



The Sysadmin's Toolbox: iftop

Sep 25, 2012 By [Kyle Rankin \(/users/kyle-rankin/\)](/users/kyle-rankin/)



in

A screenshot of the iftop command output. It shows a table with columns for interface, local and remote traffic in MB/s, and a list of remote IP addresses. The first few rows show high traffic from specific IP addresses, with the first row having a green bar next to it. The bottom of the screen shows summary statistics for the interface.

Who's using up all the bandwidth, and what are they doing? Use iftop to find out.

Longtime system administrators often take tools for granted that they've used for years and assume everyone else has heard of them. Of course, new sysadmins join the field every day, and even seasoned sysadmins don't all use the same tools. With that in

mind, I decided to write a few columns where I highlight some common-but-easy-to-overlook tools that make life as a sysadmin (and really, any Linux user) easier. My last article covered sar, a tool you can use to collect and view system metrics over time. This time, I discuss a program that's handy for viewing real-time network performance data: iftop.

Anyone who's had to use a network at a conference has experienced what happens when there just isn't enough network bandwidth to go around. While you are trying to check your e-mail, other people are streaming movies and TV shows, downloading distribution install disks, using p2p networks, upgrading their distributions or watching cat videos on YouTube. Although it's certainly frustrating to try to use one of those networks, imagine how frustrating it would be to be the admin in charge of

that network. Whether you run a conference network, a local office network or even a Web server at your house, it can be really nice to know what is using up all of your bandwidth.

iftop is a Linux command-line program designed to give you live statistics about what network connections use the most bandwidth in a nice graphical form. As you may realize from the name, iftop borrows a lot of ideas from the always-useful load troubleshooting tool top. Like top, iftop updates automatically every few seconds, and like top, by default, it sorts the output you see by what's using the most resources. Where top is concerned with processes and how much CPU and RAM they use, iftop is concerned with network connections and how much upload and download bandwidth they use.

Even though iftop is packaged for both Red Hat- and Debian-based distributions, it's probably not installed by default, so you will need to install the package of the same name. In the case of Red Hat-based distributions, you might have to pull it down from a third-party repository. Once it's installed, the simplest way to get started is just to run iftop as the root user. iftop will locate the first interface it can use and start listening in on the traffic and display output similar to what you see in Figure 1. To close the program, press q to quit just like with top.

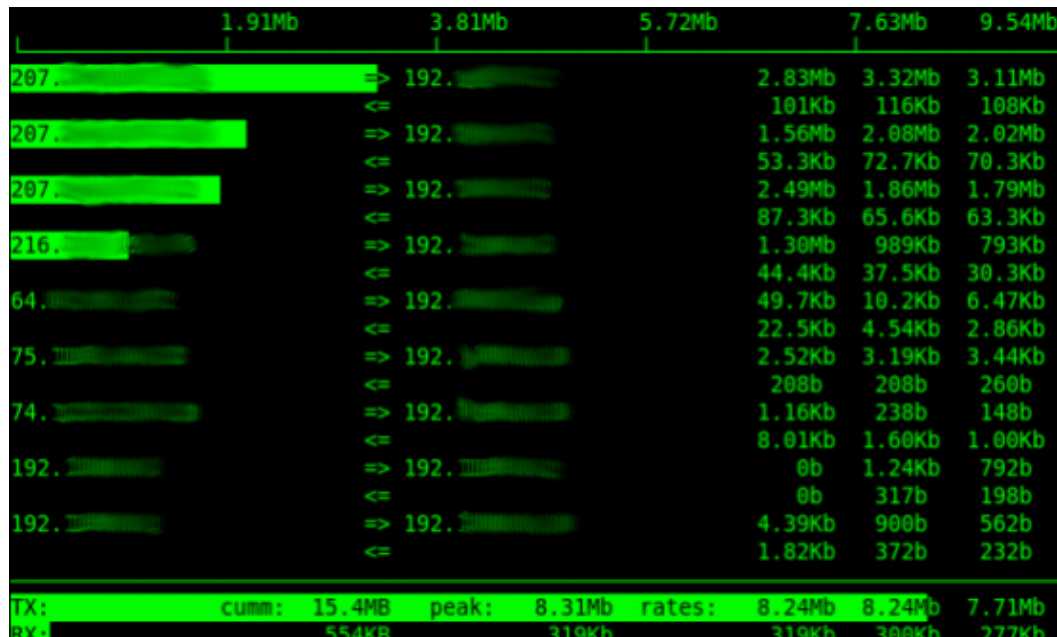




Figure 1. iftop output—the IPs have been smudged to protect the innocent.

