**实验一：使用网络测试工具测试网络状态**

1. **实验名称**

使用网络测试工具测试网络状态

1. **实验目的**

(1) 学习常用网络测试工具的基本功能和使用方法。

(2) 总结并设计使用网络测试工具测试网络状态的方法。

1. **实验完成人及完成时间**

史文翰

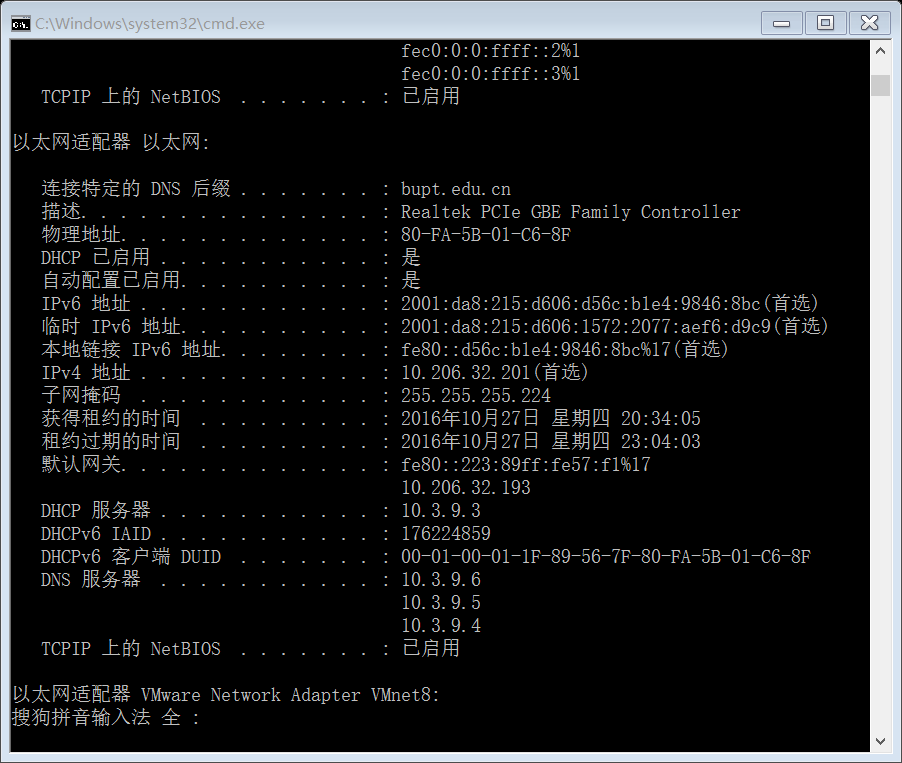
No.2014211218

Cla.2014211304

2016.10.27

1. **实验环境**

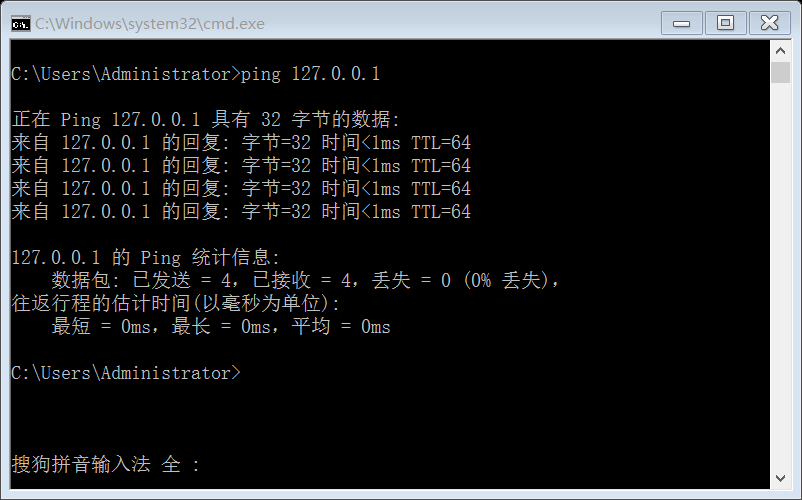
与Internet连接的笔记本电脑，Win10操作系统，通过cmd指令呼出命令行以完成实验操作。



