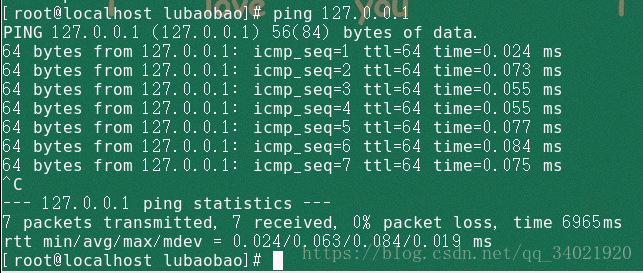
## 1、ping

ping 命令是用来测试TCP/IP 网络是否畅通或者测试网络连接速度的命令，对确定网络是否正确连接，以及网络连接的状况十分有用。  
ping命令的原理是根据计算机唯一标示的IP 地址，当用户给目的地址发送一个数据包时，对方就会返回一个同样大小的数据包，根据返回的数据包用户可以确定目的主机的存在，并初步判断目的主机的操作系统。

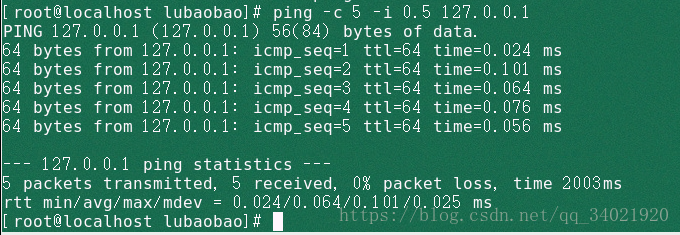
##### 用法

（1）命令格式

* **ping ( 选项）目的地址**

目的地址指的是被测计算机的IP 地址、主机名或者是域名。  
（2）实例   
  
注：Linux下的ping命令和Windows下的ping命令不同，需要Ctrl+C来终止   
（3）选项

**-d：**使用Socket的SO\_DEBUG功能；   
**-c<完成次数>：**设置完成要求回应的次数；   
**-f：**极限检测；   
**-i<间隔秒数>：**指定收发信息的间隔时间；   
**-L<网络界面>：**使用指定的网络界面送出数据包；   
**-l<前置载入>：**设置在送出要求信息之前，先行发出的数据包；   
**-n：**只输出数值；   
**-p<范本样式>：**设置填满数据包的范本样式；   
**-q：**不显示指令执行过程，开头和结尾的相关信息除外；   
**-r：**忽略普通的Routing Table，直接将数据包送到远端主机上；   
**-R：**记录路由过程；   
**-s<数据包大小>：**设置数据包的大小；   
**-v：**详细显示指令的执行过程。   
**-t<存活数值>：设置存活数值TTL的大小**

说一下其中的**-c**、 **-i**参数   
其中 –c count 次数，也就是ping的次数；-i interval 间隔 ，每次ping之间的时间空格   


### 2、telnet

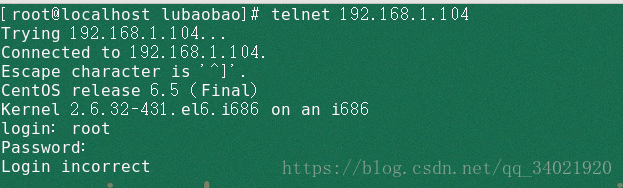
telnet命令用于登录远程主机，对远程主机进行管理。telnet因为采用明文传送报文，安全性不好，很多Linux服务器都不开放telnet服务，而改用更安全的ssh方式了。

##### 用法

（1）命令格式：

* **telnet (选项) (参数)**

（2）实例



（3）参数

* **远程主机：**指定要登录进行管理的远程主机
* **端口：**指定TELNET协议使用的端口号

（4）选项

**-8：**允许使用8位字符资料，包括输入与输出；   
**-a：**尝试自动登入远端系统；   
**-b<主机别名>：**使用别名指定远端主机名称；   
**-c：**不读取用户专属目录里的.telnetrc文件；   
**-d：**启动排错模式；   
**-e<脱离字符>：**设置脱离字符；   
**-E：**滤除脱离字符；   
**-f：**此参数的效果和指定”-F”参数相同；   
**-F：**使用Kerberos V5认证时，加上此参数可把本地主机的认证数据上传到远端主机；   
**-k<域名>：**使用Kerberos认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名；   
**-K：**不自动登入远端主机；   
**-l<用户名称>：**指定要登入远端主机的用户名称；   
**-L：**允许输出8位字符资料；   
**-n<记录文件>：**指定文件记录相关信息；   
**-r：**使用类似rlogin指令的用户界面；   
**-S<服务类型>：**设置telnet连线所需的ip TOS信息；   
**-x：**假设主机有支持数据加密的功能，就使用它；   
**-X<认证形态>：**关闭指定的认证形态。