At the very top of the screen is a scale that goes along with the bar graph iftop might display with each connection. The next rows of output correspond to each network connection between a pair of hosts. In between the two hosts are arrows that let you know the direction the traffic is flowing. The final three columns provide average bandwidth for each connection during the last 2, 10 and 40 seconds, respectively. So for instance, the very top connection in Figure 1 has averaged around 2.83Mb during the last 2 seconds, 3.32Mb during the last 10 seconds and 3.11Mb during the last 40 seconds. Underneath all the transmit and receive columns at the bottom of the screen are a series of statistics for overall transmitted and received traffic (TX and RX, respectively) including 2-, 10- and 40-second averages for both those and, finally, the totals for the interface.

Note: if you have a server with multiple interfaces, you may want iftop to monitor a different interface from the default. Just add `-i` followed by the interface to monitor when you launch iftop. For instance, to monitor eth2, I would type `iftop -i eth2`.

Disable DNS Lookups

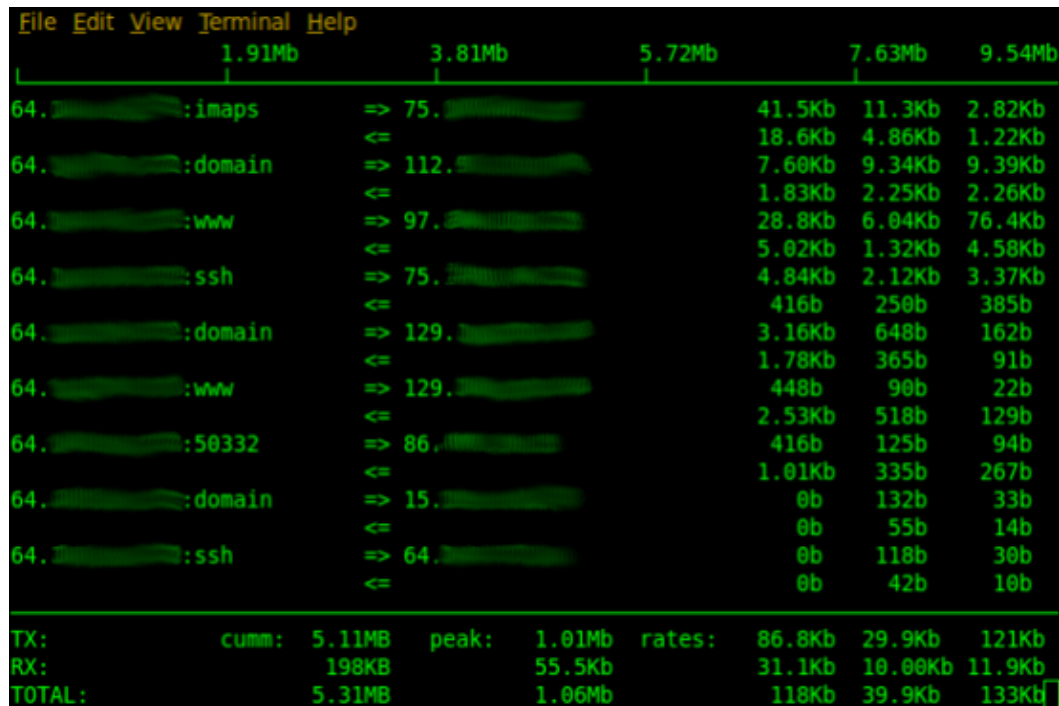
By default, when you run iftop, it will try to translate all of the IP addresses into hostnames. Sometimes this can be useful if you are diagnosing issues on a local network; however, like with a lot of other network diagnostics tools, resolving all of those IPs can slow down the program and also may contribute to the traffic you see in the output. The solution is to run iftop with the `-n` argument, so it just shows you IP addresses for everything (you always can run a DNS query against an IP you are interested in, in another window). Alternatively, if you already have iftop running, you can press `n` to disable DNS lookups.

