

# 实验 1 常用的网络命令

## 一、实验目的、性质及器材

### 1. 实验目的

- 计算机网络体系结构的相关基本概念原理
- 掌握局域网的定义和特性，熟悉局域网的几种拓扑结构，通过比较理解各自的特点。
- 了解网络使用的通信协议
- 熟悉使用 Ping、Ipconfig 等常用的网络命令。

### 2. 实验性质

验证性实验。

### 3. 实验器材

计算机（已安装 Windows 操作系统）。

## 二、实验内容

### 1. 基本知识回顾：

#### 1.1 网络的体系结构概述

计算机网络是由多种计算机和各类终端通过通信线路连接起来的复杂系统。在这个系统中，计算机型号不一、终端类型各异，加之线路类型、连接方式、同步方式、通信方式不同，给网络中各节点间的通信带来许多不便。在不同计算机系统之间，真正以协同方式进行通信是十分复杂的，为了设计这样复杂的计算机网络，早在最初设计 ARPANET 时即提出了分层的方法。用分层来实现网络的结构化设计，每层设计相应的协议，实现对应的功能。这样的“分层”可将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题总是比较易于研究和处理的。

计算机网络各层及其协议的集合，称为网络的体系结构。划分不同的层次，或层次中实现不同的功能，也就意味着不同的体系结构。

采用这种分层结构可以带来很多好处：

（1）各层之间是独立的。某一层并不需要知道它的下一层是如何实现的，而仅仅需要知道层间接口（即界面）所提供的服务。由于每一层只实现一种相对独立的功能，因而可将一个难以处理的复杂问题分解为若干个较容易处理的更小一些的问题。这样，整个问题的复杂程度就下降了。

（2）灵活性好。当任何一层发生变化时（例如技术的变化），只要层间接口关系保持不变，则这层以上或以下各层均不受影响。

（3）结构上可分割开。各层都可以采用最合适的技术来实现。

（4）易于实现和维护。这种结构使得实现和调试一个庞大而又复杂的系统变得容易，因为整个系统已被分解为若干个相对独立的子系统。

（5）能促进标准化工作，因为每一层的功能及其所提供的服务都已有了精确的说明。

#### 1.2 协议

网络协议简称协议，是为计算机网络中的数据交换建立的规则、标准或约定的集合。为了完成各层所规定的功能，每一层都要设计若干协议。协议是水平的，其所涉及的实体是通信双方的对等实体，双方共同遵守协议，在协议的约定下进行通信，完成协议约定的任务。相反，在自己的计算机上进行一个不需要和网络上其他主机进行通信的操作，尽管也有各种规定，但这些规定不能称为网络协议。

网络协议由以下三个要素组成。

- (1) 语法：即数据与控制信息的结构或格式。
- (2) 语义：即需要发出何种控制信息，完成何种动作和做出何种响应。
- (3) 同步：即事件实现顺序的详细说明。

对协议的描述通常有两种形式，一种是用便于阅读和理解的文字来描述，另一种是用程序代码来描述，但不管用哪种形式，都需要对协议做出精确的解释。

## 1.3 五层协议的体系结构

为了促进计算机网络的发展，国际标准化组织 ISO 于 1977 年成立了一个委员会，提出了不基于具体机型、操作系统或公司的网络体系结构，即 OSI 参考模型（OSI/RM），其全称为开放系统互连参考模型（Open System Interconnection Reference Model, OSI/RM）。

OSI 参考模型是一个七层的体系结构，它们由低到高分别是物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、运输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer）。第一层到第三层属于 OSI 参考模型的低三层，负责创建网络通信连接的链路；第四层到第七层为 OSI 参考模型的高四层，具体负责端到端的数据通信。

OSI 参考模型是网络技术的基础，尽管概念清楚，理论也较完整，但由于太复杂等种种原因，并没有得到市场的认可。真正占领市场并得到广泛应用的是 TCP/IP 体系结构，这是一种四层的结构，上面三层依次为应用层、运输层、网际层，最下面的网络接口层并没有具体的内容，虽然这在当时的环境下非常快速地适应了市场的需求，将一些异构的网络都包容了进来，但缺少了对物理层和数据链路层内容的约定。谢希仁教授所编著的《计算机网络》按照五层体系结构来阐述计算机网络的体系结构，更加清晰、简洁。三种体系结构的层次划分及对应关系如图 1-1 所示。

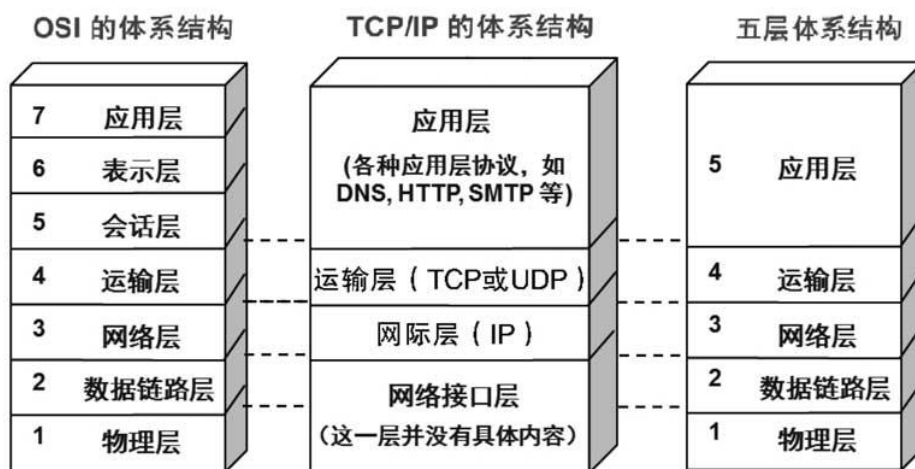


图 1-1 三种体系结构对照图

下面以五层体系结构为例对计算机网络各层所要实现的功能做简要解释。

### 1. 物理层

物理层传输数据的单位是比特，其主要关心的是在连接各种计算机的传输媒体上如何传输比特流。为了达到这个目的，物理层为建立、维护和拆除物理链路提供所需要的机械的、电气的、功能的和规程的特性。比如，用多大的电压代表“1”或“0”；当发送端发出比特“1”时，在接收端如何识别出这是比特“1”而不是比特“0”；规定连接电缆的材质、引线的数目及电缆接头的几何尺寸、锁紧装置等物理性内容。

需要注意的是，具体的连接媒介，如传输介质等，并非物理层的内容。

物理层常见设备有中继器、集线器和网线等。

### 2. 数据链路层

数据链路层主要解决利用物理地址通信的问题，传输数据的单位是帧，帧的格式中包括的信息有：地址信息部分、控制信息部分、数据部分和校验信息部分等。为了完成这一任务，数据链路层需要解决以下三个基本问题。

