Linux - 网络管理

作者：douniwan
原文链接：https://ld246.com/article/1573657890737
来源网站：链滴

网络状态查看

ifconfig

查看网络信息：

ifconfig

执行该命令输出如下：

<!-- more -->

```
huny@huny-PC:~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 80:e8:2c:12:fe:f1  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7083  bytes 2605304 (2.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7083  bytes 2605304 (2.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.33.2.70  netmask 255.255.224.0  broadcast 172.33.31.255
        inet6 fe80::434f:5457:5f70:c7d4  prefixlen 64  scopeid 0x20<link>
        ether 58:a0:23:70:e7:43  txqueuelen 1000  (Ethernet)
        RX packets 734318  bytes 432089360 (412.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 173208  bytes 18868472 (17.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

huny@huny-PC:~$
```

在输出的结果中：

其中的enp2s0,lo,wlp0s20f3是网卡。其中lo（Loopback）纯软件网络设备接口，它的ip地址永远都127.0.0.1，这个可以提供给自己本地的服务访问。

而每一个网卡下面的inet是ip（ipv4）地址，netmask是子网掩码，broadcast是广播地址

ether是网卡的**MAC**地址。然后RX，TX表示发送和接受的包的个数和大小。

route

查看网关：

route [-n]　#使用 -n 参数不解析主机名，不加 -n ，每个ip会反解为域名

执行该命令输出如下：

```
huny@huny-PC:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.33.0.1      0.0.0.0         UG    600    0        0 wlp0s20f3
172.33.0.0      0.0.0.0         255.255.224.0   U     600    0        0 wlp0s20f3
huny@huny-PC:~$
```

在输出的结果中：

其中的Destination是目标网段或者主机，Gateway是网关地址，”*” 表示目标是本主机所属的网络不需要路由，Genmask是掩码，Flags是标记，Metric是路由距离，到达指定网络所需的中转数（linu 内核中没有使用）Ref是路由项引用次数（linux 内核中没有使用），Use此路由项被路由软件查找的数，Iface该路由表项对应的网卡。

其中Flags可以为

一些标记解释

H — 目标是一个主机

G — 路由指向网关

R — 恢复动态路由产生的表项

D — 由路由的后台程序动态地安装

M — 由路由的后台程序修改

! — 拒绝路由

网络配置

ip

修改ip

ifconfig 网卡名 IP地址

修改ip并修改子网掩码

ifconfig 网关名 IP地址 netmask 子网掩码

网卡

关掉启动网卡

ifup/ ifdown 网卡名

网关

修改默认网关(0.0.0.0)

1. 先删除默认网关

route del default gw 网关地址

2. 添加网关

route add default gw 网关地址

路由

添加明细路由（访问指定的地址走指定的网关）：

route add -host 主机地址 gw 网关地址

添加明细路由（访问一个网段走指定的网关）：

route add -net 网段 netmask 子网掩码 gw 网关地址

网络故障排除

ping

ping 检测当前主机与目标主机的网络是否畅通

检测是否可以上百度：

```
huny@huny-PC:~$ ping www.baidu.com
PING www.a.shifen.com (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=1 ttl=54 time=29.5 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=2 ttl=54 time=49.4 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=3 ttl=54 time=58.6 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=4 ttl=54 time=62.2 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=5 ttl=54 time=61.4 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=6 ttl=54 time=76.8 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=7 ttl=54 time=78.2 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=8 ttl=54 time=72.4 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=9 ttl=54 time=81.2 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=10 ttl=54 time=58.0 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=11 ttl=54 time=56.9 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=12 ttl=54 time=67.9 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=13 ttl=54 time=63.7 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=14 ttl=54 time=73.1 ms
^C
--- www.a.shifen.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13018ms
rtt min/avg/max/mdev = 29.533/63.560/81.213/12.973 ms
huny@huny-PC:~$
```

使用ping的时候，在Linux不会自动停止，如果想停止要使用 ctrl+c快捷键。

也可以使用参数：-w 时间（s），这样在运行多少秒后会自动停止。

检测是否可以上百度（4s后停止）：

```
huny@huny-PC:~$ ping -w 4 www.baidu.com
PING www.a.shifen.com (14.215.177.38) 56(84) bytes of data.
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=1 ttl=54 time=31.5 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=2 ttl=54 time=33.7 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=3 ttl=54 time=30.9 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=4 ttl=54 time=32.8 ms

--- www.a.shifen.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 30.946/32.257/33.749/1.117 ms
huny@huny-PC:~$
```

traceroute

traceroute用来追踪当前主机到目标主机的状态

用法：

traceroute [参数] [主机]