1. **实验步骤与结果分析**
2. **使用ping命令测试计算机之间的连通性**
3. **弄清楚如何在本地计算机上运行ping程序。**

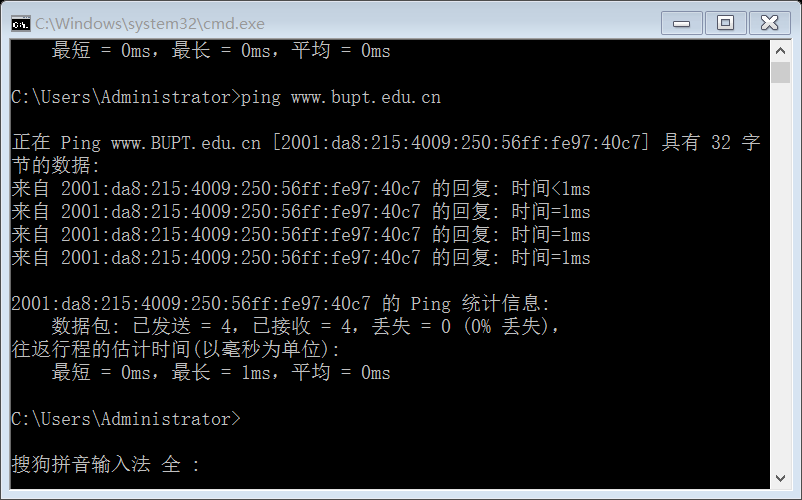
在win10环境下，使用win+R键利用cmd命令呼出命令行即可。

1. **测试本地计算机（ping 127.0.0.1），确定ping程序运行正确。**



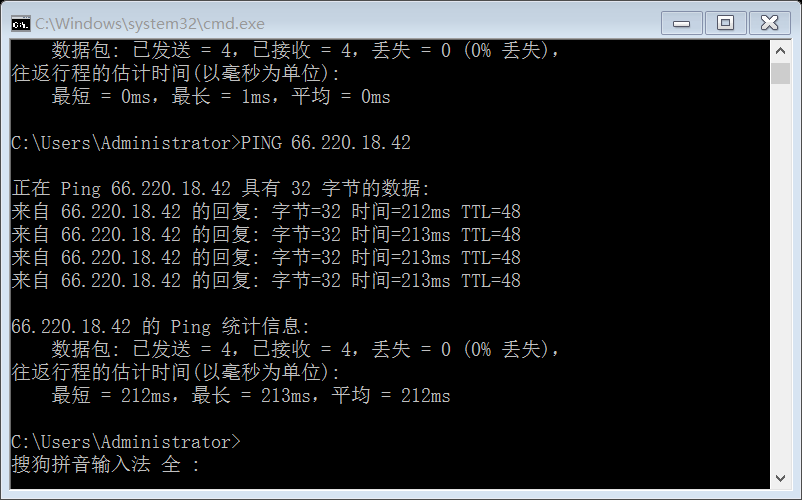
可以看出ping命令运行正确，本地还回地址可以ping通。

1. **使用ping命令确定北邮www.bupt.edu.cn是否可达。**



可以看出在当前网络环境中可以ping通北邮网址。

1. **使用搜索引擎找到另一个国家的计算机，ping该计算机。你发现的最大往返延迟是多大？**



此IP为美国洛杉矶某IP，延时可以达到213ms。

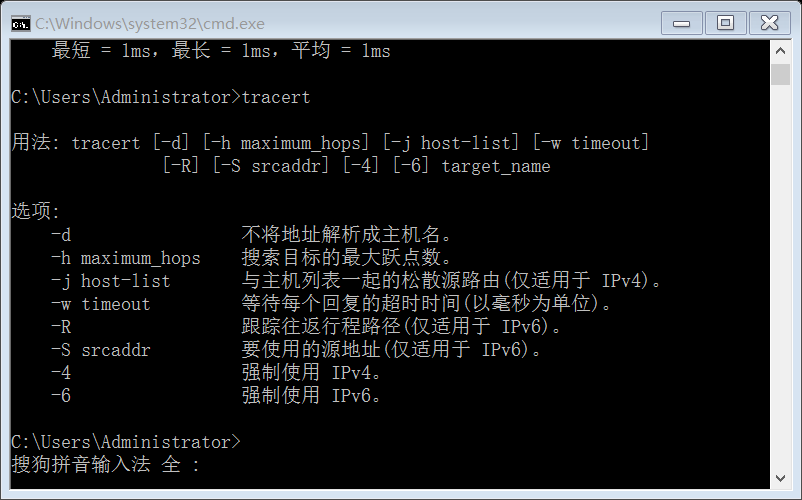
1. **当某台计算机无法正常访问远程某网站时，请问如何使用Ping命令测试和定位故障的位置。**



可以看出，ping一个被屏蔽的google官网是无法ping通的，结合前面对本地IP，本地局域网的测试，可知，错误并不发生在本地网络或计算机内部，而是在DNS服务器上。

