1、网络监控

iftop 是什么

> 在 Linux 系统下即时监控服务器的网络带宽使用情况，有很多工具，比如 iptraf、nethogs 等等，但是推荐使用小巧但功能很强大的 iftop 工具。

iftop 是 Linux 系统一个免费的网卡实时流量监控工具，类似于 top 命令。iftop 可以监控指定网卡的实时流量、端口连接信息、反向解析 IP 等，还可以精确显示本机网络流量及网络内各主机和本机相互通信的流量集合，非常适合于监控代理服务器或路由器的网络流量。

同时，iftop 对检测流量异常的主机非常有效，通过 iftop 的输出可以迅速定位主机流量异常的根源，这对于网络故障排查、网络安全检测是十分有用的。缺点就是无报表功能，且必须以 root 身份才能运行。

安装

1. 通过软件管理工具安装

```
# CentOS
$ sudo yum install iftop

# Ubuntu
$ sudo apt install iftop
```

1. 通过源代码编译安装

```
# 安装比较软件包
$ sudo um install libpcap libpcap-devel ncurses ncurses-devel flex byacc

# 下载软件包
$ wget "http://www.ex-parrot.com/~pdw/iftop/download/iftop-0.17.tar.gz"
$ tar zxvf iftop-0.17.tar.gz
$ cd iftop-0.17
$ ./configure
$ make && make install
```

常用参数

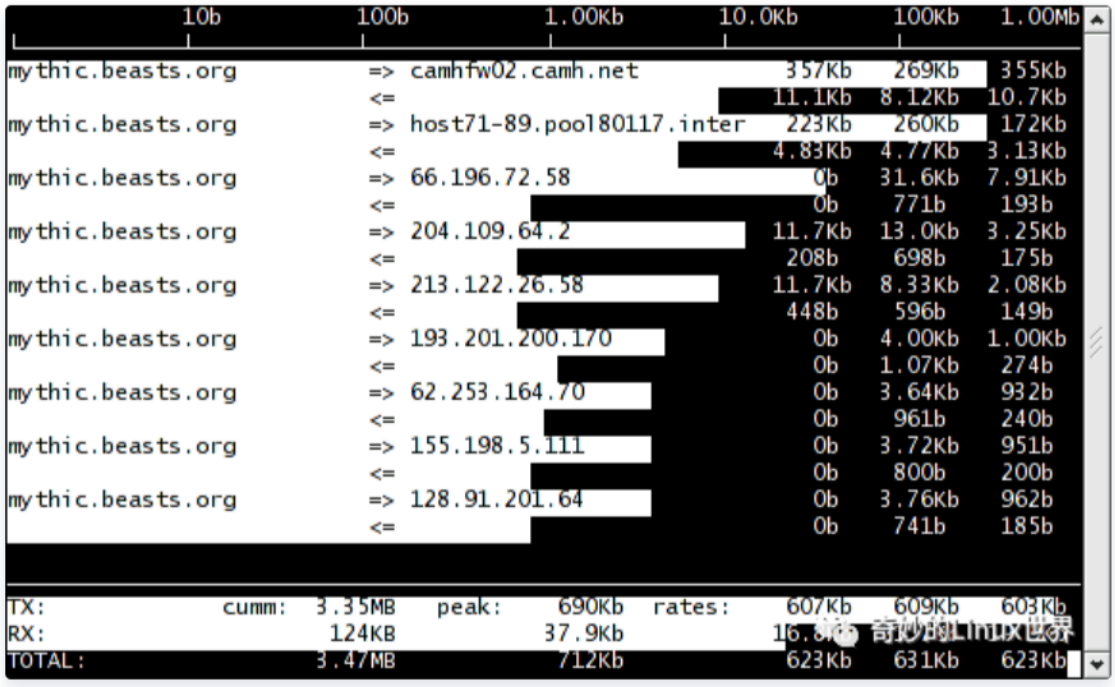
```
-i 指定需要检测的网卡， 如果有多个网络接口，则需要注意网络接口的选择，如：# iftop -i eth1
-B 将输出以 byte 为单位显示网卡流量，默认是 bit
-n 将输出的主机信息都通过 IP 显示，不进行 DNS 解析
-N 只显示连接端口号，不显示端口对应的服务名称
-F 显示特定网段的网卡进出流量  如: iftop -F 192.168.85.0/24
-h 帮助，显示参数信息
-p 以混杂模式运行 iftop，此时 iftop 可以用作网络嗅探器
-P 显示主机以及端口信息
-m 设置输出界面中最上面的流量刻度最大值，流量刻度分 5 个大段显示  如：# iftop -m 100M
-f 使用筛选码选择数据包来计数  如 iftop -f filter code
-b 不显示流量图形条
-c 指定可选的配置文件，如：iftop  -c config file
-t 使用不带 ncurses 的文本界面，
    以下两个是只和 -t 一起用的：
    -s num num 秒后打印一次文本输出然后退出，-t -s 60 组合使用，表示取 60 秒网络流量输出到终端
    -L num 打印的行数
-f 参数支持 tcpdump 的语法，可以使用各种过滤条件
```