参数：

- -d 使用Socket层级的排错功能。
- -f 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 设置来源路由网关，最多可设置8个。
- -i 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 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 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 设置本地主机送出数据包的IP地址。
- -t 设置检测数据包的TOS数值。
- -v 详细显示指令的执行过程。
- -w 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。

```
huny@huny-PC:~$ traceroute  www.baidu.com
traceroute to www.baidu.com (14.215.177.39), 30 hops max, 60 byte packets
 1  172.33.0.1 (172.33.0.1)  2.952 ms  3.214 ms  3.374 ms
 2  183.64.60.81 (183.64.60.81)  3.609 ms  3.897 ms  4.179 ms
 3  222.176.39.213 (222.176.39.213)  5.709 ms  5.868 ms  5.990 ms
```

```
 4  222.176.46.25 (222.176.46.25)  4.992 ms  6.043 ms  6.308 ms
 5  222.176.6.17 (222.176.6.17)  6.431 ms 222.176.9.121 (222.176.9.121)  6.619 ms  6.753 ms
 6  202.97.28.21 (202.97.28.21)  35.829 ms 202.97.28.162 (202.97.28.162)  32.151 ms 202.97.34
85 (202.97.34.85)  29.472 ms
 7  113.96.5.74 (113.96.5.74)  35.882 ms 113.96.4.66 (113.96.4.66)  35.834 ms 113.96.4.54 (113.
6.4.54)  33.246 ms
 8  * 98.96.135.219.broad.fs.gd.dynamic.163data.com.cn (219.135.96.98)  37.394 ms  35.895 ms
 9  14.215.32.90 (14.215.32.90)  34.492 ms  34.529 ms 14.215.32.126 (14.215.32.126)  33.039 m

10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
huny@huny-PC:~$
```

结果说明：

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s，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；如您用 traceroute -q 4 www.baidu.com ，表示向每个网关发送4个数据包。那么就会出现四个时间。

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，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，就是我们现问题所在，IDC服务商也不可能帮助我们解决。

mtr

mtr 检查到目标主机间是否有数据包丢失，比tracreoute更详细。

更多可查看MTR命令详详解

nslookup

nslookup 可以查看域名对应的ip,用于只知道域名，但是你需要ip地址的场景。

telnet

如果能与某个主机联通，但是还是不能访问某个服务，就可以查看是否端口问题。

telnet 检查与某个主机的端口的连接状态

telnet www.baidu.com 80　　#检测是否与百度的80端口是可连接的

运行结果：

```
huny@huny-PC:~$ telnet www.baidu.com 80
Trying 14.215.177.39...
Connected to www.a.shifen.com.
Escape character is '^]'.
```

如果畅通，就会出现这种显示，如果我们要退出的话可以使用ctrl+]进入如下页面：

```
huny@huny-PC:~$ telnet www.baidu.com 80
Trying 14.215.177.39...
Connected to www.a.shifen.com.
Escape character is '^]'.
^]
telnet>
```

然后输入 quit就可以退出了。

tcpdump

查看每一个发送的数据包是怎么样的（即用来网络抓包）

抓取任意网卡的80端口的数据包

tcpdump -i any -n port 80　# -i any标识所有的网卡，-n不要显示域名，显示ip

抓取某个主机的数据包

tcpdump -i any -n host 地址

抓取某个主机的某个端口的数据包

tcpdump -i any -n host 地址 and port 80 #抓取某个主机的80端口的数据包

如果想要把抓取的结果输出到某个地方，可以在命令后加-w [输出地址]：

更多详细用法，，，，，，，，待学习！！！！！！ 后面再总结，(^__^) 嘻嘻……

netstat

netstat 查看服务的监听范围的问题

-n 显示ip地址，不显示域名

t 以tcp的方式去截取

p 除了显示对应的端口外，也显示对应的进程

l tcp的一个状态

运行示例：

```
huny@huny-PC:~$ netstat -ntpl
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4300          0.0.0.0:*               LISTEN      5549/wineserver.rea
tcp        0      0 127.0.0.1:4301          0.0.0.0:*               LISTEN      5549/wineserver.rea
tcp        0      0 127.0.0.1:12333         0.0.0.0:*               LISTEN      4613/electron-ssr -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:1080          0.0.0.0:*               LISTEN      4777/python
tcp        0      0 127.0.0.1:2333          0.0.0.0:*               LISTEN      4613/electron-ssr -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
huny@huny-PC:~$
```

