linux 下网络流量实时监控工具大全

在工作中发现，经常因为业务的原因，需要即时了解某台服务器网卡的流量，虽然公司也部署了 cacti 软件，但 cacti 是五分钟统计的，没有即时性，并且有时候打开监控页面不方便，个人喜欢随手在某台服务器上输入一个命令，查看网卡即时流量。百度了一下，发现有这么几种方法，现对此类软件进行了一个总结。

一、iptraf 软件

rhel 的 iso 里有包含，我公司的系统，并没有默认安装，它功能强大，可以按照协议，网卡等进行分析。

1.1 iptraf 安装

源码安装

```
wget ftp://iptraf.seul.org/pub/iptraf/iptraf-3.0.0.tar.gz
tar zxvf iptraf-3.0.0.tar.gz
cd iptraf-3.0.0
./Setup
```

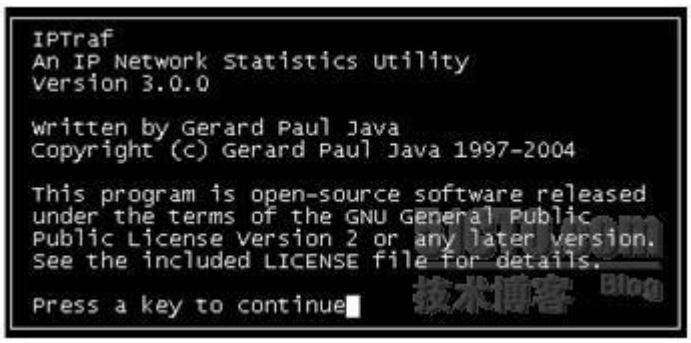
yum 方式安装

```
yum install -y iptraf
```

1.2 iptraf 使用

```
[root@kaifa opt]# iptraf
```

按任意键继续



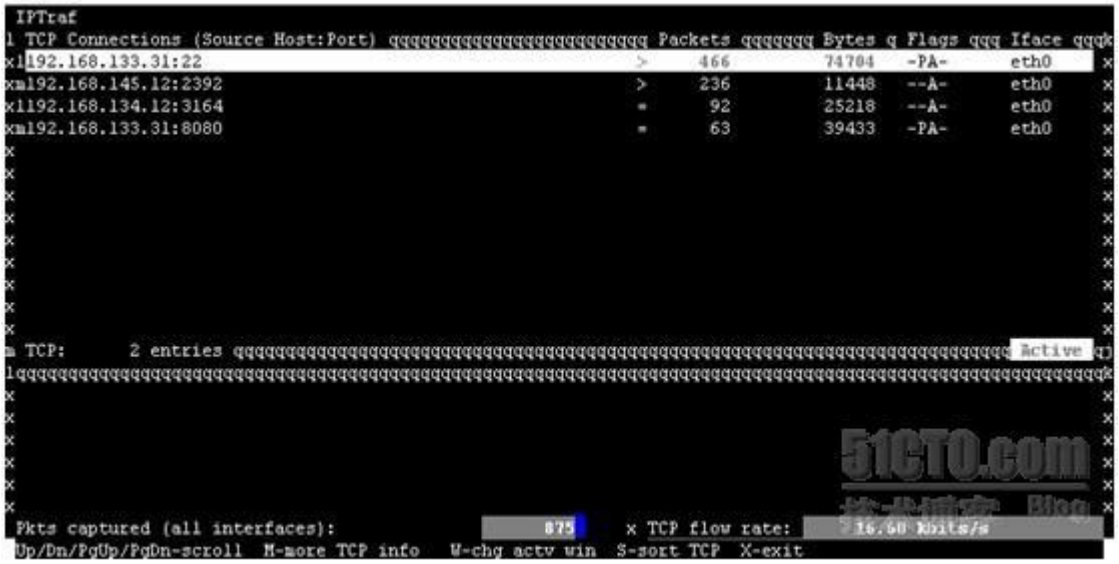
第一项：IP 流量监控

第二项：常规查看网卡流量状态。只查看各网卡的总流量

第三项：详细查看网卡流量状态。比如按 TCP，UDP，ARP 等协议查看

选 all interfaces，查看所有网卡接口

界面分上下两部分，上部分可详细显示哪个与之相连的 IP，发了多少包，即时流量是多少，下部分，可以显示 udp 等信息。



按 Q 退出监控界面，然后选择“Exit”退出 iptraf。

第二、nload 软件

rhel iso 不带，需要去第三方网站下载源码包。功能相对单一，只能查看总的流量，不能像上款的 iptraf 那样，可看总流量，可细分查看其它协议点的流量。nload 默认分为上下两块，每部分都有当前流量（Curr），平均流量(Min)，最大流量(Max)，总流量(Ttl)，

