##### 一、实验目的

学习掌握网络安全相关网络命令的使用，学习利用网络常用命令对网络安全问题进行分析判断。

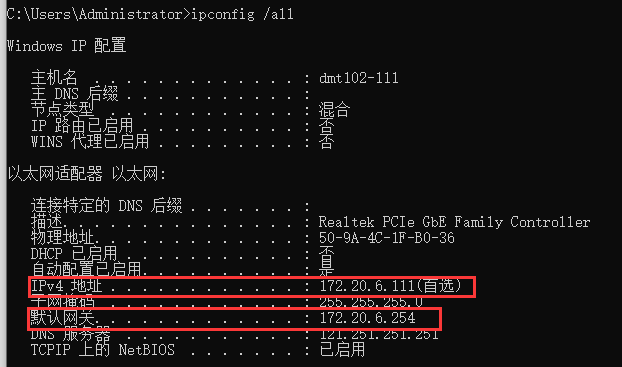
##### 二、实验环境

局域网环境；Windows或Linux平台均可（Windows命令字与Linux略有差异，例如：ipconfig vs ifconfig，tracert vs traceroute）

##### 三、实验内容

关闭本机网络协议配置中的IPv6选项，并做以下测试：

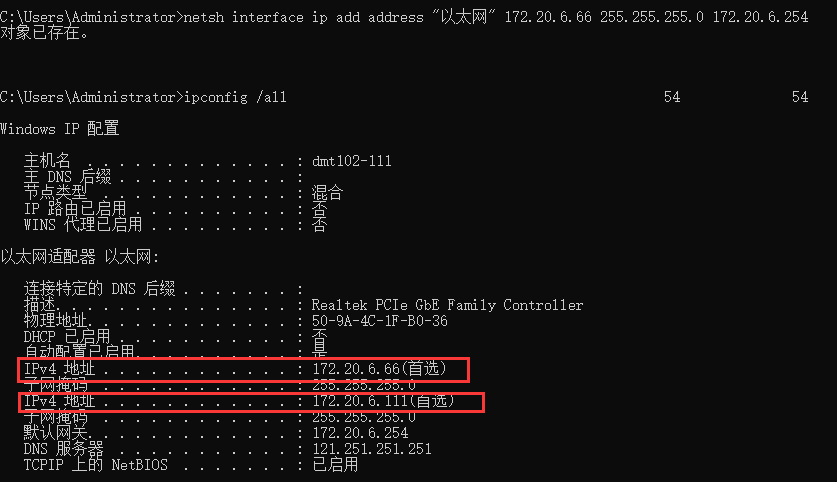
1. 运行“ipconfig/all”命令，将命令运行结果截图贴上来，并指出本机IP地址和网关IP



