**windows netstat命令**

netstat是Windows操作系统中的一个命令行工具，可以显示网络连接、路由表和网络接口等信息。该工具非常有用，可以帮助您分析网络连接问题以及查找哪些应用程序正在使用网络。

## 下面是一些常见的netstat命令选项：

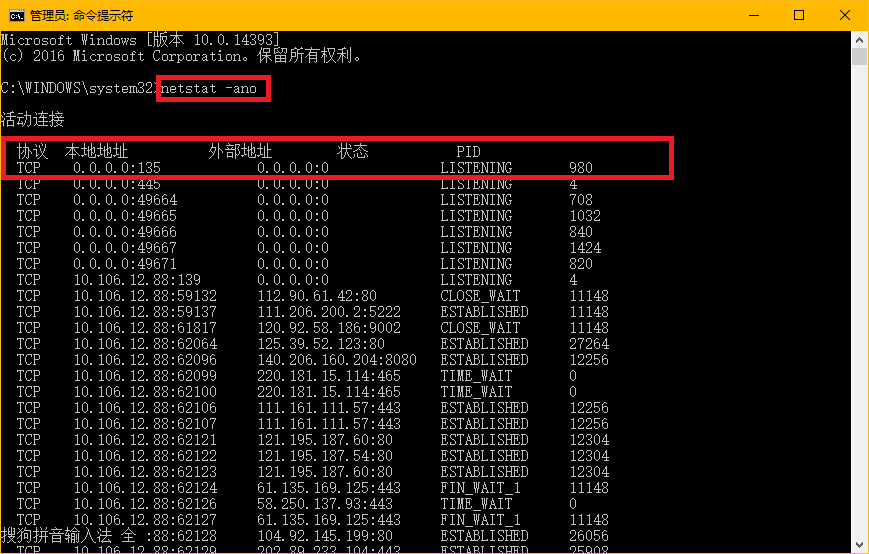
* netstat -a: 显示所有的网络连接和监听端口
* netstat -n: 显示IP地址和端口号，而不是主机名和服务名
* netstat -o: 显示每个连接的进程ID和进程名称
* netstat -b: 显示每个连接的进程名称和路径
* netstat -p <协议>: 显示指定协议的连接，例如TCP或UDP
* netstat -s: 显示各种统计信息，如TCP和UDP协议的活动连接数、错误数等
* netstat -r: 显示路由表信息
* netstat -e: 显示网络接口信息，包括传输统计数据

### 例如，如果您要查看所有TCP连接并显示每个连接的进程ID和进程名称，可以使用以下命令：

netstat -ano | find "TCP"