#### 1) 封装成帧

发送方的数据链路层需要将上层传递下来的协议数据单元封装成帧，再将其传递给下面的物理层，而物理层则

将其作为比特流传输出去。接收方的物理层收到比特流后，将其交给上面的数据链路层，而数据链路层会按照与发送方对等的协议将其划分为一个个的帧，再将数据部分交给上面的协议。

### 2) 透明传输

透明传输用来解决帧里面的数据部分因含有与帧定界符相同的内容而被误认为是帧定界符的问题，因为这会导致一个帧被非正常地结束，产生无效帧。链路层协议会采用一些方法破坏掉其中与帧定界符相同的内容，这就是透明传输的含义，透明在这里的意思就是看不见。

### 3) 差错检测

在物理层传输比特时，由于信号质量的问题，可能会导致比特在接收方出现误码现象。因此，数据链路层设计了差错检测的功能，以防止出现差错的帧继续在网络中占用资源，检测出差错的帧将被接收方丢弃。

数据链路层常见设备有网卡、网桥和交换机等。

## 3. 网络层

网络层传送的数据单位是 IP 数据报，也称为 IP 分组或分组、包。

网络层最主要的功能就是路由选择功能。在计算机网络中进行通信的两台计算机之间可能要经过许多节点和链路，还可能要经过好几个路由器所连接的通信子网。网络层的任务就是选择路由，使发送站的运输层所传下来的报文能够按照目的 IP 地址找到目的站，并交付给目的站的运输层。

网络层常见设备有路由器、防火墙、多层交换机等。

## 4. 运输层

网络层找到对方的 IP 接口，运输层则要进一步找到对方的应用进程。运输层通信的两端是指操作系统中的应用进程，因为真正的通信是操作系统中应用进程之间的通信。

运输层提供了两个主要的协议，即 TCP（传输控制协议）和 UDP（用户数据报协议），TCP 用来提供面向连接的、可靠的服务，数据传输单位是报文段；而 UDP 提供无连接的、尽最大努力的传输服务，其传输单位为用户数据报。两种协议为上面的应用层提供了不同的传输服务。

## 5. 应用层

应用层是网络体系结构的最高层，是直接为应用进程提供服务的。常见应用层协议有虚拟终端协议（TELNET）、文件传输协议（FTP）、简单邮件传送协议（SMTP）、超文本传输协议（HTTP）和域名系统（DNS）等。许多应用程序调用了应用层协议的服务。当然，应用层为完成功能，也会向下面的运输层请求服务。

## 2. 常用网络命令简介

目前使用的 Windows 都自带了大量的测试程序，如果能够掌握这些工具的功能，并熟练使用，将会帮助我们更好地使用和管理网络。本节以 Windows 系统下的命令为例进行说明。

### 2.1 ping 命令

#### 1. 功能

ping 命令是最常用的命令，特别是在组网中。ping 命令基于 ICMP 协议，在源站点执行，向目的站点发送 ICMP 回送请求报文，目的站点在收到报文后向源站点返回 ICMP 回送回答报文，源站点把返回的结果信息显示出来。

该命令用来测试站点之间是否可达，若可达，则可进一步判断双方的通信质量，包括稳定性等。

需要注意的是，有些主机为了防止通过 ping 探测，通过防火墙设置禁止 ping 或者在参数中设置禁止 ping，这样就不能通过 ping 确定该主机是否处于开启状态或者其他情况。

有关 ICMP 的详细解释参见《计算机网络》（第 8 版）教材第 146~149 页。

#### 2. 命令格式

Windows 系统用户可单击（win10 为右击）“开始”→“运行”（快捷键：window + r）选项，并键入 cmd，打开命令程序（如需使用管理员权限，win10 系统右击“开始”→“管理员”）。在命令提示符后，按如下格式输入：

```
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]
      [-4] [-6] 目标主机
```

其中，目标主机可以是 IP 地址或者域名。

#### 3. 命令参数

命令参数及其含义如下。

```
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。
```

#### 4. 常见用法实验

1) ping www.163.com

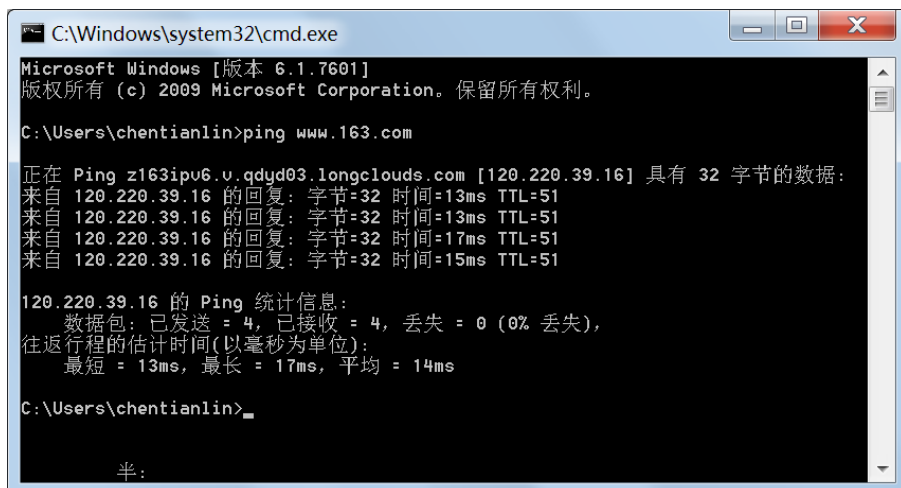
在 Windows 中, ping 命令发送 4 个 ICMP 回送请求, 每个 32 字节, 正常会收到 4 个响应。比如, 下面是 ping 网易的命令。

```
C:\Users\zj>ping www.163.com

正在 Ping z163ipv6.v.bsgslb.cn [60.222.11.28] 具有 32 字节的数据:

来自 60.222.11.28 的回复: 字节=32 时间=13ms TTL=58
来自 60.222.11.28 的回复: 字节=32 时间=14ms TTL=58
来自 60.222.11.28 的回复: 字节=32 时间=15ms TTL=58
来自 60.222.11.28 的回复: 字节=32 时间=13ms TTL=58

60.222.11.28 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 = 13ms, 最长 = 15ms, 平均 = 13ms
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。

C:\Users\chentianlin>ping www.163.com

正在 Ping z163ipv6.v.qdyd03.longclouds.com [120.220.39.16] 具有 32 字节的数据:
来自 120.220.39.16 的回复: 字节=32 时间=13ms TTL=51
来自 120.220.39.16 的回复: 字节=32 时间=13ms TTL=51
来自 120.220.39.16 的回复: 字节=32 时间=17ms TTL=51
来自 120.220.39.16 的回复: 字节=32 时间=15ms TTL=51

120.220.39.16 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 = 13ms, 最长 = 17ms, 平均 = 14ms

C:\Users\chentianlin>
```

