**Networking Security in Linux**

1. **traceroute**

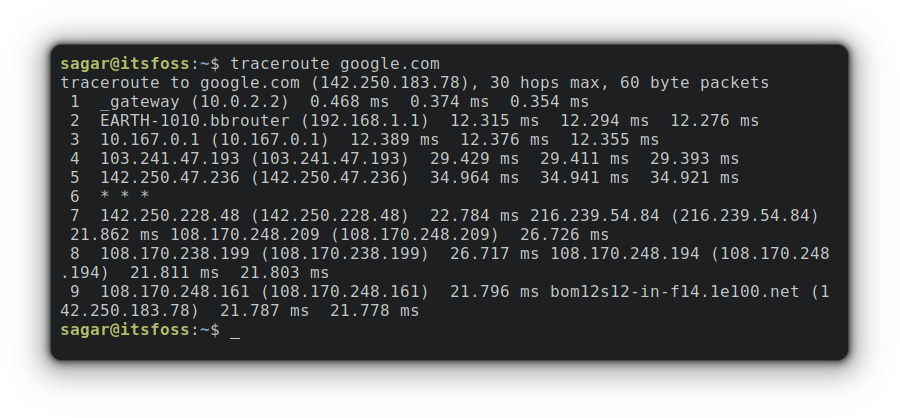
Using the traceroute command, you can identify the route taken by packets to reach the host. And it can be quite useful when you want to interrogate the transmission of data packets and hops taken by packets.

By default, your system may not have traceroute installed and if you’re on Debian-derivative (including Ubuntu), installation is single command ahead:

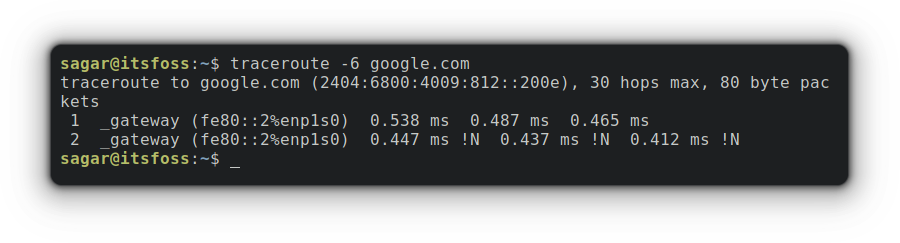
**apt install traceroute**

For example, I’d be tracerouting packets to google.com

**traceroute google.com**

[](https://itsfoss.com/content/images/wordpress/2022/08/traceroute-google.com_.png)

By default, traceroute will utilize IPv4 but you can change this behavior by using -6 option that will indicate traceroute to use IPv6. Let me show you how:

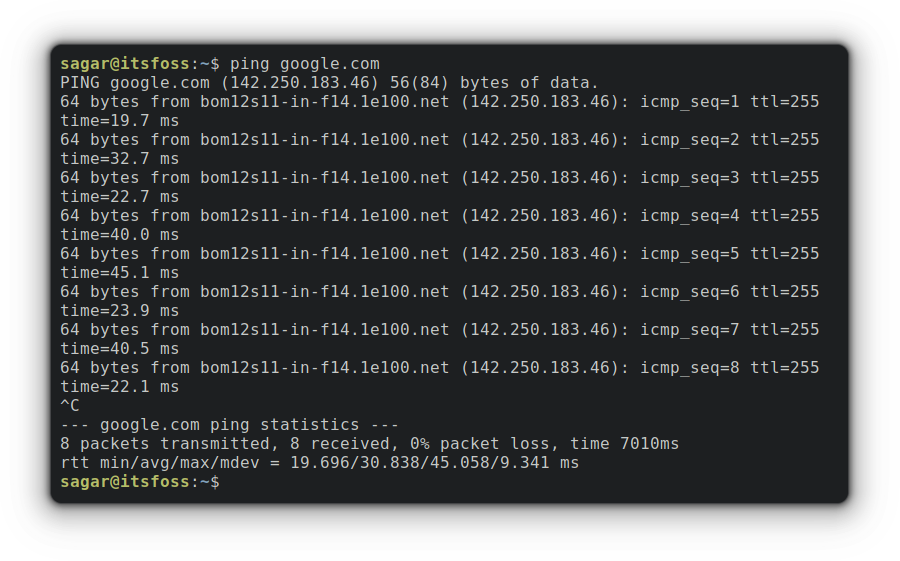
[](https://itsfoss.com/content/images/wordpress/2022/08/traceroute-6-google.com_.png)

**2. ping**

The ping (Packet Internet Groper) command can be considered one of the most important commands while troubleshooting your network, as it is the most common way to check the connectivity between the host and the server.

