tracert 与ping的使用

无论你是一个网络维护人员，还是正在学习TCP/IP协议，了解和掌握一些常用的**网络测试命令**将会有助于您更快地**检测到网络故障所在**，同时也会有助你您了解**网络通信的内幕**。

下面我们逐步介绍几个常用的命令：

TTL字段指定IP包被路由器丢弃之前允许通过的最大网段数量。

TTL 一般设为64，经过一个路由器减1，当减为0时，不再转发，直接丢掉IP包。

**ping和tracert**使用方法都一样，在命令后面加IP地址或者域名。**ping 主要是用来查看到目的地址的时延和丢包情况**，**tracert是用来查看所经过的每一跳路由，可以具体判断时延变大或者丢包的点。**

# ping命令：判断本主机到其他主机（IP地址或域名）的网络线路是否连通。

当您的机器**不能访问Internet**，首先确认是否是**本地局域网的故障**。假定局域网的代理服务器IP地址为202.168.0.1，您可以使用**ping 202.168.0.1命令**查看本机是否和代理服务器连通。此外可以**测试本机的网卡是否正常工作**，使用 ping 127.0.0.1命令。一般返回ping的信息就表示本地到该主机的网络线路连通。

但是很多服务器**为了防止攻击**，一般**会关闭对ping的响应**。所以**ping一般作为测试连通性使用**。**ping命令后，会接收到对方发送的回馈信息，其中记录着对方的IP地址和TTL。**TTL是该字段指定IP包被路由器丢弃之前允许通过的最大网段数量。TTL是IPv4包头的一个8 bit字段。例如IP包在服务器中发送前设置的TTL是64，你使用ping命令后，得到服务器反馈的信息，其中的TTL为56，说明途中一共经过了8道路由器的转发，每经过一个路由，TTL减1。

# tracert命令

**tracert命令用来显示数据包到达目标主机所经过的路径（路由器），并显示到达每个节点（路由器）的时间**。

**tracert命令**是使用从本地到目标网站所在网络服务器的一系列网络节点的访问速度，网络节点最多支持显示30个。命令格式是tracert加空格加目标网站名称（也可以输入目标网站的IP地址）。

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**。

tracert命令的原理：Tracert 先发送 TTL 为 1 的回应数据包，当数据包上的 TTL在路由器收到后TTL自动减1 ，一旦某个服务器将TTL减1后，等于了0，**路由器应该将“ICMP Time Exceeded”的消息发回源计算机**，源计算机就根据收到的信息判断达到的路由器和所用时间。**下次再次发送数据包时，将TTL递增 1，继续上述测试，直到目标响应或 TTL 达到最大值，从而确定路由**。**通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL过期的数据包，这在 Tracert 实用程序中看不到，我们会显示请求超时的请求信息。**

下图所示，我们测试到新浪的路经过了8道路由，同时根据上图测试ping 新浪时候，TTL=56，说明新浪的TTL初始设置为64，经过8道路由后到达我们客户机，还剩下64-8 = 56。**下图中请求超时的反馈信息是因为路由器对ping命令做了处理，关闭了ping的响应，所以我们收不到发给它的反馈信息**。

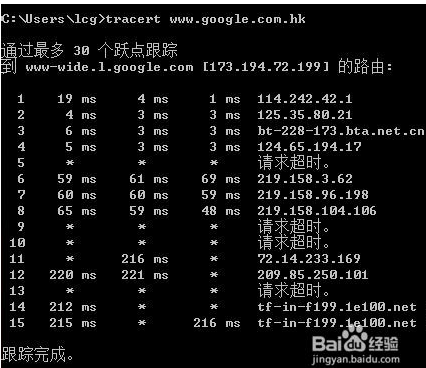


先以百度为例，输入tracert www.baidu.com，回车。

等待片刻显示【跟踪完成】，可以看到追踪的结果。一共途径9个节点，其中有3个节点无法显示速度，其它节点的速度都在5ms以内。这种10个节点以内可以完成追踪的网站访问速度都是不错的。