### 3、netstat

netstat命令用来打印Linux中网络系统的状态信息，可让你得知整个Linux系统的网络情况

##### 用法

（1）命令格式

* **netstat（选项）**

（2）选项

**-a或–all：**显示所有连线中的Socket；   
**-A<网络类型>或–<网络类型>：**列出该网络类型连线中的相关地址；   
**-c或–continuous：**持续列出网络状态；   
**-C或–cache：**显示路由器配置的快取信息；   
**-e或–extend：**显示网络其他相关信息；   
**-F或–fib：**显示FIB；   
**-g或–groups：**显示多重广播功能群组组员名单；   
**-h或–help：**在线帮助；   
**-i或–interfaces：**显示网络界面信息表单；   
**-l或–listening：**显示监控中的服务器的Socket；   
**-M或–masquerade：**显示伪装的网络连线；   
**-n或–numeric：**直接使用ip地址，而不通过域名服务器；   
**-N或–netlink或–symbolic：**显示网络硬件外围设备的符号连接名称；   
**-o或–timers：**显示计时器；   
**-p或–programs：**显示正在使用Socket的程序识别码和程序名称；   
**-r或–route：**显示Routing Table；   
**-s或–statistice：**显示网络工作信息统计表；   
**-t或–tcp：**显示TCP传输协议的连线状况；   
**-u或–udp：**显示UDP传输协议的连线状况；   
**-v或–verbose：**显示指令执行过程；   
**-V或–version：**显示版本信息；   
**-w或–raw：**显示RAW传输协议的连线状况；   
**-x或–unix：**此参数的效果和指定”-A unix”参数相同；   
**–ip或–inet：**此参数的效果和指定”-A inet”参数相同

（3）实例

netstat -a //列出所有端口

netstat -at //列出所有tcp端口

netstat -au //列出所有udp端口

在这里显示所有的TCP端口



netstat -l //只显示监听端口

netstat -lt //只列出所有监听 tcp 端口

netstat -lu //只列出所有监听 udp 端口

和上面的图相比，可以看到只显示出了监听状态的TCP端口   


### 4、ifconfig

ifconfig命令被用于配置和显示Linux内核中网络接口的网络参数。用ifconfig命令配置的网卡信息，在网卡重启后机器重启后，配置就不存在。要想将上述的配置信息永远的存的电脑里，那就要修改网卡的配置文件了。

##### 用法

（1）命令格式

* **ifconfig（参数）**

（2）实例   


eth0表示第一块网卡，可以看到这个网卡的信息

* HWaddr表示网卡的物理地址即MAC地址，可以看到目前这个网卡的MAC地址是：00:0C:29:A7:C0:6C
* inet addr用来表示网卡的IP地址，此网卡的IP地址是：192.168.1.106
* 广播地址Bcast：192.168.1.255
* 掩码地址Mask：255.255.255.0

lo是表示主机的回环地址，这个一般是用来测试一个网络程序，但又不想让局域网或外网的用户能够查看，只能在此台主机上运行和查看所用的网络接口。

（3）参数

**add<地址>：**设置网络设备IPv6的ip地址   
**del<地址>：**删除网络设备IPv6的IP地址   
**down：**关闭指定的网络设备   
**io\_addr< I/O地址>：**设置网络设备的I/O地址   
**irq< IRQ地址>：**设置网络设备的IRQ；   
**media<网络媒介类型>：**设置网络设备的媒介类型；   
**mem\_start<内存地址>：**设置网络设备在主内存所占用的起始地址；   
**metric<数目>：**指定在计算数据包的转送次数时，所要加上的数目；   
**mtu<字节>：**设置网络设备的MTU；   
**netmask<子网掩码>：**设置网络设备的子网掩码；   
**tunnel<地址>：**建立IPv4与IPv6之间的隧道通信地址；   
**up：**启动指定的网络设备；   
**-broadcast<地址>：**将要送往指定地址的数据包当成广播数据包来处理；   
**-pointopoint<地址>：**与指定地址的网络设备建立直接连线，此模式具有保密功能；   
**-promisc：**关闭或启动指定网络设备的promiscuous模式；   
**IP地址：**指定网络设备的IP地址；   
**网络设备：**指定网络设备的名称。

### 5、route

route命令用来显示并设置Linux内核中的网络路由表，route命令设置的路由主要是静态路由。   
要注意的是，直接在命令行下执行route命令来添加路由，不会永久保存，当网卡重启或者机器重启之后，该路由就失效了；可以在**\*/etc/rc.local**中添加route命令来保证该路由设置永久有效。