可以看到, ping 命令没有带任何参数, 返回 4 个响应。每个响应中, TTL 值指明该 IP 分组可以经过的最大路由器数量。由统计信息可以看出: 发送 4 个请求, 收到 4 个响应, 丢失率为 0%; 最长、最短及平均往返时延, 时延越短, 说明连通越好。根据这些信息可初步判断本机和目标主机的连通状态。

可经常通过 ping 127.0.0.1 来检测本地主机是否正确地安装和配置了 TCP/IP。

2) ping -n 20 www.163.com

通过这个命令可以自己定义发送的回送请求个数, 对衡量网络速度很有帮助。比如该命令可以测试发送 20 个数据包的情况, 通过查看返回的平均时间、最长时间、最短时间来衡量网络连通状态。

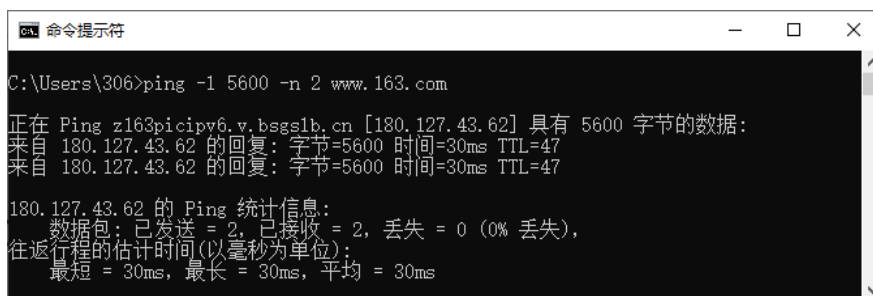
3)ping -t www.163.com

该命令会一直进行下去,直到按“Ctrl+C”组合键停止。若要查看统计信息并继续 ping 操作,可以按“Ctrl+Break”组合键。

4)ping -l 5600 -n 2 www.163.com

在默认的情况下,Windows 中 ping 发送的数据包大小为 32 字节,该命令设置回送请求个数为 2,数据包的大小为 5600 字节,但需要注意该值最大为 65500 字节。

```
C:\Users\zj>ping -l 5600 -n 2 www.163.com
正在 ping z163ipv6.v.bsgslb.cn [60.222.11.25] 具有 5600 字节的数据:
来自 60.222.11.25 的回复: 字节=5600 时间=28ms TTL=58
来自 60.222.11.25 的回复: 字节=5600 时间=23ms TTL=58
60.222.11.25 的 ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 23ms, 最长 = 28ms, 平均 = 25ms
```

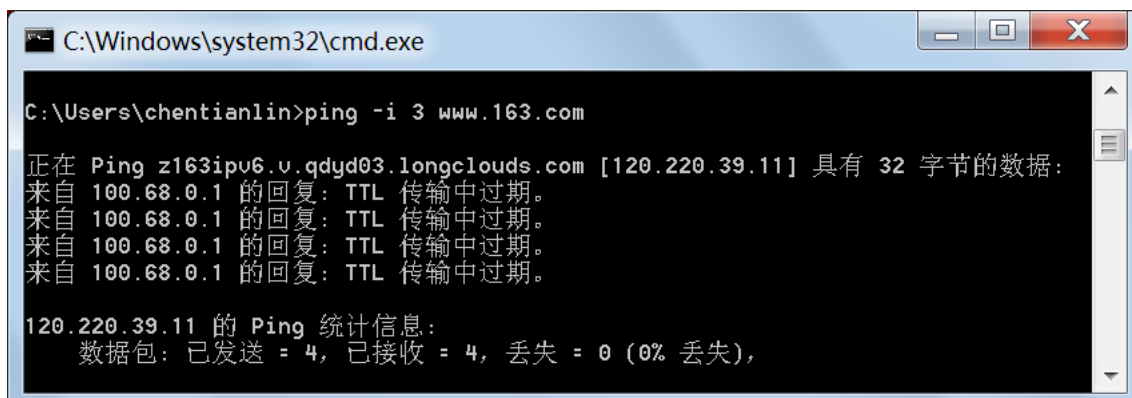


```
命令提示符
C:\Users\306>ping -l 5600 -n 2 www.163.com
正在 Ping z163picipv6.v.bsgslb.cn [180.127.43.62] 具有 5600 字节的数据:
来自 180.127.43.62 的回复: 字节=5600 时间=30ms TTL=47
来自 180.127.43.62 的回复: 字节=5600 时间=30ms TTL=47
180.127.43.62 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 30ms, 最长 = 30ms, 平均 = 30ms
```

5)ping -i 3 www.163.com

该命令设置 ICMP 请求报文中的 TTL 值为 3,这个值在每经过一个路由器时会被减 1,当被减小到 1 时,路由器会将该分组丢弃,造成超时。所以,当 TTL 值太小时,可能会出现本来网络是通的,但由于 TTL 值耗尽而导致的超时现象,对此要合理判断。以下为命令运行情况。

```
C:\Users\zj>ping -i 3 www.163.com
正在 ping z163ipv6.v.bsgslb.cn [60.222.11.21] 具有 32 字节的数据:
来自 218.26.125.125 的回复: TTL 传输中过期
来自 218.26.125.125 的回复: TTL 传输中过期
来自 218.26.125.125 的回复: TTL 传输中过期
来自 218.26.125.125 的回复: TTL 传输中过期
60.222.11.21 的 ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```



```
C:\Windows\system32\cmd.exe
C:\Users\chentianlin>ping -i 3 www.163.com
正在 Ping z163ipv6.v.qdyd03.longclouds.com [120.220.39.11] 具有 32 字节的数据:
来自 100.68.0.1 的回复: TTL 传输中过期。
来自 100.68.0.1 的回复: TTL 传输中过期。
来自 100.68.0.1 的回复: TTL 传输中过期。
来自 100.68.0.1 的回复: TTL 传输中过期。
120.220.39.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

可见,该请求并未到达目的主机,显然,这并非是网络不通,而是 TTL 值被耗尽了。

6)ping -n 1 -r 7 www.163.com

该命令设置发送 1 个请求分组,最多记录 7 个路由节点。其中,路由节点的数量最大设置为 9,若需要查看更多路由节点,可使用 tracert 命令(后面会介绍)。

```

C:\Users\zj>ping -n 1 -r 7 www.163.com
正在 ping z163ipv6.v.bsgslb.cn [60.222.11.29] 具有 32 字节的数据:
来自 60.222.11.29 的回复: 字节=32 时间=165ms TTL=58
    路由: 118.81.238.68 ->
           218.26.122.106 ->
           218.26.125.5 ->
           60.222.6.189 ->
           60.222.10.25 ->
           60.222.11.1 ->
           60.222.11.29
60.222.11.29 的 ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 165ms, 最长 = 165ms, 平均 = 165ms

