traceroute

显示数据包到主机间的路径

补充说明

traceroute命令 用于追踪数据包在网络上的传输时的全部路径，它默认发送的数据包大小是40字节。

通过traceroute我们可以知道信息从你的计算机到互联网另一端的主机是走的什么路径。当然每次数据包由某一同样的出发点（source）到达某一同样的目的地(destination)走的路径可能会不一样，但基本上来说大部分时候所走的路由是相同的。

traceroute通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。一条路径上的每个设备traceroute要测3次。输出结果中包括每次测试的时间(ms)和设备的名称（如有的话）及其ip地址。

语法

```
traceroute(选项)(参数)
```

选项

```
-d 使用Socket层级的排错功能；
-f<存活数值>：设置第一个检测数据包的存活数值TTL的大小；
-F 设置勿离断位；
-g<网关>：设置来源路由网关，最多可设置8个；
-i<网络界面>：使用指定的网络界面送出数据包；
-I 使用ICMP回应取代UDP资料信息；
-m<存活数值>：设置检测数据包的最大存活数值TTL的大小；
-n 直接使用IP地址而非主机名称；
-p<通信端口>：设置UDP传输协议的通信端口；
-r 忽略普通的Routing Table，直接将数据包送到远端主机上。
-s<来源地址>：设置本地主机送出数据包的IP地址；
-t<服务类型>：设置检测数据包的TOS数值；
-v 详细显示指令的执行过程；
-w<超时秒数>：设置等待远端主机回报的时间；
-x 开启或关闭数据包的正确性检验。
```

参数

主机：指定目的主机IP地址或主机名。

实例

```
traceroute www.58.com
traceroute to www.58.com (211.151.111.30), 30 hops max, 40 byte packets
 1  unknown (192.168.2.1)  3.453 ms  3.801 ms  3.937 ms
 2  221.6.45.33 (221.6.45.33)  7.768 ms  7.816 ms  7.840 ms
 3  221.6.0.233 (221.6.0.233)  13.784 ms  13.827 ms 221.6.9.81 (221.6.9.81)
9.758 ms
 4  221.6.2.169 (221.6.2.169)  11.777 ms 122.96.66.13 (122.96.66.13)  34.952
ms 221.6.2.53 (221.6.2.53)  41.372 ms
```

```
 5  219.158.96.149 (219.158.96.149)  39.167 ms  39.210 ms  39.238 ms
 6  123.126.0.194 (123.126.0.194)  37.270 ms 123.126.0.66 (123.126.0.66)
37.163 ms  37.441 ms
 7  124.65.57.26 (124.65.57.26)  42.787 ms  42.799 ms  42.809 ms
 8  61.148.146.210 (61.148.146.210)  30.176 ms 61.148.154.98 (61.148.154.98)
32.613 ms  32.675 ms
 9  202.106.42.102 (202.106.42.102)  44.563 ms  44.600 ms  44.627 ms
10  210.77.139.150 (210.77.139.150)  53.302 ms  53.233 ms  53.032 ms
11  211.151.104.6 (211.151.104.6)  39.585 ms  39.502 ms  39.598 ms
12  211.151.111.30 (211.151.111.30)  35.161 ms  35.938 ms  36.005 ms
```

记录按序列号从1开始，每个纪录就是一跳，每跳表示一个网关，我们看到每行有三个时间，单位是ms其实就是-q的默认参数。探测数据包向每个网关发送三个数据包后，网关响应后返回的时间；如果用traceroute -q 4 www.58.com，表示向每个网关发送4个数据包。

有时我们traceroute一台主机时，会看到有一些行是以星号表示的。出现这样的情况，可能是防火墙封掉了ICMP的返回信息，所以我们得不到什么相关的数据包返回数据。

有时我们在某一网关处延时比较长，有可能是某台网关比较阻塞，也可能是物理设备本身的原因。当然如果某台DNS出现问题时，不能解析主机名、域名时，也会 有延时长的现象；您可以加-n参数来避免DNS解析，以IP格式输出数据。

如果在局域网中的不同网段之间，我们可以通过traceroute 来排查问题所在，是主机的问题还是网关的问题。如果我们通过远程来访问某台服务器遇到问题时，我们用到traceroute 追踪数据包所经过的网关，提交IDC服务商，也有助于解决问题；但目前看来在国内解决这样的问题是比较困难的，就是我们发现问题所在IDC服务商也不可能帮助我们解决。

跳数设置

```
[root@localhost ~]# traceroute -m 10 www.baidu.com
traceroute to www.baidu.com (61.135.169.105), 10 hops max, 40 byte packets
 1  192.168.74.2 (192.168.74.2)  1.534 ms  1.775 ms  1.961 ms
 2  211.151.56.1 (211.151.56.1)  0.508 ms  0.514 ms  0.507 ms
 3  211.151.227.206 (211.151.227.206)  0.571 ms  0.558 ms  0.550 ms
 4  210.77.139.145 (210.77.139.145)  0.708 ms  0.729 ms  0.785 ms
 5  202.106.42.101 (202.106.42.101)  7.978 ms  8.155 ms  8.311 ms
 6  bt-228-037.bta.net.cn (202.106.228.37)  772.460 ms bt-228-025.bta.net.cn
(202.106.228.25)  2.152 ms 61.148.154.97 (61.148.154.97)  772.107 ms
 7  124.65.58.221 (124.65.58.221)  4.875 ms 61.148.146.29 (61.148.146.29)
2.124 ms 124.65.58.221 (124.65.58.221)  4.854 ms
 8  123.126.6.198 (123.126.6.198)  2.944 ms 61.148.156.6 (61.148.156.6)
3.505 ms 123.126.6.198 (123.126.6.198)  2.885 ms
 9  * * *
10  * * *
```

其它一些实例

```
traceroute -m 10 www.baidu.com # 跳数设置
traceroute -n www.baidu.com    # 显示IP地址，不查主机名
traceroute -p 6888 www.baidu.com  # 探测包使用的基本UDP端口设置6888
traceroute -q 4 www.baidu.com  # 把探测包的个数设置为值4
traceroute -r www.baidu.com    # 绕过正常的路由表，直接发送到网络相连的主机
```

```
traceroute -w 3 www.baidu.com  # 把对外发探测包的等待响应时间设置为3秒
```