Show Port Data

When you run iftop on a server that might serve multiple purposes, it can be handy to know whether all of that upstream traffic is accessing your Web server, your mail server or something else. Alternatively, if you are trying to figure out what's using up all of your download bandwidth, it can be handy to see whether the top connections

are Web connections or some rsync job you have running. To figure all of this out, iftop allows you to toggle the port display on and off. Press the p key while iftop is running, and it will display the ports used for both the source and destination IP for all traffic.

The one big downside to showing both the source and destination ports used for a connection is that you'll find in many cases you are concerned only with one or the other. For instance, if you are running a Web server, you may notice that a lot of traffic is going to your Web port (labeled www in iftop), but all of the ports used by IPs accessing your Web server use all sorts of high ports. In that case, you can press either S or D to toggle the display of either source or destination ports, respectively. Figure 2 shows an example of iftop output where I've chosen to display only the source ports.



The screenshot shows the iftop terminal interface. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. Below it, a header row shows cumulative traffic: 1.91Mb, 3.81Mb, 5.72Mb, 7.63Mb, and 9.54Mb. The main table lists connections with source IP, source port, destination IP, and traffic rates. Source ports are highlighted in green. At the bottom, summary statistics for TX, RX, and TOTAL are shown.

	1.91Mb	3.81Mb	5.72Mb	7.63Mb	9.54Mb
64.100.100.100:imaps	=> 75.100.100.100		41.5Kb	11.3Kb	2.82Kb
			18.6Kb	4.86Kb	1.22Kb
64.100.100.100:domain	=> 112.100.100.100		7.60Kb	9.34Kb	9.39Kb
			1.83Kb	2.25Kb	2.26Kb
64.100.100.100:www	=> 97.100.100.100		28.8Kb	6.04Kb	76.4Kb
			5.02Kb	1.32Kb	4.58Kb
64.100.100.100:ssh	=> 75.100.100.100		4.84Kb	2.12Kb	3.37Kb
			416b	250b	385b
64.100.100.100:domain	=> 129.100.100.100		3.16Kb	648b	162b
			1.78Kb	365b	91b
64.100.100.100:www	=> 129.100.100.100		448b	90b	22b
			2.53Kb	518b	129b
64.100.100.100:50332	=> 86.100.100.100		416b	125b	94b
			1.01Kb	335b	267b
64.100.100.100:domain	=> 15.100.100.100		0b	132b	33b
			0b	55b	14b
64.100.100.100:ssh	=> 64.100.100.100		0b	118b	30b
			0b	42b	10b
<hr/>					
TX:	cumm: 5.11MB	peak: 1.01Mb	rates: 86.8Kb	29.9Kb	121Kb
RX:	198KB	55.5Kb	31.1Kb	10.00Kb	11.9Kb
TOTAL:	5.31MB	1.06Mb	118Kb	39.9Kb	133Kb

Figure 2. iftop with only the source ports displayed.

For me, the really great thing about iftop is that it's a relatively simple command-line tool. It's true that a number of other programs exist that can provide fancy

Web-based graphs of your network traffic, and I think those are great for trending network data just like they are for trending system load and other metrics. What I like about iftop is the same thing I like about top—when there's a problem, you can get instant real-time data about your system that updates as the situation progresses.

Kyle Rankin is a systems architect; the current president of the North Bay Linux Users' Group; and the author of The Official Ubuntu Server Book, Knoppix Hacks, Knoppix Pocket Reference, Linux Multimedia Hacks, and Ubuntu Hacks.

Comments

Comment viewing options

☐ Threaded list - expanded ☐ Date - newest first ☐ 50 comments per page

Select your preferred way to display the comments and click "Save settings" to activate your changes.

[Usefulness on a LAN \(/content/sysadmins-toolbox-iftop#comment-373540\)](/content/sysadmins-toolbox-iftop#comment-373540)

Submitted by Anonymous (not verified) on Thu, 09/27/2012 - 07:31.