```

如果多运行几次该命令，可以发现其经过的路由节点不是完全一样的，这是因为每个 IP 分组都是独立路由的结果。

## 2.2 ipconfig 命令

### 1. 功能

该命令用于显示、更新和释放网络地址设置，包括 IP 地址、子网掩码、网关地址和 DNS 服务器设置等。

### 2. 命令格式

命令格式如下所示：

```

ipconfig [/allcompartments] [/? | /all |
                                             /renew [adapter] | /release [adapter] |
                                             /renew6 [adapter] | /release6 [adapter] |
                                             /flushdns | /displaydns | /registerdns |
                                             /showclassid adapter |
                                             /setclassid adapter [classid] |
                                             /showclassid6 adapter |
                                             /setclassid6 adapter [classid] ]

```

其中，adapter 为连接名称，允许使用通配符\*和?。

### 3. 命令参数

命令参数及其含义如下所示：

- |   |               |                            |
|---|---------------|----------------------------|
| ➤ | /?            | 显示帮助消息。                    |
| ➤ | /all          | 显示完整配置信息。                  |
| ➤ | /release      | 释放指定适配器的 IPv4 地址。          |
| ➤ | /release6     | 释放指定适配器的 IPv6 地址。          |
| ➤ | /renew        | 更新指定适配器的 IPv4 地址。          |
| ➤ | /renew6       | 更新指定适配器的 IPv6 地址。          |
| ➤ | /flushdns     | 清除 DNS 解析程序缓存。             |
| ➤ | /registerdns  | 刷新所有 DHCP 租约并重新注册 DNS 名称。  |
| ➤ | /displaydns   | 显示 DNS 解析程序缓存的内容。          |
| ➤ | /showclassid  | 显示适配器允许的所有 IPv4 DHCP 类 ID。 |
| ➤ | /setclassid   | 修改 IPv4 DHCP 类 ID。         |
| ➤ | /showclassid6 | 显示适配器允许的所有 IPv6 DHCP 类 ID。 |
| ➤ | /setclassid6  | 修改 IPv6 DHCP 类 ID。         |

### 4. 常见用法实验

#### 1) ipconfig

默认情况下，仅显示绑定到 TCP/IP 适配器的 IP 地址、子网掩码和默认网关。

```
C:\Users\zj>ipconfig
```

无线局域网适配器 无线网络连接:

```
连接特定的 DNS 后缀 . . . . . :  
本地链接 IPv6 地址. . . . . : fe80::cf5:4314:2bb0:3b29%15  
IPv4 地址 . . . . . : 192.168.1.7  
子网掩码 . . . . . : 255.255.255.0  
默认网关. . . . . : 192.168.1.1
```



## 2) ipconfig/all

显示接口网络详细信息（以无线网卡接口为例）。

```
C:\Users\zj>ipconfig /all
```

无线局域网适配器 无线网络连接:

```
连接特定的 DNS 后缀 . . . . . :  
描述. . . . . : Intel(R) WiFi Link 1000 BGN  
物理地址. . . . . : 74-E5-0B-57-6D-84  
DHCP 已启用 . . . . . : 是  
自动配置已启用. . . . . : 是  
本地链接 IPv6 地址. . . . . : fe80::cf5:4314:2bb0:3b29%15(首选)  
IPv4 地址 . . . . . : 192.168.1.7(首选)  
子网掩码 . . . . . : 255.255.255.0  
获得租约的时间 . . . . . : 2020 年 1 月 2 日 20:28:23
```



```

租约过期的时间 . . . . . : 2020年1月7日 15:16:46
默认网关. . . . . : 192.168.1.1
DHCP 服务器 . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 376759563
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-18-C8-61-C9-F0-DE-F1-E7-7F-2F
DNS 服务器 . . . . . : fe80::1%15
                        192.168.1.1
TCPIP 上的 NetBIOS . . . . . : 已启用

```

```

C:\Windows\system32\cmd.exe
C:\Users\chentianlin>ipconfig /all

Windows IP 配置

主机名 . . . . . : chentianlin-PC
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : DHCP HOST

无线局域网适配器 无线网络连接:

连接特定的 DNS 后缀 . . . . . : DHCP HOST
描述. . . . . : TP-LINK Wireless USB Adapter
物理地址. . . . . : 30-B4-9E-BD-16-EE
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::b8f1:b9be:f0ca:b977%14(首选)
IPv4 地址 . . . . . : 192.168.0.100(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2020年10月14日 10:56:34
租约过期的时间 . . . . . : 2020年10月14日 12:56:34
默认网关. . . . . : 192.168.0.1
DHCP 服务器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 355513502
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-21-5D-A1-8B-30-9C-23-4E-5

DNS 服务器 . . . . . : 192.168.1.1
                        192.168.0.1
TCPIP 上的 NetBIOS . . . . . : 已启用

以太网适配器 本地连接:

```

### 3) ipconfig/release

释放所有适配器的 IP 地址。

```

C:\Users\zj>ipconfig /release

Windows IP 配置

不能在无线网络连接 2 上执行任何操作，它已断开媒体连接。

以太网适配器 本地连接 2:

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

无线局域网适配器 无线网络连接 2:

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

无线局域网适配器 无线网络连接:

连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::cf5:4314:2bb0:3b29%15
默认网关. . . . . :

```



```
C:\Windows\system32\cmd.exe
C:\Users\chentianlin>ipconfig /release

Windows IP 配置

不能在 本地连接 上执行任何操作，它已断开媒体连接。

无线局域网适配器 无线网络连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::b8f1:b9be:f0ca:b977%14
    默认网关. . . . . :

以太网适配器 本地连接:

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

隧道适配器 isatap.DHCP HOST:

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

隧道适配器 本地连接* 4:

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

隧道适配器 Teredo Tunneling Pseudo-Interface:

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

C:\Users\chentianlin>
```

#### 4) ipconfig/renew

更新所有适配器，重新获得 IP 地址。

```
C:\Users\zj>ipconfig /renew

Windows IP 配置

不能在 本地连接 2 上执行任何操作，它已断开媒体连接。
不能在 无线网络连接 2 上执行任何操作，它已断开媒体连接。

以太网适配器 本地连接 2:

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

无线局域网适配器 无线网络连接 2:

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

无线局域网适配器 无线网络连接:
```

```
C:\Windows\system32\cmd.exe
C:\Users\chentianlin>ipconfig /renew

Windows IP 配置

不能在 本地连接 上执行任何操作，它已断开媒体连接。

无线局域网适配器 无线网络连接:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::b8f1:b9be:f0ca:b977%14
    IPv4 地址 . . . . . : 192.168.0.100
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.0.1

以太网适配器 本地连接:

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

隧道适配器 isatap.DHCP_HOST:

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

隧道适配器 本地连接* 4:

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

隧道适配器 Teredo Tunneling Pseudo-Interface:

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

C:\Users\chentianlin>
```

