iftop Live bandwidth by host

START HERE

`sudo` › `iftop` › `-i` › *<if>*
Watch an interface

`sudo` › `iftop` › `-nNP`
No lookups, show ports

`s` / `d`
Group by source / dest

`t`
Cycle line modes

`1` / `2` / `3`
Sort by average

`P`
Pause display

`l`
Filter hostnames

`q`
Quit

CONCEPTS

iftop needs raw packet capture: run it with sudo and name the interface with -i, or it picks the first one.

iftop -nNP who talks
Sort 1-3 2s / 10s / 40s
Filter l or -f
Capture tcpdump
Reading a busy link

The three columns are average rates over 2, 10 and 40 seconds; the bottom bar shows cumulative, peak and rate totals.

Only IP traffic is counted: -f is wrapped as (filter) and ip. Monitor only networks you are authorised to.

DISPLAY

`r` Toggle hostname resolution

`p` Toggle port display

`S` Toggle source port

`D` Toggle destination port

DISPLAY (cont.)

`t` Cycle line display modes

Two-line mode, then one-line sent, received or total.

`P` Pause the display

`o` Freeze current ordering

Hidden hosts are still counted in the totals.

`j` / `k` Scroll the host list

SORTING AND GROUPING

`s` Aggregate by source host

`d`
Aggregate by destination host

`1` / `2` / `3`
Sort by column 1, 2 or 3

Default is column 2, the 10 second average.

`<` Sort by source name

`>` Sort by destination name

`l` Filter hostnames by regex

Display only; capture and totals are unaffected.

SORTING AND GROUPING (cont.)

`f` Edit the capture filter live

Can take about 40 s to fully apply; may misbehave.

`h` / `?` Show built-in help

COMMAND LINE

`iftop` › `-i` › *<if>*
Listen on an interface

`iftop` › `-n`
No hostname lookups

`iftop` › `-N`
No port-to-service names

`iftop` › `-P` Show ports

`iftop` › `-B`
Rates in bytes, not bits

`iftop` › `-f` › `"<filter>"`
Capture filter (pcap syntax)

`iftop` › `-F` › *<net/mask>*
Measure direction relative to a network

`iftop` › `-G` › *<net6/mask>*
Same, for IPv6

`iftop` › `-p`
Promiscuous mode

COMMAND LINE (cont.)

`iftop` › `-b` No bar graphs

`iftop` › `-m` › *<limit>*
Bar scale limit (K, M, G)

`iftop` › `-l`
Count link-local IPv6

`iftop` › `-c` › *<file>*
Use another config file

Default is ~/.iftoprc; flags override it.

`iftop` › `-t`
Plain text output, no ncurses

`iftop` › `-h` Print usage

RECIPES

Who is eating the uplink

```
sudo iftop -i eth0 -nNP -B
# press s or d to group by
host, 2 to sort by 10s
```

One host or one port

```
sudo iftop -i eth0 -f "host
<ip>"
sudo iftop -i eth0 -f "port
443"
```

Separate in from out on a LAN

```
sudo iftop -i eth0 -F
192.168.1.0/24
# direction is now relative to
that network
```