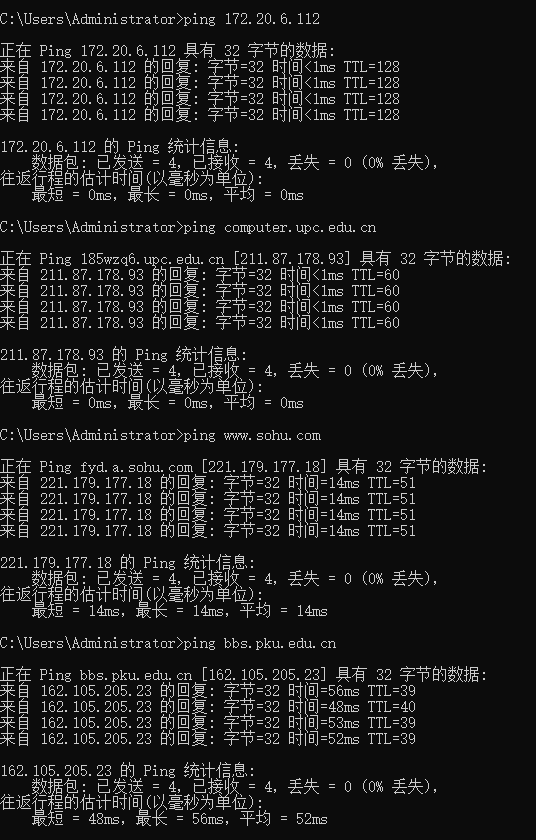
本机IP:172.20.6.111

默认网关：172.20.6.254

请尝试如何使用ipconfig命令或其它命令设置网卡IP地址，并测试是否可以将1个网卡设置为多个IP地址。



1. 运行“ping”命令，目标参数分别是 邻居IP、computer.upc.edu.cn 和 www.sohu.com，bbs.pku.edu.cn，将结果截图贴上来



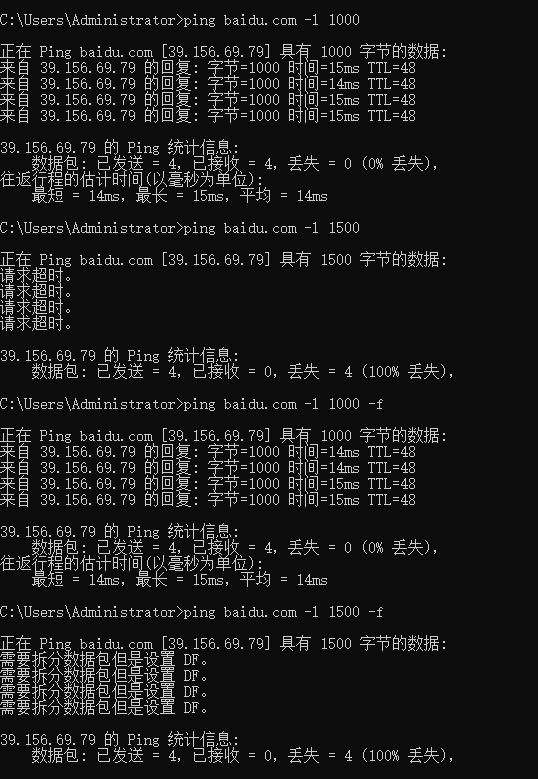
(1). 分别使用以下不同的ping命令进行测试，查看返回结果有何异同？ 试解释原因。

ping x.x.x.x -l 1000

ping x.x.x.x -l 1500

ping x.x.x.x -l 1000 -f

ping x.x.x.x -l 1500 -f



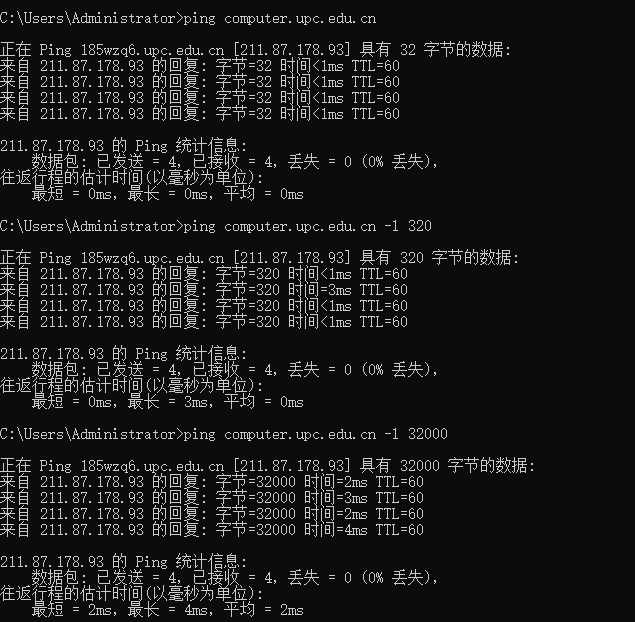
[注：第一个参数 -l 是小写的L，不是 1]

