iftop

一款实时流量监控工具

补充说明

iftop命令是一款实时流量监控工具，监控TCP/IP连接等，缺点就是无报表功能。必须以root身份才能运行。

语法

```
iftop(选项)
```

选项

```
iftop: display bandwidth usage on an interface by host

Synopsis: iftop -h | [-npblNBP] [-i interface] [-f filter code]
    [-F net/mask] [-G net6/mask6]

   -h                  display this message
   -n                  don't do hostname lookups
   -N                  don't convert port numbers to services
   -p                  run in promiscuous mode (show traffic between other
                       hosts on the same network segment)
   -b                  don't display a bar graph of traffic
   -B                  Display bandwidth in bytes
   -i interface        listen on named interface
   -f filter code      use filter code to select packets to count
                      (default: none, but only IP packets are counted)
   -F net/mask         show traffic flows in/out of IPv4 network
   -G net6/mask6       show traffic flows in/out of IPv6 network
   -l                  display and count link-local IPv6 traffic (default:
off)
   -P                  show ports as well as hosts
   -m limit            sets the upper limit for the bandwidth scale
   -c config file      specifies an alternative configuration file
   -t                  use text interface without ncurses

   Sorting orders:
   -o 2s                Sort by first column (2s traffic average)
   -o 10s               Sort by second column (10s traffic average)
[default]
   -o 40s               Sort by third column (40s traffic average)
   -o source            Sort by source address
   -o destination       Sort by destination address

   The following options are only available in combination with -t
   -s num              print one single text output afer num seconds, then
quit
   -L num              number of lines to print
```

界面说明

> 第一行为带宽，这里为1Mbit,不是字节哦. 连接列表，最后三列分别是2秒，10秒和40秒的平均流量 => 代表发送
> <= 代表接收 最后三行表示发送，接收和全部的流量， 第二列为你运行iftop到目前流量，第三列为高峰值，第四列为平均值。

实例

```
iftop            # 默认是监控第一块网卡的流量
iftop -i eth1    # 监控eth1
iftop -n         # 直接显示IP, 不进行DNS反解析
iftop -N         # 直接显示连接埠编号, 不显示服务名称
iftop -F 192.168.1.0/24 or 192.168.1.0/255.255.255.0  # 显示某个网段进出封包流量
```