界面操作

1. 界面信息

安装完 `iftop` 工具后，直接输入 `iftop` 命令即可显示网卡实时流量信息。在默认情况下，`iftop` 显示系统第一块网卡的流量信息，如果要显示指定网卡信息，可通过 `“-i”` 参数实现。执行 `“iftop -P -i eth0”` 命令，得到如下图所示的 `iftop` 的一个典型输出界面。

- 第一部分
  - iftop 输出中最上面的一行，此行信息是流量刻度，用于显示网卡带宽流量。
- 第二部分
  - 此部分为分割线中间的部分，其中又分别分为左、中、右三列。左列和中列，记录了哪些 IP 或主机正在和本机的网络进行连接。其中，中列的“=>”代表发送数据，“<=”代表接收数据，通过这个指示箭头可以很清晰地知道两个 IP 之间的通信情况。最右列又分为三小列，这些实时参数分别表示外部 IP 连接到本机 2 秒内、10 秒内和 40 秒内的平均流量值。
  - 另外，这个部分还有一个流量图形条，流量图形条是对流量大小的动态展示，以第一部分中的流量刻度为基准。通过这个流量图形条可以很方便地看出哪个 IP 的流量最大，进而迅速定位网络中可能出现的流量问题。
- 第三部分
  - 位于 iftop 输出的最下面，可以分为三行，其中，“TX”表示发送数据，“RX”表示接收数据，“TOTAL”表示发送和接收全部流量。与这三行对应的有三列，其中“cum”列表示从运行 iftop 到目前的发送、接收和总数据流量。“peak”列表示发送、接收以及总的流量峰值。“rates”列表示过去 2s、10s、40s 的平均流量值。



1. 交互操作

在 `iftop` 的实时监控界面中，还可以对输出结果进行交互式操作，用于对输出信息进行整理和过滤，在上图所示界面中，按键 `“h”` 即可进入交互选项界面，如下图所示。`iftop` 的交互功能和 `Linux` 下的 `top` 命令非常类似，交互参数主要分为 `4` 个部分，分别是一般参数、主机显示参数、端口显示参数和输出排序参数。相关参数的含义如下表所示。

```
1 | 参数        含义
```

参数	含义
P	通过此键可切换暂停/继续显示
h	通过此键可在交互参数界面/状态输出界面之间来回切换
b	通过此键可切换是否显示平均流量图形条
B	通过此键可切换显示2秒、10秒、40秒内的平均流量
T	通过此键可切换是否显示每个连接的总流量
j/k	按j键或k键可以向上或向下滚动屏幕显示当前的连接信息
l	通过此键可打开iftop输出过滤功能，比如输入要显示的IP，按回车后，屏幕就只显示与这个IP相关
L	通过此键可切换显示流量刻度范围，刻度不同，流量图形条会跟着变化
q	通过此键可退出iftop流量监控界面
n	通过此键可使iftop输出结果以IP或主机名的方式显示
s	通过此键可切换是否显示源主机信息
d	通过此键可切换是否显示远端目标主机信息
t	通过此键可切换iftop显示格式，连续按此键可依次显示：以两行显示发送接收流量、以一行显示发
N	通过此键可切换显示端口号/端口号对应服务名称
S	通过此键可切换是否显示本地源主机的端口信息
D	通过此键可切换是否显示远端目标主机的端口信息
p	通过此键可切换是否显示端口信息
1/2/3	根据最近 2 秒、10 秒、40 秒的平均网络流量排序
<	通过此键可根据左边的本地主机名或IP地址进行排序
>	通过此键可根据远端目标主机的主机名或IP地址进行排序
o	通过此键可切换是否固定显示当前的连接

使用示例

1. 显示网卡 eth0 的信息，主机通过 ip 显示

```
$ iftop -i eth0 -n
```

1. 显示端口号（添加 -P 参数，进入界面可通过 p 参数关闭）

```
$ iftop -i eth0 -n -P
```

1. 显示将输出以 byte 为单位显示网卡流量,默认是 bit

```
$ iftop -i eth0 -n -B
```

1. 显示流量进度条

```
## 进入界面后按下 L
$ iftop -i eth0 -n
```

1. 显示每个连接的总流量

```
## 进入界面后按下 T
$ iftop -i eth0 -n
```

1. 显示指定 ip 172.17.1.158 的流量

```
进入界面后按下 l 后,再输入 172.17.1.158 并回车)
$ iftop -i eth0 -n
```