5) ipconfig/flushdns

清空本机 DNS 缓存。

```
C:\Users\zj>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

6) ipconfig/allcompartments/all

显示有关所有接口的详细信息。

另外，对于 release 和 renew，这两个参数只能在向 DHCP 租用 IP 地址的计算机上起作用。release 将所有租用 IP 地址归还给 DHCP，而 renew 则重新租用 DHCP 分配的 IP 地址。当然，如果未指定适配器名称，则会释放或更新所有绑定到 TCP/IP 适配器的 IP 地址租约。

## 2.3 netstat 命令

### 1. 功能

netstat 是 Windows 系统提供的用于查看与 TCP、IP、UDP 和 ICMP 协议相关统计数据网络工具，能检验本机各端口的网络连接情况。

### 2. 命令格式

命令格式如下所示：

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
```

### 3. 命令参数

命令参数及其含义如下所示：

➤	-a	显示所有连接和侦听端口。
➤	-b	显示在创建每个连接或侦听端口时所涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件显示创建连接或侦听端口时所涉及的组件序列。在此情况下，可执行程序的名称位于底部[]中，它调用的组件位于顶部，直至达到TCP/IP。 注意，运行此参数很耗时，并且当你没有足够权限时不能使用。
➤	-e	显示以太网统计。此选项可以与 -s 选项结合使用。
➤	-f	显示外部地址的完全限定域名 (FQDN)。
➤	-n	以数字形式显示地址和端口号。
➤	-o	显示拥有的与每个连接关联的进程 ID。
➤	-p proto	显示 proto 指定的协议的连接;proto 可以是下列任何一个:TCP、UDP、TCPv6 或 UDPv6。
➤	-r	显示路由表。
➤	-s	显示每个协议的统计数据。
➤	-p	用于指定默认的子网。
➤	-t	显示当前连接卸载状态。 interval 重新显示选定的统计数据、各个显示间暂停的间隔秒数。按“Ctrl+C”组合键停止重新显示统计数据。如果省略，则 netstat 将打印当前的配置信息一次。

#### 4. 常见用法实验

##### 1) netstat -a

该命令显示所有连接和监听端口。

下面是命令执行后的部分内容。其中，协议指连接所用的协议；本地地址指本机地址及端口；外部地址指远端主机地址及端口，端口也用协议代替；状态指协议所处的状态。

```
C:\Users\zj>netstat -a
```

活动连接			
协议	本地地址	外部地址	状态
TCP	192.168.1.7:51664	123.125.52.61:http	TIME_WAIT
TCP	192.168.1.7:51666	45:https	CLOSE_WAIT
TCP	192.168.1.7:51667	45:https	CLOSE_WAIT
TCP	192.168.1.7:51670	203.208.43.100:https	ESTABLISHED
TCP	192.168.1.7:51671	230:http	ESTABLISHED
TCP	192.168.1.7:51672	220.181.38.156:http	ESTABLISHED
TCP	192.168.1.7:51673	230:http	ESTABLISHED
TCP	192.168.1.7:51674	tsa01s07-in-f10:https	SYN_SENT
TCP	192.168.1.7:51675	tsa01s09-in-f14:https	SYN_SENT
TCP	192.168.1.7:51676	39.96.128.53:http	ESTABLISHED
TCP	192.168.1.7:51677	119.188.96.39:http	ESTABLISHED
TCP	192.168.1.7:51678	221.7.140.182:http	LAST_ACK
UDP	[fe80::cf5:4314:2bb0:3b29%15]:1900	*:*	
UDP	[fe80::cf5:4314:2bb0:3b29%15]:2177	*:*	
UDP	[fe80::cf5:4314:2bb0:3b29%15]:50506	*:*	

如果系统正在运行 P2P 类型的应用，比如一些下载类的软件，那么这些应用会不断地与外部地址建立 TCP 连接，从而获取下载资源。这种情况下，在本命令执行后就会发现大量本地端口正在与外部建立 TCP 连接，请读者自行测试。关于 TCP、UDP 及端口的内容请查阅教材相关内容。

##### 2) netstat -n

本选项用于以数字形式显示地址和端口号，比如 -a 参数中的主机名在这里会被显示成 IP 地址。

在测试命令前，也可以先访问一些 Web 站点，紧接着运行本命令，观察其中的活动连接。运行本命令后显示的

部分结果如下：

```
C:\Users\zj>netstat -n
```

活动连接			
协议	本地地址	外部地址	状态
TCP	192.168.1.7:50804	203.119.129.47:443	ESTABLISHED
TCP	192.168.1.7:50805	42.236.37.156:80	ESTABLISHED
TCP	192.168.1.7:50806	42.236.38.71:80	ESTABLISHED
TCP	192.168.1.7:50828	42.236.37.155:80	ESTABLISHED
TCP	192.168.1.7:50835	223.167.166.52:80	ESTABLISHED
TCP	192.168.1.7:51432	60.222.11.25:443	ESTABLISHED
TCP	192.168.1.7:51540	111.206.63.21:80	TIME_WAIT
TCP	192.168.1.7:51541	218.26.34.45:443	CLOSE_WAIT
TCP	192.168.1.7:51542	218.26.34.45:443	CLOSE_WAIT
TCP	192.168.1.7:51552	211.144.24.78:443	TIME_WAIT
TCP	192.168.1.7:51560	221.204.23.3:443	TIME_WAIT
TCP	192.168.1.7:51561	120.52.30.45:443	ESTABLISHED
TCP	192.168.1.7:51562	221.204.13.129:443	ESTABLISHED
TCP	192.168.1.7:51564	211.144.24.235:443	ESTABLISHED

3) 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的总字节数、错误数、删除数，以及数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。

这个参数选项可以用来统计一些基本的网络流量。



	接收的	发送的
字节	2840179645	733066460
单播数据包	19007980	10452170
非单播数据包	149835	84140
丢弃	0	0
错误	0	0
未知协议	0	

4) netstat -s

本选项能够按照各个协议分别显示其统计数据，默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计数据。如果应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么就可以用本选项来查看一下所显示的信息，仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

下面是运行本命令后显示的部分结果。

```
C:\Users\zj>netstat -s
```

#### IPv4 统计信息

接收的数据包	= 64377
接收的标头错误	= 39
接收的地址错误	= 0
转发的数据报	= 0
接收的未知协议	= 0
丢弃的接收数据包	= 2460
传送的接收数据包	= 67616
输出请求	= 76260
路由丢弃	= 0
丢弃的输出数据包	= 141
输出数据包无路由	= 16
需要重新组合	= 3
重新组合成功	= 1
重新组合失败	= 0
数据报分段成功	= 0
数据报分段失败	= 0
分段已创建	= 0