ss

ss 查看服务的监听范围的问题

使用参数与netstat差不多相同：

运行示例：

```
huny@huny-PC:~$ ss -ntpl
State       Recv-Q Send-Q                                          Local Address:Port
                                                  Peer Address:Port
LISTEN      0      80                                              127.0.0.1:3306
                                                   *:*
LISTEN      0      50                                                   *:139
                                                 *:*
LISTEN      0      10                                              127.0.0.1:4300
                                                   *:*                users:(("TIM.exe",pid=6046,fd=262),("wineser
er.real",pid=5549,fd=75))
LISTEN      0      10                                              127.0.0.1:4301
```

```
                                        *:*                 users:(("TIM.exe",pid=6046,fd=263),("wineser
er.real",pid=5549,fd=275))
LISTEN     0      511                                        127.0.0.1:12333
                                         *:*                users:(("electron-ssr",pid=4613,fd=106))
LISTEN     0      5                                          127.0.0.1:631
                                       *:*
LISTEN     0      512                                        127.0.0.1:1080
                                         *:*                users:(("python",pid=4777,fd=6))
LISTEN     0      511                                        127.0.0.1:2333
                                         *:*                users:(("electron-ssr",pid=4613,fd=110))
LISTEN     0      50                                         *:445
                                     *:*
LISTEN     0      50                                         :::139
                                   :::*
LISTEN     0      5                                          ::1:631
                                   :::*
LISTEN     0      50                                         :::445
                                   :::*
huny@huny-PC:~$
```

常用网络配置文件

关于网络的配置文件有:

主机地址配置文件:/etc/hosts

网络服务信息文件:/etc/services

允许与拒绝地址配置文件:/etc/hosts.allow和/etc/hosts.deny

网络配置文件:/etc/network/interfaces

主机查找配置文件:/etc/host.conf

名称服务器查找顺序配置文件:/etc/resolv.conf

网卡参数配置文件:/etc/network/interfaces

/etc/hosts

主机地址配置文件/etc/hosts，也叫本地主机文件，其内容为IP地址与其对应的主机名，用来实现将机名称解析为IP地址。

hosts文件是Linux系统中一个负责IP地址与域名快速解析的文件，以ASCII格式保存在“/etc”目录，文件名为“hosts”。hosts文件包含了IP地址和主机名之间的映射，还包括主机名的别名。

在没有域名服务器的情况下，系统上的所有网络程序都通过查询该文件来解析对应于某个主机名的IP址，否则就需要使用DNS服务程序来解决。通常可以将常用的域名和IP地址映射加入到hosts文件中实现快速方便的访问。 Linux主机名的相关配置文件就是/etc/hosts;这个文件告诉本主机哪些域名对那些ip，那些主机名对应哪些ip：

列如我的hosts文件：

```
huny@huny-PC:/etc$ cat /etc/hosts
#格式：IP地址 主机名/域名 主机别名
127.0.0.1    localhost
```

```
127.0.1.1   huny-PCs

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
huny@huny-PC:/etc$
```

一般情况下hosts文件的每行为一个主机，每行由三部份组成，每个部份由空格隔开。其中#号开头的做说明，不被系统解释。

这里可以稍微解释一下主机名(hostname)和域名(Domain）的区别：

主机名通常在局域网内使用，通过hosts文件，主机名就被解析到对应ip；

域名通常在internet上使用，但如果本机不想使用internet上的域名解析，这时就可以更改hosts文件加入自己的域名解析。

查看修改自己的hostname：

```
huny@huny-PC:/etc$ hostname        #查看自己的hostname
huny-PC
huny@huny-PC:/etc$ sudo hostname huny     #修改自己的hostname
[sudo] huny 的密码：
huny@huny-PC:/etc$ hostname
huny
huny@huny-PC:/etc$
```

通过hostname 工具来设置主机名只是临时的，下次重启系统时，此主机名将不会存在；

永久设置主机名：

修改/etc/hostname，里面写入需要的设置的主机名即可，重启或注销登陆后生效。

也可以使用命令：hostnamectl set-hostname 主机名

其余配置信息可参考络配置文件