**apt install iputils-ping**

**ping google.com**

[](https://itsfoss.com/content/images/wordpress/2022/08/ping-google.com_.png)

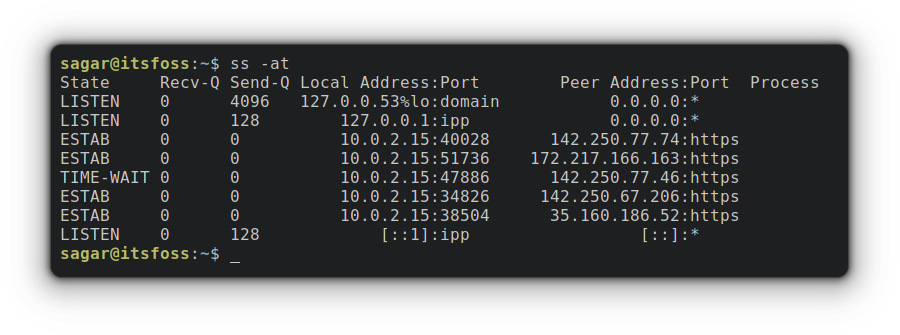
**3. ss**

The ss (socket statistics) command is used to detail about network socket (endpoint for sending and receiving data across the network).

To list all the listening and non-listening TCP connection, you have to use -at option as shown below:

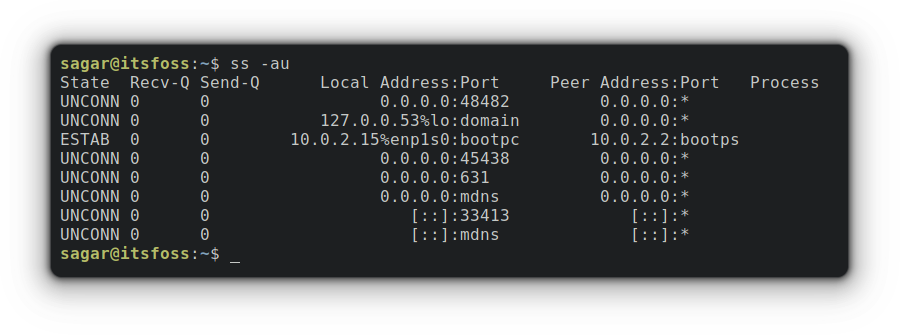
**apt install iproute2**

**ss -at**

[](https://itsfoss.com/content/images/wordpress/2022/08/ss-at.png)

Similarly, you can do the same with UDP ports using -au option:

**ss -au**

[](https://itsfoss.com/content/images/wordpress/2022/08/ss-au.png)

**4. dig**

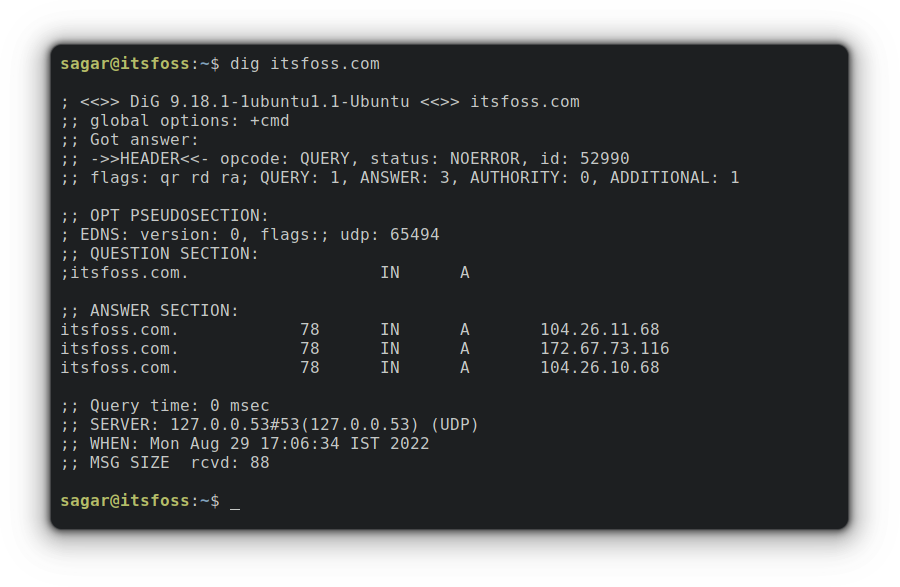
The [dig (Domain Information Groper) command](https://linuxhandbook.com/dig-command/?ref=itsfoss.com) is used to fetch all the necessary information about the DNS name server.

