里的.telnetrc 文件。
-d 启动排错模式。
-e<脱离字符> 设置脱离字符。
-E 滤除脱离字符。
-f 此参数的效果和指定"-F"参数相同。
-F 使用 Kerberos V5 认证时，加上此参数可把本地主机的认证数据上传到远端主机。
-k<域名> 使用 Kerberos 认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名。
-K 不自动登入远端主机。
-l<用户名称> 指定要登入远端主机的用户名称。
-L 允许输出 8 位字符资料。
-n<记录文件> 指定文件记录相关信息。
-r 使用类似 rlogin 指令的用户界面。
-S<服务类型> 设置 telnet 连线所需的 IP TOS 信息。
-x 假设主机有支持数据加密的功能，就使用它。
-X<认证形态> 关闭指定的认证形态。

例如：telnet　192.168.120.206 登录到远程主机

10. tracet 指令

实现了路由追踪，路由器追踪功能，能够帮网络管理员了解网络通行情况，同时也是网络管理人员很好的辅助工具！通过路由器追踪可以轻松的查处从我们电脑所在地到目标地之间所经常的网络节点，并可以看到通过各个节点所花费的时间。

常用的指令格式就是 tracet 网站/ip 地址

4. 实验设计：

(1) ARP 指令：
- 学习 ARP 指令，了解基本原理
- 使用指令显示当前所有的表项
- 添加主机，并将网络地址跟物理地址相对应
- 分析结果
- 总结 ARP 指令的实践

(2) ftp 指令
- 学习 ftp 指令，了解基本原理
- 使用 ftp 指令上传下载文件
- 分析结果
- 总结实践经验

(3) ipconfig 指令：
- 学习 ipconfig 指令，了解基本原理
- 使用 ipconfig 指令

- 分析 ipconfig 指令的返回结果
- 总结 ipconfig 指令

(4) Nbtstat 指令：
- 学习 Nbtstat 指令，了解基本原理
- 使用 Nbtstat 指令查看名称表
- 查看 ip 地址的 NBT 缓存
- 查看本地 NetBIOS 名称
- 分析结果
- 总结实践

(5) Net 指令：
- 学习 Net 指令，了解基本原理
- 使用 net 指令发送信息
- 使用 net 指令查看服务状态
- 分析结果
- 总结实践

(6) Netstat 指令：
- 学习 Netstat 指令，了解基本原理和用法
- 使用 Netstat 指令查看所有连接
- 使用 Netstat 指令查看某一端口的进程
- 使用 Netstat 指令查看某一进程的端口
- 分析结果
- 总结实验

(7) Ping 指令：
- 学习 ping 指令，了解基本原理和用法
- 使用 ping 指令
- 分析结果
- 总结实验

(8) Route 指令：
- 学习 Route 指令，了解基本原理和用法
- 使用 Route 指令添加路由
- 使用 Route 指令删除路由
- 使用 Route 指令显示路由

(9) Telnet 指令：
- 学习 Telnet 指令，了解基本原理和用法
- 使用 Telnet 指令
- 分析结果对比与 ping 的不同

(10) tracet 指令
- 学习 Tracet 指令，了解基本原理
- 使用 Tracet 指令
- 总结分析 Tracet 指令

5. 实验过程：

(1) ARP 指令：
- 使用 arp 指令查看当前所有的表项

```
(base) PS C:\Users\15858> arp -a

接口: 10.162.107.120 --- 0x6
  Internet 地址         物理地址              类型
  10.162.255.253        d4-c1-c8-8e-11-30     动态
  10.162.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

可以发现其中有动态的也有静态的
例如第一个是动态的大概率是路由器的动态 ip，而对应的是物理地址就是 MAC 地址。
然后我们不妨使用 ipconfig 指令来验证

```
(base) PS C:\Users\15858> ipconfig

Windows IP 配置


以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::2f84:c2ce:bb23:986e%6
   IPv4 地址 . . . . . . . . . . . . : 10.162.107.120
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . : 10.162.255.253

以太网适配器 蓝牙网络连接:
```

可以发现这个**默认网关**也就是路由器的 ip 地址和上边的动态 ip 地址是**一样的**，所以证明了我们的猜想。

- 使用 arp 指令只显示一项

```
(base) PS C:\Users\15858> arp -a 10.162.255.253

接口: 10.162.107.120 --- 0x6
  Internet 地址         物理地址              类型
  10.162.255.253        d4-c1-c8-8e-11-30     动态
```

- 使用 arp 添加主机