#### IPv4 的 TCP 统计信息

主动开放	= 2955
被动开放	= 14
失败的连接尝试	= 414
重置连接	= 274
当前连接	= 10
接收的分段	= 76398
发送的分段	= 56839

重新传输的分段	= 11459
---------	---------

#### IPv4 的 UDP 统计信息

接收的数据报	= 4468
无端口	= 2452
接收错误	= 0
发送的数据报	= 7720

#### IPv6 的 UDP 统计信息

接收的数据报	= 1274
无端口	= 1221
接收错误	= 0
发送的数据报	= 2871

```
C:\Windows\system32\cmd.exe
C:\Users\chentianlin>netstat -s

IPu4 统计信息

接收的数据包                = 3820799
接收的标头错误              = 0
接收的地址错误              = 0
转发的数据报                = 0
接收的未知协议              = 0
丢弃的接收数据包            = 3901
传送的接收数据包            = 3841675
输出请求                    = 2120709
路由丢弃                    = 0
丢弃的输出数据包            = 115
输出数据包无路由            = 127
需要重新组合                = 2
重新组合成功                = 1
重新组合失败                = 0
数据报分段成功              = 1
数据报分段失败              = 0
分段已创建                  = 8

IPu6 统计信息

接收的数据包                = 855
接收的标头错误              = 0
接收的地址错误              = 416
转发的数据报                = 0
接收的未知协议              = 0
丢弃的接收数据包            = 204
传送的接收数据包            = 546
输出请求                    = 5672
路由丢弃                    = 0
丢弃的输出数据包            = 0
输出数据包无路由            = 10
需要重新组合                = 0
重新组合成功                = 0
重新组合失败                = 0
数据报分段成功              = 0
数据报分段失败              = 0
分段已创建                  = 0
```

##### 5) netstat -r

本选项可以显示关于路由表的信息，除了显示有效路由，还显示当前有效的连接。下面是部分运行结果，路由知识请参考《计算机网络》（第7版）教材相关部分。

```
C:\Users\zj>netstat -r

=====
接口列表
21...00 ff d0 c2 0e 4d ..... Sangfor SSL VPN CS Support System VNIC
17...74 e5 0b 57 6d 85 ..... Microsoft Virtual WiFi Miniport Adapter #2
16...74 e5 0b 57 6d 85 ..... Microsoft Virtual WiFi Miniport Adapter
15...74 e5 0b 57 6d 84 ..... Intel(R) WiFi Link 1000 BGN
22...00 00 00 00 00 00 00 e0  Microsoft ISATAP Adapter #2
24...00 00 00 00 00 00 00 e0  Microsoft ISATAP Adapter #3
=====

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        192.168.1.1 192.168.1.7 25
127.0.0.0      255.0.0.0      在链路上   127.0.0.1 306
127.0.0.1      255.255.255.255 在链路上   127.0.0.1 306
127.255.255.255 255.255.255.255 在链路上   127.0.0.1 306
192.168.1.0     255.255.255.0 在链路上   192.168.1.7 281
192.168.1.7     255.255.255.255 在链路上   192.168.1.7 281
192.168.1.255   255.255.255.255 在链路上   192.168.1.7 281
192.168.182.0   255.255.255.0 在链路上   192.168.182.1 276
224.0.0.0       240.0.0.0      在链路上   192.168.182.1 276
```

255.255.255.255	255.255.255.255	在链路上	127.0.0.1	306
255.255.255.255	255.255.255.255	在链路上	192.168.1.7	281
255.255.255.255	255.255.255.255	在链路上	192.168.246.1	276
255.255.255.255	255.255.255.255	在链路上	192.168.182.1	276

---

永久路由:

网络地址	网络掩码	网关地址	跃点数
0.0.0.0	0.0.0.0	10.50.9.254	默认

---

IPv6 路由表

---

活动路由:

跃点数	网络目标	网关
1	306 ::1/128	在链路上
15	281 fe80::/64	在链路上

---

永久路由:

无

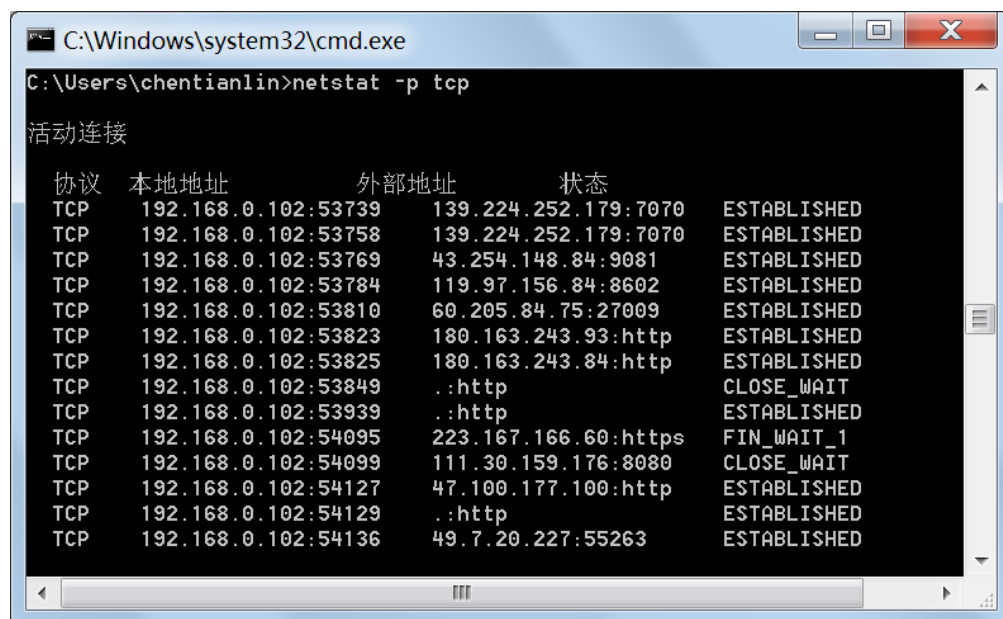
#### 6) netstat -p tcp

显示 TCP 协议的连接。-p 后面的参数也可以是下列任何一个: UDP、TCPv6 或 UDPv6。

C:\Users\zj>netstat -p tcp

活动连接

协议	本地地址	外部地址	状态
TCP	127.0.0.1:5357	zj-PC:53035	TIME_WAIT
TCP	127.0.0.1:5357	zj-PC:53039	TIME_WAIT
TCP	127.0.0.1:52498	zj-PC:54530	ESTABLISHED
TCP	127.0.0.1:52499	zj-PC:52500	ESTABLISHED
TCP	127.0.0.1:52500	zj-PC:52499	ESTABLISHED
TCP	127.0.0.1:54530	zj-PC:52498	ESTABLISHED
TCP	192.168.1.7:52501	223.167.166.52:http	ESTABLISHED
TCP	192.168.1.7:52504	hn:http	ESTABLISHED
TCP	192.168.1.7:52505	hn:http	ESTABLISHED
TCP	192.168.1.7:52547	203.119.218.69:https	ESTABLISHED
TCP	192.168.1.7:53024	45:https	CLOSE_WAIT
TCP	192.168.1.7:53034	203.208.50.167:https	ESTABLISHED
TCP	192.168.1.7:53040	tsa01s07-in-f14:https	SYN_SENT
TCP	192.168.1.7:53041	tsa01s07-in-f14:https	SYN_SENT