To install the dig utility on Ubuntu-based distros, follow the given command:

**apt install dnsutils**

Now, let me show you how to get info from a specific DNS, and for this example, I’d be using itsfoss.com as DNS.

dig itsfoss.com

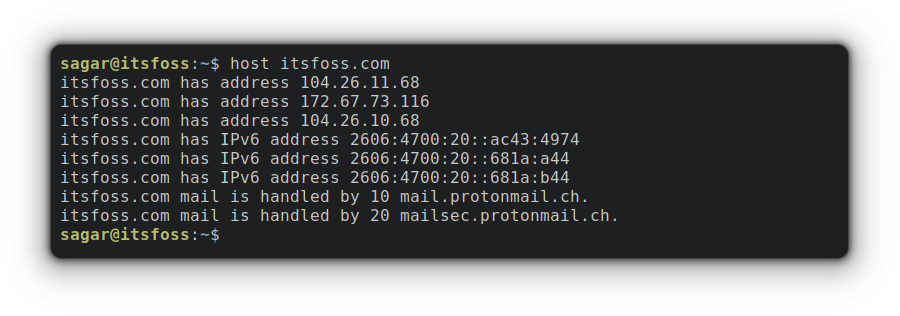
[](https://itsfoss.com/content/images/wordpress/2022/08/dig-itsfoss.com_.png)

**5. host**

The host command is mainly used to get the IP address of a specific domain, or you can get the domain name from a specific IP address. In other words, it’s just a DNS lookup utility.

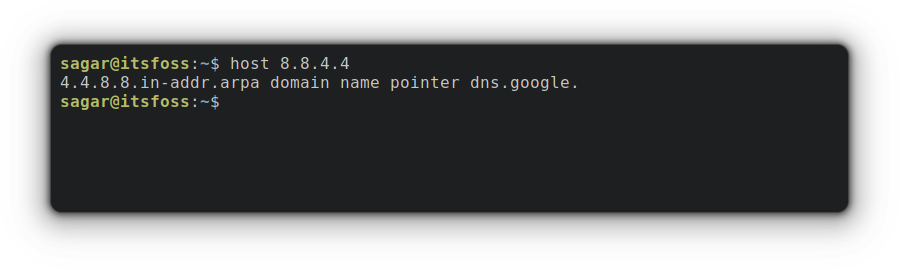
To find the IP of the domain, you just have to append the domain name with the host command. Let me show you how:

**host itsfoss.com**

[](https://itsfoss.com/content/images/wordpress/2022/08/host-itsfoss.com_.png)

Similarly, you can use an IP address to fetch the domain name:

**host 8.8.4.4**

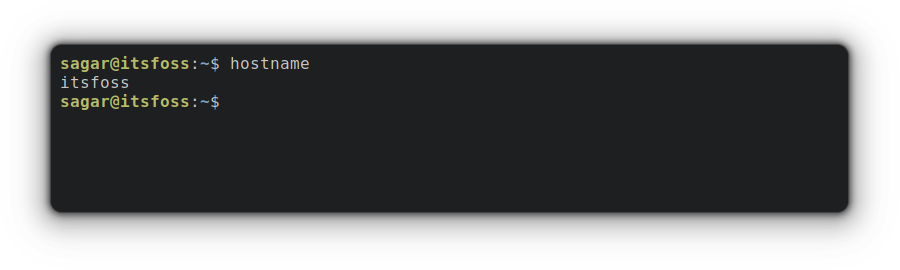
[](https://itsfoss.com/content/images/wordpress/2022/08/host-8.8.4.4.png)

**6. hostname**

You must be familiar with this command if you’ve been using Linux for a while, as this is mostly used to [change the hostname of your system](https://itsfoss.com/change-hostname-ubuntu/) and NIS (Network Information System) domain name.

