Measuring Network Activity

LPIC-2: Linux Engineer (201-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the metrics used to measure network performance.
2. Utilize iftop, sar, mtr, ip, and ss to gather information about network performance.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- *ntop* / *ntopng*
  - ntopng website (https://www.ntop.org/products/traffic-analysis/ntop/)
  - `sudo apt install ntopng`
  - Pretty heavy on dependencies
  - Runs a web server
- *iftop*
  - May not be installed by default, but very lightweight
  - `sudo apt install iftop -y`
  - `sudo iftop`
- Limiting *iftop* to a single interface
  - `sudo iftop -i eth0`
- Historical data
  - *sar*
  - `sar -n DEV`
    - Show device statistics
  - `sar -n EDEV`
    - Show device errors
  - `sar -n IP`
    - Show IPv4 statistics
- Pull *sar* data for a particular time frame
  - `sar -n DEV -f /var/log/sysstat/sa19 -s 00:00:00 -e 08:00:00`
  - `sar -n DEV -f /var/log/sysstat/sa18 -s 00:00:00 -e 08:00:00 --iface=ens33`
- *mtr*
  - Advanced trace route utility
  - `mtr www.google.com`
  - Can display AS numbers
    - `mtr -z www.slashdot.org`
- General network data tools
  - `ip` - Displays network settings
  - `netstat`/`ss` - Display socket statistics

        - `ss -natp`
    - `lsof` - Displays ports opened by processes
        - `sudo lsof -iTCP -sTCP:ESTABLISHED`