深 圳 大 学 实 验 报 告

课 程 名 称：计算机网络

实验项目名称：常用的网络命令

学　　院：计算机与软件学院

专　　业：计算机科学与技术

指 导 教 师：邹永攀

报告人：刘睿辰　学号：2018152051　班级：数计班

实 验 时 间：2021 年 3 月 16 日

实验报告提交时间：2021 年 3 月 29 日

教务处制

实验目的与要求：

1. 了解 ping、traceroute 等常用网络工具的功能以及使用方法，并通过这些工具发现或者验证网络中的故障。

2. 学习安装、使用协议分析软件，掌握基本的数据报捕获、过滤和协议的分析技巧。

方法、步骤：

1. 实验环境及要求：windows 操作系统，具有 internet 连接；

2. 实验步骤：练习使用 10 个常用的网络命令，对每个网络命令的原理进行阐述，特别是 ping、ipconfig、Tracert、ARP 和 FTP 五个指令需要重点阐述（越详细越深入越好）；

3. 请一一展示十个网络命令的基本用法及具体示例，并就各个网络命令执行后所得到的结果进行解释说明（具体示例越全面越好）。

实验过程及内容：

1. ping 命令

1.1 ping 命令介绍

ping 是一个测试程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。如果 ping 运行正确，就可以排除网络访问层、网卡、Modem 的 I/O 线路、电缆和路由器等存在的故障。

1） 按缺省设置，运行 Ping 命令时发送 4 个 ICMP（Internet Control Message Protocol，Internet 控制报文协议）“回送请求”，每个 32 字节数据；若正常应得到 4 个回送应答，如图 1 所示。

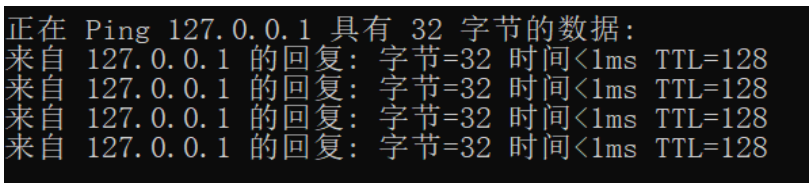

图 1. ping 命令的四个回送应答

2） ping 能够以毫秒为单位显示发送“回送请求”到返回“回送应答”之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接，速度比较快。正如图 1 所示，时间$< 1ms$，应答时间比较短。

3） ping 还能显示 TTL（Time To Live，存在时间值）。通过 TTL 值推算数据包已经通过了多少个路由器：**源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）-返回时 TTL 值**。

根据我们图 1 中 TTL=128，这里就是没有经过任何路由器，因为这是与本地计算机的连接。但如果假如 TTL=119，那么经过的路由器个数就是 128-119=9 个，因为$119 < 2^7 = 128 < 2^8$。

综上所述，我们认为 ping 命令有以下几个作用：

1） 用来检测网络的连通情况和分析网络速度；

2） 根据域名得到服务器 IP；

3） 根据 ping 返回的 TTL 值来判断对方所使用的操作系统及数据包经过路由器数量。

1.2 ping 功能实际操作

1.2.1 ping 127.0.0.1。

在有类 IP 地址的规定中，第一部分是 1-126 为 A 类地址，128-191 为 B 类地址，那么中间留的 127.0.0.1 被称为本地回环地址，主要作用有两个：

1） 测试本机的网络配置，能 ping 通 127.0.0.1 说明本机的网卡和 IP 协议安装都没有问题；

2） 另一个作用是某些 server/client 的应用程序在运行时需调用服务器上的资源，一般要指定 server 的 IP 地址，但当该程序要在同一台机器上运行而没有别的 server 时就可以把 server 的资源装在本机，server 的 IP 地址设为 127.0.0.1 也同样可以运行。

验证如图 2 所示，TCP/IP 的安装或运行不存在基本问题。

```
C:\Users\未央>ping 127.0.0.1

正在 Ping 127.0.0.1 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128

127.0.0.1 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 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 2. ping 127.0.0.1 结果

事实上，我们改用指令 127.1 也是可以行得通的，如图 3 所示。这是什么原因呢？事实上，IP 地址由 32 位二进制数字构成，也就是四部分数字。由于 Windows 操作系统具有自动填充 “.0”的功能，因此我们可将“127.0.0.1”变为“127.1”。

```
C:\Users\未央>ping 127.1

正在 Ping 127.0.0.1 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128

127.0.0.1 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 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 3. ping 127.1 结果和之前一样

1.2.2 ping 本机 IP

这个功能在于检查本地配置或安装是否存在问题。那么如何查看本机 IP 地址呢？这个要用到后面的一条指令，也就是 ipconfig。输入这条指令之后会有很多地址，那就要看当前的网络状态。如果当前电脑连接的是 Wi-Fi，那么我们就要看无线局域网适配器 WLAN 中的地址；如果电脑连接的是网线，那么我们要看的就是以太网中的地址。

输入 ipconfig 之后回车，观察未断开的连接，我们看到的结果如图 4 所示。

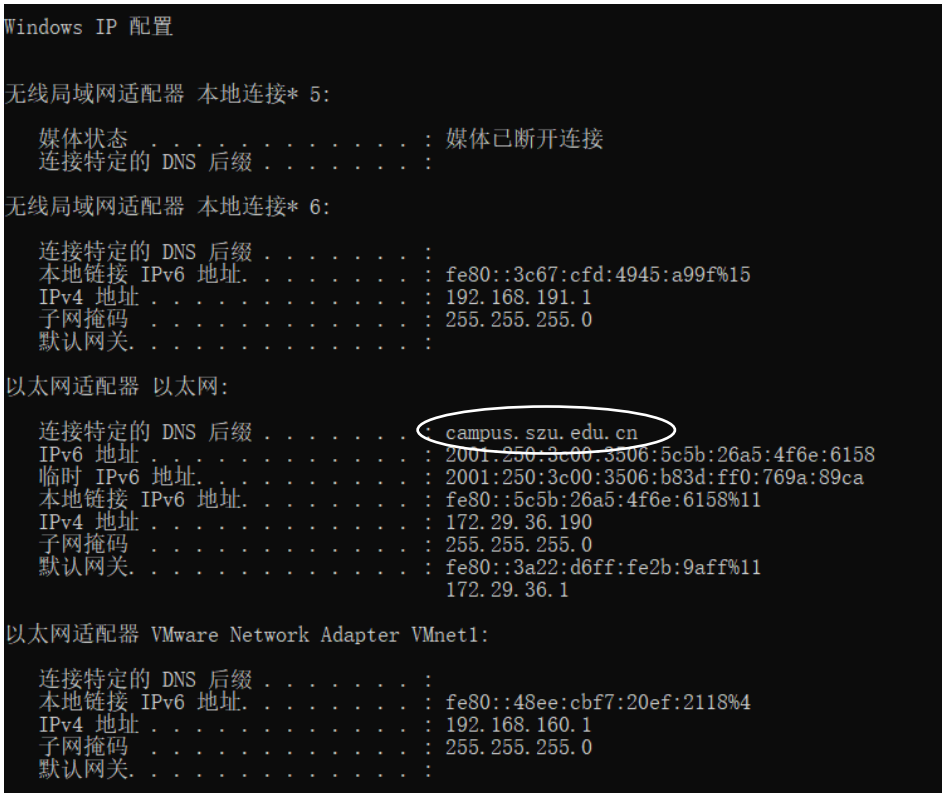

图 4. 本机 windows IP 配置

图中出现了多个 IP 地址。如果我们的电脑连接的是网线，那么很明显应该是以太网中的 IPv4 地址，这一点从以太网的 DNS 后缀中也可以看得出来（图中标识部分）。至于另一个以太网适配器，是本台电脑*linux*虚拟机的地址。至于上面的无线局域网适配器（本地连接*6），这个 IP 是保留 IP，使用保留 IP 的网络只能内部通信，而不能与其他网络互连。

如果我们换成 Wi-Fi 连网，那么将会看到无线局域网适配器 WLAN 变成如图 5 所示的结果。

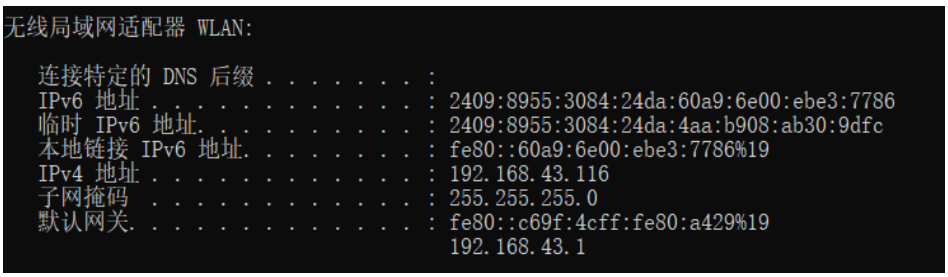

图 5. 无线局域网适配器 WLAN 地址

所以在连接网线的时候，我们最终的 IP 地址就是 172.29.36.190。此时 ping 本机 IP，可以得到如图 6 所示的结果，说明本地配置或安装不存在问题。

1.2.3 ping 局域网内其他 IP

这个命令经过本地计算机的网卡及网络电缆到达其他计算机，再返回。如收到回送应答，表明本地网络的网卡和载体运行正确。但如果收到 0 个回送应答，表示

子网掩码不正确或网卡配置错误或电缆系统有问题。

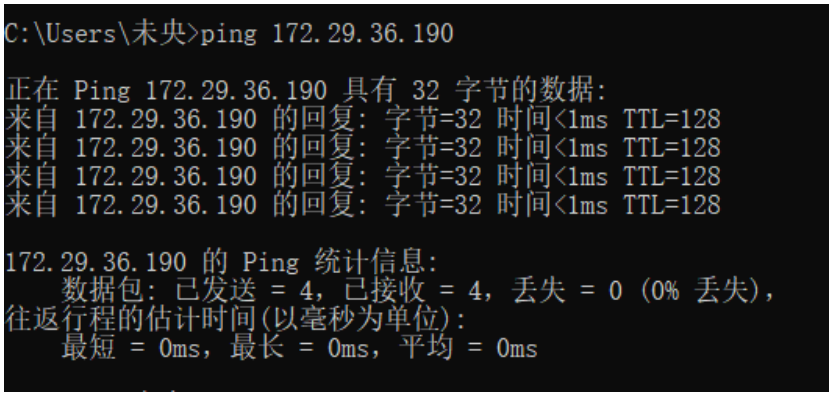

图 6. ping 本机 IP 得到的结果

这里要注意，当路由器设置了 AP 隔离(Access Point Isolation)，这就使得电脑之间不能进行互相访问，所以如果两台电脑都连接了网线，这样可能无法互相 ping 通。为了能在同一个局域网下互相 ping 通，可以设置路由器取消 AP 隔离，这样两台电脑都连接这个路由器，这样就可以互相 ping 通。