(2). 键入以下命令进行ping测试，并解释3次结果中差异和原因

ping computer.upc.edu.cn

ping computer.upc.edu.cn -l 320

ping computer.upc.edu.cn -l 32000



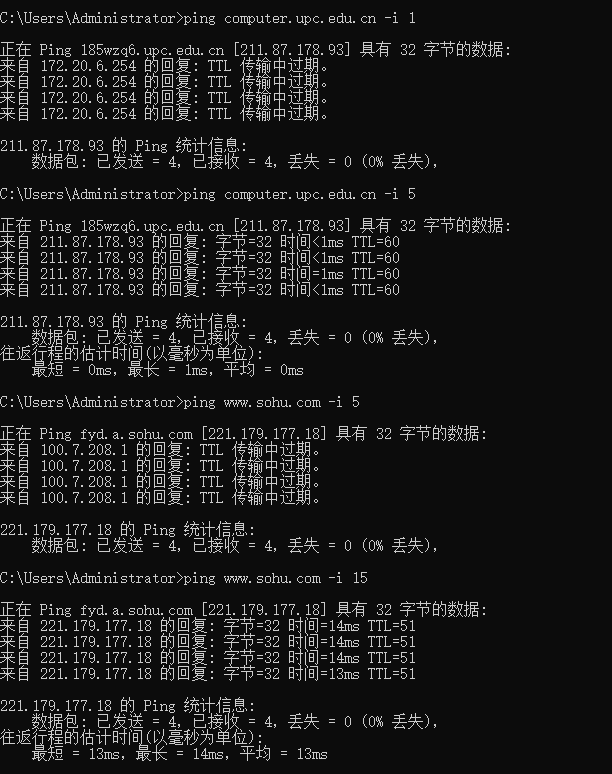
(3). 分别使用以下不同的ping命令进行测试，查看结果有何异同？试解释原因

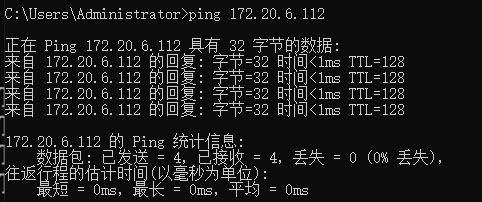
ping computer.upc.edu.cn -i 1

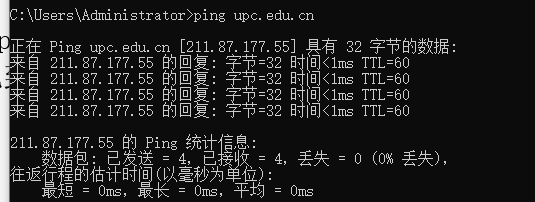
