陕西科技大学

《计算机网络安全》实验报告

实验一：Windows 基本常用网络命令

学　　生：

学　　院：电子信息与人工智能学院

专　　业：网络工程

指导教师：张楠

2022 年 6 月 2 日

实验一 Windows 基本常用网络命令

班级：_____ _____ _____

实验预习报告

一、实验目的

1、掌握常用的 Windows 网络命令
2、熟悉使用命令查看 Windows 系统的网络状态
3、了解 Windows 系统下常见的网络工具

二、实验要求

参照实验教程，在 Windows 系统下使用相应的网络命令了解相应的网络状态和网络配置，并能利用网络命令进行故障诊断，学会日常操作中利用网络命令控制网络状况的方法。

三、实验原理

1、Windows 系统下，安装了 TCP/IP 协议栈可以实现大多数网络通信的需求，而且 Windows 系统附带了较多的网络测试工具，我们可以使用命令行来调用这些工具，更改 Windows 系统的网络设置。

2、Windows 系统具有完整的图形化界面，可以通过系统设置、控制面板等更改系统设置，可以直观的看到网络的连接状态。

四、实验预习内容

1、ICMP 协议

ICMP 协议是互联网控制消息协议的缩写，它是 TCP/IP 协议族中的一个重要子协议，用于在 IP 主机和路由器之间传递控制消息，报告主机是否可达、路由是否可用等。

ICMP 协议有两大类报文，分别是查询报文和差错报文，它们用不同的类型和代码字段来表示不同的消息含义。

2、ping 命令和 tracert 命令

ICMP 协议的典型应用有 ping 命令和 tracert 命令，它们分别利用 ICMP 的 echo 信息和超时信息来检测网络连通性和路径信息。

ping 命令是通过发送和接收 ICMP 的 echo 请求和 echo 应答报文来测试目的地址是否可达，以及网络延迟和丢包率。ping 命令的使用方法是在命令行后面加上目的地址的 IP 或域名。tracert 命令是通过发送不同 TTL 值的 ICMP 回显请求报文，并接收 ICMP 超时或目的不可达报文来确定数据包到达目的地址所经过的路由器，并显示每一跳的延迟。tracert 命令的使用方法也是在命令行后面加上目的地址的 IP 或域名。

ping 命令和 tracert 命令的相同点是都可以用来检测网络连通性，不同点是 ping 命令只能显示目的地址是否可达，而 tracert 命令还可以显示到达目的地址所经过的路径。另外，ping 命令可以持续发送数据包直到中断，而 tracert 命令只发送一定数量的数据包。

3、ipconfig 查看和更改网络信息

ipconfig 命令是一个用于显示和修改计算机的 TCP/IP 网络配置的命令。它可以用来查看计算机的 IP 地址、子网掩码、默认网关、DNS 服务器等信息，也可以用来刷新 DNS 缓存、释放和续订 DHCP 分配的 IP 地址等。ipconfig 命令可以跟不同的参数来实现不同的功能，如：

(1)ipconfig /all：显示所有接口的完整 TCP/IP 配置信息。

(2)ipconfig /flushdns：刷新 DNS 解析器缓存，可以解决一些 DNS 解析不正常、错误的问题。

(3)ipconfig /release：释放当前 DHCP 分配的 IP 地址配置，使系统将地址归还给 DHCP 服务器的 IP 地址池。

(4)ipconfig /renew：续订 DHCP 分配的 IP 地址配置，使系统重新获得 IP 地址的租期，在部分情况下 DHCP 服务器到期后会强制回收 IP 地址。

4、arp 命令查看和修改 arp 映射表

arp 命令是一个用于管理和显示系统的 ARP 缓存信息的命令。它可以用来查看、添加、删除或修改 ARP 缓存中的 IP 地址和 MAC 地址的对应关系，也可以用来实现 IP 地址和 MAC 地址的静态绑定。arp 命令的使用方法是在命令行窗口

中输入 arp，后面可以跟不同的参数来实现不同的功能，如：

(1)arp -a：显示所有接口的当前 ARP 缓存表，可以指定 IP 地址或接口地址来显示特定的条目。

(2)arp -d：删除指定的 IP 地址项，可以指定接口地址来删除特定接口上的项。

(3)arp -s：添加一个静态 ARP 缓存项，需要指定 IP 地址和 MAC 地址

5、netstat 命令

netstat 命令是一个用于显示网络连接、路由表、接口统计、多播组成员等信息的命令。它可以用来检查本机的网络状态，诊断网络问题，监控网络性能等。netstat 命令可以跟不同的参数来实现不同的功能，如：