这里我们打开手机热点，这也相当于取消了 AP 隔离的路由器，观察对方无线局域网适配器 WLAN 下的 IP 地址，这样就可以 ping 通，如图 7 所示。

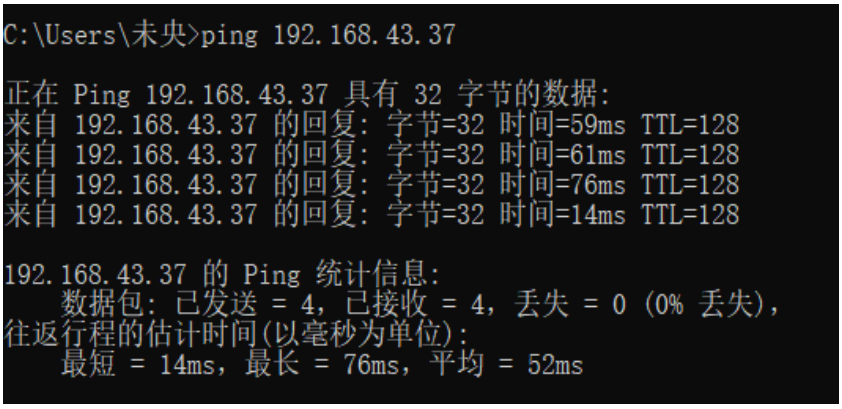

图 7. ping 局域网内其他 IP

1.2.4 ping 网关 IP

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够做出应答。

这里我们依然使用 ipconfig 命令来查看网关 IP，如图 8 所示。

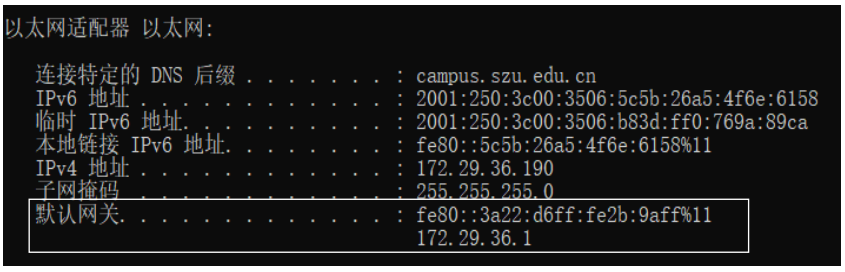

图 8. 查看网关 IP

接下来我们 ping 这个地址，结果如图 9 所示。可以看到，局域网中的路由器运行正常并能够做出应答。

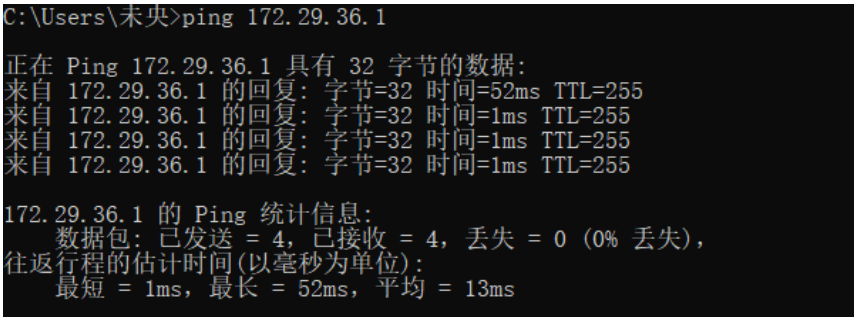

图 9. ping 网关 IP 发现网关路由器正常运行并能够做出应答

1.2.5 ping 远程 IP

如收到 4 个应答，表示成功使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

用户可以 ping 远程 IP。也就代表用户可以访问这个地址。举例来说，如果我们能够 ping 百度的 IP，那也就是说我们可以访问百度。

我们查到百度的 IP 地址为 180.101.49.12

然后我们 ping 这个地址，如图 10 所示，收到 4 个应答，我们可以成功访问百度。

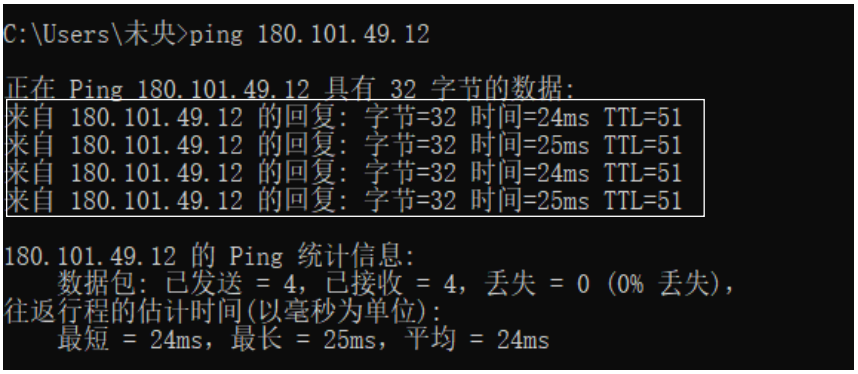

图 10. ping 百度 IP 应答正常

1.2.6 对某个域名执行 ping 命令

本地计算机必须先通过 DNS 服务器将域名转换成 IP 地址。如果出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障。利用该命令实现域名对 IP 地址的转换功能。

事实上，这个功能可以验证远程 IP 的访问。例如，我们对 www.baidu.com 这个域名访问，这样一来，本地计算机会将域名转换为 IP 地址，我们需要观察该 IP 地址与之前的 IP 地址是否都能够访问同一个域名即可。如图 11 所示，域名转化成的 IP 地址与 1.2.5 节能达到的域名相同，证明我们在 1.2.5 中的结论是正确的，我们可以访问这个域名。

但是，如果访问国外网站或者某些部门的内部网的时候，将会出现超时的问题。以深大的 Blackboard 为例为例，当我们 ping 这个域名的时候，将会出现如图 11 所示的情况。这就说明在没有 VPN 的情况下，我们无法解析这个域名。那如果打开了 VPN，这就相当于建立了 Intranet（内部网）在公众网络上的延伸，它可以提供与专用网一样的安全性、可管理性和传输性能，而建设、运转和维护网络的工作也从企业内部的 IT 部门剥离出来，交由运营商来负责。

打开了内部网 VPN 之后，我们再来 ping 这个域名，就可以得到如图 12 所示的情况，证明此时我们可以访问这个域名了。

```
C:\Users\未央>ping elearning.szu.edu.cn

正在 Ping elearning.szu.edu.cn [116.13.96.90] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

图 11. ping 深大 Blackboard 出现请求超时的情况

```
C:\Users\未央>ping elearning.szu.edu.cn

正在 Ping elearning.szu.edu.cn [116.13.96.90] 具有 32 字节的数据:
来自 116.13.96.90 的回复: 字节=32 时间=1ms TTL=247
来自 116.13.96.90 的回复: 字节=32 时间=2ms TTL=247
来自 116.13.96.90 的回复: 字节=32 时间=1ms TTL=247
来自 116.13.96.90 的回复: 字节=32 时间=2ms TTL=247

116.13.96.90 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 = 1ms, 最长 = 2ms, 平均 = 1ms
```

图 12. 打开 VPN 之后 ping 深大 Blackboard 成功

1.2.7 含参 ping 指令

之前的所有 ping 指令都没有带参数,这就导致了我们所有的操作都是基于 ping 命令的默认版本。事实上，ping 命令可以通过加参数的方法来改变默认设置。为了找到这些参数设置，我们直接输入 ping 然后回车，得到如图 13 所示的结果，这里显示了 ping 命令的所有参数。