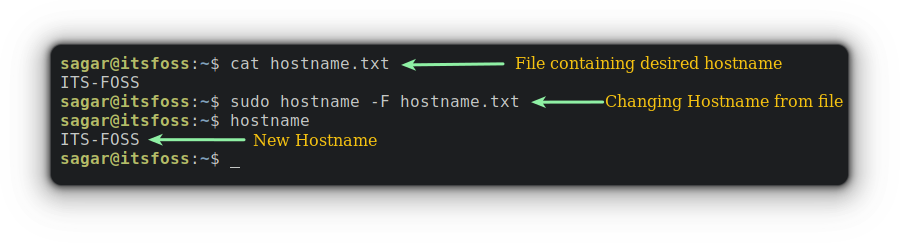
When used without any options, it gets the current hostname of the system:

**Hostname**

[](https://itsfoss.com/content/images/wordpress/2022/08/hostname.png)

Changing the hostname from a file containing the desired hostname is yet another interesting feature of this utility.

sudo hostname -F <filename>

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-hostname-f.png)

**7. curl**

The curl (Client URL) command is mostly used to transfer data over the network and supports various protocols including HTTP, FTP, IMAP, and many others.

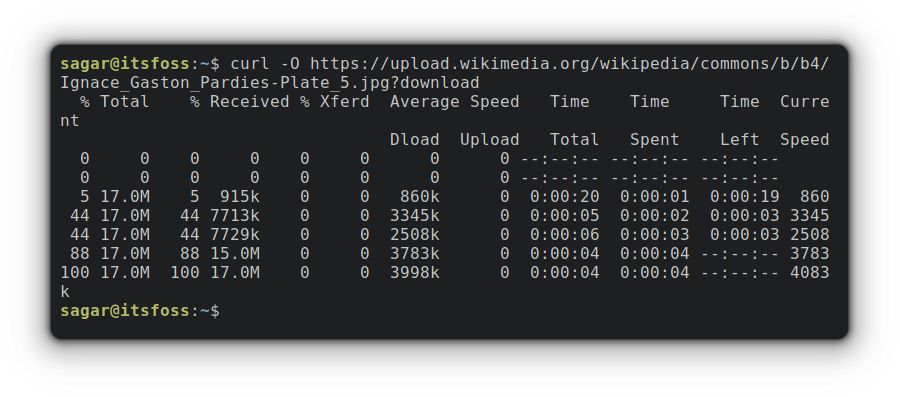
This tool is preferred in automation as it is built to work without any human interaction and can also be used in endpoint testing, Debugging, and error logging.

The curl utility does not come pre-installed and if you’re on any Debian-derivative, you just have to use the following command for installation:

**apt install curl**

It is quite easy to download files [using the curl command](https://linuxhandbook.com/curl-command-examples/?ref=itsfoss.com), You just have to use -O option with the URL, and you’d be good to go!

**curl -O http://www.google.com/robots.txt**

[](https://itsfoss.com/content/images/wordpress/2022/08/curl-o-url.png)

While downloading large files, the progress bar can be quite convenient, and you can do the same with curl using -# option.

[](https://itsfoss.com/content/images/wordpress/2022/08/curl-o.png)

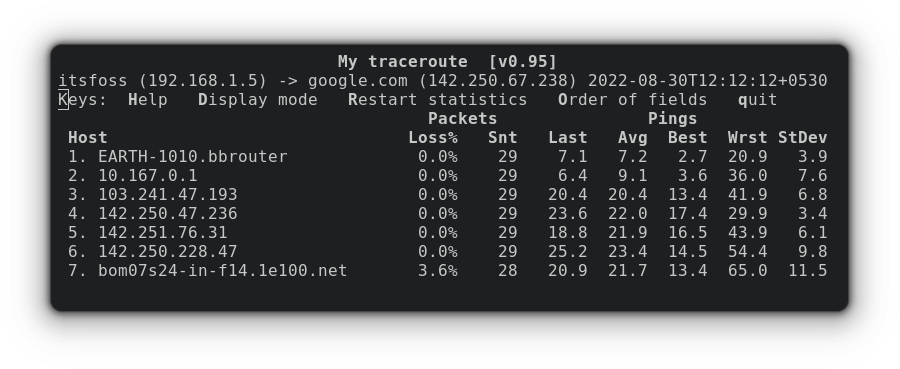
**8. mtr**

It is a combination of ping and traceroute utilities and is mainly used for network diagnostics and gives live look at network response and connectivity.