##### 用法

（1）命令格式

* **route（选项）（参数）**

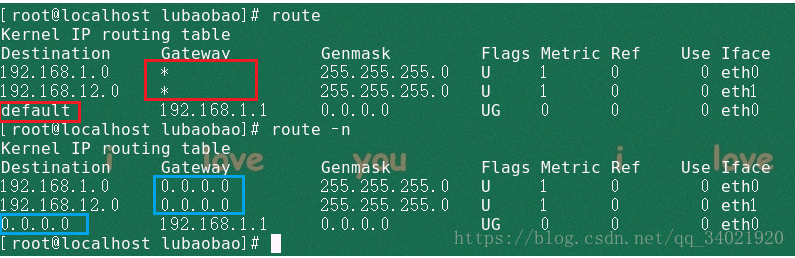
（2）选项

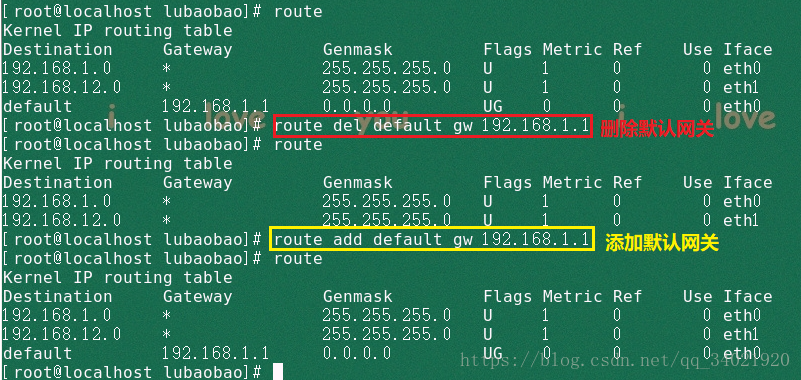
**-A：**设置地址类型；   
**-C：**打印将Linux核心的路由缓存；   
**-v：**详细信息模式；   
**-n：**不执行DNS反向查找，直接显示数字形式的IP地址；   
**-e：** netstat格式显示路由表；   
**-net：**到一个网络的路由表；   
**-host：**到一个主机的路由表。

（3）参数

**Add：**增加指定的路由记录   
**Del：**删除指定的路由记录   
**Target：**目的网络或目的主机   
**gw：**设置默认网关   
**mss：**设置TCP的最大区块长度(MSS)，单位为MB   
**window：**指定通过路由表的TCP连接的TCP窗口大小   
**dev：**路由记录所表示的网络接口

（4）实例

显示当前路由，从图中可以看出加了选项-n的变化   


删除和添加设置默认网关   


### 6、arp

arp命令用于操作主机arp缓冲区，可以显示arp缓冲区的所有条目、删除指定条目或增加静态IP地址与MAC地址的对应关系

##### 用法

（1）命令格式

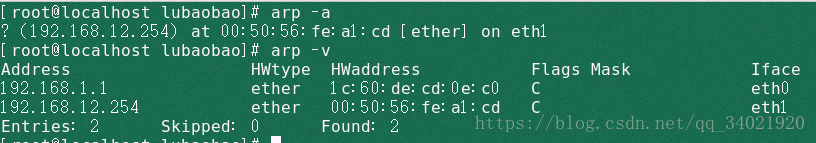
* **arp（选项）（参数）**

（2）选项

**-a<主机>：**显示arp缓冲区的所有条目   
**-H<地址类型>：**指定arp指令使用的地址类型   
**-d<主机>：**从arp缓冲区中删除指定主机的arp条目   
**-D：**使用指定接口的硬件地址   
**-e：**以Linux的显示风格显示arp缓冲区中的条目   
**-i<接口>：**指定要操作arp缓冲区的网络接口   
**-s<主机><硬件地址>：设置指定主机的IP地址与MAC地址的静态映射**   
**-n：**以数字方式显示arp缓冲区中的条目   
**-v：**显示详细的arp缓冲区条目，包括缓冲区条目的统计信息   
**-f<文件>：**设置主机的IP地址与MAC地址的静态映射

（3）参数

* **主机：查询arp缓冲区中指定主机的arp条目。**

（4）实例   


### 7、traceroute

traceroute命令用于追踪数据包在网络上传输时的全部路径，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

##### 用法

（1）命令格式

* **traceroute（选项）（参数）**

（2）选项

**-d：**使用Socket层级的排错功能   
**-f<存活时间>：**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   
**-l：**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   
**-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

（3）参数

* **主机：指定目的主机IP地址或主机名**

（4）实例   
  
从图中可以看出记录按序列号从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；   
在后面一部分我们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。