```
用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

选项:
    -t             Ping 指定的主机，直到停止。
                   若要查看统计信息并继续操作，请键入 Ctrl+Break;
                   若要停止，请键入 Ctrl+C。
    -a             将地址解析为主机名。
    -n count       要发送的回显请求数。
    -l size        发送缓冲区大小。
    -f             在数据包中设置“不分段”标记(仅适用于 IPv4)。
    -i TTL         生存时间。
    -v TOS         服务类型(仅适用于 IPv4。该设置已被弃用，
                   对 IP 标头中的服务类型字段没有任何
                   影响)。
    -r count       记录计数跃点的路由(仅适用于 IPv4)。
    -s count       计数跃点的时间戳(仅适用于 IPv4)。
    -j host-list   与主机列表一起使用的松散源路由(仅适用于 IPv4)。
    -k host-list    与主机列表一起使用的严格源路由(仅适用于 IPv4)。
    -w timeout     等待每次回复的超时时间(毫秒)。
    -R             同样使用路由标头测试反向路由(仅适用于 IPv6)。
                   根据 RFC 5095，已弃用此路由标头。
                   如果使用此标头，某些系统可能丢弃
                   回显请求。
    -S srcaddr     要使用的源地址。
    -c compartment 路由隔离舱标识符。
    -p             Ping Hyper-V 网络虚拟化提供程序地址。
    -4             强制使用 IPv4。
    -6             强制使用 IPv6。
```

图 13. ping 命令的所有参数

这里面就举例进行说明

1） $ping + IP/域名 - t$

根据图 13 中对于该命令的解释，我们发现 ping 命令的默认执行次数是 4 次，也就是我们会收到 4 个应答。这个命令可以让我们对 IP 进行连续访问，直到点击 Ctrl + C 才能终止，如图 14 所示。

图 14. ping -t 命令

当然，点击 Ctrl + C 之后会导致访问的终止。如果我们只想查看当前的统计信息而不想让其停止访问，我们可以使用 Ctrl + break 指令。

2） $ping + IP - l\ size$

指定 ping 命令中的数据长度为 m 字节，缺省为 32 字节，也就是规定了发送缓冲区的大小。例如，$ping\ -l\ 100\ www.baidu.com$，那么本地计算机就会用 100 字节的数据包去 ping www.baidu.com，系统默认的数据包是 32 字节，最大的字节数是 65527。效果如图 15 所示。如白色框部分标记，字节数目已经变成了 100 个，这就是用 100 字节的数据包去 ping 百度。

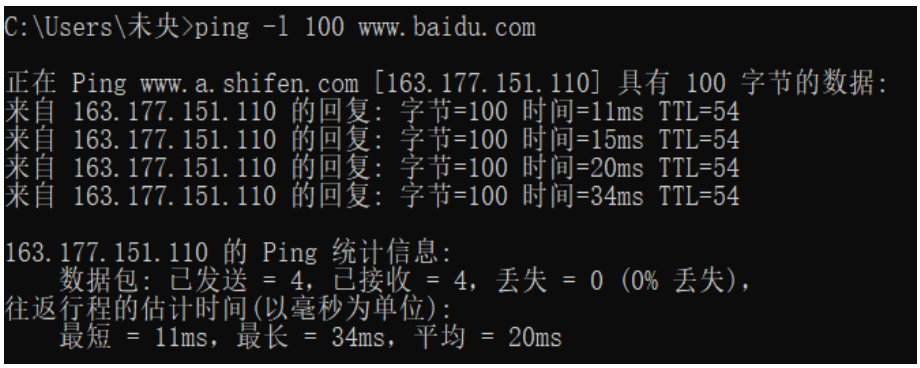

图 15. ping -l size 指令

3） $ping\ +\ IP\ -n\ count$

ping 命令默认情况下返回 4 个应答。这里如果我们想多返回几个应答，就可以通过这种方法进行尝试。如图 16 所示，如果我们想得到 6 个应答，那么就使用该指令进行设置，可以看到产生了 6 个应答。

图 16. ping -n count 指令

4） $ping\ -a + IP$

ping-a 可以解析计算机名。就是可以通过 ping 它的 IP 地址，可以解析出主机名。例如，我们知道了自己的 IP 地址之后，就可以使用该条指令解析出我们的主机名，如图 17 所示。

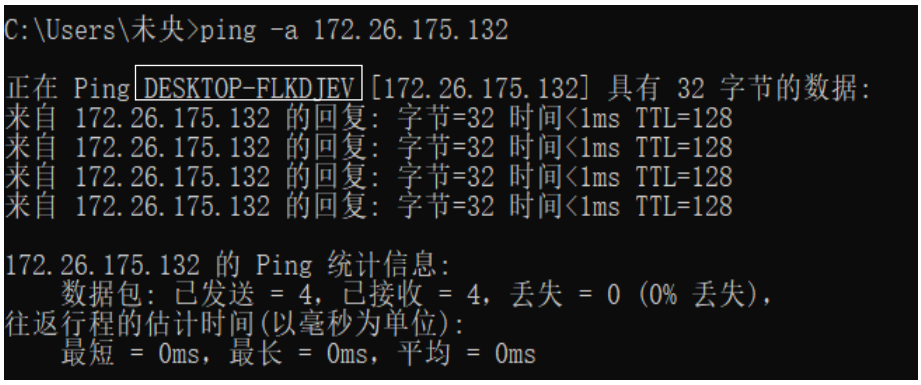

图 17. ping -a 指令

2. ipconfig 命令

2.1 ipconfig 命令介绍

ipconfig 实用程序可用于显示当前的 TCP/IP 配置的设置值，这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。但是，如果你的计算机和所在的局域网使用了动态主机配置协议（Dynamic Host Configuration Protocol，DHCP，Windows NT 下的一种把较少的 IP 地址分配给较多主机使用的协议，类似于拨号上网的动态 IP 分配），通过 ipconfig 可以了解计算机是否成功租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前 IP 地址、子网掩码和缺省网关实际上是进行测试和故障分析的必要项目。

2.2 ipconfig 功能实际操作

2.2.1 ipconfig

此时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。输入该命令之后得到如图 18 所示的结果。其中，我们看到有许多的地址。下面我们来进行说明：

1） 以太网适配器（以太网）：电脑连接学校网线的时候才会显示 IP 地址。当前由于处在 Wi-Fi 环境下，所以此时并没有网线接入，所以此时也是断开连接的状态。而我们之前图 4 中是连接网线的时候，所以当时存在 IP 地址；

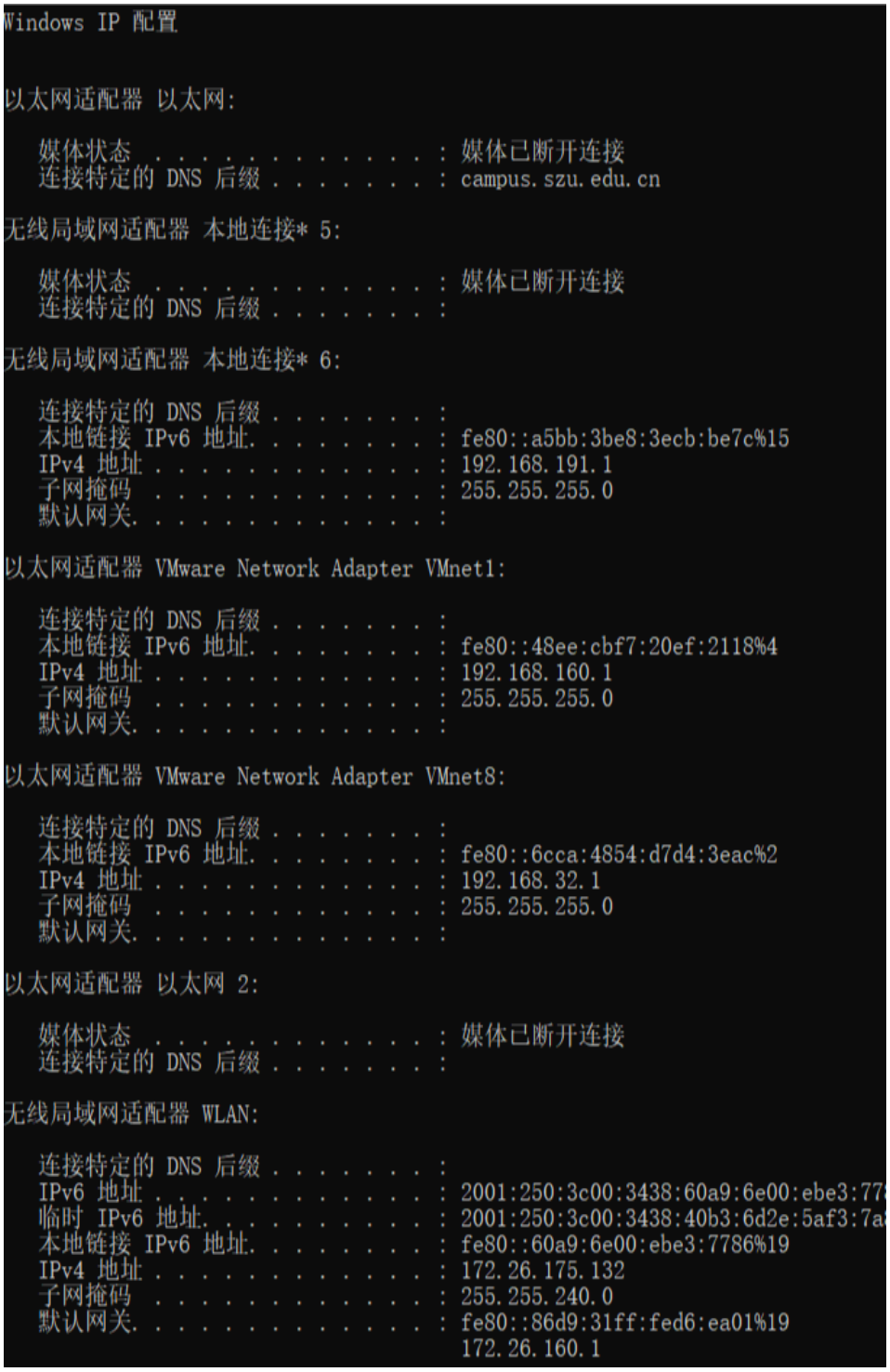

图 18. ipconfig 指令

2） 无线局域网适配器（本地连接*6）属于电脑热点，当关闭了 PC 的热点之后，这个连接就会显示断开；

3） VMware Network Adapter VMnet1/8，这两个网卡是虚拟机的，通过这两个网卡，虚拟机可以通过宿主机的网线上网；

4） 无线局域网适配器 WLAN，这个是电脑连接 Wi-Fi 的时候会显示 IP 地址。由于本机当前连接的是 Wi-Fi，所以在这里显示了本机 IP。

2.2.2 ipconfig/all

当使用 all 选项时，ipconfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息(如 IP 地址)，并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

那么 ipconfig/all 和 ipconfig 的区别在哪里呢？

1） 显示的设备的网络参数内容不同。ipconfig 在命令提示符里面会显示出的是本机的 IP 地址以及子网掩码和默认网关。ipconfig/all 显示的网络参数不仅包含了 ipconfig 在命令提示符里面的内容，还包含了 DHCP 服务器参数以及 DNS 参数等。

2） 显示的设备硬件信息不同。ipconfig 在命令提示符里面仅显示该计算机的适配器连接状态。ipconfig/all 会在命令提示符里面显示计算机的适配器物理地址、以及适配器的型号或名称等信息。

我们输入该条指令，观察一下结果，这里由于整体内容太长且部分内容在图 18 中已经体现出来，所以这里面我们以突出不同点为主。以当下连接 Wi-Fi 的状态为例，我们对比两条指令的不同之处，如图 19 所示。

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2001:250:3c00:3438:60a9:6e00:ebe3:7786
   临时 IPv6 地址. . . . . . . . . . : 2001:250:3c00:3438:c99d:431f:493:7104
   本地链接 IPv6 地址. . . . . . . . : fe80::60a9:6e00:ebe3:7786%19
   IPv4 地址 . . . . . . . . . . . . : 172.26.175.132
   子网掩码 . . . . . . . . . . . . : 255.255.240.0
   默认网关. . . . . . . . . . . . . : fe80::86d9:31ff:fed6:ea01%19
                                       172.26.160.1
```