1. **使用traceroute命令测试计算机之间的路由器**
2. **弄清楚如何在本地计算机上运行traceroute程序**

由于是win10环境，使用tracert命令等价于traceroute。

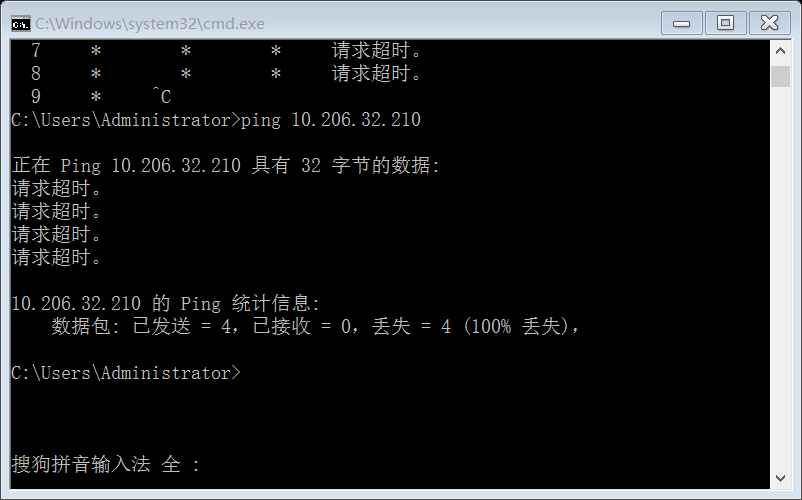


1. **选择本地网络中的一台目标主机，运行traceroute命令，观察并分析结果；**

已知同学的笔记本电脑的IP是10.206.32.210，对这个IP进行tracert。

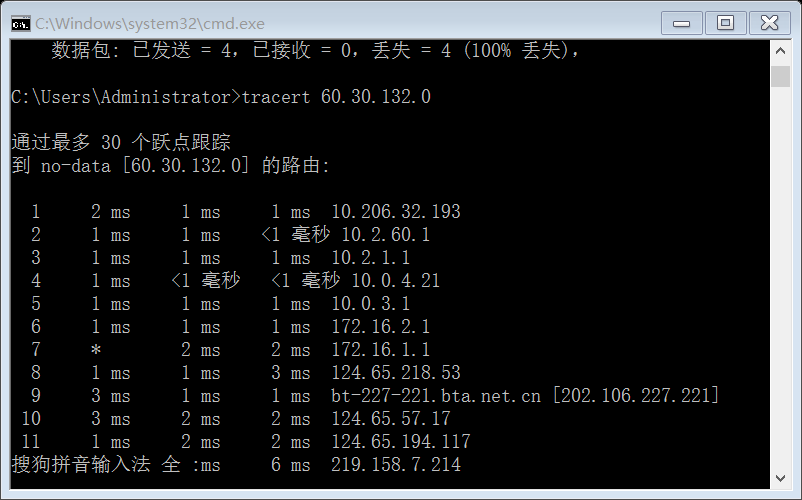


可以看出没有找到路由，我们再利用ping试一下。



上网查询资料后得知，一般的主机禁用ICMP协议，减少自身信息在互联网中的暴露，因此ping不通也tracetr不通，tracert的本质就是多次的ping。