(1)netstat -a：显示所有连接状态，包括 TCP、UDP 和 Unix 域套接字。

(2)netstat -t：显示 TCP 连接状态。

(3)netstat -u：显示 UDP 连接状态。

(4)netstat -n：不使用域名解析功能，直接使用 IP 地址和端口号显示连接信息。

(5)netstat -p：显示正在使用套接字的程序识别码和程序名称

实验一 Windows 基本常用网络命令

班级：_____ _____ _____

实验报告

一、实验目的

1、掌握常用的 Windows 网络命令
2、熟悉使用命令查看 Windows 系统的网络状态
3、了解 Windows 系统下常见的网络工具

二、实验要求

参照实验教程，在 Windows 系统下使用相应的网络命令了解相应的网络状态和网络配置，并能利用网络命令进行故障诊断，学会日常操作中利用网络命令控制网络状况的方法。

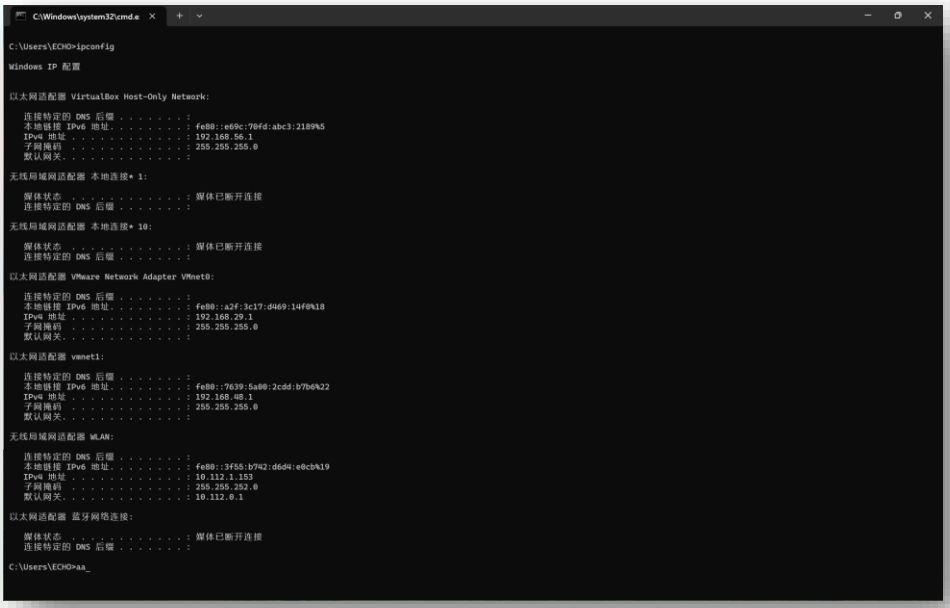
三、实验原理

1、Windows 系统下，安装了 TCP/IP 协议栈可以实现大多数网络通信的需求，而且 Windows 系统附带了较多的网络测试工具，我们可以使用命令行来调用这些工具，更改 Windows 系统的网络设置。