图 19(a)．ipconfig 指令（无线局域网适配器 WLAN）

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
   物理地址. . . . . . . . . . . . . : 30-D1-6B-F4-E1-47
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2001:250:3c00:3438:60a9:6e00:ebe3:7786(首选)
   临时 IPv6 地址. . . . . . . . . . : 2001:250:3c00:3438:c99d:431f:493:7104(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::60a9:6e00:ebe3:7786%19(首选)
   IPv4 地址 . . . . . . . . . . . . : 172.26.175.132(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.240.0
   获得租约的时间  . . . . . . . . . : 2021年3月18日 18:02:30
   租约过期的时间  . . . . . . . . . : 2021年3月19日 0:02:30
   默认网关. . . . . . . . . . . . . : fe80::86d9:31ff:fed6:ea01%19
                                       172.26.160.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.62.111
   DHCPv6 IAID . . . . . . . . . . . : 355520875
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-22-FE-2F-73-8C-16-45-DD-07-D9
   DNS 服务器  . . . . . . . . . . . : 192.168.247.6
                                       192.168.247.26
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

图 19(b)．ipconfig/all 指令（无线局域网适配器 WLAN）

对比之后可以发现，ipconfig/all 语句明显比 ipconfig 指令要更加详细，包含了 DHCP 服务器参数以及 DNS 参数等，如白色标记位置所示。此外，适配器物理地址、适配器的名称信息都在该指令下被给出。

2.2.3 ipconfig/release(IPv4)

这条指令在于将所有接口的租用 IPv4 地址重新交付给 DHCP 服务器也就是归还 IP 地址。因为有时候我们要更新 IP 地址，这样的话首先应该先归还原来的 IP 地址，然后再进行更新。所以输入以下指令之后，再次观察无线局域网适配器 WLAN，得到如图 20 所示的结果，发现租用的 IP 地址已经消失了。

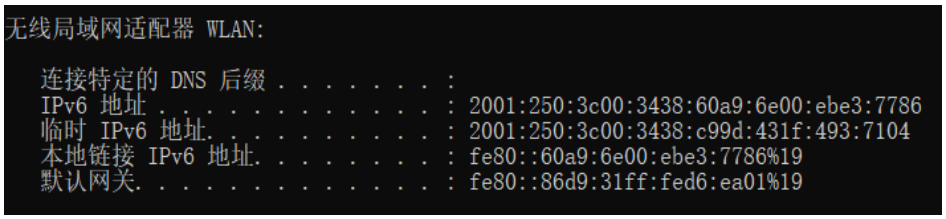

图 20. ipconfig/release 指令（无线局域网适配器 WLAN）

2.2.4 ipconfig/renew (IPv4)

接着上一小节的工作，当我们归还了 IP 地址之后该申请一个新的 IP 地址了。本地计算机设法与 DHCP 服务器取得联系，并租用一个 IP 地址。值得一提的是，多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

我们输入该指令，再次观察无线局域网适配器 WLAN，得到如图 21 所示的结果。我们这里面得到了一个新的 IP 地址，如图 21 中白色标记位置。

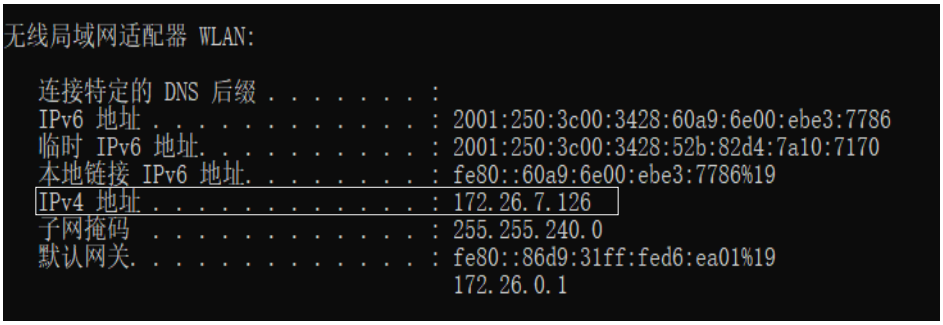

图 21. ipconfig/renew 指令（无线局域网适配器 WLAN）

2.2.5 其他功能

事实上，ipconfig 有很多参数以供设置。我们输入 ipconfig/?指令，得到所有参数如图 22 所示。

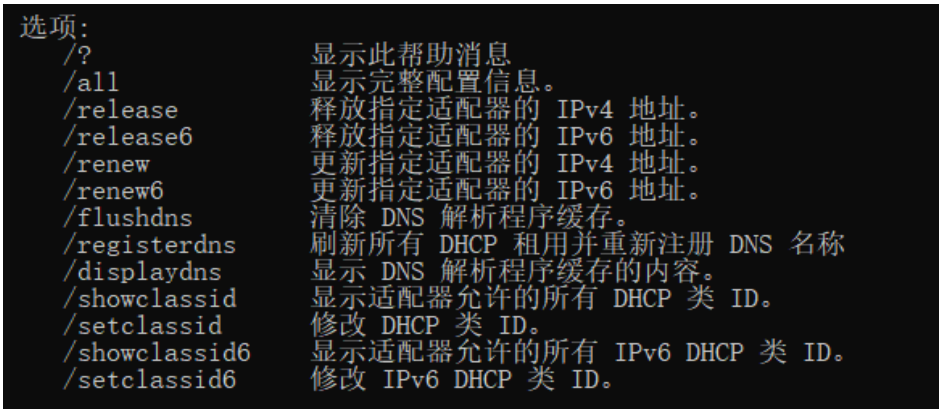

图 22. Ipconfig 所有可设置的参数

我们看到，上述的 release/renew 是针对 IPv4 网络的，而针对 IPv6 网络的也有相应的参数。还有展示所有 DNS 解析程序缓存内容、显示所有 DHCP 类 ID 的功能等等。

3. Netstat 命令

3.1 Netstat 命令介绍

Netstat 是一个监控 TCP/IP 网络的非常有用的工具，它可以显示路由表、实际的网络

连接以及每一个网络接口设备的状态信息。Netstat 还可以用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

3.2 Netstat 功能实际操作

3.2.1 *netstat – s*

我们在命令行打出该指令，分层显示了 IPv4 和 IPv6 的统计信息，以 IPv4 为例，包括有 IPv4 统计信息、ICMPv4(Internet Control Message Protocol，因特网控制报文协议)统计信息、IPv4 的 TCP(Transmission Control Protocol，传输控制协议)统计信息、IPv4 的 UDP(User Datagram Protocol，用户数据包协议)统计信息。

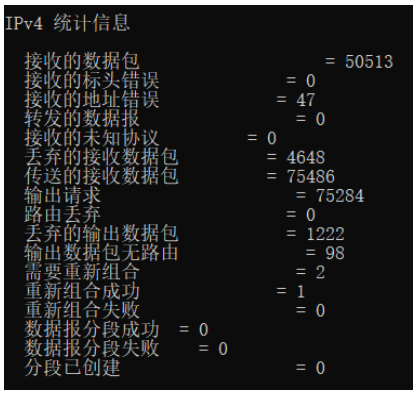

图 23(a). *netstat – s*（IPv4 统计信息）

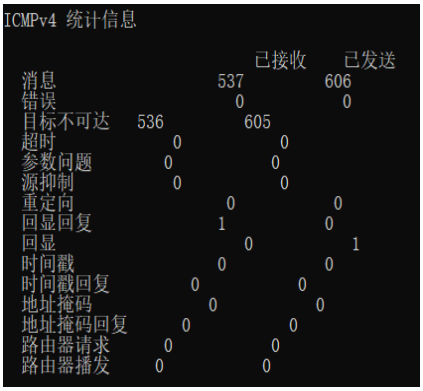

图 23(b). *netstat – s*（ICMPv4 统计信息）

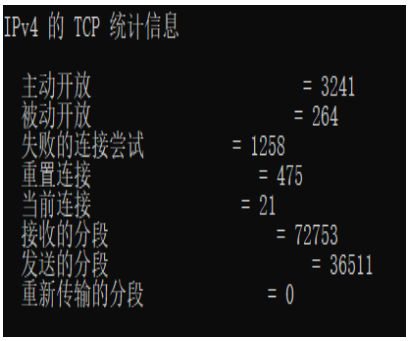

图 23(c). *netstat – s*（TCP 统计信息）

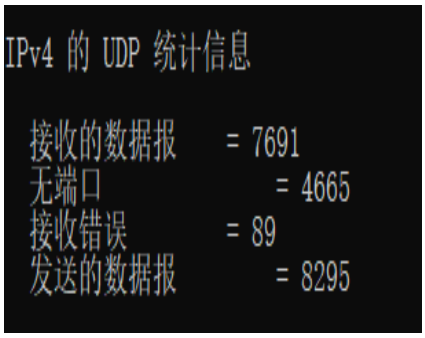

图 23(d). *netstat – s*（UDP 统计信息）

图 23. *netstat – s*功能实现

3.2.2 *netstat – e*

本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报总字节数、错误数、删除数、数据报的数量和广播的数量。这个选项可以用来统计一些基本的网络流量）。