The simplest way to use mtr is to append a domain name or IP address with it, and it will give a live traceroute report.

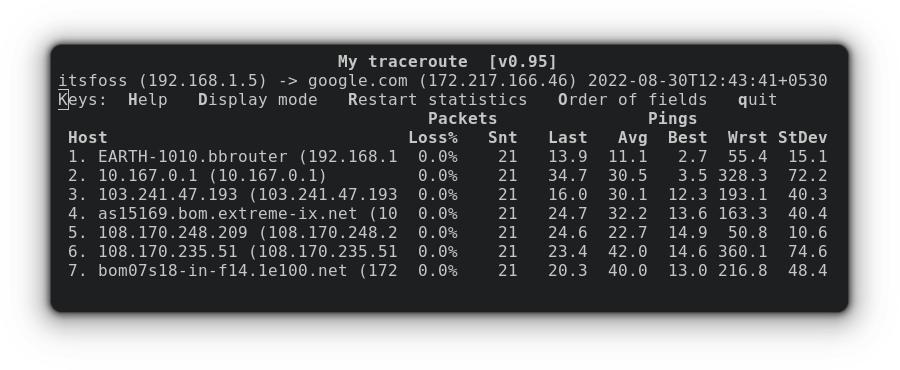
**apt-get install mtr**

**mtr [URL/IP]**

[](https://itsfoss.com/content/images/wordpress/2022/08/mtr-google.com_.png)

And if you want mtr to show both hostnames and IP addresses, you can pair it with -b option as shown below:

mtr -b [URL]

[](https://itsfoss.com/content/images/wordpress/2022/08/mtr-b.png)

**9. ifplugstatus**

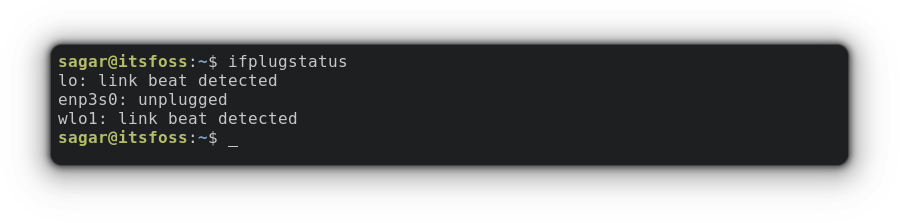
The ifplugstatus is one of the most basic yet useful enough to troubleshoot connectivity at the basic level. And is used to detect the link status of a local ethernet and works similarly to mii-diag, mii-tool, and ethtool by supporting APIs for all 3.

For installation on Ubuntu-based distros, you can follow the given command:

**apt install ifplugd**

This utility does not have any fancy options and often used without being paired with any:

**ifplugstatus**

[](https://itsfoss.com/content/images/wordpress/2022/08/ifplugstatus.png)

**10. iftop**

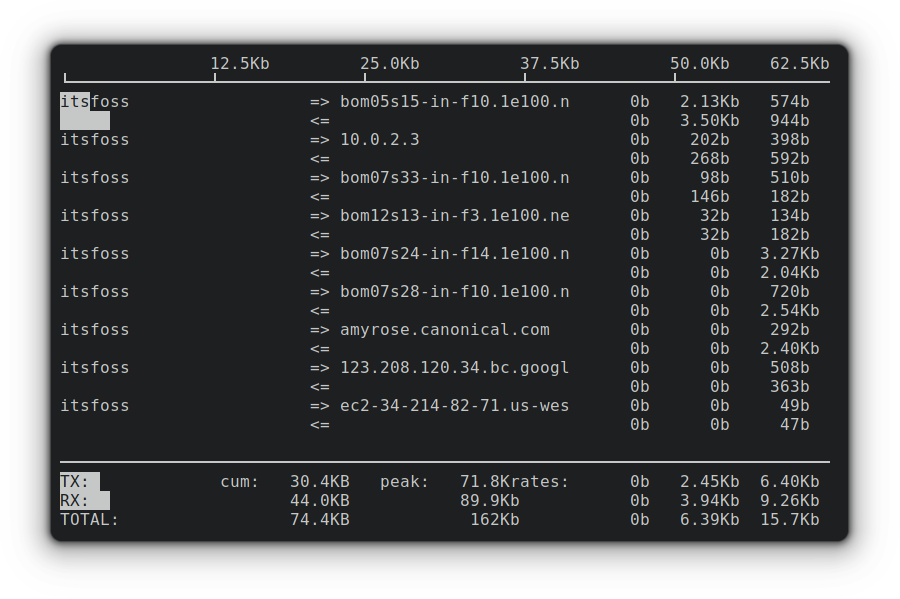
The iftop (Interface TOP) is often used by admins to monitor stats related to bandwidth and can also be used as a diagnostic tool when you’re having issues with the network.