1. **选择本市内其它高校的一台目标主机，运行traceroute命令，观察并分析结果**



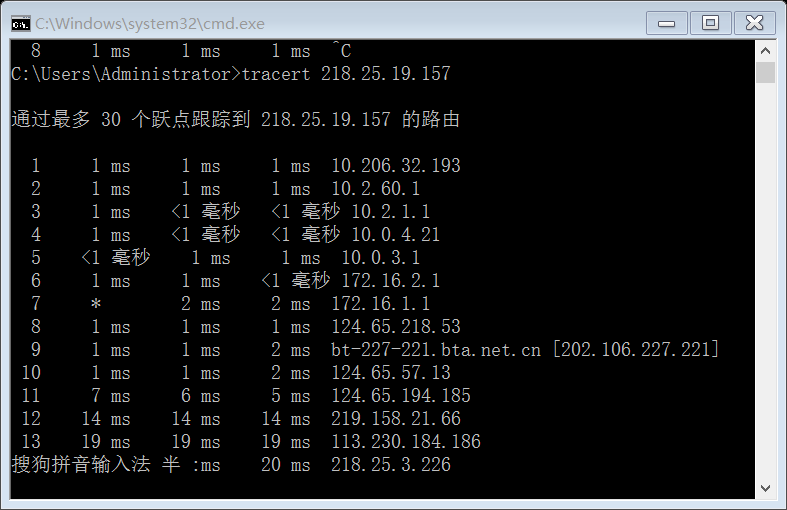
可以看出10.206.32.193实际上是我们的本地局域网的网关，数据包想到目的地必须第一步经过这个网关，这是正确的，由于篇幅问题，我们没有等到它找到目标IP就结束了这个过程。

1. **选择国内其它省的一台目标主机，运行traceroute命令，观察并分析结果；**



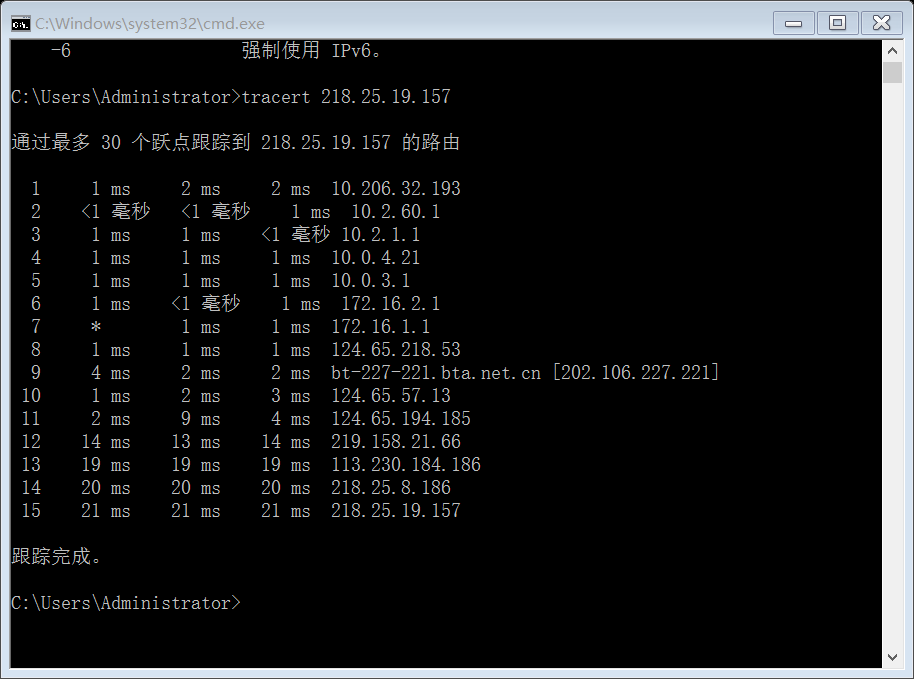
这里给出了一个在沈阳某主机IP的结果，可以看出最后完成了相应的跟踪，到达了目标IP，从第14跳可以看出，此时数据包已进入沈阳，测试阶段进入到尾声，而最开始以10开头的均是北京邮电大学的NAT网关。