这将显示所有的TCP连接，包括每个连接的本地地址和远程地址、状态、进程ID和进程名称。

## 使用示例： -a 、-n 、-o

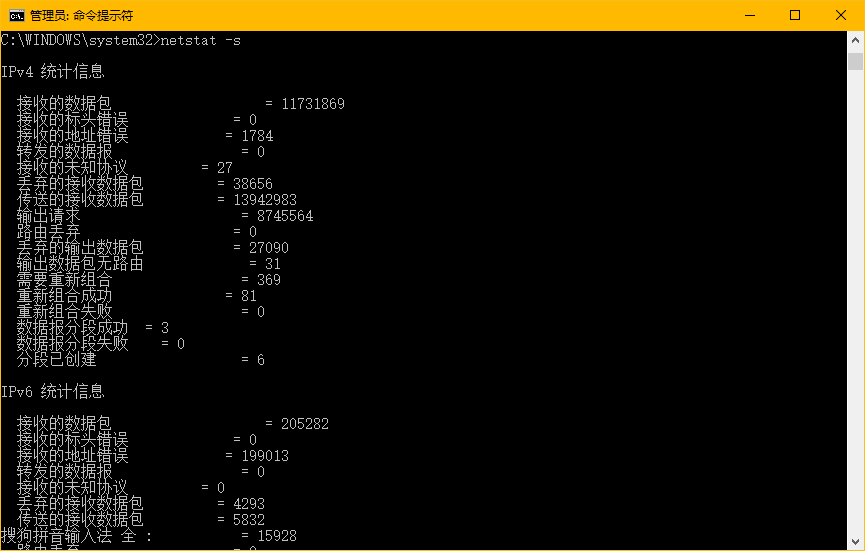


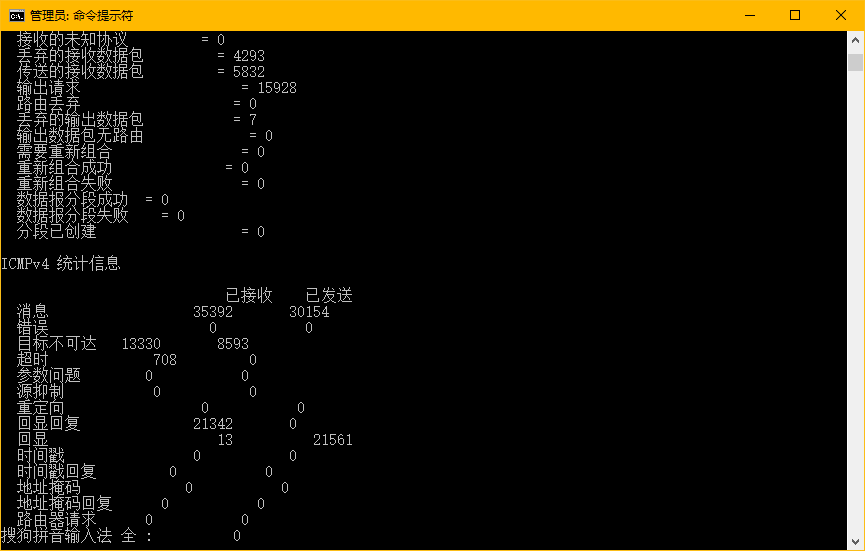
　　　　　其中本地地址之后的数字即为端口号，如图中 135、445 等，其中最后一列 PID 即为进程 id。

　　　　　netstat -e 示例 ：

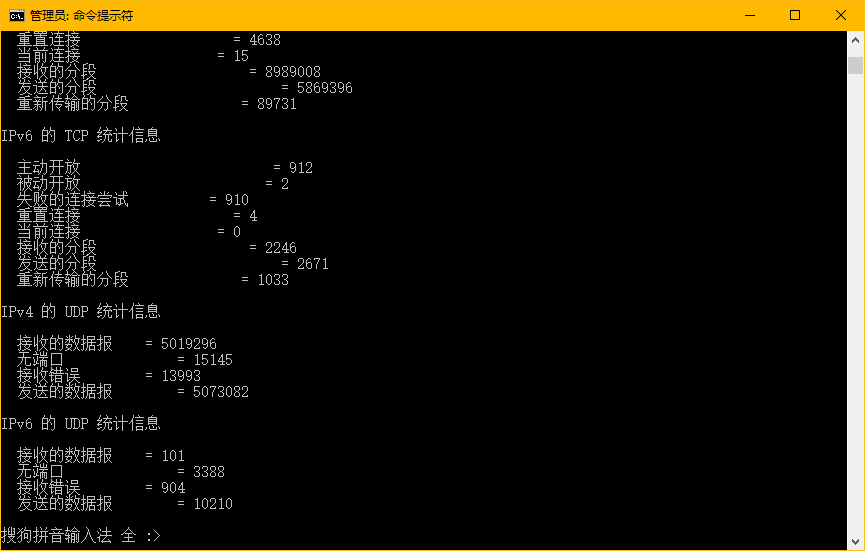


　　　　　netstat -s 示例：









 　　　　以上即为 netstat 命令常用参数的示例，一般只需记住 -a 、-n 、-o 参数即可。

## 在cmd下常用的形式为netstat -相关参数,下面是状态说明

LISTEN：侦听来自远方的TCP端口的连接请求

SYN-SENT：再发送连接请求后等待匹配的连接请求

SYN-RECEIVED：再收到和发送一个连接请求后等待对方对连接请求的确认

ESTABLISHED：代表一个打开的连接

FIN-WAIT-1：等待远程TCP连接中断请求，或先前的连接中断请求的确认

FIN-WAIT-2：从远程TCP等待连接中断请求

CLOSE-WAIT：等待从本地用户发来的连接中断请求

CLOSING：等待远程TCP对连接中断的确认

LAST-ACK：等待原来的发向远程TCP的连接中断请求的确认

TIME-WAIT：等待足够的时间以确保远程TCP接收到连接中断请求的确认

CLOSED：没有任何连接状