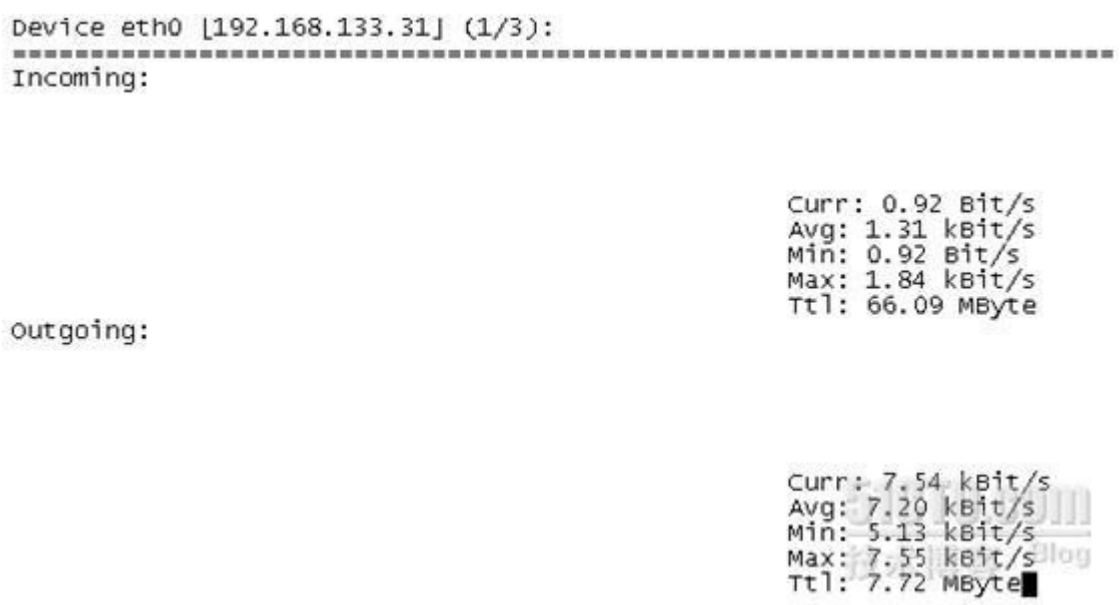
看起来还是比较直观的。

2.1 nload 安装

```
wget http://www.roland-riegel.de/nload/nload-0.7.2.tar.gz
tar zxvf nload-0.7.2.tar.gz
cd nload-0.7.2
./configure &ndash;prefix=/usr/local/nload
make
make install
```

2.2 nload 使用

```
[root@kaifa opt]# /usr/local/nload/bin/nload eth0
```



第三、ifstat 软件

rhel iso 不自带，虽然到第三方网站下载源码包，编译安装。这个软件还有 windows 版，它可以报告网卡接口流量状态，能查看网卡的流出和流入的字节，是按每秒生产一次数据。

3.1 ifstat 安装

```
wget http://gael.roualland.free.fr/ifstat/ifstat-1.1.tar.gz
tar -zxvf ifstat-1.1.tar.gz
cd ifstat-1.1
./configure   --prefix=/usr/local/ifstat
make
```

make install

3.2 ifstat 使用

```
[root@kaifa ifstat-1.1]# /usr/local/ifstat/bin/ifstat
       eth0
 KB/s in  KB/s out
    0.12      0.24
    0.21      0.12
    0.15      0.12
    0.39      0.12
    0.06      0.12
    0.06      0.12
    0.06      0.12
```