1. **不同时间内重复执行步骤(2)-(4)，观察并分析比较结果，你能够得到什么结论？**

我们选择在另一个时间段重复进行步骤（4），其中IP地址是相同的。

可以看出各跳的节点IP均相同，但延时略有区别，这与网络波动和测试时网络的实际情况相关。

再选取不同的日期发送，得到结果如下（时隔一个月）

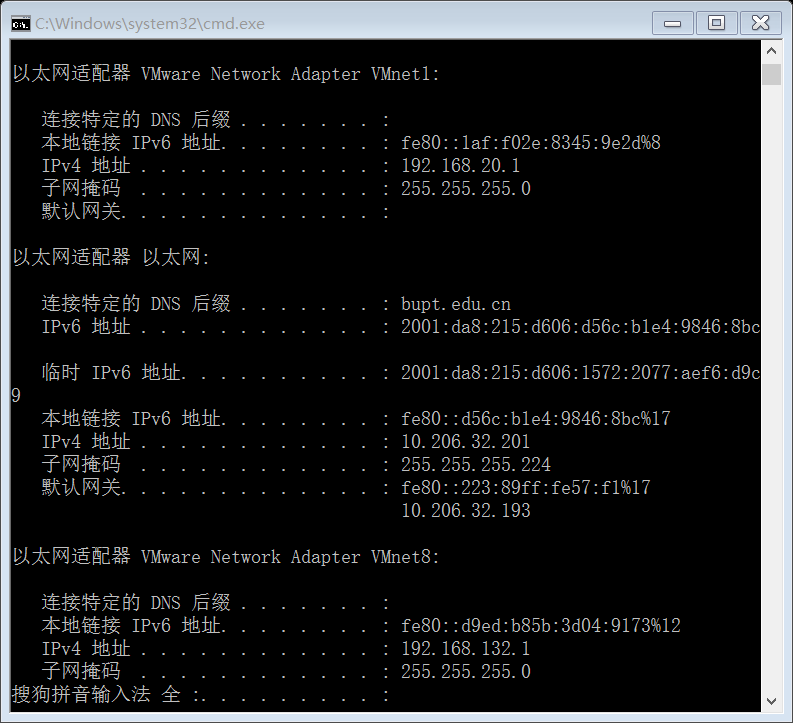


可以看出不仅是各路由之间的延迟变化，其中一些路由节点本身也发生了变化。这说明tracert指令是依赖于当前网络情况的，不同时间使用tracert同一个ip地址，得到的延迟和路由节点都会有所不同。