#### 7) netstat -s -p tcp

该命令可显示当前 TCP 连接, 并对 TCP 协议进行统计。除了 TCP 协议, 还可以是下列任何一个: IP、IPv6、ICMP、ICMPv6、TCPv6、UDP 或 UDPv6。

下面是命令运行结果的部分内容。



```
C:\Users\zj>netstat -s -p tcp
IPv4 的 TCP 统计信息
    主动开放                = 3893
    被动开放                = 221
    失败的连接尝试          = 791
    重置连接                = 327
    当前连接                = 9
    接收的分段              = 105146
    发送的分段              = 77375
    重新传输的分段          = 20766
活动连接
    协议  本地地址                外部地址                状态
    TCP   192.168.1.7:52547          203.119.218.69:https    ESTABLISHED
    TCP   192.168.1.7:53049          45:https                CLOSE_WAIT
    TCP   192.168.1.7:53057          106.11.250.27:https     TIME_WAIT
    TCP   192.168.1.7:53062          tsa01s08-in-f46:https   SYN_SENT
    TCP   192.168.1.7:53063          tsa01s08-in-f46:https   SYN_SENT
```

2.4 arp 命令

1. 功能  
arp 命令用来显示和修改 IP 地址与物理地址之间的映射关系，即 IP 地址到物理地址的转换表，该转换表保存在本地 arp 缓存中。

2. 命令格式  
命令格式如下：

```
arp -s inet_addr eth_addr [if_addr]
arp -d inet_addr [if_addr]
arp -a [inet_addr] [-N if_addr] [-v]
```

3. 命令参数  
命令参数及其含义如下所示：

- -a 通过询问当前协议数据，显示当前 arp 项。
- -g 与-a 相同。
- -v 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。
- inet\_addr 指定 Internet 地址。
- -N if\_addr 显示 if\_addr 指定的网络接口的 arp 项。
- -d 删除 inet\_addr 指定的主机。inet\_addr 可以是通配符\*，以删除所有主机。
- -s 添加主机并且将 Internet 地址 inet\_addr 与物理地址 eth\_addr 相关联。物理地址是用连字符分隔的 6 个十六进制字节。该项是永久的。
- eth\_addr 指定物理地址。
- if\_addr 如果存在，此项指定地址转换表应修改的接口的 Internet 地址。如果不存在，则使用第一个适用的接口。

4. 常见用法实验

1) arp-a  
显示 arp 缓存中的 IP 地址和硬件地址的对应关系。如果不止一个网络接口使用 arp，则显示每个接口的 arp 项。下面是含三个接口的 arp 命令运行结果。  
如果只想显示某个指定 IP 的 arp 记录，则可用如下命令：

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

Internet 地址	物理地址	类型
192.168.1.1	90-86-9b-87-bb-00	动态
192.168.1.4	d4-a1-48-44-f7-3b	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	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: 192.168.1.7 --- 0xf
```

Internet 地址	物理地址	类型
192.168.182.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	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: 192.168.182.1 --- 0x13
```

Internet 地址	物理地址	类型
192.168.246.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	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

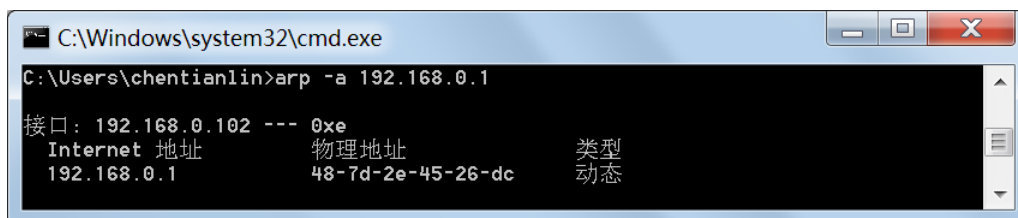
```
接口: 192.168.246.1 --- 0x14
```



如果只显示某个接口的 arp 缓存记录，则可用如下命令：

```
C:\Users\zj>arp -a 192.168.1.1
```

Internet 地址	物理地址	类型
192.168.1.1	90-86-9b-87-bb-00	动态



2) arp-s 167.56.85.112 00-1a-00-62-c6-08

该命令将在 arp 缓存中添加一条静态 arp 条目。运行该命令后，请查看添加效果。

3) arp-d 167.56.85.112

该命令将删除刚刚添加的 arp 条目，请自行验证。

另外，在一些 Windows 系统（如 Windows 7）中，当运行 arp 命令添加静态记录或删除某记录时，有时会被提示“请求的操作需要提升”，这需要使用管理员身份运行命令程序。在“开始”处搜到命令程序后，单击鼠标

右键并选择“以管理员身份运行”命令即可。

## 2.5 tracert 命令

### 1. 功能

tracert 用于探测源节点到目的节点之间数据报经过的全部路径。IP 数据报的 TTL 值在每经过一个路由器的转发后减 1，当 TTL=0 时，则向源节点报告 TTL 超时。利用这个特性，可将第一个数据报的 TTL 值置为 1，内部封装无法交付的 UDP 用户数据报，这样，途经的第一个路由器将向源节点报告 TTL 超时，第二个数据报将 TTL 赋值为 2，以此类推，直到到达目的站点或 TTL 达到最大值 255，这样就可以得到沿途的路由器 IP 地址。详见《计算机网络》（第 7 版）教材第 150 页。

