nethogs Bandwidth per process

CONCEPTS

nethogs groups traffic by process, not by host or port. It reads packets with libpcap and matches connections to PIDs through /proc, so it is Linux only.

Packets libpcap
↓ match
Connection socket inode
↓ /proc
Process PID, program
How a byte gets a name

Traffic it cannot tie to a process, such as short-lived connections, shows up as 'unknown TCP'. Ignore it unless it is large.

Use iftop to see which hosts talk, nethogs to see which program does.

RUN

`sudo nethogs`
Monitor all running interfaces

`sudo nethogs <if> <if>`
Monitor only these interfaces

`sudo nethogs -a`
Include loopback and down interfaces

`sudo nethogs -d <sec>`
Set refresh interval (default 1)

`sudo nethogs -c <n>`
Quit after n refreshes

`sudo nethogs -P <pid>`
Show only this process

`sudo nethogs -f '<filter>'`
Apply a pcap filter (experimental)

`sudo nethogs -C`
Count UDP as well as TCP

`sudo nethogs -p`
Promiscuous capture (not advised)

`sudo nethogs -g <n>`
Prune dead entries every n refreshes

RUN (cont.)

`nethogs -V`
Print version

`nethogs -h`
Print help

DISPLAY

`-v 0`
Rates in kB/s (default)

`-v 1`
Total kB

`-v 2`
Total bytes

`-v 3`
Total MB

`-v 4`
Rates in MB/s

`-v 5`
Rates in GB/s

`-l`
Show full command line

`-b`
Show program basename only

`-s`
Start sorted by sent

INTERACTIVE KEYS

`q`
Quit

`r`
Sort by received

`s`
Sort by sent

`m`
Cycle kB/s, kB, B, MB, MB/s, GB/s

`l`
Toggle full command line

`b`
Toggle program basename

Press Ctrl+C to quit as well (fixed in 0.9.0); on older builds use q.

OUTPUT

`sudo nethogs -t`
Trace mode: plain text, no curses

`sudo nethogs -t -c <n>`
Print n samples and exit

`sudo nethogs -t -d <sec>`
Trace with a custom interval

Trace mode prints one line per process and refresh: program/PID/UID, then sent and received. Good for logs and pipes.

PERMISSIONS

`sudo setcap "cap_net_admin, cap_net_raw, cap_dac_read_search, cap_sys_ptrace+pe" $(which nethogs)`
Allow non-root use

`getcap $(which nethogs)`
Check granted capabilities

Packet capture needs root. A permissions error or missing process names usually means root or the capabilities below are absent.

RECIPES

Log per-process traffic for a minute

```
sudo nethogs -t -d 5 -c 12 > nethogs.log
```

Which program is eating the Wi-Fi

```
sudo nethogs wlan0
# press r to sort by received
# press m to switch to totals
```

Watch one service

```
pid=$(pidof firefox | cut -d' ' -f1)
sudo nethogs -P "$pid" -b
```

Non-root monitoring

```
sudo setcap "cap_net_admin,
cap_net_raw,cap_dac_read_search,
cap_sys_ptrace+pe" /usr/sbin/
nethogs
nethogs eth0
```