我们打印该指令，得到如图 24 所示的结果。

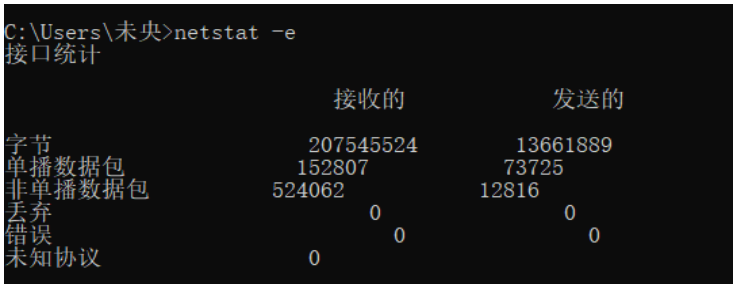

图 24. *netstat – e*功能实现

3.2.3 $netstat -r$

本选项显示关于路由表的信息，类似于 route print 命令时看到的信息。除显示有效路由外，还显示当前有效的连接。

首先打印了接口列表，也就是 ipconfig 语句中出现的所有接口，如图 25(a)所示。

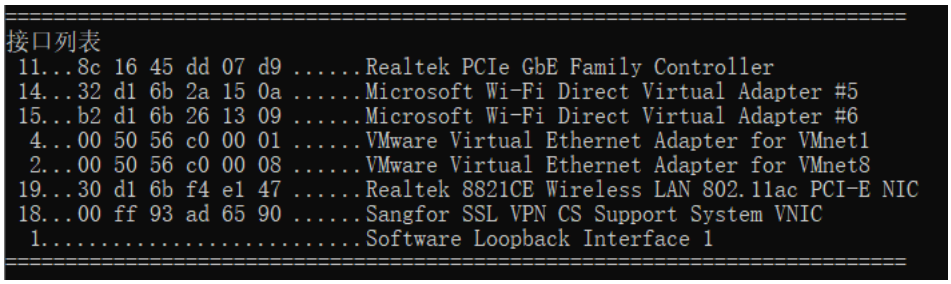

图 25(a). $netstat -r$功能实现（1）

然后就将 IPv4 和 IPv6 的路由表分别打印了出来。以 IPv4 为例，我们得到了如图 25(b)的路由表。

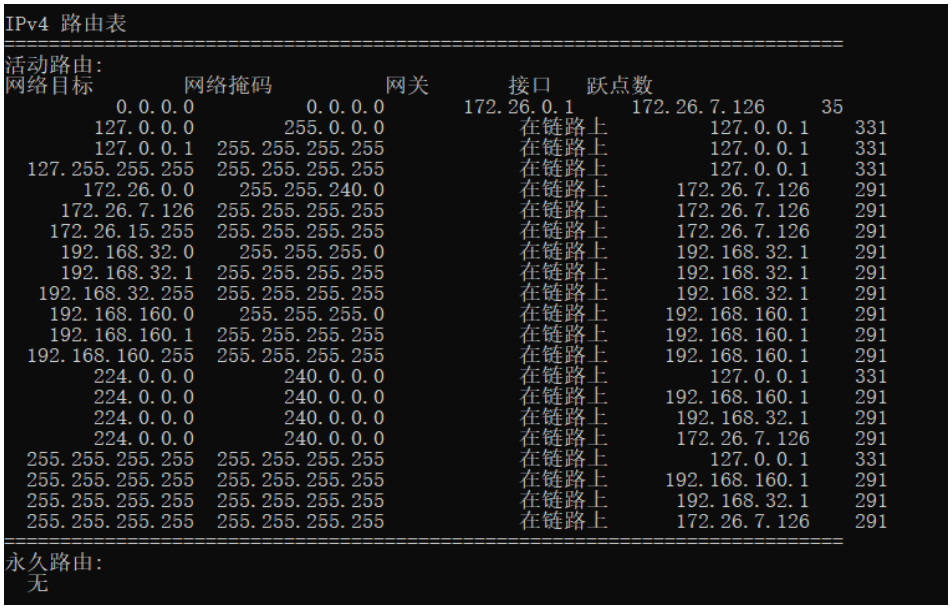

图 25(b). $netstat -r$功能实现（2）

3.2.4 $netstat -a$

本选项显示一个有效连接信息列表，包括已建立的连接（Established），也包括监听连接请求（Listening）的那些连接。

这里由于连接比较多，我们仅截取部分 TCP 协议的连接，可以看到最右边一栏的状态有已建立以及监听连接请求，如图 26 所示。

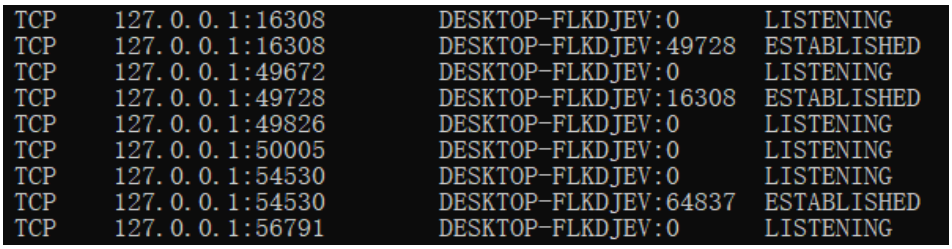

图 26. $netstat -a$功能实现

3.2.5 $netstat -n$

显示所有已建立的有效连接（包括在 ICQ 连接时查获对方的 IP 和端口）。

执行该指令，得到如图 27 所示的结果。

```
C:\Users\未央>netstat -n

活动连接

  协议   本地地址          外部地址        状态
  TCP    127.0.0.1:16308        127.0.0.1:49728        ESTABLISHED
  TCP    127.0.0.1:49728        127.0.0.1:16308        ESTABLISHED
  TCP    127.0.0.1:54530        127.0.0.1:64936        ESTABLISHED
  TCP    127.0.0.1:64936        127.0.0.1:54530        ESTABLISHED
  TCP    127.0.0.1:64937        127.0.0.1:64938        ESTABLISHED
  TCP    127.0.0.1:64938        127.0.0.1:64937        ESTABLISHED
  TCP    172.26.7.126:63732     40.90.189.152:443      ESTABLISHED
  TCP    172.26.7.126:63758     118.31.166.55:443      ESTABLISHED
  TCP    172.26.7.126:64033     121.51.140.150:8080    ESTABLISHED
  TCP    172.26.7.126:64696     64.233.189.188:5228    ESTABLISHED
  TCP    172.26.7.126:64907     112.80.255.27:443      TIME_WAIT
  TCP    172.26.7.126:64944     112.80.255.27:443      ESTABLISHED
  TCP    172.26.7.126:64945     112.80.255.27:443      ESTABLISHED
  TCP    172.26.7.126:64947     13.107.4.52:80         TIME_WAIT
  TCP    172.26.7.126:64952     52.109.124.51:443      TIME_WAIT
  TCP    172.26.7.126:64953     52.109.124.51:443      TIME_WAIT
  TCP    172.26.7.126:64954     220.181.43.14:8888     ESTABLISHED
  TCP    172.26.7.126:64955     220.181.107.200:443    ESTABLISHED
```

图 27. $netstat -n$功能实现

4. Tracert 命令

4.1 Tracert 命令介绍

Tracert 命令可以用来跟踪数据报使用的路由(路径)，并列出在所经过的每个路由器上所花的时间。因此，Tracert 一般用来检测故障的位置。该实用程序跟踪的路径是源计算机到目的计算机的一条路径，**但不能保证或认为数据报总遵循这个路径**。

简单来说，Tracert 是一个简单的网络诊断工具，可以列出分组经过的路由节点，以及它在 IP 网络中每一跳的延迟。(这里的延迟是指：分组从信息源发送到目的地所需的时间，延迟也分为许多的种类传播延迟、传输延迟、处理延迟、排队延迟等，是大多数网站性能的瓶颈之一)。

4.2 Tracert 功能实际操作

4.2.1 Tracert 基本功能

Tracert 的基本功能就是跟踪数据报使用的路径。所以当我们在指令后面添加一个域名或者 IP 之后，就会显示到达该地址的时间和经过的 IP 地址。

以访问深大 Blackboard 为例，我们的运行结果如图 28 所示。

```
C:\Users\未央>tracert elearning.szu.edu.cn

通过最多 30 个跃点跟踪
到 elearning.szu.edu.cn [116.13.96.90] 的路由:

  1     3 ms    55 ms    32 ms  172.26.240.1
  2     *        *        *     请求超时。
  3    12 ms     3 ms     3 ms  192.168.255.46
  4    93 ms    98 ms   404 ms  172.21.216.9
  5    42 ms    97 ms    98 ms  172.21.216.130
  6     *        *        *     请求超时。
  7     4 ms     3 ms    53 ms  116.13.96.90

跟踪完成。
```

图 28. $tracert$功能实现

我们对结果进行分析：

1） tracert 命令用于确定 IP 数据包访问目标所采取的路径，显示从本地到目标网站所在网络服务器的一系列网络节点的访问速度，最多支持显示 30 个网络节点。

2） 从图中我么可以看出，我们经过了 4 个路由节点到达了目的服务。第一个一般是我们的机器是从该 IP 出去的，从第二个开始，非超时的才是我们经过的路由，最后一个就是我们的目的地。

3） 中间的三列，时间单位是 ms，分别表示连接到每个路由节点的速度，返回速度和多次链接反馈的平均值。这里我们看到了一些用“*”表示的时间，说明这个 IP 在这个路由节点有问题。

4） 如果返回消息是超时，则表示这个路由节点和当前我们使用的宽带，是无法联通的，至于原因，就有很多种了，比如：特意在路由上做了过滤限制，或者确实是路由的问题等，需要具体问题具体分析。这里我们第二行和第六行出现了超时的问题，由于我们使用 VPN 进行访问，而有时候 VPN 的流量比较大，导致我们的线路出现拥挤的情况，所以个别时候可能会出现超时的情况。

5） 另外，我们认为一般 10 个节点以内可以完成跟踪的网站，访问速度都是不错的；10 到 15 个节点之内才完成跟踪的网站，访问速度则比较差，如果超过 30 个节点都没有完成跟踪的网站，则可以认为目标网站是无法访问的。

4.2.2 Tracert 的其他功能

Tracert 和其它命令一样都可以设置附加参数。我们在命令行键入 Tracert 之后会有用法提示如图 29 所示。

```
C:\Users\未央>tracert

用法: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

选项:
    -d                  不将地址解析成主机名。
    -h maximum_hops     搜索目标的最大跃点数。
    -j host-list        与主机列表一起的松散源路由(仅适用于 IPv4)。
    -w timeout          等待每个回复的超时时间(以毫秒为单位)。
    -R                  跟踪往返行程路径(仅适用于 IPv6)。
    -S srcaddr          要使用的源地址(仅适用于 IPv6)。
    -4                  强制使用 IPv4。
    -6                  强制使用 IPv6。
```

图 29. *tracert*参数设置

例如，使用$-h\ maximum_hops$的时候可以设置最大跃点数。我们重复 tracert 深大的 Blackboard，然后设置跃点数为 4，可以看到如图 30 所示的结果。

```
C:\Users\未央>tracert -h 4 elearning.szu.edu.cn

通过最多 4 个跃点跟踪
到 elearning.szu.edu.cn [116.13.96.90] 的路由:

  1    11 ms   110 ms   129 ms  172.26.240.1
  2     *        *        *     请求超时。
  3    11 ms     3 ms   152 ms  192.168.255.46
  4   102 ms     5 ms  1052 ms  172.21.216.9

跟踪完成。
```

图 30. $tracert-h\ maximum_hops$命令使用

5. Route 命令

5.1 Route 命令介绍

Route 用来显示、人工添加和修改路由表项目。 大多数主机都驻留在只连接一台路由器的网段上。由于只有一台路由器，因此不存在使用哪一台路由器将数据报发表到远程计算机上去的问题，该路由器的 IP 地址可作为该网段上所有计算机的缺省网关来输入。但是，当网络上拥有两个或多个路由器时，可能想让某些远程 IP 地址通过某个特定的路由器来传递，而其他的远程 IP 则通过另一个路由器来传递。在这种情况下，必须人工将项目添加到路由器和主机上的路由表中。