```
(base) PS C:\Users\15858> arp -s 123.55.88.222 00-aa-00-62-c6-09
ARP 项添加失败: 请求的操作需要提升。
```

发现直接添加主机不可以，猜想是因为权限问题，需要用管理员权限才能够添加
然后用**管理员权限打开终端**后发现添加成功了

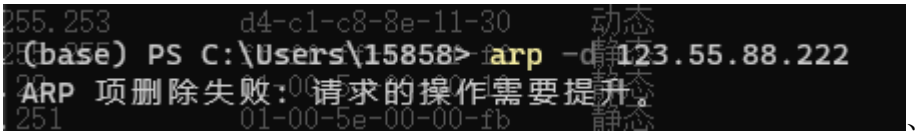
```
(base) PS C:\Users\15858> arp -s 123.55.88.222 00-aa-00-62-c6-09
(base) PS C:\Users\15858> arp -a

接口: 10.162.107.120 --- 0x6
  Internet 地址         物理地址              类型
  10.162.255.253        d4-c1-c8-8e-11-30     动态
  10.162.255.255        ff-ff-ff-ff-ff-ff     静态
  123.55.88.222         00-aa-00-62-c6-09     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

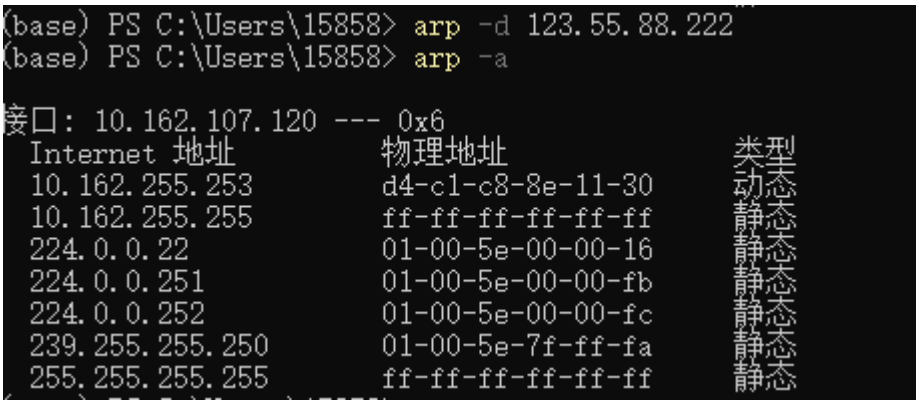
总结：确实应该要用管理员权限要不然一般的程序直接就可以修改这个表，导致系统无法连接网络。

- 使用 arp 删除主机

同样的是需要的管理员权限



使用管理员权限后：



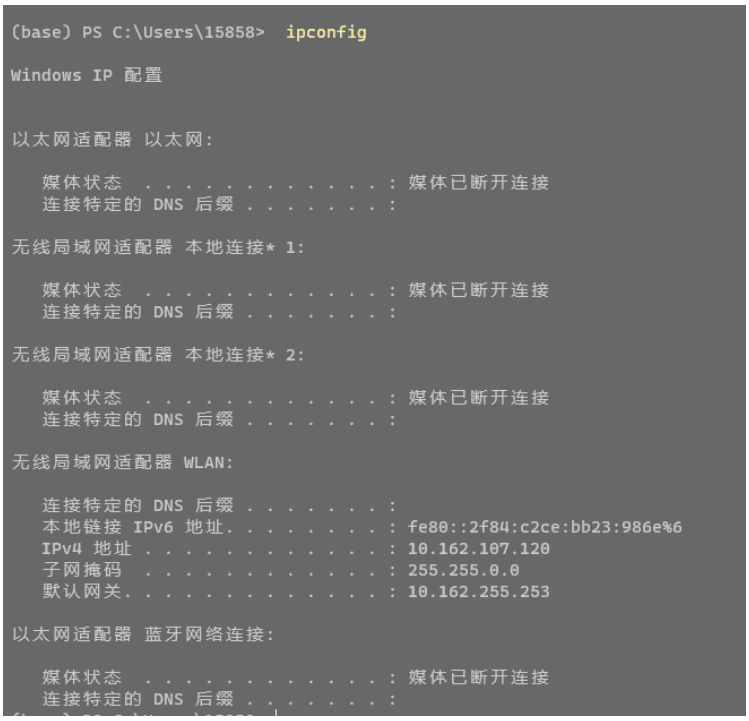
发现删除成功了

(2) ftp 指令

(3) ipconfig 指令

我们之前在 arp 指令时候就已经用过了 ipconfig 这一指令，但是我们还需要仔细地在深入使用一下

- ipconfig 显示 WLAN 配置信息



结果分析：

可以发现以太网，本地连接 1 ，本地连接 2，蓝牙网络连接，都没有连接，只有无线局域网 WLAN 连接了，检查自己电脑后，确实如此，我的本机电脑只连接了 wifi，所以只有 wifi 有信息，然后我们再仔细分析一

