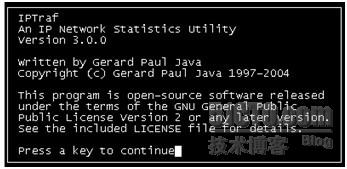
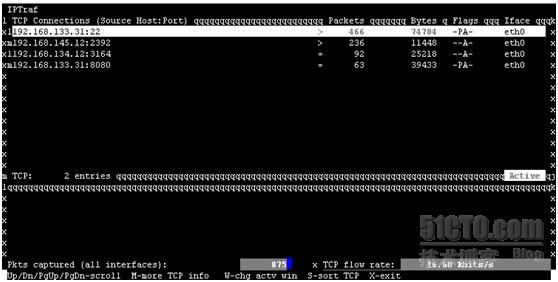
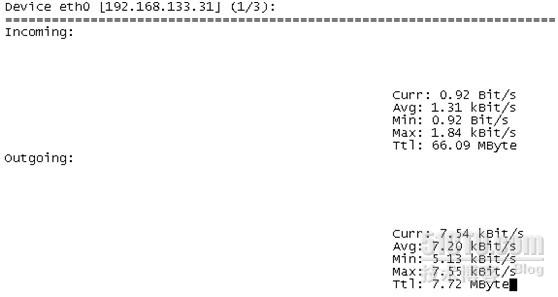
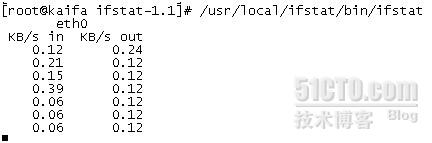
**inux下网络流量实时监控工具  
大全**

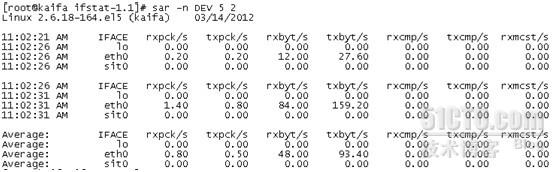
    在工作中发现，经常因为业务的原因，需要即时了解某台服务器网卡的流量，虽然公司也部署了cacti软件，但cacti是五分钟统计的，没有即时性，并且有时候打开监控页面不方便，个人喜欢随手在某台服务器上输入一个命令，查看网卡即时流量。百度了一下，发现有这么几种方法，现对此类软件进行了一个总结。  
 **一、iptraf软件**  
   rhel的iso里有包含，我公司的系统，并没有默认安装，它功能强大，可以按照协议，网卡等进行分析。  
1.1 iptraf安装  
源码安装  
wget ftp://iptraf.seul.org/pub/iptraf/iptraf-3.0.0.tar.gz  
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  
[](http://img1.51cto.com/attachment/201203/134124722.jpg)  
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  
[](http://img1.51cto.com/attachment/201203/134140353.jpg)  
选all interfaces，查看所有网卡接口  
 [](http://img1.51cto.com/attachment/201203/134156623.jpg)

   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。  
[](http://img1.51cto.com/attachment/201203/134218744.jpg)

按Q退出监控界面，然后选择&ldquo;Exit&rdquo;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  
   
[](http://img1.51cto.com/attachment/201203/134258487.jpg)

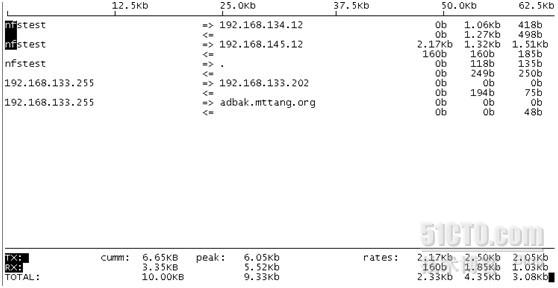
**第三、ifstat软件**  
    rhel iso不自带，虽然到第三方网站下载源码包，编译安装。这个软件还有windows版，它可以报告网卡接口流量状态，能查看网卡的流出和流入的字节，是按每秒生产一次数据。  
3.1 ifstat安装

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  
 [](http://img1.51cto.com/attachment/201203/134450854.jpg)

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  
 [](http://img1.51cto.com/attachment/201203/134336395.jpg)

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 &ndash;prefix=/usr/local/iftop  
make  
make install  
5.2 iftop使用  
[root@nfstest opt]# /usr/local/iftop/sbin/iftop  
 [](http://img1.51cto.com/attachment/201203/134356475.jpg)

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

本文出自 “[系统网络运维](http://369369.blog.51cto.com/)” 博客，请务必保留此出处<http://369369.blog.51cto.com/319630/805726>