5.2 Route 功能实际操作

5.2.1 route print

本命令用于显示路由表中当前项目。在命令行打印出这条指令，以 IPv4 为例，我们得到的结果如图 31 所示。就这一运行结果，和我们之前的指令 netstat -r 的结果是一致的。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    172.26.240.1   172.26.240.132     40
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
     172.26.240.0    255.255.240.0         在链路上     172.26.240.132    296
   172.26.240.132  255.255.255.255         在链路上     172.26.240.132    296
   172.26.255.255  255.255.255.255         在链路上     172.26.240.132    296
     192.168.32.0    255.255.255.0         在链路上      192.168.32.1    291
     192.168.32.1  255.255.255.255         在链路上      192.168.32.1    291
   192.168.32.255  255.255.255.255         在链路上      192.168.32.1    291
    192.168.160.0    255.255.255.0         在链路上     192.168.160.1    291
    192.168.160.1  255.255.255.255         在链路上     192.168.160.1    291
  192.168.160.255  255.255.255.255         在链路上     192.168.160.1    291
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上     172.26.240.132    296
        224.0.0.0        240.0.0.0         在链路上     192.168.160.1    291
        224.0.0.0        240.0.0.0         在链路上      192.168.32.1    291
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上     172.26.240.132    296
  255.255.255.255  255.255.255.255         在链路上     192.168.160.1    291
  255.255.255.255  255.255.255.255         在链路上      192.168.32.1    291
===========================================================================
永久路由:
  无
```

图 31. route print 命令使用

5.2.2 *route add*

本命令可将路由项目添加给路由表。

我们在命令行输入 route 之后点击回车，可以看到 route 的提示信息，如图 32 所示。

```
只有在 PRINT 命令中才允许模式匹配。
诊断信息注释:
    无效的 MASK 产生错误，即当 (DEST & MASK) != DEST 时。
    示例: > route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
            路由添加失败: 指定的掩码参数无效。
            (Destination & Mask) != Destination。
```

图 32. route 提示信息

有了这个提示信息，我们就使用这个命令进行添加。注意，在添加路由表的时候我们需要管理员权限运行。打开管理员权限的方法就是，在输入 cmd 出现命令提

示符之后，以管理员权限进行打开就可以。

例如，如果要设定一个到目的网络 157.0.0.0 的路由，其间要经过 3 个路由器网段，首先要经过本地网络上的一个路由器（所接端口 IP 为 157.55.80.1，子网掩码为 255.0.0.0），则应该输入以下命令。如图 33 所示，添加成功。

```
C:\WINDOWS\system32> route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3
 操作完成!
```

图 33. route add 指令

为了查看是否添加成功，我们再次使用 print 命令，可以看到已经添加进了路由表，如图 34 所示。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    172.26.240.1   172.26.240.132     35
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
        157.0.0.0        255.0.0.0   157.55.80.1   172.26.240.132     38
     172.26.240.0    255.255.240.0         在链路上     172.26.240.132    291
    172.26.240.132  255.255.255.255         在链路上     172.26.240.132    291
    172.26.255.255  255.255.255.255         在链路上     172.26.240.132    291
      192.168.32.0    255.255.255.0         在链路上      192.168.32.1    291
```

图 34. route print 指令显示已经成功添加

5.2.3 route change

本命令用来修改数据的传输路由。但不能用本命令来改变数据的目的地。

以刚刚添加的路由项目为例，我们用如下指令进行修改，如图 35 所示。

Route change+目的路由+mask 子网掩码+所接端口 IP + metric 路由器网段数

```
C:\WINDOWS\system32>route change 157.0.0.0 MASK 255.0.0.0 202.96.123.250 METRIC 3
 操作完成!
```