3.3 相关参数

-l　　监测环路网络接口（lo）。缺省情况下，ifstat 监测活动的所有非环路网络接口。经使用发现，加上-l 参数能监测所有的网络接口的信息，而不是只监测 lo 的接口信息，也就是说，加上-l 参数比不加-l 参数会多一个 lo 接口的状态信息。

-a　监测能检测到的所有网络接口的状态信息。使用发现，比加上-l 参数还多一个 plip0 的接口信息，搜索一下发现这是并口（网络设备中有一 个叫 PLIP (Parallel Line Internet Protocol). 它提供了并口...）

-z　隐藏流量是无的接口，例如那些接口虽然启动了但是未用的

-i　指定要监测的接口,后面跟网络接口名

-s　等于加-d snmp:[comm@][#]host[/nn]] 参数，通过 SNMP 查询一个远程主机

-h 显示简短的帮助信息

-n 关闭显示周期性出现的头部信息（也就是说，不加-n 参数运行 ifstat 时最顶部会出现网络接口的名称，当一屏显示不下时，会再一次出现接口的名称，提示 我们显示的流量信息具体是哪个网络接口的。加上-n 参数把周期性的显示接口名称关闭，只显示一次）

-t 在每一行的开头加一个时间 戳（能告诉我们具体的时间）

-T 报告所有监测接口的全部带宽（最后一列有个 total，显示所有的接口的 in 流量和所有接口的 out 流量，简单的把所有接口的 in 流量相加,out 流量相 加）

-w　用指定的列宽，而不是为了适应接口名称的长度而去自动放大列宽

-W 如果内容比终端窗口的宽度还要宽就自动换行

-S 在同一行保持状态更新（不滚动不换行）注：如果不喜欢屏幕滚动则此项非常方便，与 bmon 的显示方式类似

-b 用 kbits/s 显示带宽而不是 kbytes/s(bit 和 byte 有何区别应该都知道吧)

-q 安静模式，警告信息不出现

-v 显示版本信息

-d 指定一个驱动来收集状态信息

第四、sar 软件

这个工具 RHEL iso 里包含，它是一个优秀的性能监控工具，不仅仅监控网络，它可以显示 cpu，运行队列，磁盘 i/o，分页(交换区)，内存，CPU 中断等性能数据。Sar 命令在 sysstat 包中，我公司系统没有安装此包，所以要安装它，才有 sar 命令。

4.1 sar 安装

Yum install sysstat

4.2 sar 使用

```
[root@kaifa ifstat-1.1]# sar -n DEV 5 2
Linux 2.6.18-164.el5 (kaifa)    03/14/2012

11:02:21 AM     IFACE   rxpck/s   txpck/s   rxbyt/s   txbyt/s   rxcmp/s   txcmp/s  rxmcst/s
11:02:26 AM        lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
11:02:26 AM      eth0      0.20      0.20     12.00     27.60      0.00      0.00      0.00
11:02:26 AM      sit0      0.00      0.00      0.00      0.00      0.00      0.00      0.00

11:02:26 AM     IFACE   rxpck/s   txpck/s   rxbyt/s   txbyt/s   rxcmp/s   txcmp/s  rxmcst/s
11:02:31 AM        lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
11:02:31 AM      eth0      1.40      0.80     84.00    159.20      0.00      0.00      0.00
11:02:31 AM      sit0      0.00      0.00      0.00      0.00      0.00      0.00      0.00

Average:        IFACE   rxpck/s   txpck/s   rxbyt/s   txbyt/s   rxcmp/s   txcmp/s  rxmcst/s
Average:           lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
Average:         eth0      0.80      0.50     48.00     93.40      0.00      0.00      0.00
Average:         sit0      0.00      0.00      0.00      0.00      0.00      0.00      0.00
```