ping computer.upc.edu.cn -i 5

ping www.sohu.com -i 5

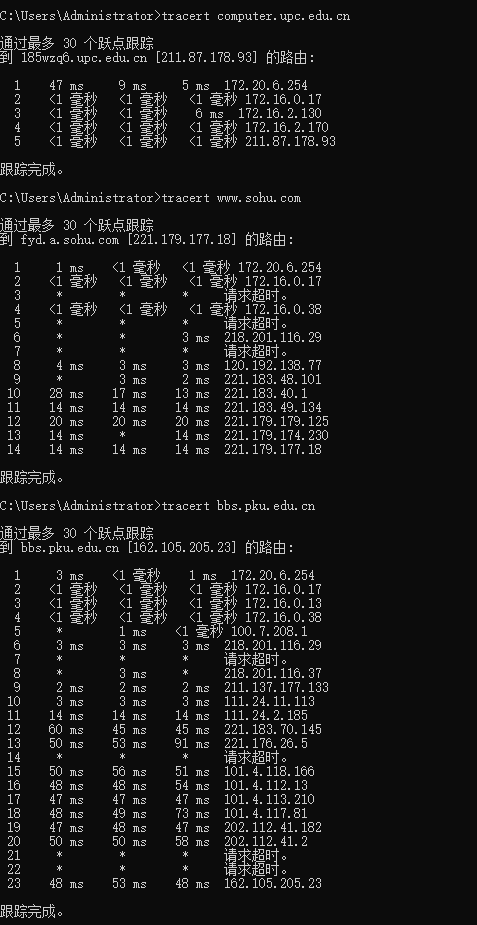
ping www.sohu.com -i 15

 (4) 不同操作系统如Linux,Win98,Win8等的TTL初始值是不同的，请根据本次ping结果，给出目标主机的操作系统类型的初步判断。



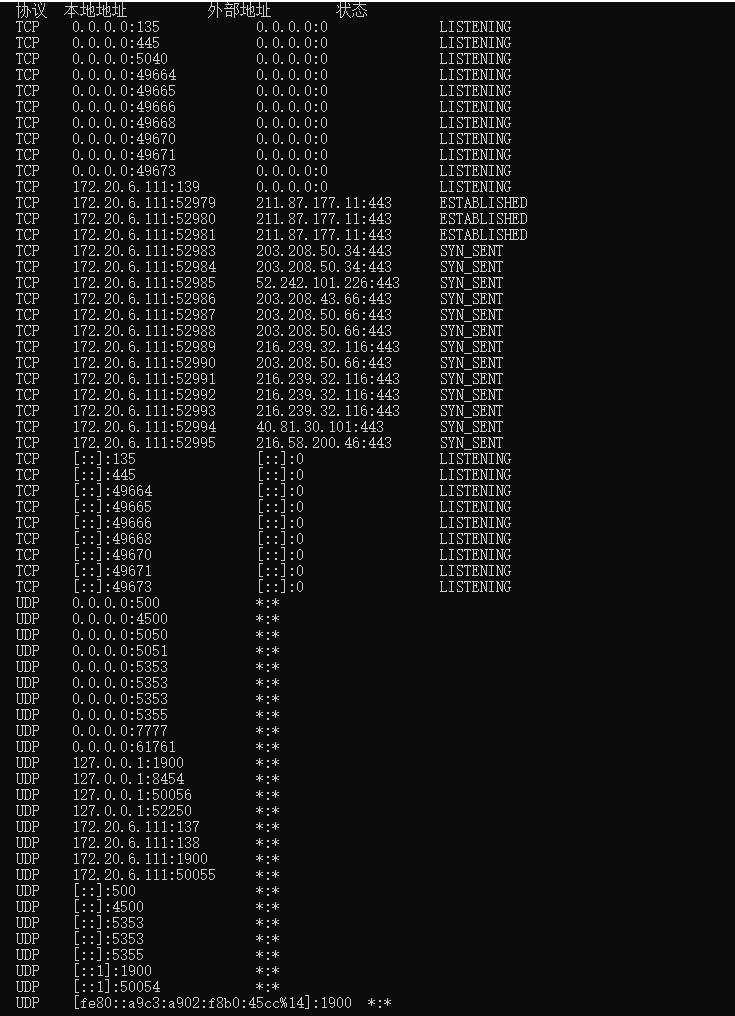


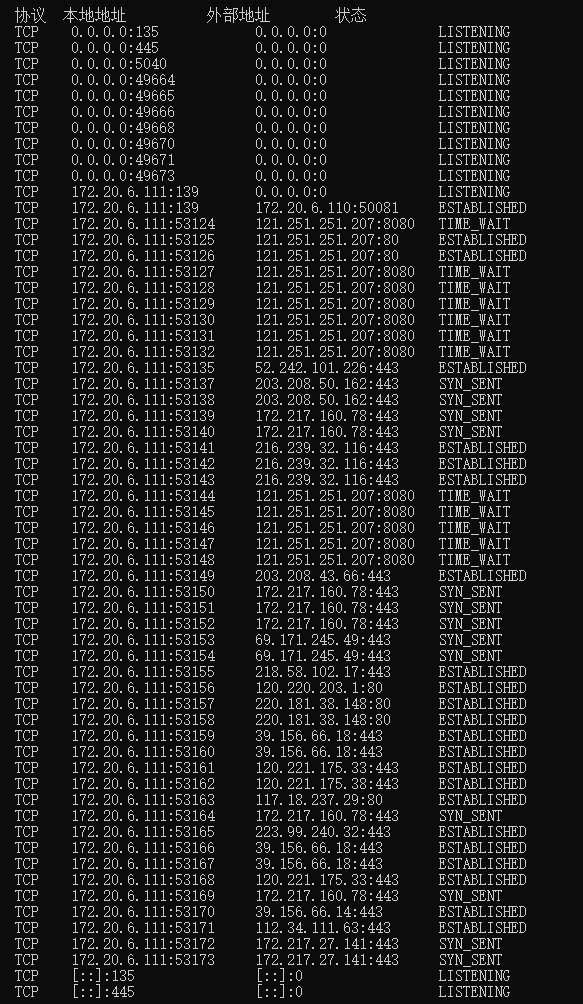