下无线局域网适配器下的信息

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::2f84:c2ce:bb23:986e%6
   IPv4 地址 . . . . . . . . . . . . : 10.162.107.120
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . : 10.162.255.253
```

在查阅资料过后清楚了：

连接特定的 DNS 后缀：网卡对应的 DNS 服务器帮助解析 IP。本地的连接没有 DNS 服务器则空。

本地链接 IPv6 地址：IPv6 表示法的 IP 地址%后面的 14 是网络号的个数。

子网掩码：化成二进制，前面是 1 的表示为网络号，后面为 0 的表示为主机号。

默认网关：默认网关 IP 地址，意思是一台主机如果找不到可用的网关，就把数据包发给默认指定的网关，由这个网关来处理数据包。也就是路由器的地址。

这个功能我们就大致清楚了

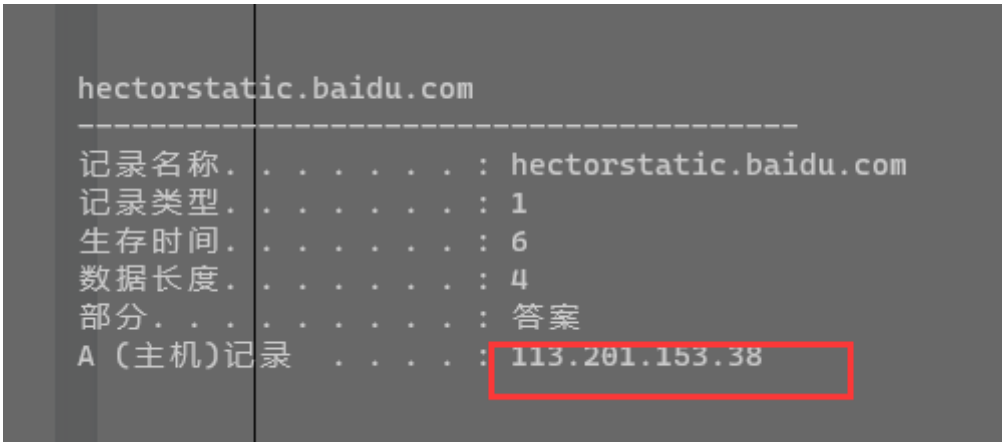
- 显示本机上的 DNS 域名解析列表

可以发现上边有对应的域名和对应的 ip 地址不过还有一些不认识，猜想应该是实时增加的，就是本地访问后会保存起来

然后我访问了一个网页：www.baidu.com

发现这个表增加了：

所以这就证实了我的猜想，在访问网页时首先会查询 DNS 然后保存下来
但是会不会反复增加呢？
答案是不会，因为我又关闭浏览器重新打开百度后发现并没有增加



只不过发现 ip 地址变了，这说明百度的网站不止一个服务器，还有很多，每次访问都会分配不同的服务器，可能这就是通过 DNS 来实现分布式的功能吧。
可能还能深究但是由于篇幅和能力有限，便先止步于此。
- ipconfig flushdns 删除本机上的 DNS 域名解析列表

可以发现这个操作并**不像 arp 的映射表一样需要管理员权限，**而是直接就可以删除但是删除后任然还是保留着系统一些默认的 DNS 的信息，**还有一些预先设置的 DNS。**（这部分可能也比较有趣）

因为里面有我之前配置过的谷歌翻译的 DNS 哈哈哈，之前并不懂是什么原理，现在好像可以一探究竟了。

这部分放在的实验过程的最后

(4) Nbtstat 指令

- nbtstat -A 127.0.0.1 列出指定 IP 地址的远程机器的名称表

(5) Net 指令

(6) Netstat 指令

(7) Ping 指令

(8) Route 指令

(9) Telnet 指令

6. 结论与分析：

(针对实验结果，对其正确性、创新性进行分析；写出遇到的问题及其解决方案，本次实验心得体会）

【过程记录（源程序、测试用例、测试结果等）】