This utility requires manual installation and can be easily installed on machines running Ubuntu by the given command:

**apt install iftop**

When iftop is used without any options, it shows bandwidth stats of the default interface:

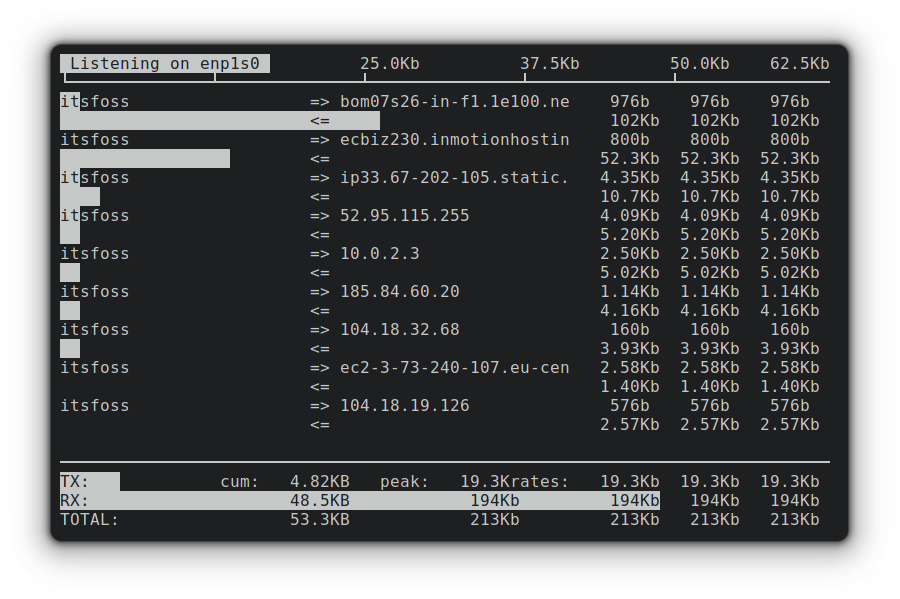
**iftop**

[](https://itsfoss.com/content/images/wordpress/2022/08/iftop.png)

And you can also specify the network device by appending the device name with -i option.

sudo iftop -i <DeviceName>

In my case its, enp1s0 so my output will be as follows:

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-iftop-i-enp1s0.png)