3、 运行“tracert”命令，目标参数为 computer.upc.edu.cn、www.sohu.com、bbs.pku.edu.cn，将结果截图贴上来，并指出从本机到三个目标地址分别转发了多少步

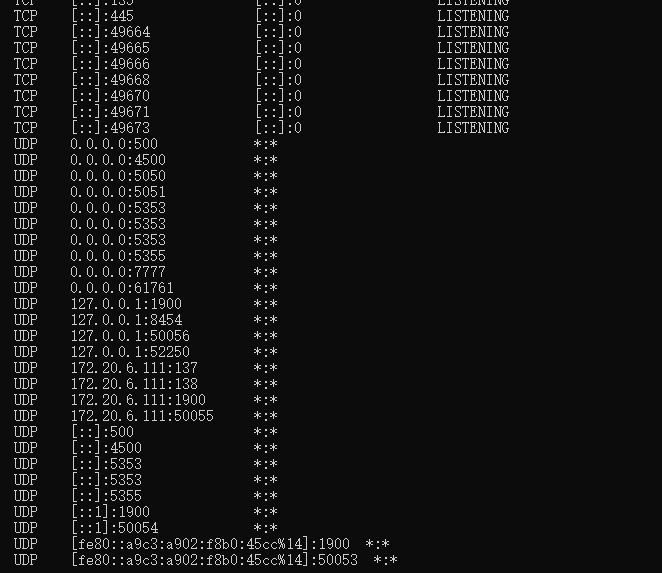


4、根据2和3的结果，试探究：Ping命令返回结果中TTL的变化，与tracert跃点数之间有什么关系？这种关系是否一定准确？如果不准确，请分析导致不准确的原因。

5、 执行命令 netstat -an，查看本机开放的端口号情况；点击浏览器访问百度或者搜狐等网址后，再次执行 netstat -an，查看并分析两次端口情况的差异。