测试谷歌网站，途径节点15个，前面几个节点的速度在5ms，后面几个为60ms，最后的节点则都在200ms以上，说明网络访问情况比较差。



**跟踪IEEE官网**：ieeexplore.ieee.org 140.98.193.112



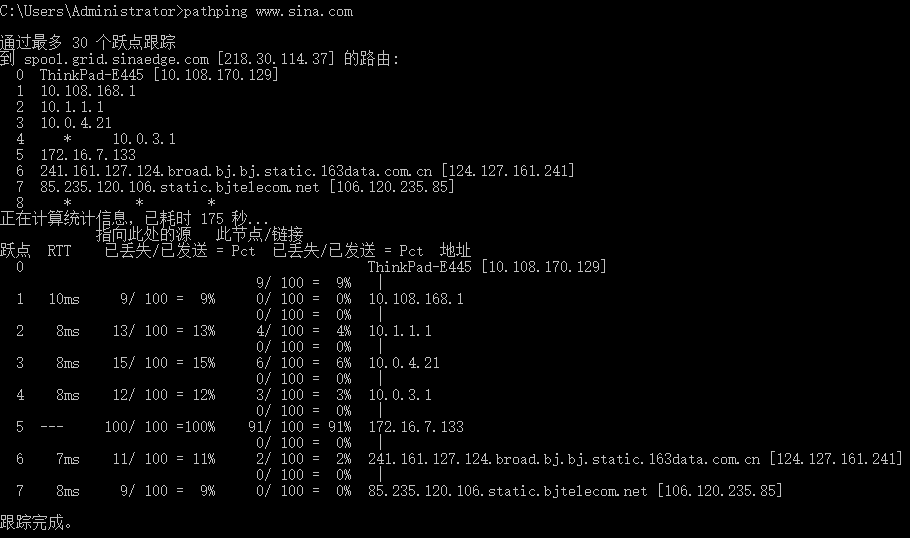
# pathping

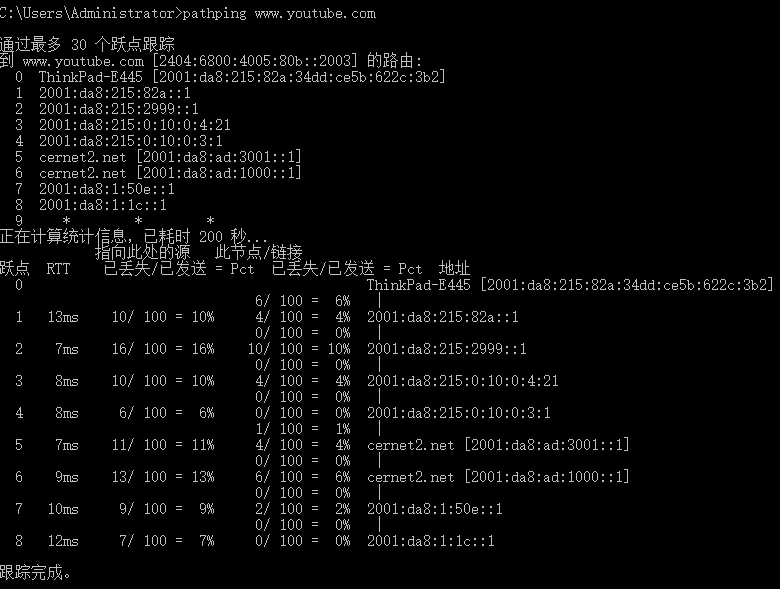
pathping 命令是一个**路由跟踪工具**，它将 **ping 和 tracert 命令的功能与这两个工具所不提供的其他信息结合起来，综合了二者的功能**。

pathping会先显示中间的通过的路由器（类似tracert命令得到的信息），然后对每个中间路由器（节点）发送一定数量的ping包，通过统计他们对ping包响应的数据包来分析通信质量。上面也提到了，有的路由器对ping关闭了响应，所以有的节点的丢包率会达到100%，所以这种一般就是关闭了ping回复。你可以自己ping试一下。**还有，对ping包丢弃程度只是节点本身对ping的处理，并不一定影响他的通信，你可以看到，关闭ping命令节点的下一个节点返回到数据是正常的，说明回复的包都成功发送回来**。

总之，**pathping 命令**在一段时间内将数据包发送到将到达最终目标的路径上的每个路由器，然后根据从每个跃点返回的数据包计算结果。**由于命令显示数据包在任何给定路由器或链接上丢失的程度，因此可以很容易地确定可能导致网络问题的路由器或链接。**下图所示，我们看到，达到第二个就终止了，因为第二道节点（路由器），不支持ping，然后，程序就终止不在继续往下探测了。







# nslookup

**nslookup命令用于解析域名，一般用来检测本机的DNS设置是否配置正确**。如： **nslookup** 网站域名，即可解析出网站的IP地址。如图，可以看出解析www.163.com的时候，可以解析出它所有的IP地址，而如果网路出现异常或者无法收到服务器发送来的信息时候，会出现下面第二张图片的显示。服务器和Address代表是解析这些IP地址和域名的DNS服务器信息。比如我使用的DNS是**jtjndc007.home.langchao.com**, DNS服务器地址是**10.100.1.11**.

# [www.baidu.com](http://www.baidu.com)

## ping [www.baidu.com](http://www.baidu.com)

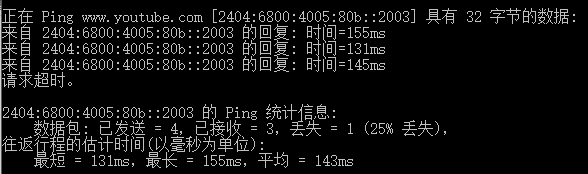


## tracert [www.baidu.com](http://www.baidu.com)



# [www.youtube.com](http://www.youtube.com)

## ping [www.youtube.com](http://www.youtube.com)



## tracert [www.youtube.com](http://www.youtube.com)