**11. tcpdump**

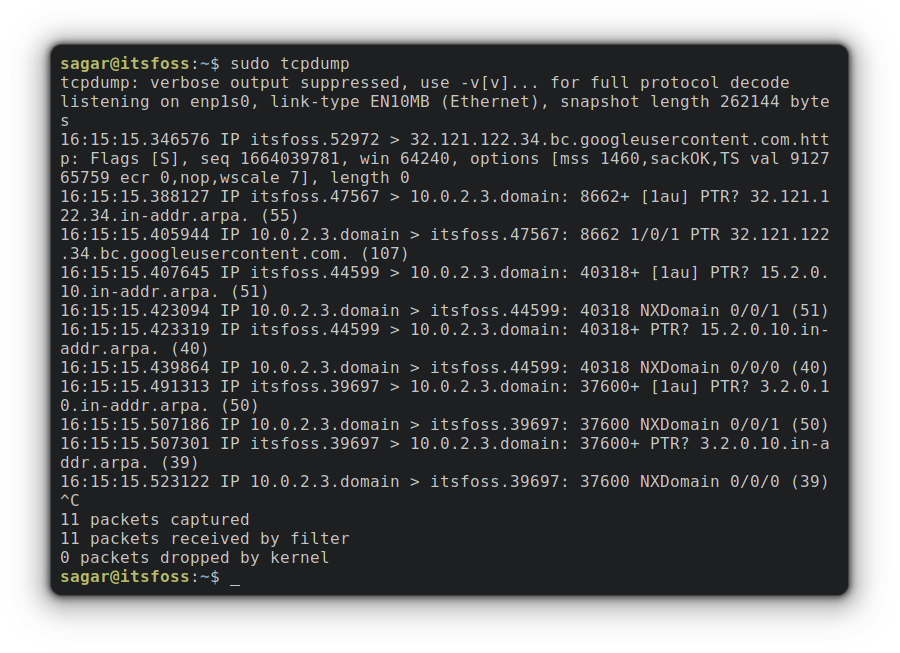
The tcpdump is a packet sniffing and analyzing utility used to capture, analyze and filter network traffic. It can also be used as a security tool because it saves captured data in pcap file which can be [accessed through Wireshark](https://itsfoss.com/install-wireshark-ubuntu/).

Like many other tools, tcpdump does not come pre-installed, and you can follow the given command for installation if you’re on Ubuntu base.

**apt install tcpdump**

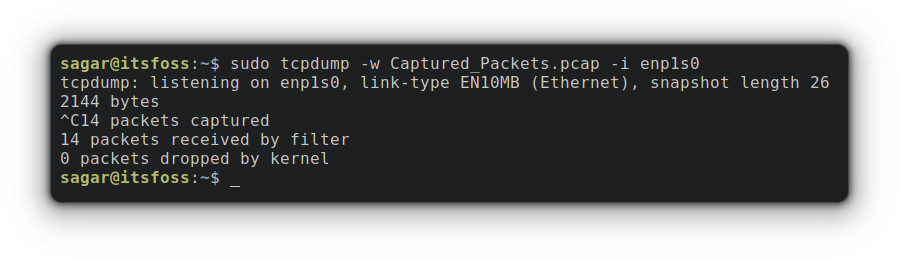
Once you’re done with the installation, you can get capture packets for the current interface as given below:

**tcpdump**

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-tcpdump.png)

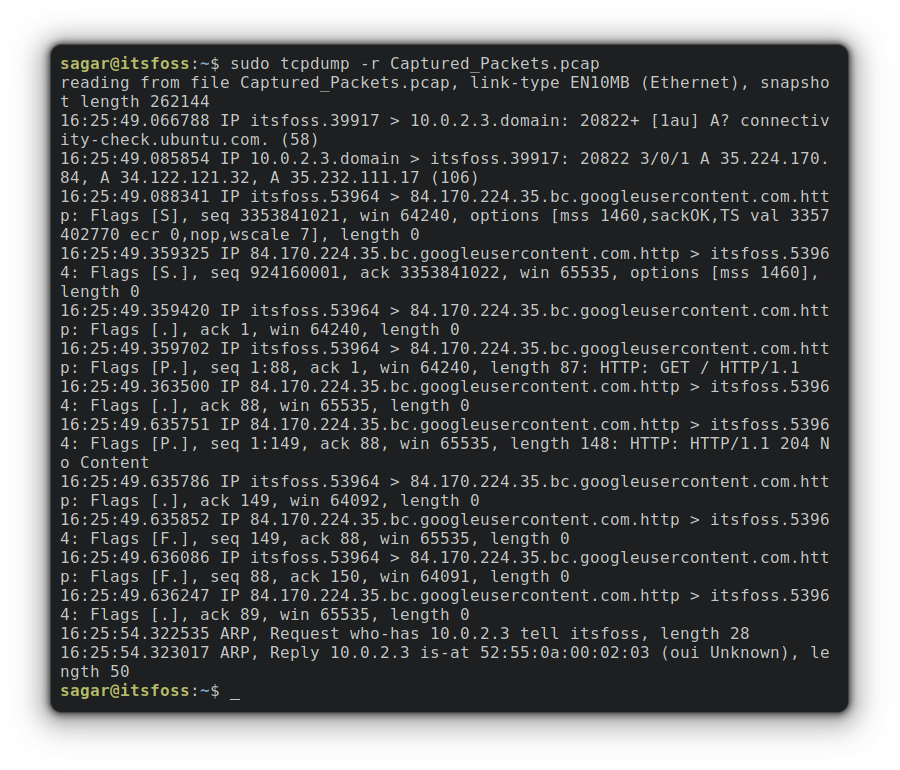
So how about saving captured packets in pcap file? Let me show you how:

sudo tcpdump -w Captured\_Packets.pcap -i <networkdevice>

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-tcpdump-w-.png)