实战

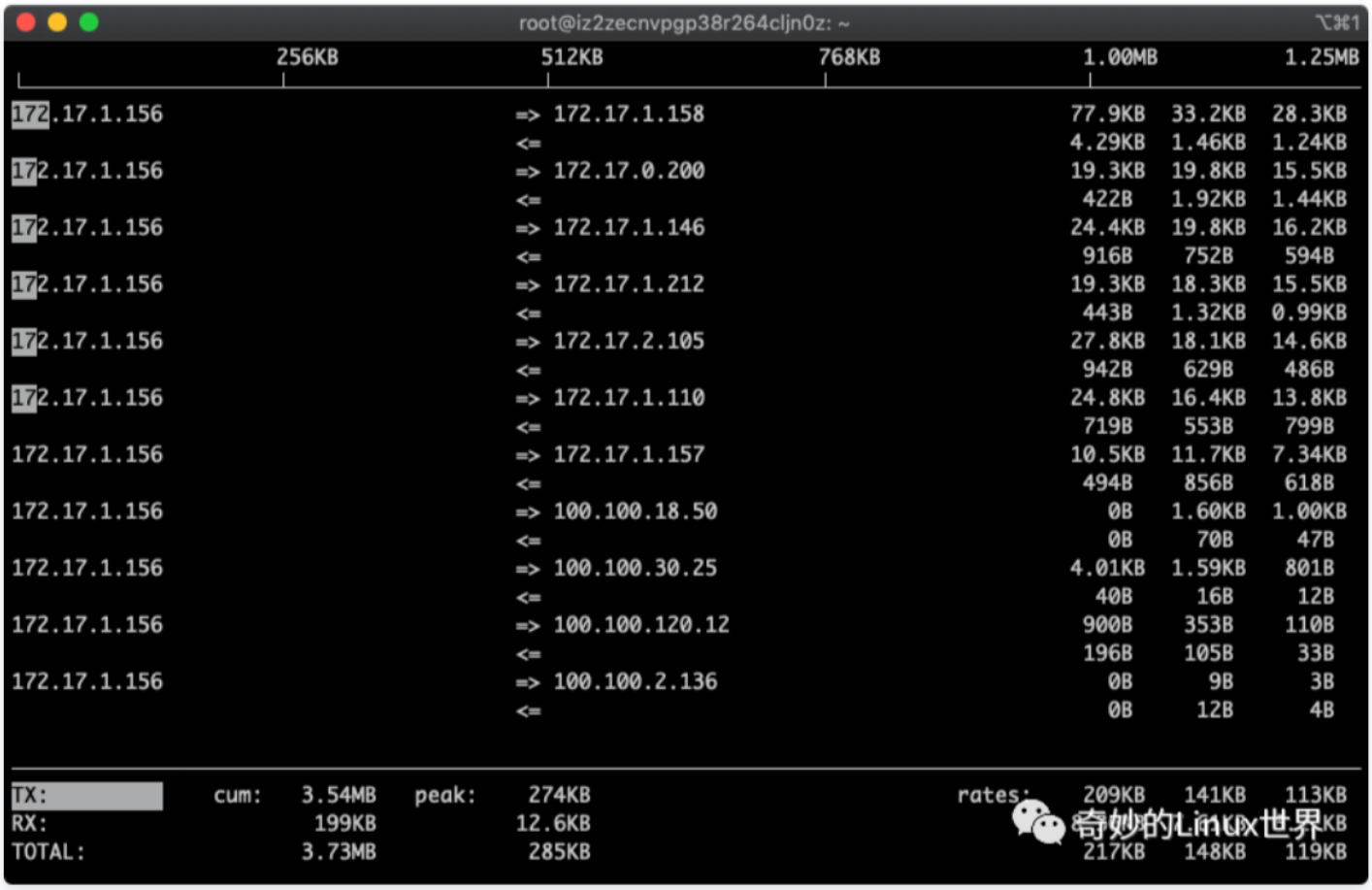
下面我们将通过找出最费流量的 IP 和端口号这一具体实例，来演示 iftop 强大的功能。