图 35. route change 指令进行修改

我们需要检查一下是否成功修改。继续 print 一下，看到结果如图 36 所示，传输路由已经发生了修改。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    172.26.240.1   172.26.240.132     35
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
        157.0.0.0        255.0.0.0  202.96.123.250   172.26.240.132     38
     172.26.240.0    255.255.240.0         在链路上     172.26.240.132    291
    172.26.240.132  255.255.255.255         在链路上     172.26.240.132    291
    172.26.255.255  255.255.255.255         在链路上     172.26.240.132    291
```

图 36. route change 指令修改成功

5.2.4 route delete

本命令可以从路由表中删除路由。指令格式：route delete + address

我们输入这条指令，在进行 print，发现已经没有了这个网络目标，如图 37 所示。

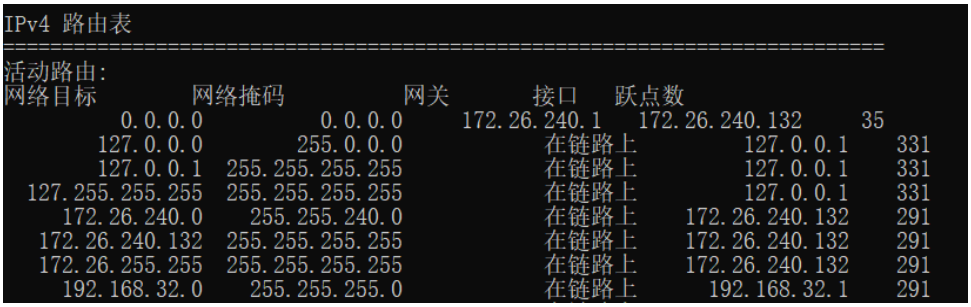

图 37. route delete 指令删除成功

6. ARP (Address Resolution Protocol，地址转换协议)

6.1 ARP 命令介绍

ARP 用于确定对应 IP 地址的网卡物理地址。ARP 命令能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。使用 ARP 命令，也可以用人工方式输入静态的网卡物理/IP 地址对。可使用这种方式为缺省网关和本地服务器等常用主机进行操作，有助于减少网络上的信息量。

ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。按照缺省设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。需要通过 ARP 命令查看高速缓存中的内容时，请最好先 ping 此台计算机。

6.2 ARP 功能实际操作

6.2.1 在没有参数的情况下输入 ARP，将提示 ARP 的所有功能，如图 38 所示。

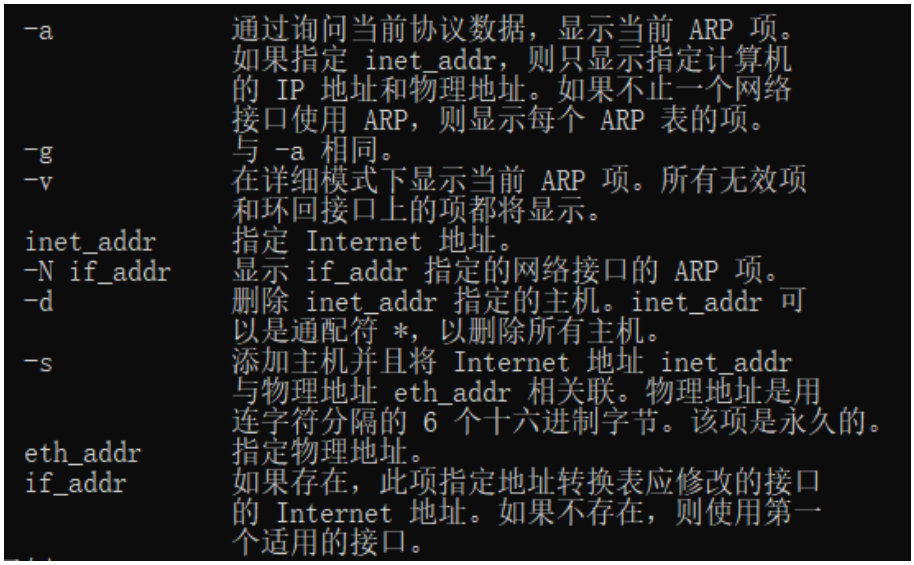

图 38. ARP 指令所有参数及其功能

6.2.2 $arp\ -a$或$arp-g$

此命令用于查看高速缓存中的所有项目。

我们输入该条指令，结果如图 39 所示。观察这个结果，这正是分别对应了 VMware Network Adapter VMnet8、VMware Network Adapter VMnet1 以及无线局域网适配器 WLAN。由于当前电脑连接的是 Wi-Fi，所以目前只有这三个 IP 地址。

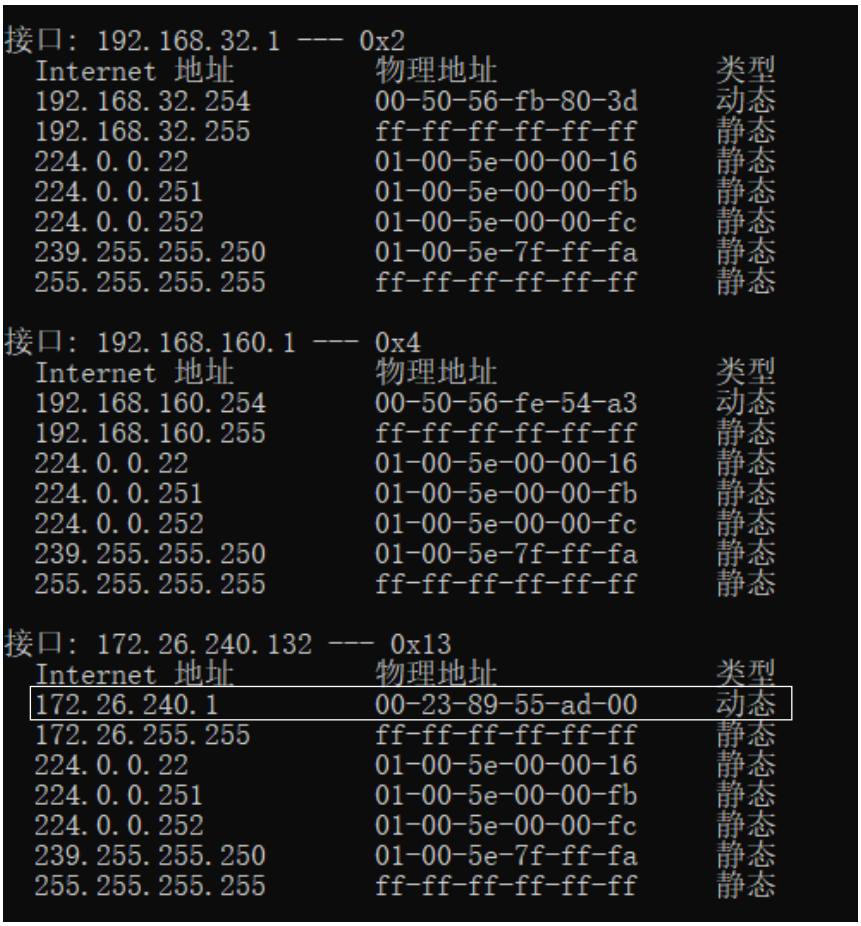

图 39. ARP -a 指令运行结果

6.2.3 $arp\ -a\ IP$

如果有多个网卡，那么使用 ARP -a 加上接口 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。也就是说，这个命令规定了只显示某个网卡的信息。

如果我们以无线局域网适配器 WLAN 为例，以图 39 中标记位置为例，想只显示此处的物理地址，那么调用如下指令，看到只显示了这一项，如图 40 所示。

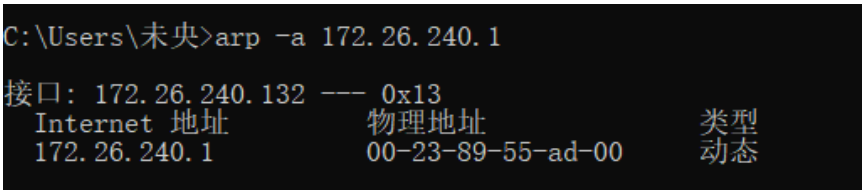

图 40. ARP -a IP 指令运行结果

6.2.4 $arp\ -s\ IP +$ 物理地址

可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

注意，该条指令依然需要管理员权限。如图 41 所示，添加语句键入后没有问题不会有提示信息。

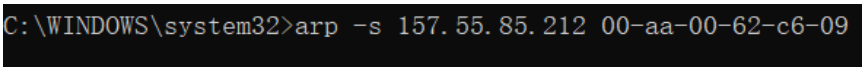

图 41. 向 ARP 高速缓存中输入静态项目

然后再次 ARP -a，发现了这条新加上去的静态项目，如图 42 所示。

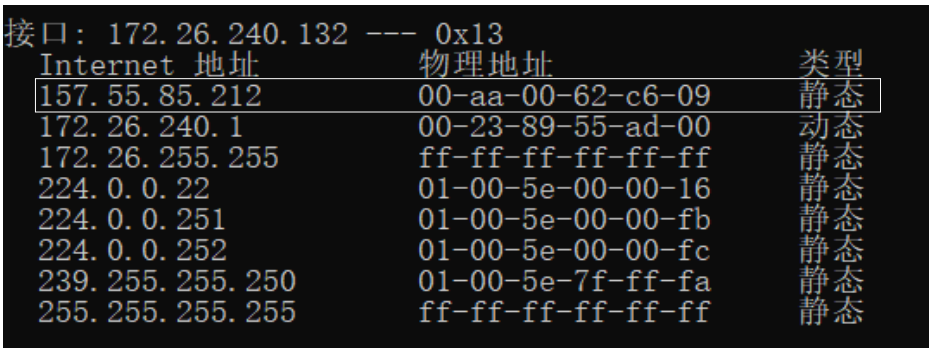

图 42. 向 ARP 高速缓存中输入静态项目成功

6.2.5 $arp\ -d\ IP+$ 物理地址

使用本命令能够人工删除一个静态项目。以我们刚才添加的 IP 地址为例，如果我们想删除它，那么久键入这条指令，然后再查看高速缓存，如图 43 所示。对比图 42 和图 43，即可发现 157.55.85.212 这个 IP 已经被删除。

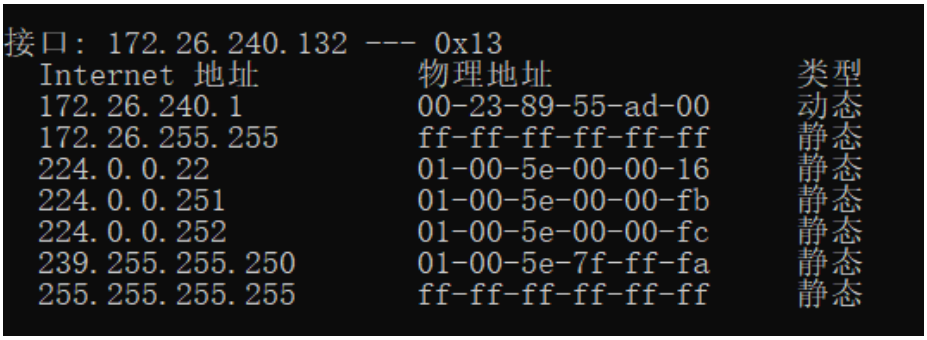

图 43. 在 ARP 高速缓存中删除静态项目成功

6.2.6 其它功能

之前我们的$arp-a$显示了 VMware Network Adapter VMnet8、VMware Network Adapter VMnet1 以及无线局域网适配器 WLAN 的高速缓存中的所有项目。如果我们只是想看其中一类的项目怎么选择参数呢？

指令：$arp-a-n+$ 接口 IP

如图 44 所示，我们按照该指令输入，得到了 VMware Network Adapter VMnet8 中的项目。

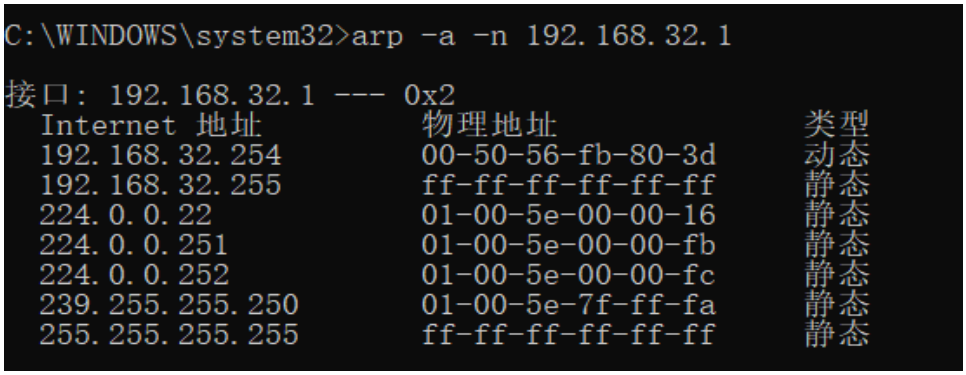

图 44. 在 ARP -a -n 指令

此外，我们可以使用-v 选项。-v 选项只能和 ARP –a 一起使用，在详细模式下显示当前 ARP 项。所有无效项和环回接口上的项都将显示。如下图所示，能看到本地环回接口的 ARP 项。

如图 45 所示，本地的 ARP 项在-v 参数的存在下被显示出来，而在之前是没有显示的。

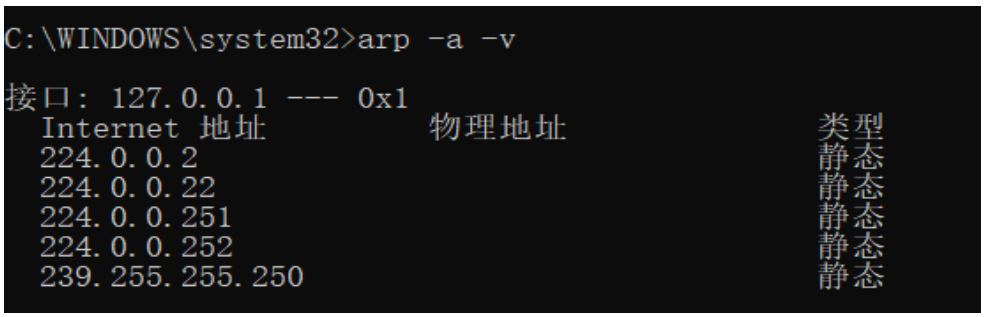

图 45. 在 ARP -a -v 指令

7. *Nslookup*命令

7.1 *Nslookup*命令介绍

*Nslookup*命令的功能是查询一台机器的 IP 地址和其对应的域名，通常它能监测网络中 DNS 服务器是否能正确实现域名解析它，它的运行需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

7.2 *Nslookup*功能实际操作

我们在*Nslookup*后面加入一个域名，然后回车，如图 46 所示，我们在非权威应答中得到了百度的 IP 地址，为 183.232.231.174 或者 183.232.231.172。经过验证，发现 IP 地址是正确的。

图 46. *Nslookup*指令解析域名

此外，该指令还能进行反向解析。例如我们得到了谷歌的 IP 为 172.217.25.196，然后使用指令$nslookup\ -qt = ptr\ IP$进行反向解析，得到如图 47 所示的结果。

8. *Netsh* (Network Shell，网络配置工具)

8.1 *Netsh*命令介绍

Windows 系统下提供的功能强大的网络配置命令行工具，它允许从本地或远程显示或修改当前正在运行的主机网络配置。该工具既可以命令行交互运行，手动输入命令，也可以在脚本中使用，通过批处理模式运行一组命令。

```
C:\Users\未央>nslookup -qt=ptr 172.217.25.196
服务器:  RT-N56U_B1.lan
Address:  192.168.123.1

非权威应答:
196.25.217.172.in-addr.arpa     name = nrt12s13-in-f196.1e100.net
196.25.217.172.in-addr.arpa     name = nrt12s13-in-f4.1e100.net
```

图 47. *Nslookup*指令反向解析

8.2 *Netsh*功能实际操作

指令格式：

netsh [−*a AliasFile*] [−*c Context*] [−*r RemoteMachine*] [*Command* | − *f ScriptFile*]

例如，我们想看一下防火墙配置文件，输入命令：

netsh advfirewall show allprofiles

结果如图 48 所示，所有的防火墙配置文件都被打印了出来。