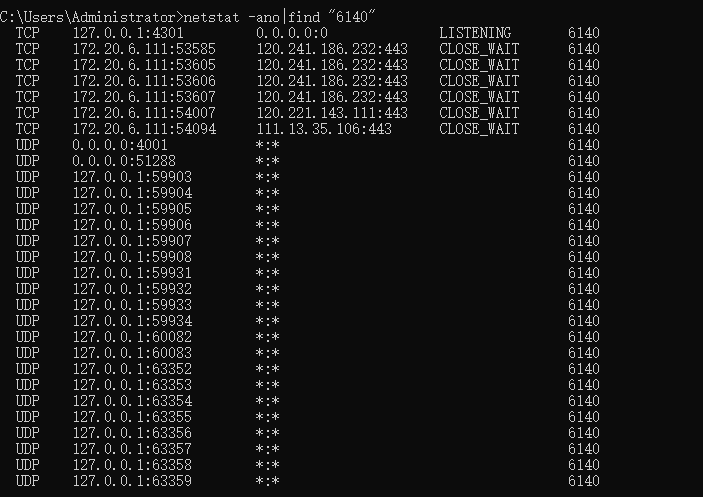


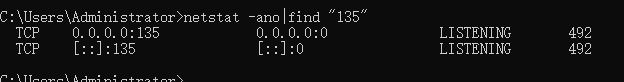


使用netstat命令，测试一下QQ聊天软件使用了什么协议和什么端口；

选择一个本机的开放端口号（如135、445），请确定占用该端口的任务进程并截图上来。



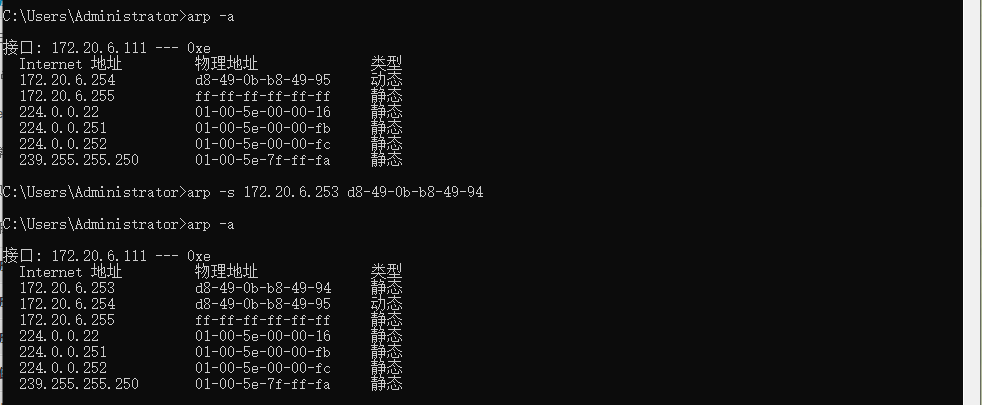






6、运行命令“arp -a”，查看本机所存在的IP——MAC地址映射表

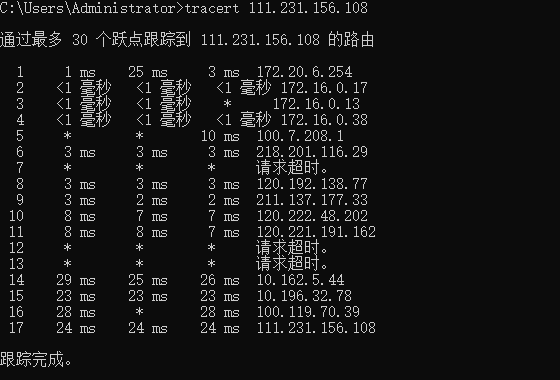
尝试为本机arp映射表添加一个静态arp表项，并把结果截图上来，并解释其意义。

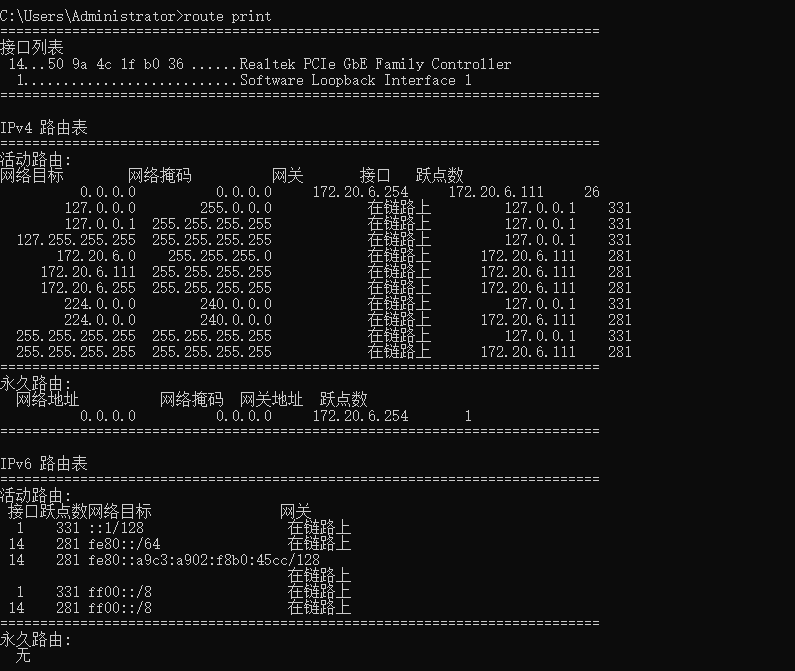


7、运行命令“route print”，查看本机路由表

尝试为本机路由表增加一个永久路由项，如：111.231.156.108（对应的是拼\*\*官网），网关部分填充一个假冒的IP，查看增加后的路由表项，并测试增加表项前后的访问结果，截图上来并解释原因。

备注：mask 255.255.255.255 或者不填写











\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

四、附件：命令字详解

Windows提供了一组用来测试网络状态的网络命令，常用的有ping，ipconfig，tracert和netstate命令等，这些常用网络命令对于我们使用和维护网络是有意义的。

1、Ping连接测试命令

Ping命令是测试网络联接状况以及信息包发送和接收状况的常用命令。Ping向目标主机(地址)发送一个回送请求数据包，要求目标主机收到请求后给予答复，从而判断网络的响应时间和本机是否与目标主机(地址)联通。如果执行Ping不成功，则可以预测故障出现在以下几个方面：网线故障，网络适配器配置不正确，IP地址不正确。

命令格式：ping IP地址或主机名 [-t] [-a] [-n count] [-l size]

常用参数含义：

-t不停地向目标主机发送数据；

-a 以IP地址格式来显示目标主机的网络地址；

-n count 指定要Ping多少次，具体次数由count来指定；

-l size 指定发送到目标主机的数据包的大小。

2、Tracert数据包跟踪命令

Tracert命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间，分析网络延时产生的原因。命令功能同Ping类似，但它所获得的信息要比Ping命令详细得多，它把数据包所走的全部路径、节点的IP以及花费的时间都显示出来。该命令比较适用于大型网络。

命令格式：tracert IP地址或主机名 [-d][-h maximumhops][-j host\_list] [-w timeout]

参数含义：

-d 不解析目标主机的名字；