1. 进入界面

```
$ iftop -i eth0 -nNB -m 10M
```

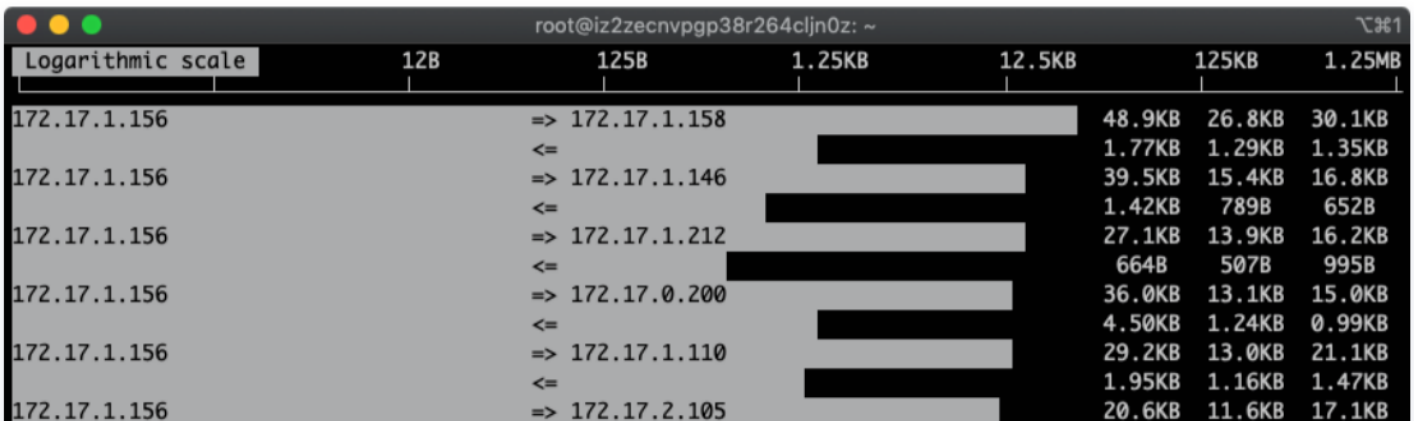
- -i 指定网卡，
- -n 代表主机通过ip显示不走DNS
- -N 只显示连接端口号，不显示端口对应的服务名称(不加会显示如ssh这样的服务名称，不便于排查)
- -B 指定显示单位为Kb，默认是bit，太小！
- -m 设置输出界面中最上面的流量刻度最大值，流量刻度分5个大段显示

进入后界面如下:



1. 按下 L 显示流量刻度

L 参数直接显示进度条，方便人类阅读。



```
                                <=                                    553B    725B   1.27KB
172.17.1.156                    => 172.17.1.157                      12.5KB  5.09KB  7.14KB
                                <=                                    946B    626B    547B
172.17.1.156                    => 100.100.18.50                        0B  1.60KB  1.20KB
                                <=                                      0B    70B     56B
172.17.1.156                    => 100.100.30.25                        0B    999B    697B
                                <=                                      0B     17B      9B
172.17.1.156                    => 100.100.120.13                       0B    173B     86B
                                <=                                      0B     65B     33B
172.17.1.156                    => 100.100.18.22                        0B     15B      5B
                                <=                                      0B     19B      6B

TX:             cum:   13.0MB   peak:   283KB                  rates:  214KB  102KB  126KB
RX:                     752KB           16.3KB                         [illegible]
TOTAL:                 13.7MB           299KB                          226KB  108KB  133KB
```


1. 按下 T 显示总量

有个总数统计，看着方便!

```
root@iz2zecnvpgp38r264cljn0z: ~                                              ⌥⌘1
                1B              12B             125B            1.25KB          12.5KB          125KB           1.25MB
172.17.1.156                    => 172.17.1.110                      3.78MB  164KB   42.4KB  22.1KB
                                <=                                    143KB  2.46KB   994B   1.03KB
172.17.1.156                    => 172.17.1.158                      6.14MB  46.4KB  30.4KB  30.8KB
                                <=                                    273KB  0.98KB  1.23KB  1.34KB
172.17.1.156                    => 172.17.1.146                      3.53MB  35.0KB  19.4KB  17.6KB
                                <=                                    134KB  1.32KB   820B    701B
172.17.1.156                    => 172.17.1.212                      3.43MB  34.4KB  16.9KB  18.3KB
                                <=                                    240KB  1.45KB   853B   1.50KB
172.17.1.156                    => 172.17.0.200                      3.17MB  21.9KB  14.7KB  16.2KB
                                <=                                    219KB   418B    432B   1.11KB
172.17.1.156                    => 172.17.2.105                      3.26MB  20.9KB  13.8KB  15.3KB
                                <=                                    151KB   344B    350B    469B
172.17.1.156                    => 172.17.1.157                      1.50MB  11.3KB  6.05KB  7.80KB
                                <=                                    116KB   640B    464B    568B
172.17.1.156                    => 100.100.120.12                    5.07KB   865B    173B    130B
                                <=                                   1.91KB   326B     65B     49B
172.17.1.156                    => 100.100.30.25                      173KB     0B    192B    766B
                                <=                                   2.43KB     0B      8B     14B
172.17.1.156                    => 100.100.2.136                      244B    45B     9B      6B
                                <=                                    365B    61B     12B     9B
172.17.1.156                    => 100.100.18.50                     31.9KB     0B      0B    816B
                                <=                                   1.48KB     0B      0B     38B

TX:             cum:   25.6MB   peak:   335KB                  rates:  335KB  144KB  130KB
RX:                    1.38MB           12.9KB                         [illegible]
TOTAL:                 27.0MB           343KB                          343KB  149KB  137KB
```