2、Windows 系统具有完整的图形化界面，可以通过系统设置、控制面板等更改系统设置，可以直观的看到网络的连接状态。

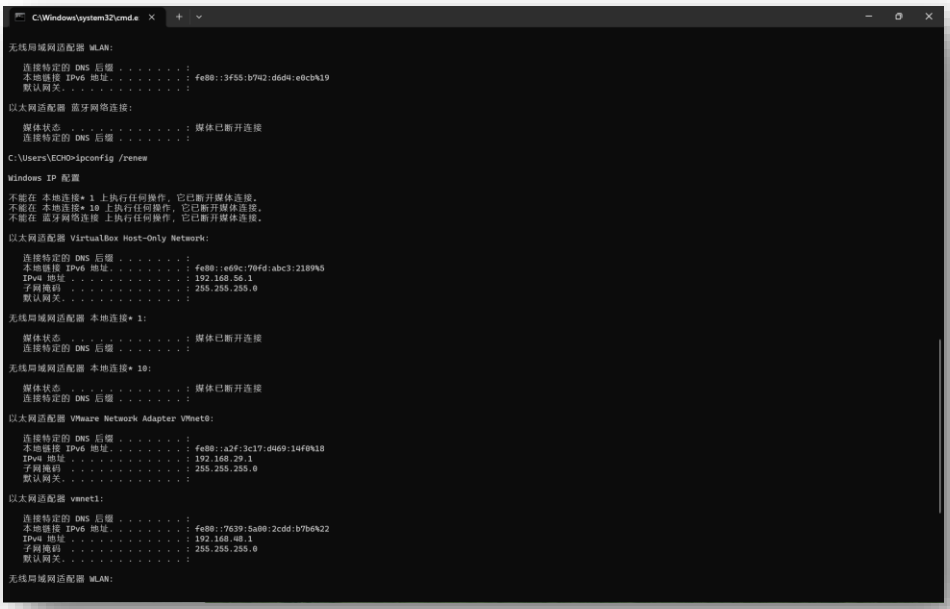
四、实验内容

1、使用 ipconfig 命令查询本机的网络连接状况



从命令运行的结果当中可以知道，本机当前的网卡（物理网卡、蓝牙和虚拟网卡等）的连接状态以及对应的 IP（v4 和 v6）地址、掩码、网关、DNS 等信息。从中可以知道，当前本机的主用网络为 WLAN 网卡，其地址为 10.112.1.153，这个 WiFi 是图书馆的网络。

执行 ipconfig /release 和 ipconfig /renew 命令，尝试重新租用一个 IP 地址。



可以看到，执行 release 之后，WLAN 没有 IP 地址了，重新 renew 后，WLAN 获得了新的 IP 地址。

2、使用 ping 命令尝试发送 icmp 报文到指定主机，探测到指定主机的连接是否正常

通过上面的 ipconfig 命令，我们知道了当前的网关为 10.112.0.1，可以尝试 ping 之，测试是否连通。

```
C:\Users\ECHO>ping 10.112.0.1

正在 Ping 10.112.0.1 具有 32 字节的数据:
来自 10.112.0.1 的回复: 字节=32 时间=3ms TTL=255
来自 10.112.0.1 的回复: 字节=32 时间=3ms TTL=255
来自 10.112.0.1 的回复: 字节=32 时间=4ms TTL=255
来自 10.112.0.1 的回复: 字节=32 时间=3ms TTL=255

10.112.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms, 最长 = 4ms, 平均 = 3ms

C:\Users\ECHO>_
```

和网关之间正常连通。

测试到外网是否连通，在这里以服务器 minmin.cloud 为目标。

```
C:\Users\ECHO>ping minmin.cloud

正在 Ping minmin.cloud [106.13.29.165] 具有 32 字节的数据:
来自 106.13.29.165 的回复: 字节=32 时间=48ms TTL=47
来自 106.13.29.165 的回复: 字节=32 时间=49ms TTL=47
来自 106.13.29.165 的回复: 字节=32 时间=50ms TTL=47
来自 106.13.29.165 的回复: 字节=32 时间=52ms TTL=47

106.13.29.165 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 48ms, 最长 = 52ms, 平均 = 49ms

C:\Users\ECHO>_
```

到外网正常连通。

测试到不可达地址是否连通，这里以 google.com 为目标。

```
C:\Users\ECHO>ping google.com

正在 Ping gOOglE.cOM [142.251.43.14] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

142.251.43.14 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\ECHO>_
```

到 google.com 全部丢失。

综上，ping 命令可以测试网络的连通性，但是有的时候也会存在不准确的情况，比如某些节点会丢弃 icmp 报文，或者某些设备不响应 icmp 报文。

3、使用 tracert 命令进行网络探测

可以通过 tracert 命令测试到某一个网络的路径，以 222.24.93.30 为例

```
C:\Users\ECHO>tracert 222.24.93.30

通过最多 30 个跃点跟踪到 222.24.93.30 的路由

  1     4 ms     3 ms     4 ms  10.196.1.1
  2     6 ms     4 ms     4 ms  222.24.93.30

跟踪完成。

C:\Users\ECHO>_
```

在测试其它网络路径的时候，发现总会通过 222.24.93.30，为此，可以推测该地址为校园网核心层相关设备的接口地址或者虚拟网关备份组的地址，可以借由 tracert 命令来推测网络结构。有的时候会发现，tracert 命令的第一跳不是默认网关，这种情况据推测应该是由于 vrrp 备份组所导致的。