-h maximum\_hops 指定搜索到目标地址的最大跳跃数；

-j host\_list 按照主机列表中的地址释放源路由；

-w timeout 指定超时时间间隔，程序默认的时间单位是毫秒。

3、IPconfig网络配置参数查看命令

IPconfig命令显示所有当前的TCP/IP网络和DNS域名系统的参数设置。

命令格式：

ipconfig[/all][/batch file][/renew all][/release all][/renew n][/release n]

参数含义：

/? 显示帮助信息；

/all 显示现时所有网络连接的设置；

/release 释放某一个网络上的IP位置；

/renew 更新某一个网络上的IP位置；

/flushdns把DNS解析器的暂存内容全数删除。

4、Netstat网络运行状态查看命令

Netstat命令可以帮助网络管理员了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息。

命令格式：

netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

参数含义：

-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涉及的可执行程序；

-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 显示指定的协议的连接；

-r 显示路由表；

-s 显示每个协议的统计；

-t 显示当前连接卸载状态；

interval 重新显示选定的统计，各个显示间暂停的间隔秒数。

5、arp地址解析协议命令字

显示和修改地址解析协议(ARP)使用的“IP 到物理”地址转换表。

ARP -s inet\_addr eth\_addr [if\_addr]

ARP -d inet\_addr [if\_addr]

ARP -a [inet\_addr] [-N if\_addr] [-v]

-a 通过询问当前协议数据，显示当前 ARP 项。

如果指定 inet\_addr，则只显示指定计算机

的 IP 地址和物理地址。如果不止一个网络

接口使用 ARP，则显示每个 ARP 表的项。

-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。

6、route路由命令

操作网络路由表。

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

-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，重新启动系统时，

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。

interface 指定路由的接口号码。

METRIC 指定跃点数，例如目标的成本。