1. 按下 3，根据最近 40s 统计排序

用平均值来统计最权威点

```
root@iz2zecnvpgp38r264cljn0z: ~                                              ⌥⌘1
Sort by col 3 1B                12B             125B            1.25KB          12.5KB          125KB           1.25MB
172.17.1.156                    => 172.17.1.158                      8.30MB  37.2KB  34.7KB  33.7KB
                                <=                                    370KB  2.09KB  1.83KB  1.48KB
172.17.1.156                    => 172.17.1.146                      4.82MB  19.1KB  21.3KB  20.5KB
                                <=                                    207KB   742B    963B   1.23KB
172.17.1.156                    => 172.17.1.212                      4.67MB  30.3KB  19.0KB  20.2KB
                                <=                                    305KB  1.50KB  1000B   1.08KB
172.17.1.156                    => 172.17.1.110                      5.11MB  26.0KB  16.9KB  16.9KB
                                <=                                    202KB  1.30KB   626B    910B
172.17.1.156                    => 172.17.2.105                      4.37MB  21.9KB  17.7KB  17.1KB
                                <=                                    189KB   440B    632B    550B
```

```
172.17.1.156                => 172.17.0.200          4.25MB  21.5KB  16.4KB  16.7KB
                            <=                        250KB   440B    446B    501B
172.17.1.156                => 172.17.1.157          2.07MB  9.37KB  7.76KB  8.57KB
                            <=                        158KB   588B    668B    656B
172.17.1.156                => 100.100.18.50         48.2KB    0B    1.61KB  1.21KB
                            <=                       2.39KB    0B     82B     61B
172.17.1.156                => 100.100.30.25          250KB  4.41KB  1.71KB   929B
                            <=                       3.34KB   40B     20B     12B
172.17.1.156                => 100.100.18.22         1.34KB    0B      0B     34B
                            <=                       7.22KB    0B      0B    185B
172.17.1.156                => 100.100.120.13        3.38KB    0B      0B     86B
                            <=                       1.28KB    0B      0B     33B

TX:             cum:   34.7MB   peak:    290KB   rates:    170KB  137KB  136KB
RX:                    1.81MB            11.7KB             [illegible]KB
TOTAL:                 36.5MB            300KB              177KB  144KB  143KB
```

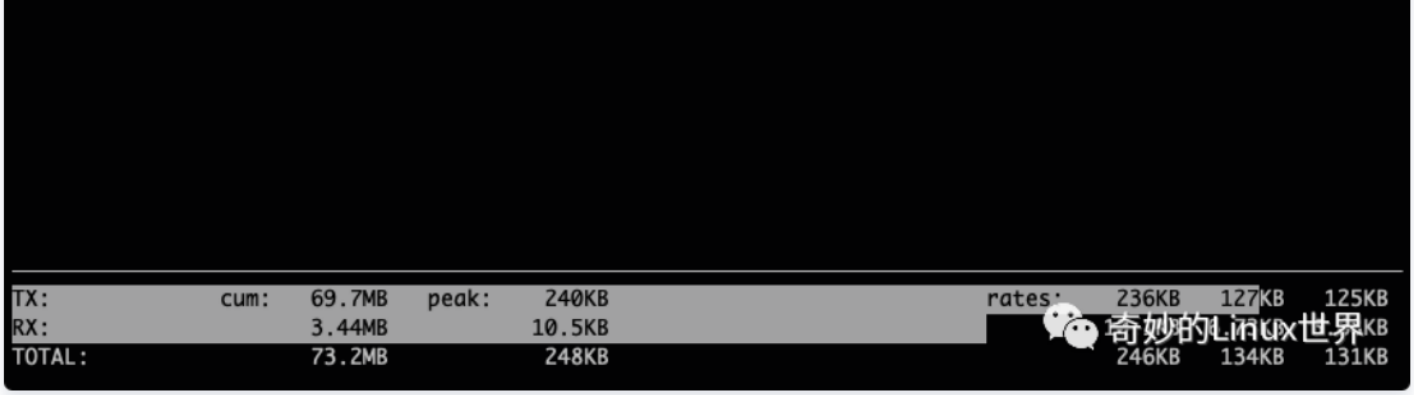

1. 按下 t，发送和接受合成一行

```
root@iz2zecnvpgp38r264cljn0z: ~                                          ⌥⌘1
One line per host          12B          125B         1.25KB        12.5KB          125KB         1.25MB
172.17.1.156                      <=> 172.17.1.158                 11.0MB  25.6KB  28.2KB  31.9KB
172.17.1.156                      <=> 172.17.2.105                 5.81MB  17.1KB  13.3KB  18.2KB
172.17.1.156                      <=> 172.17.1.146                 6.34MB  16.0KB  16.1KB  18.0KB
172.17.1.156                      <=> 172.17.1.212                 6.23MB  18.8KB  15.3KB  16.8KB
172.17.1.156                      <=> 172.17.0.200                 5.65MB  26.7KB  12.8KB  15.6KB
172.17.1.156                      <=> 172.17.1.110                 5.33MB  14.4KB  12.7KB  15.4KB
172.17.1.156                      <=> 172.17.1.157                 2.80MB  6.80KB  5.66KB  7.81KB
172.17.1.156                      <=> 100.100.18.50                50.3KB    0B    1.68KB  1.26KB
172.17.1.156                      <=> 100.100.30.25                 328KB  4.75KB  1.94KB  0.99KB
172.17.1.156                      <=> 100.100.120.13               4.65KB    0B      0B     119B
172.17.1.156                      <=> 100.100.120.12               4.49KB    0B     238B    115B
172.17.1.156                      <=> 100.100.2.136                 212B     0B      0B      5B
172.17.1.156                      <=> 100.100.5.1                   152B     76B     15B     4B
172.17.1.156                      <=> 10.143.0.45                    76B     0B      8B      2B

TX:             cum:   43.5MB   peak:    299KB   rates:    125KB  103KB  121KB
RX:                    2.22MB            15.0KB             [illegible]KB
TOTAL:                 45.7MB            308KB              130KB  108KB  126KB
```