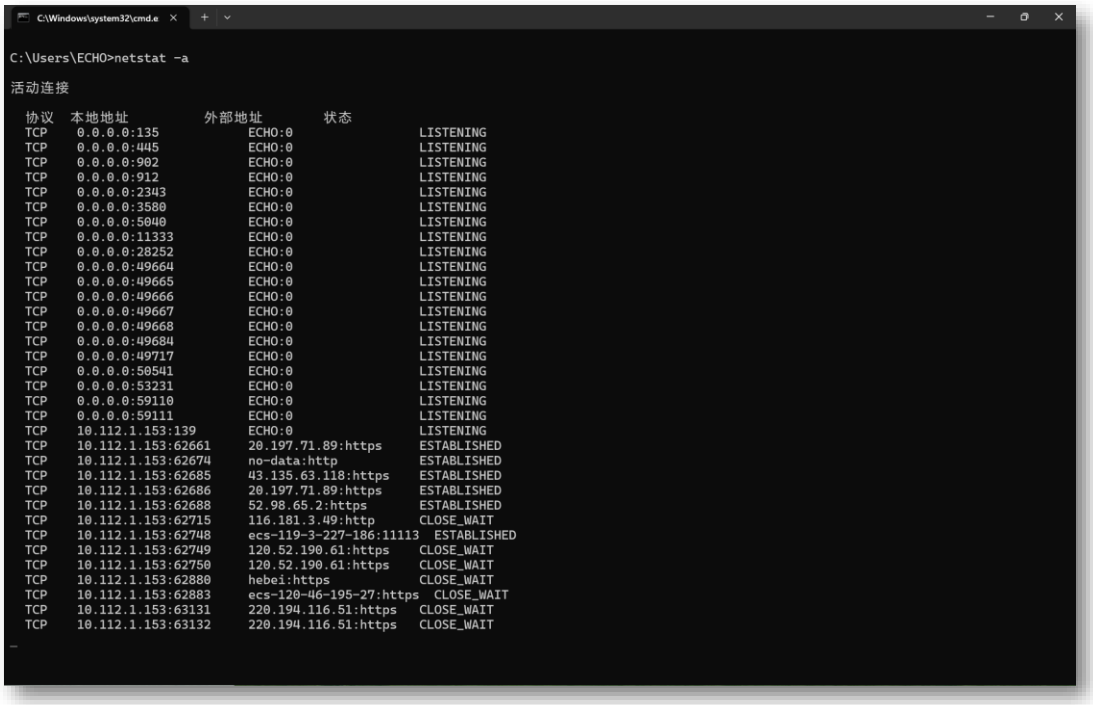
4、使用 arp 命令来查询 arp 表

查看 arp 表中的所有条目：

```
C:\Users\ECHO>arp -a

接口: 192.168.56.1 --- 0x5
  Internet 地址         物理地址              类型
  192.168.56.255        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

接口: 192.168.29.1 --- 0x12
  Internet 地址         物理地址              类型
  192.168.29.255        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

接口: 10.112.1.153 --- 0x13
  Internet 地址         物理地址              类型
  10.112.0.1            18-2a-d3-f7-cd-40     动态
  10.112.3.255          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

接口: 192.168.48.1 --- 0x16
  Internet 地址         物理地址              类型
  192.168.48.255        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
```

可以看到，在 WLAN 接口上，arp 表具有：网关地址、广播地址、组播地址的 arp 表项。由于校园网可能针对网络中的设备进行了隔离，故 ping 同一个网络中的设备时，arp 请求和响应似乎被抛弃了，无法通过 ping 其它设备来更新 arp 表的项目。

5、使用 netstat 命令查看网络连接状态



可以看到本机上活动的网络连接状态。

由于 UDP 无连接且本机此时没有运行基于 UDP 的应用程序，故表中全为 TCP 连接，可以看到有处于监听的、连接已建立的、被动关闭的 TCP 连接，其中大多数是 HTTP 服务在运行。

五、实验结论

1、Windows 系统中常用的网络测试命令有 ping、tracert、arp、netstat 等，它们可以用来查看、测试网络状态，有利于排除网络故障。

2、大多测试命令基于 ICMP 运行，如果相关网络设备丢弃 ICMP 报文，则该测试命令也会出现相应问题，比如：ping 不通但是可以上网，tracert 时有的节点为*号。

3、可以借助网络测试命令摸清网络大致结构，为维护网络提供了极大方便。