命令后面 5 2 意思是：每 5 秒钟取一次值，取 2 次。

IFACE：LAN 接口

rxpck/s：每秒钟接收的数据包

txpck/s：每秒钟发送的数据包

rxbyt/s：每秒钟接收的字节数

txbyt/s：每秒钟发送的字节数

rxcmp/s：每秒钟接收的压缩数据包

txcmp/s：每秒钟发送的压缩数据包

rxmcst/s：每秒钟接收的多播数据包

第五、iftop 软件

RHEL iso 不自带，iftop 可以用来监控网卡的实时流量（可以指定网段）、反向解析 IP、显示端口信息等

5.1 iftop 安装

rhel6.0 以上系统安装,需要 libpcap-devel-1.4.0-1

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

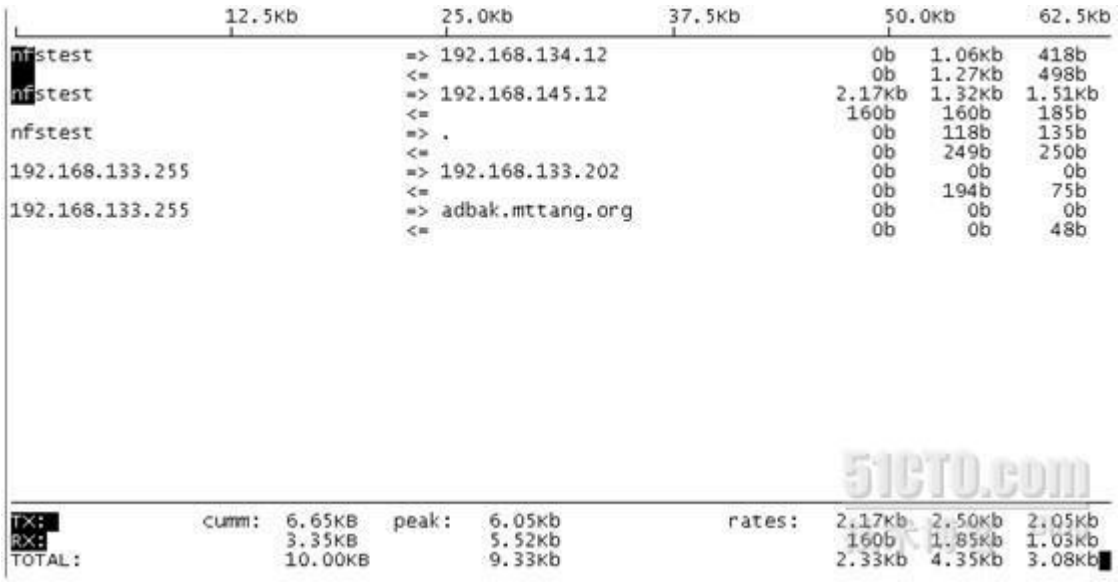
./configure –prefix=/usr/local/iftop

make

make install

5.2 iftop 使用

[root@nfstest opt]# /usr/local/iftop/sbin/iftop



5.3、界面相关说明

界面上面显示的是类似刻度尺的刻度范围，为显示流量图形的长条作标尺用的。

中间的<= =>这两个左右箭头，表示的是流量的方向。

TX：发送流量

RX：接收流量

TOTAL：总流量

Cumm：运行 iftop 到目前时间的总流量

peak：流量峰值

rates：分别表示过去 2s 10s 40s 的平均流量

5.4、相关参数

常用的参数

-i 设定监测的网卡，如：# iftop -i eth1

-B 以 bytes 为单位显示流量(默认是 bits)，如：# iftop -B

-n 使 host 信息默认直接都显示 IP，如：# iftop -n

-N 使端口信息默认直接都显示端口号，如: # iftop -N

-F 显示特定网段的进出流量，如# iftop -F 10.10.1.0/24 或# iftop -F 10.10.1.0/255.255.255.0

-h（display this message），帮助，显示参数信息

-p 使用这个参数后，中间的列表显示的本地主机信息，出现了本机以外的 IP 信息;

-b 使流量图形条默认就显示;

-f 这个暂时还不太会用，过滤计算包用的;

-P 使 host 信息及端口信息默认就都显示;

-m 设置界面最上边的刻度的最大值，刻度分五个大段显示，例：# iftop -m 100M