1. 多按几次 B，查看最近 2s、10s、40s 的统计

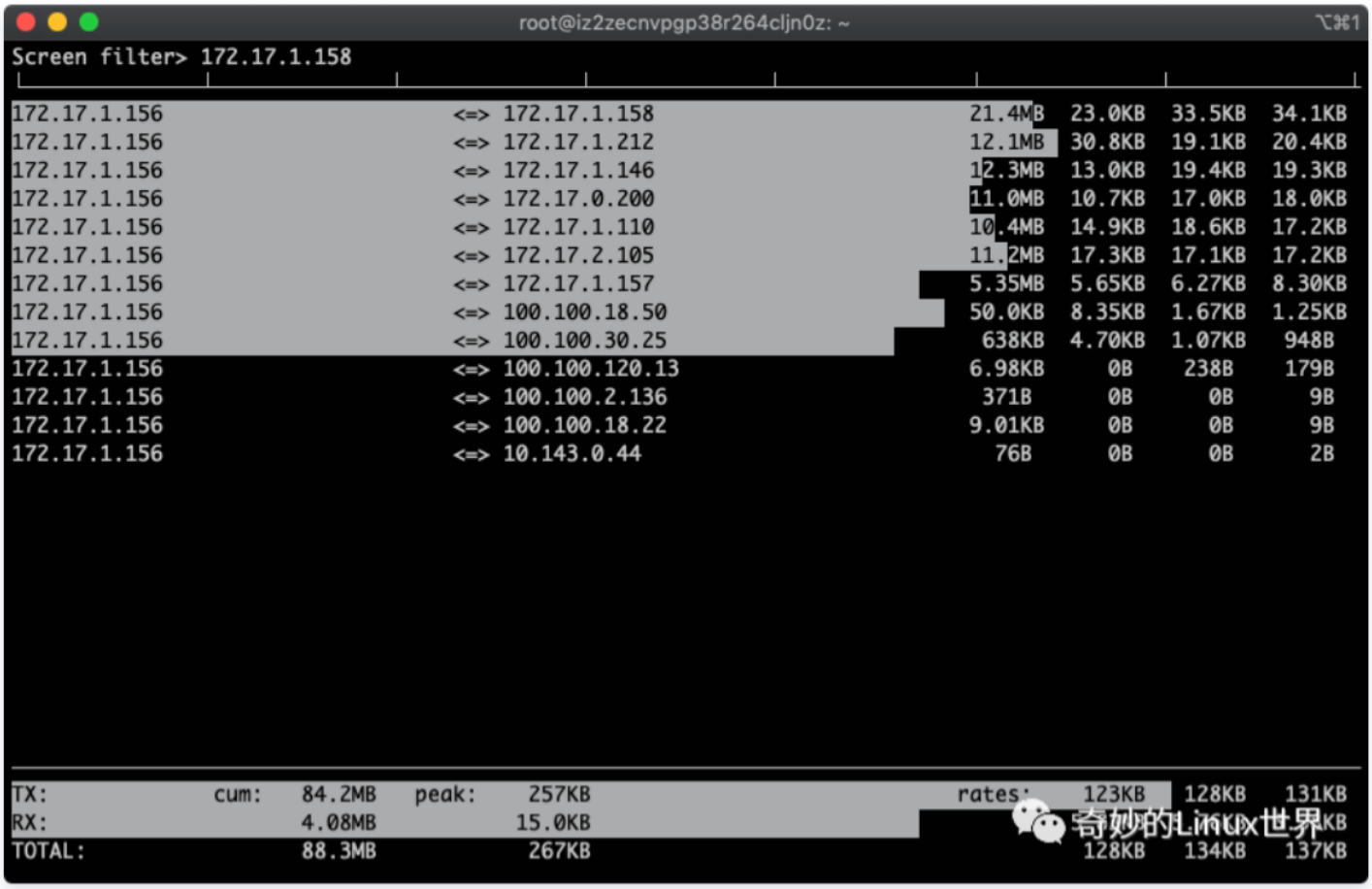
```
root@iz2zecnvpgp38r264cljn0z: ~                                          ⌥⌘1
Bars show 2s average       12B          125B         1.25KB        12.5KB          125KB         1.25MB
172.17.1.156                      <=> 172.17.1.158                 17.7MB  51.0KB  30.4KB  32.3KB
172.17.1.156                      <=> 172.17.1.146                 10.2MB  42.9KB  18.5KB  18.5KB
172.17.1.156                      <=> 172.17.2.105                 9.33MB  40.9KB  22.4KB  18.5KB
172.17.1.156                      <=> 172.17.1.212                 10.1MB  29.3KB  16.3KB  17.5KB
172.17.1.156                      <=> 172.17.0.200                 9.08MB  39.2KB  15.9KB  17.2KB
172.17.1.156                      <=> 172.17.1.110                 8.64MB  26.2KB  16.5KB  15.9KB
172.17.1.156                      <=> 172.17.1.157                 4.52MB  13.0KB  10.9KB  8.66KB
172.17.1.156                      <=> 100.100.18.50                50.3KB    0B    1.67KB  1.26KB
172.17.1.156                      <=> 100.100.30.25                 529KB  3.95KB   809B   1.10KB
172.17.1.156                      <=> 100.100.120.12               6.98KB    0B     238B    179B
```