### 2. 命令格式

命令格式如下所示：

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

### 3. 命令参数

命令参数及其含义如下所示：

➤ -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。

### 4. 常见用法实验

1) tracert [www.163.com](http://www.163.com)

```
C:\Users\zj>tracert www.163.com
通过最多 30 个跃点跟踪
到 z163ipv6.v.bsghlb.cn [60.222.11.27] 的路由:
 1    3 ms    3 ms    3 ms  192.168.1.1 [192.168.1.1]
 2    7 ms   11 ms    8 ms  1.20.185.183.adsl-pool.sx.cn [183.185.20.1]
 3   12 ms   31 ms   34 ms  149.124.26.218.internet.sx.cn [218.26.124.149]
 4   16 ms   16 ms   13 ms  242.5.222.60.adsl-pool.sx.cn [60.222.5.242]
 5   59 ms   67 ms   67 ms  190.6.222.60.adsl-pool.sx.cn [60.222.6.190]
 6   25 ms   19 ms   18 ms  22.10.222.60.adsl-pool.sx.cn [60.222.10.22]
 7   14 ms   14 ms   13 ms  27.11.222.60.adsl-pool.sx.cn [60.222.11.27]
跟踪完成。
```

```
C:\Windows\system32\cmd.exe

C:\Users\chentianlin>tracert www.163.com

通过最多 30 个跃点跟踪
到 z163ipv6.v.qdyd03.longclouds.com [120.220.39.18] 的路由:

 1  <1 毫秒  <1 毫秒  <1 毫秒  192.168.0.1
 2  1 ms     1 ms     1 ms     192.168.1.1
 3  5 ms     5 ms     3 ms     100.68.0.1
 4  *        *        *        请求超时。
 5  4 ms     3 ms     3 ms     211.137.177.129
 6  *        12 ms    11 ms    211.137.177.65
 7  15 ms    *        16 ms    120.222.48.66
 8  16 ms    14 ms    14 ms    120.220.36.22
 9  15 ms    13 ms    13 ms    120.220.36.46
10  17 ms    17 ms    16 ms    192.168.20.34
11  17 ms    18 ms    15 ms    10.10.45.2
12  15 ms    14 ms    15 ms    10.10.1.70
13  14 ms    13 ms    17 ms    120.220.39.241
14  14 ms    15 ms    14 ms    120.220.39.18

跟踪完成。
```

tracert 后面可跟域名或 IP 地址，默认的 TTL 值为 30。读者可观察如下命令执行情况。

命令结果清晰地显示了去往目的地所经过的路由，[]前面是 IP 对应的主机名。从命令执行结果可以看到，封装同一 TTL 值的数据报被发送三次。

2) tracert -h 5 60.222.11.27

该命令设置 TTL 值为 5，请运行该命令并观察结果。

```
C:\Windows\system32\cmd.exe

C:\Users\chentianlin>tracert -h 5 60.222.11.27

通过最多 5 个跃点跟踪
到 27.11.222.60.adsl-pool.sx.cn [60.222.11.27] 的路由:

 1  3 ms     <1 毫秒  1 ms     192.168.0.1
 2  1 ms     1 ms     1 ms     192.168.1.1
 3  41 ms    8 ms     3 ms     100.68.0.1
 4  10 ms    *        *        218.201.96.193
 5  6 ms     7 ms     3 ms     211.137.177.129

跟踪完成。
```

## 2.6 route 命令

### 1. 功能

用来增加、删除或显示本地路由表。

### 2. 命令格式

命令格式如下所示：

```
ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC
metric] [IF inte]
```

### 3. 命令参数

命令参数及其含义如下所示：

➤ -f	清除所有网关项的路由表。如果与某个命令结合使用，在运行该命令前，应清除路由表。
➤ -p	与 add 命令结合使用时，将路由设置为在系统引导期间保持不变。默认情况下，重启不保存路由。忽略所有其他命令，这始终会影响相应的永久路由。Windows 95 不支持此选项。
➤ -4	强制使用 IPv4。
➤ -6	强制使用 IPv6。
➤ command	其中之一： print        打印路由； add         添加路由； delete      删除路由； change      修改现有路由。
➤ destination	指定主机。
➤ MASK	指定下一个参数为网络掩码值。
➤ netmask	指定此路由项的子网掩码值。如果未指定，其默认设置为 255.255.255.255。
➤ gateway	指定网关。
➤ inte	指定路由的接口号码。
➤ METRIC	指定跃点数，例如目标的成本。

#### 4. 常见用法实验

##### 1) route print

该命令效果同 netstat-r 完全一致，不再介绍。

```

C:\Windows\system32\cmd.exe

C:\Users\chentianlin>route print
=====
接口列表
14...30 b4 9e bd 16 ee .....TP-LINK Wireless USB Adapter
11...30 9c 23 4e 5f 7b .....Intel(R) Ethernet Connection (2) I219-LM
1.....Software Loopback Interface 1
15...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

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          0.0.0.0      192.168.0.1  25
127.0.0.0          255.0.0.0
127.0.0.1          255.255.255.255  在链路上    127.0.0.1  306
127.255.255.255    255.255.255.255  在链路上    127.0.0.1  306
192.168.0.0        255.255.255.0    在链路上    192.168.0.102 281
192.168.0.102      255.255.255.255  在链路上    192.168.0.102 281
192.168.0.255      255.255.255.255  在链路上    192.168.0.102 281
224.0.0.0          240.0.0.0        在链路上    127.0.0.1  306
224.0.0.0          240.0.0.0        在链路上    192.168.0.102 281
255.255.255.255    255.255.255.255  在链路上    127.0.0.1  306
255.255.255.255    255.255.255.255  在链路上    192.168.0.102 281
=====
永久路由:
无

IPv6 路由表
=====
活动路由:
如果跃点数网络目标      网关          接口
1      306 ::1/128          在链路上
14     281 fe80::/64        在链路上
14     281 fe80::b8f1:b9be:f0ca:b977/128 在链路上
1      306 ff00::/8          在链路上
14     281 ff00::/8          在链路上
=====
永久路由:
无

```

##### 2) route add 10.0.0.0 mask 255.0.0.0 192.168.182.1 if 19

该命令将增加一条目的地址为 10.0.0.0、掩码为 255.0.0.0 的路由条目。命令运行结束后，读者使用 route print

命令查看，可以看到该条目已经被添加到本地路由表中。

3) `route delete 10.0.0.0 mask 255.0.0.0`

运行本命令后，刚刚添加的路由条目被删除，读者可自行查看。

需要注意的是，`route` 后面添加命令参数需要以管理员身份运行命令行处理程序。

当命令为 `route print` 或 `route delete` 时，目标或网关可以为通配符（通配符指定为星号“\*”），否则可能会忽略网关参数。如果 `Dest` 包含一个“\*”或“？”，则会将其视为 Shell 模式，并且只打印匹配目标路由。“\*”匹配任意字符串，而“？”匹配任意一个字符。

### 3. 实验作业：

- （1）用 `ping` 命令测试本机 TCP/IP 的工作情况，记录下相关信息。
- （2）使用 `ipconfig` 命令测试本机 TCP/IP 网络配置，记录下相关信息。
- （3）使用 `tracert` 命令测试本机到 `www.sohu.com` 服务器所经过的路由数，记录下相关信息。