**3、使用ipconfig命令获取主机和网路信息**

**(1) 弄清楚如何在本地计算机上运行Ipconfig程序；**

使用ipconfig命令。



**(2) 使用Ipconfig命令获取本机的IP地址和子网掩码以及默认网关信息；**

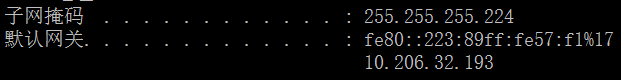
由上图可以看出，本机IPV6地址为



IPV4地址为

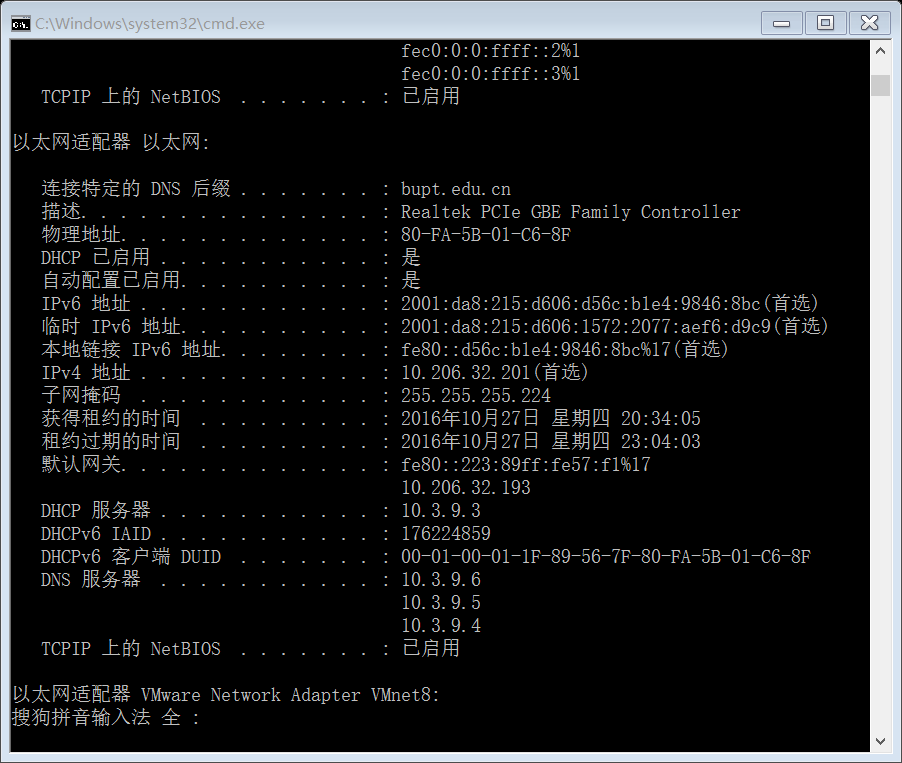


默认网关为



**(3) 使用Ipconfig命令获取本机的MAC地址；**

增加/ALL后，我们可以查看到mac地址信息。

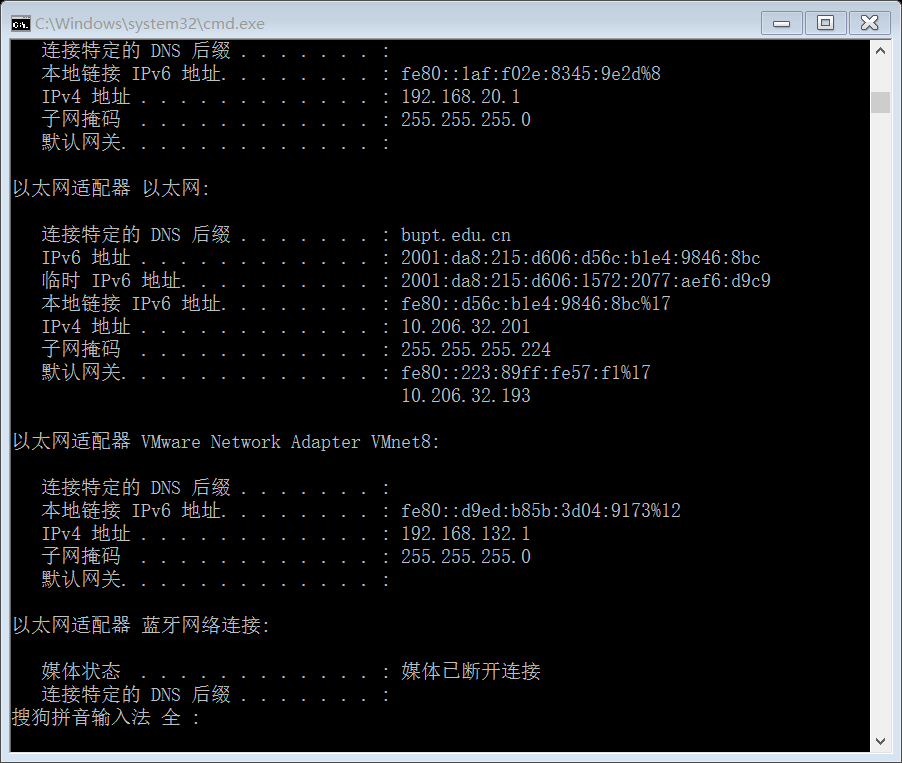


可以看出MAC地址为



**(4) 向DHCP服务器归还IP地址并重新申请分配一个新的IP地址，比较新分配的地址与原地址并分析解释原因。**

使用ipconfig /renew后，命令行信息为



与之前的信息比较可知，IPV4地址和V6地址均与之前相同。

这是由于：之前租用的地址并未被占用，DHCP分配算法会重新将上一个释放掉的且仍未被使用的IP地址再次分给有需求的主机，因此我们得到了两个相同的地址。

1. **分析与思考**
2. **使用网络测试工具能做些什么事情？**

可以检查网络故障，可以对故障进行大体的过程判断，使故障原因被约束在一个较小的范围内，方便进一步的测试和调试。

我认为，网络测试工具也可以用来做网络攻击的“踩点”，一些命令可以获取足够多的对方的网络信息（如主机名，网关，开放端口等），在对方主机的网络防御措施很薄弱的前提下，可以有针对性的对其进行网络攻击。

一些命令还可以刻意造成网络拥塞，如ping命令甚至可以造成目标服务器瘫痪，因此现在很多服务器禁用ping命令。