Question: to get useful information about how much bandwidth different users (on different machines) are using on a LAN, how would you use this?

I guess I think you'd have to install iftop on each user's machine and then collect the data from each of those

machines somehow?

At the present time, I use a FREESCO gateway on my LAN, but I plan to make that go away. Until it goes away, I guess I might install iftop on the gateway, but later???



[For LAN monitoring I use top](#) ([//content/sysadmins-toolbox-iftop#comment-373541](#))

Submitted by Anonymous (not verified) on Thu, 09/27/2012 - 08:21.

For LAN monitoring I use top and port mirroring on my switches. When I only want to monitor WAN traffic I mirror the switch port connected to my border router to another switch port and plug that into a box running top. It gives a fantastic breakdown of usage. When I'm working on internal issues I Split mirror all ports to a couple ports and connect them to the monitoring machine.



[err ntop not top. Silly](#) ([//content/sysadmins-toolbox-iftop#comment-373542](#))

Submitted by Anonymous (not verified) on Thu, 09/27/2012 - 09:44.

err ntop not top. Silly phone autocorrect.



[nethogs tool still looks more](#) ([//content/sysadmins-toolbox-iftop#comment-373533](#))

Submitted by Anonymous (not verified) on Thu, 09/27/2012 - 03:49.

nethogs tool still looks more usable to me



[What about those servers which iftop cannot be installed on?](#) ([//content/sysadmins-toolbox-iftop#comment-373532](#))

Submitted by Ronen Gottlieb (not verified) on Thu, 09/27/2012 - 03:03.

Here is what I usually use and it's out of the box:

```
ethtool -S eth0
netstat -s
netstat -i
cat /proc/net/dev
ifconfig eth0
sar -n DEV 1 3
/proc/class/net/$dev/statistics
```



[Fantastic! Just what I needed!](#) ([//content/sysadmins-toolbox-iftop#comment-373529](#))

Submitted by Rob (not verified) on Wed, 09/26/2012 - 23:06.

iftop and iptraf is just the kind of tool that I needed! This is awesome. Thanks a million!!!!
Yummy!



[iptraf \(/content/sysadmins-toolbox-iftop#comment-373522\)](#)

Submitted by Chris X (not verified) on Wed, 09/26/2012 - 14:54.

I didn't know about iftop. Instead, I use iptraf which has quite a few fancy features in addition to the real time useful display. I often need to log into a server and find out who is hogging all the bandwidth. But since I myself am logged in, I can't include my ssh connection or the results get silly. With iptraf, I can filter that out or set display update intervals to minimize it.



While covering interesting tops, don't forget about iotop which looks at disk io usage.

[Holy crap iptraf is awesome! \(/content/sysadmins-toolbox-iftop#comment-373524\)](#)

Submitted by [Andre \(http://andredublin.com\)](http://andredublin.com) (not verified) on Wed, 09/26/2012 - 16:03.

Holy crap iptraf is awesome! Thanks!



[Reply to comment | Linux Journal \(/content/sysadmins-toolbox-iftop#comment-373521\)](#)

Submitted by [Dhtmlcentral \(http://www.dhtmlcentral.com\)](http://www.dhtmlcentral.com) (not verified) on Wed, 09/26/2012 - 14:10.

My brother suggested I might like this website. He was entirely right.
This post actually made my day. You can not imagine just how much time I had spent for this information!
Thanks!



Post new comment

Please note that comments may not appear immediately, so there is no need to repost your comment.

Your name:

E-mail:

The content of this field is kept private and will not be shown publicly.

Homepage:

Subject:

Comment: *

Allowed HTML tags: <a> <cite> <code> <pre><tt> <dl> <dt> <dd> <i> <blockquote>

Lines and paragraphs break automatically.

Web page addresses and e-mail addresses turn into links automatically.

☒ Notify me when new comments are posted

☒ All comments ☐ Replies to my comment

By submitting this form, you accept the [Mollom privacy policy](http://mollom.com/web-service-privacy-policy) (<http://mollom.com/web-service-privacy-policy>).

Preview