```
C:\Users\未央>netsh wlan show drivers

接口名称: WLAN

    驱动程序                  : Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
    供应商                    : Realtek Semiconductor Corp.
    提供程序                  : Realtek Semiconductor Corp.
    日期                      : 2020/4/27
    版本                      : 2024.0.8.122
    INF 文件                  : oem49.inf
    类型                      : 本机 WLAN 驱动程序
    支持的无线电类型          : 802.11n 802.11g 802.11b 802.11ac 802.11n 802.11a
    支持 FIPS 140-2 模式: 是
    支持 802.11w 管理帧保护 : 是
    支持的承载网络  : 否
    基础结构模式中支持的身份验证和密码:
                                开放式              无
                                WPA2 - 个人         CCMP
                                开放式              WEP-40bit
                                开放式              WEP-104 位
                                开放式              WEP
                                WPA - 企业          TKIP
                                WPA - 个人          TKIP
                                WPA2 - 企业         TKIP
                                WPA2 - 个人         TKIP
                                WPA - 企业          CCMP
                                WPA - 个人          CCMP
                                WPA2 - 企业         CCMP
                                WPA3 - 个人         CCMP
                                供应商定义的            TKIP
                                供应商定义的            CCMP
                                供应商定义的            供应商定义的
                                供应商定义的            供应商定义的
                                WPA2 - 企业         供应商定义的
                                WPA2 - 企业         供应商定义的
                                供应商定义的            供应商定义的
                                供应商定义的            供应商定义的
    支持的无线显示器: 是 (图形驱动程序: 是, WLAN 驱动程序: 是)
```

图 48. *netsh*指令查看防火墙配置

9. FTP (File Transfer Protocol，文件传输协议)

9.1 FTP 命令

Windows 系统提供的 FTP 工具，客户端用户连接远程 FTP 服务器，实现文件共享和传输，下载 FTP 服务器资源文件，或上传客户端文件。

9.2 FTP 功能实际操作

9.2.1 FTP 软件下载

这里面我们选择 FTP 开源服务站点 https://www.filezilla.cn/，下载$filezilla$这个 FTP 软件。

下载好以后我们添加一个名为lrc的用户，不需要设置密码，如图 49 所示。

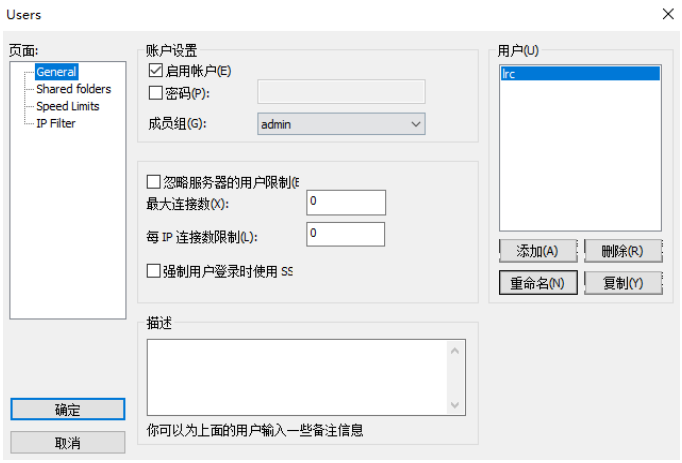

图 49. 为 FTP 工具添加用户

然后我们使用另一台电脑准备进行文件传输。首先，将这台电脑的 PC 热点打开，得知 PC 热点的 IP 地址之后，然后在另一台电脑上使用 FTP 指令访问该 IP，如图 50 所示，已经连接到了这台电脑。连接上这台电脑之后，我们就可以执行一些操作。

```
C:\Users\D4N13L\Desktop>ftp 192.168.191.1
连接到 192.168.191.1。
220-FileZilla Server 涓  构鐗?0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
用户(192.168.191.1:(none)): lrc
331 Password required for lrc
密码:
230 Logged on
```

图 50. 连接这台电脑

9.2.2 FTP 功能实践

首先，我们打印 FTP 的所有功能，如图 51 所示。

```
C:\Users\未央>ftp
ftp> ?
命令可能是缩写的。  命令为:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp>
```

图 51. FTP 工具的所有功能

我们先设置主文件夹，也就是要访问该电脑中的哪个盘。我们设置 D 盘为访问主文件夹，如图 52 所示。然后使用dir指令，显示 D 盘所有的文件，如图 53 所示。

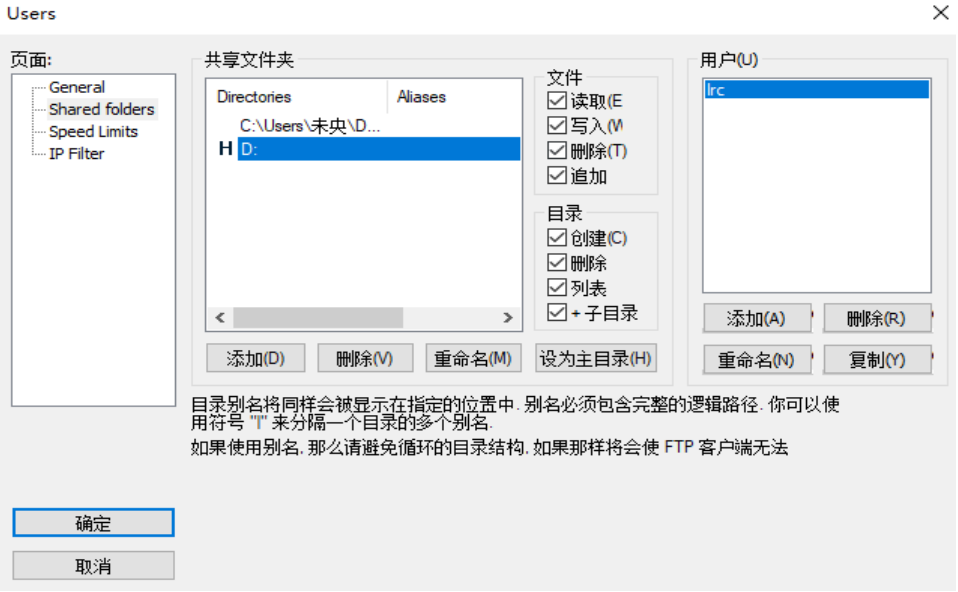

图 52. FTP 设置 D 盘为访问文件夹

```
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp              0 Sep 22  2018 $RECYCLE.BIN
drwxr-xr-x 1 ftp ftp              0 Jul 14  2019 2345Downloads
drwxr-xr-x 1 ftp ftp              0 Feb 06  2021 37694a642772509165fe015d7dc3644e
drwxr-xr-x 1 ftp ftp              0 Oct 13  2020 Access数据库
-r--r--r-- 1 ftp ftp         287382 Mar 03  2019 adSafe2.0.2QiHu（adsafe插件版）.crx
drwxr-xr-x 1 ftp ftp              0 Nov 13  2020 Anaconda
drwxr-xr-x 1 ftp ftp              0 Sep 01  2020 Android Studio
drwxr-xr-x 1 ftp ftp              0 Mar 15 15:41 AxGlyph
drwxr-xr-x 1 ftp ftp              0 Jan 26  2021 AxMath
drwxr-xr-x 1 ftp ftp              0 Feb 09  2021 BaiduNetdiskDownload
drwxr-xr-x 1 ftp ftp              0 Dec 30  2020 CloudMusic
drwxr-xr-x 1 ftp ftp              0 Mar 09  2018 cn_office_professional_plus_2016_x86_x64_dvd_6969182
drwxr-xr-x 1 ftp ftp              0 Oct 26  2020 CTex
drwxr-xr-x 1 ftp ftp              0 Sep 04  2019 DaBaiCai
drwxr-xr-x 1 ftp ftp              0 Jul 02  2020 Dev-Cpp
drwxr-xr-x 1 ftp ftp              0 Sep 13  2020 donotknow
drwxr-xr-x 1 ftp ftp              0 Jan 04  2019 Download
```

图 53. $FTP-dir$指令访问文件夹中的所有文件

接下来我们尝试抓取文件。使用 get 指令，如图 54 所示，抓取成功。

```
ftp> get Readme.txt
200 Port command successful
150 Opening data channel for file download from server of "/Readme.txt"
226 Successfully transferred "/Readme.txt"
ftp: 收到 2601 字节，用时 0.00秒 2601000.00千字节/秒。
```

图 54. $FTP-get$指令抓取文件夹中的所有文件

为了检查是否成功抓取，我们将保存位置设置为桌面，也就是在 FTP 中 cd desktop，然后可以看到该文件已经被保存在桌面了，如图 55 所示。

图 55. $FTP-get$指令抓取文件成功

10. Net (网络管理命令)

10.1 Net 命令介绍

Net 命令是一个命令行命令，通过它可以查看和管理网络的环境、服务、用户、登陆等信息内容。要想获得 Net 的命令帮助，在命令行控制台下输入 NET /?就可以得到 Net 的所有命令列表。

10.2 Net 功能实际操作

10.2.1 Net 展示全部功能

在命令行输入 Net ？之后得到全部的结果，如图 56 所示。

```
C:\Users\未央>net ?
此命令的语法是:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

图 56. 查看*net*指令全部操作

10.2.2 根据 10.2.1 中的方法，我们进行举例阐述。例如，想查看账户信息，就选择 accounts 选项，如图 57 所示。

```
C:\Users\未央>net accounts
强制用户在时间到期之后多久必须注销?:      从不
密码最短使用期限(天):                    0
密码最长使用期限(天):                    42
密码长度最小值:                          0
保持的密码历史记录长度:                  None
锁定阈值:                                从不
锁定持续时间(分):                        30
锁定观测窗口(分):                        30
计算机角色:                              WORKSTATION
命令成功完成。
```

图 57. *net accounts*指令查看账户信息

或者想查看当前用户，那么选择 user 选项，得到结果如图 58 所示。

```
C:\Users\未央>net user

\\DESKTOP-FLKDJEV 的用户帐户

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
WDAGUtilityAccount       未央
命令成功完成。
```

图 58. *net user*指令查看用户

实验结论：

1. 网络命令虽然种类繁多，但是很多指令的功能都是近似的；
2. 通过 ipconfig 指令，我们可以发现当连接 Wi-Fi 的时候和连接网线的时候，IP 地址是不一样的；
3. IP 地址并非一成不变，每次查询的时候都会有不同。但是 IP 地址很重要，每次到达一个 IP 地址的时候都会经过很多 IP 地址，所以事实上当我们在访问百度的时候经过了很多我们之前并不知道的过程。

心得体会：

本次实验让我获益匪浅。之前在使用计算机的时候，没有网络的概念，只知道利用域名或者输入想要检索的信息进行搜索。但事实上，每一个域名都有 IP 地址，我们访问域名事实上访问的都是一个个地址。这也体现了计算机网络的条理性和复杂性。

指导教师批阅意见：

成绩评定：

指导教师签字：邹永攀

2021 年 3 月　　日

备注：