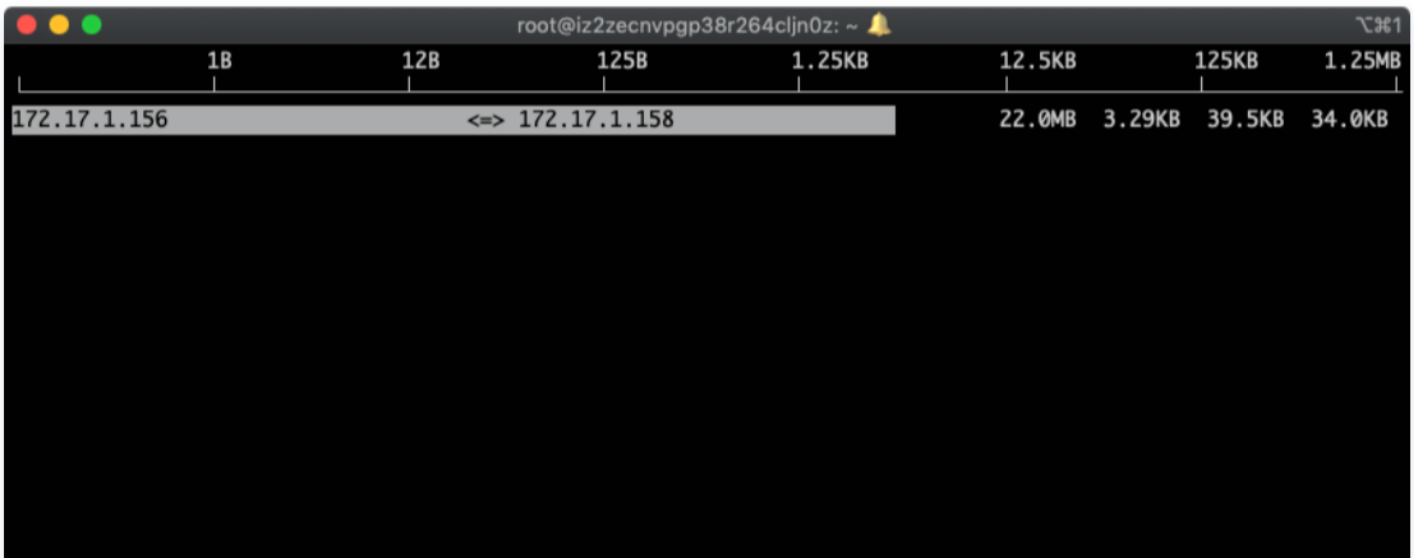
没错，图中的 172.17.1.158 就是我们找到的流量用得最多的 IP

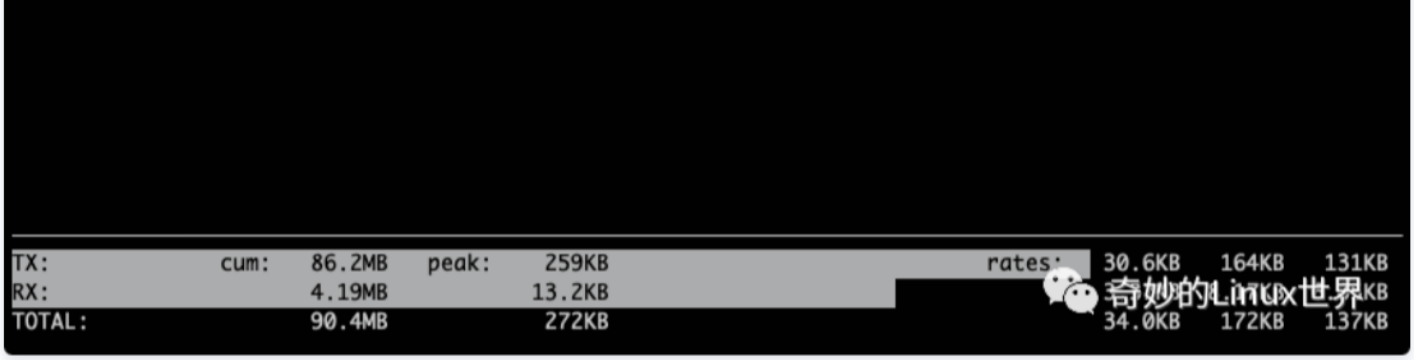
1. 筛选指定 IP 172.17.1.158

