net start 查看开启了哪些服务

sc query 查所有开启的服务

sc query > net.txt 重定向

sc query type= all state= all > aa.txt 查所有的服务

sc delete service 删除服务，服务名都要加双引号，不能单引号

net start service　 开启服务

net stop service 停止某服务

net pause service 暂停某服务

net continue service 重新激活挂起的服务。

Telnet是进行远程登录的标准协议和主要方式它为用户提供了在本地计算机上完成远程主机工作的能力。可以用telnet命令来测试端口号是否正常打开还是关闭状态。

**> telnet -help**

> telnet 127.0.0.1 检验Telnet服务是否开启

**使用Telnet测试端口**

> telnet 127.0.0.1 80

netstat -a 查看开启了哪些端口,常用netstat -an   
netstat -n 查看端口的网络连接情况，常用netstat -an   
netstat -v 查看正在进行的工作   
netstat -p 协议名 例：netstat -p tcq/ip 查看某协议使用情况（查看tcp/ip协议使用情况）   
netstat -s 查看正在使用的所有协议使用情况   
nbtstat -A ip 对方136到139其中一个端口开了的话，就可查看对方最近登陆的用户名（03前的为用户名）-注意：参数-A要大写

net view 查看本地局域网内开启了哪些共享   
net view ip 查看对方局域网内开启了哪些共享   
net config 显示系统网络设置   
net logoff 断开连接的共享   
  
  
net user guest 12345 用guest用户登陆后用将密码改为12345   
net password 密码 更改系统登陆密码

tracert -参数 ip(或计算机名) 跟踪路由（数据包），参数：“-w数字”用于设置超时间隔。   
ping ip(或域名) 向对方主机发送默认大小为32字节的数据，参数：“-l[空格]数据包大小”；“-n发送数据次数”；“-t”指一直ping。   
ping -t -l 65550 ip 死亡之ping(发送大于64K的文件并一直ping就成了死亡之ping)   
ipconfig (winipcfg) 用于windows NT及XP(windows 95 98)查看本地ip地址，ipconfig可用参数“/all”显示全部配置信息