### 8、host

host命令是常用的分析域名查询工具，可以检测域名系统工作是否正常

##### 用法

（1）命令格式

* **host（选项）（参数）**

（2）选项

**-a：**显示详细的DNS信息   
**-c<类型>：**指定查询类型，默认值为“IN”   
**-C：**查询指定主机的完整SOA记录   
**-r：**在查询域名时，不使用递归的查询方式   
**-t<类型>：**指定查询第域名信息类型   
**-v：**显示指令执行的详细信息   
-a：显示详细的DNS信息；   
**-w：**如果域名服务器没有给出应答信息，则一直等待，直到域名服务器给出应答   
**-W<时间>：**指定域名查询的最长时间，如果在指定时间内域名服务器没有给出应答信息，则退出指令   
**-4：**使用IPv4   
**-6：**使用IPv6

（3）参数

* **主机：要查询的主机信息**

（4）实例   


### 9、tcpdump

tcpdump命令是一款抓取数据包的工具，它可以打印所有经过网络接口的数据包的头信息，也可以使用-w选项将数据包保存到文件中，方便以后分析。

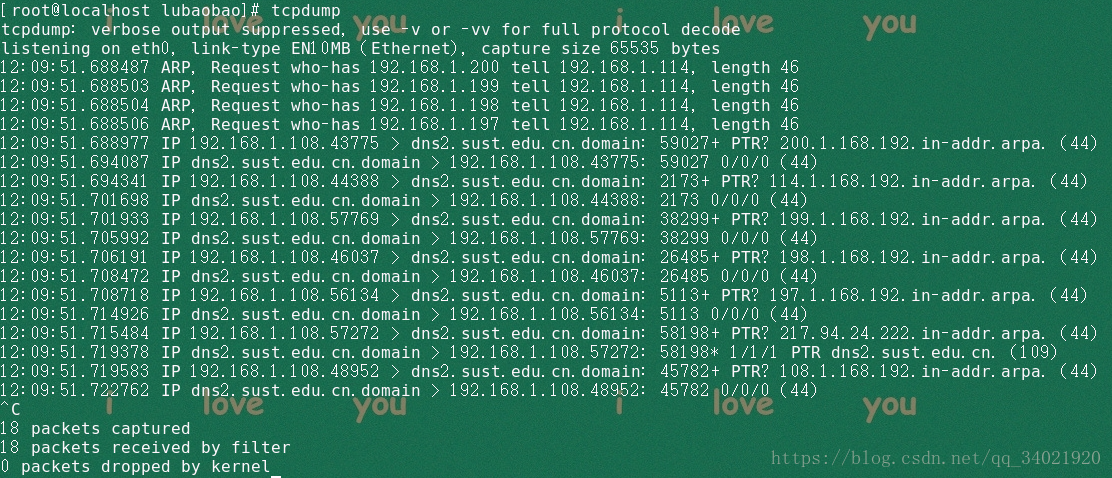
##### 用法

（1）命令格式

* **tcpdump（选项）**

（2）选项

**-a：**尝试将网络和广播地址转换成名称；   
**-c<数据包数目>：**收到指定的数据包数目后，就停止进行倾倒操作；   
**-d：**把编译过的数据包编码转换成可阅读的格式，并倾倒到标准输出；   
**-dd：**把编译过的数据包编码转换成C语言的格式，并倾倒到标准输出；   
**-ddd：**把编译过的数据包编码转换成十进制数字的格式，并倾倒到标准输出；   
**-e：**在每列倾倒资料上显示连接层级的文件头；   
**-f：**用数字显示网际网络地址；   
**-F<表达文件>：**指定内含表达方式的文件；   
**-i<网络界面>：**使用指定的网络截面送出数据包；   
**-l：**使用标准输出列的缓冲区；   
**-n：**不把主机的网络地址转换成名字；   
**-N：**不列出域名；   
**-O：**不将数据包编码最佳化；   
**-p：**不让网络界面进入混杂模式；   
**-q ：**快速输出，仅列出少数的传输协议信息；   
**-r<数据包文件>：**从指定的文件读取数据包数据；   
**-s<数据包大小>：**设置每个数据包的大小；   
**-S：**用绝对而非相对数值列出TCP关联数；   
**-t：**在每列倾倒资料上不显示时间戳记；   
**-tt：**在每列倾倒资料上显示未经格式化的时间戳记；   
**-T<数据包类型>：**强制将表达方式所指定的数据包转译成设置的数据包类型；   
**-v：**详细显示指令执行过程；   
**-vv：**更详细显示指令执行过程；   
**-x：**用十六进制字码列出数据包资料；   
**-w<数据包文件>：**把数据包数据写入指定的文件。

（3）实例   
tcpdump：监视第一个网络接口上流过的所有数据包(带上-i选项，是监视指定网络接口)   


展开阅读全文

原文地址：https://blog.csdn.net/qq\_34021920/article/details/80543315