按下 I, 输入172.17.1.158，出现如下



回车后生效

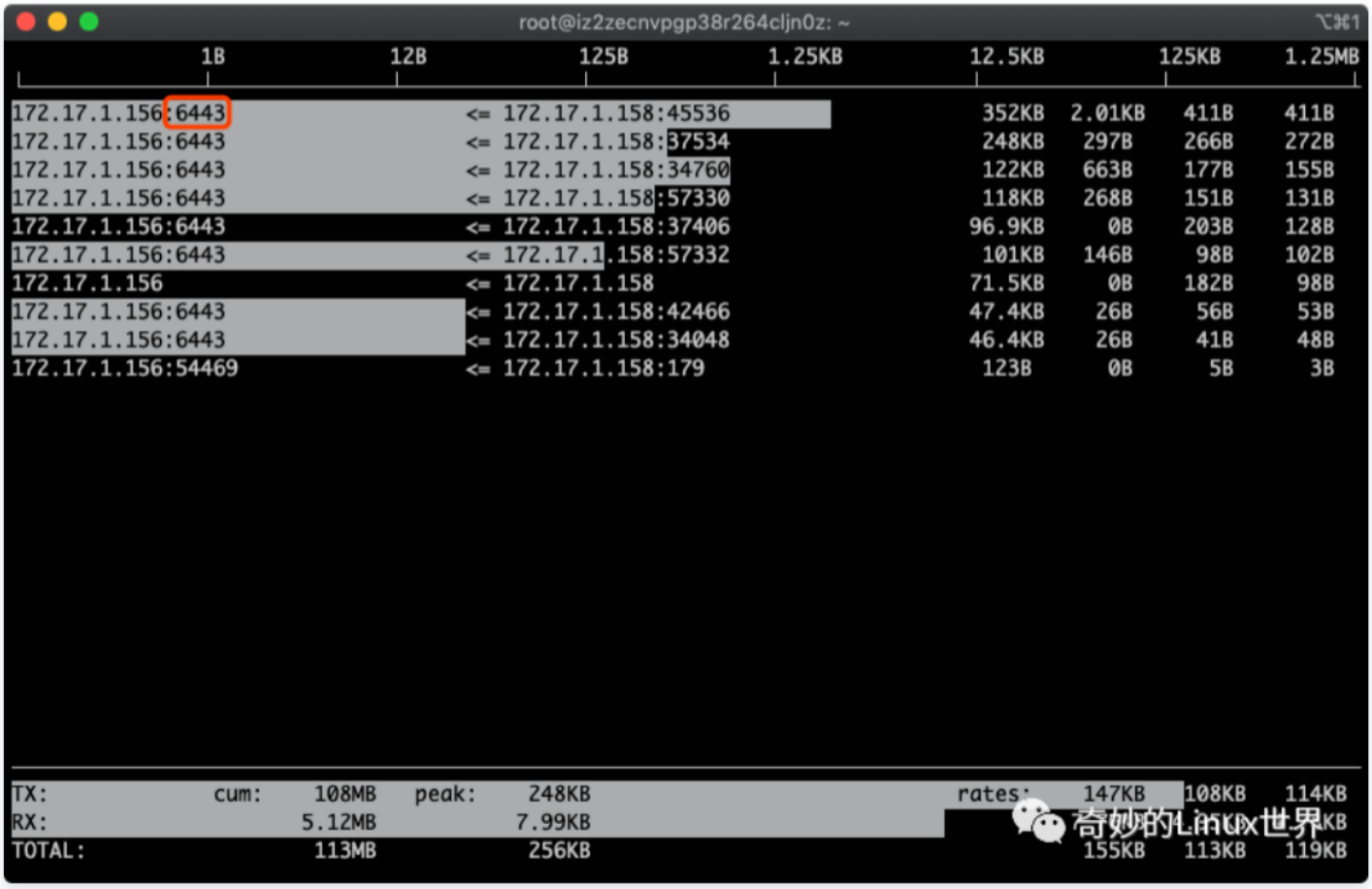




这下就只看到这个 IP 的流量监控了

1. 找到这个 IP 哪个端口流量用得最多

按下 p, 根据端口号显示



到这里，我们就学会了如何找出流量用得最多的 IP 和端口号。