1. **上网搜索，还有哪些网络测试工具？它们各有什么应用特点？**

一些其他的命令如netstat命令可以帮助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，可以统计目前总共有哪些网络连接正在运行。

route命令用来显示、添加和修改计算机中的路由表的表项。

1. **ICMP协议是因特网与IP协议配合使用的，其具有灵活和强大的系统间调整和差错报告功能，你能够参照ping和traceroute的设计思路也基于ICMP协议设计1-2个简单实用的网络测试命令吗？**

可以利用ICMP做报文的重定向。先检测一台机器到另一台机器的报文传输路线是否是最优的（通过一些测量指标，做出是否需要重定向的判断），如果检测到的路由与最优路由差别很大，则发送ICMP重定向报文以请求主机选择另一条路由，同时再次启用这个机制，直到与最优解相差在一个阈值之内时，在一段时间内一直使用这个较优路径。

1. **当某主机与网络的连接出现故障时，你会如何检测故障？请设计出使用网络命令检测和获取网络状态和相关参数的方法并设计验证一下你的方法的可行性。**

从本次实验整体学习的测试工具来看，可以先利用ping命令做筛查，首先ping还回地址127.0.0.1以排除TCP/IP协议族的故障，其次利用ping本机IP可以测试自身的网卡驱动是否安装正确，网线是否安装正确。再利用ping局域网内IP可以排除子网掩码、网卡配置、路由器、交换机等的不正确连接和故障。得知自己本地网关IP后，ping网关IP可以确保本地路由器工作正常。最后，如果无法登陆某一个网站，可以试图用ping该远程域名，如果ping不同则情况比较多样，可能是DNS服务器禁用了ping命令导致无法ping通。