To access the saved file, you need to use -r option by appending file name:

**tcpdump -r Captured\_Packets.pcap**

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-tcpdump-r-filename.png)

**12. ethtool**

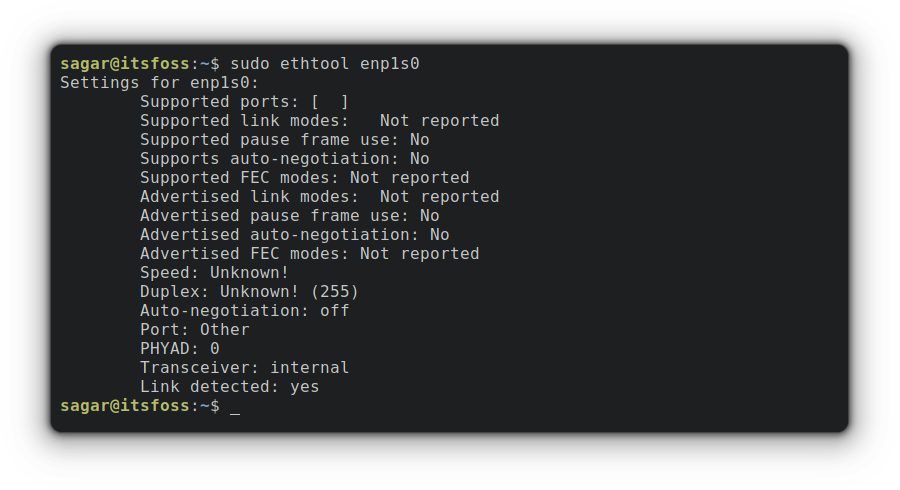
As its name suggests, the ethtool utility is primarily concerned with managing ethernet devices. Using this utility allows you to tweak network card speed, auto-negotiation, and much more.

But it may not be pre-installed on your machine and can be installed on a Ubuntu-powered machine by utilizing the given command:

**apt install ethtool**

To fetch the interface details, you just have to append the device name with the command as shown below:

sudo ethtool <InterfaceName>

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-ethtool-enp1s0.png)

**13. nmap**

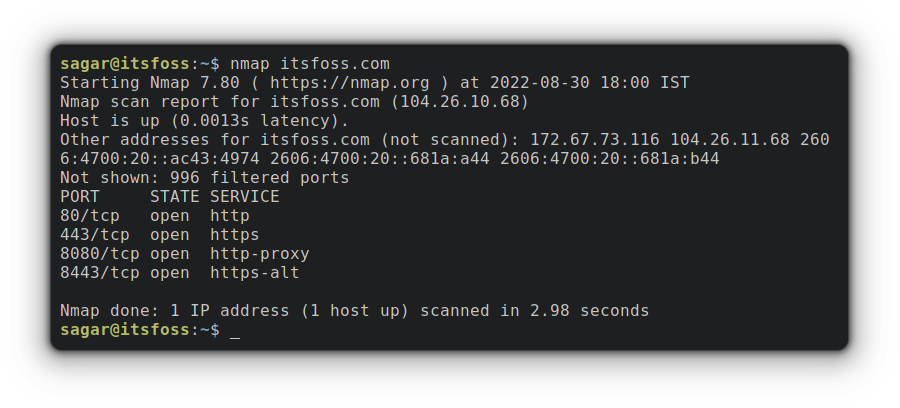
The nmap is a tool to explore and audit network security. It is often used by hackers and security enthusiasts as it allows you to get real-time info on the network, IPs connected to your network in a detailed manner, port scanning, and much more.

For installation of nmap utility on Ubuntu-based distros, utilize the given command:

**apt install nmap**

Let’s start scanning with hostname:

**nmap itsfoss.com**

[](https://itsfoss.com/content/images/wordpress/2022/08/nmap-itsfoss.com_.png)

**14. bmon**

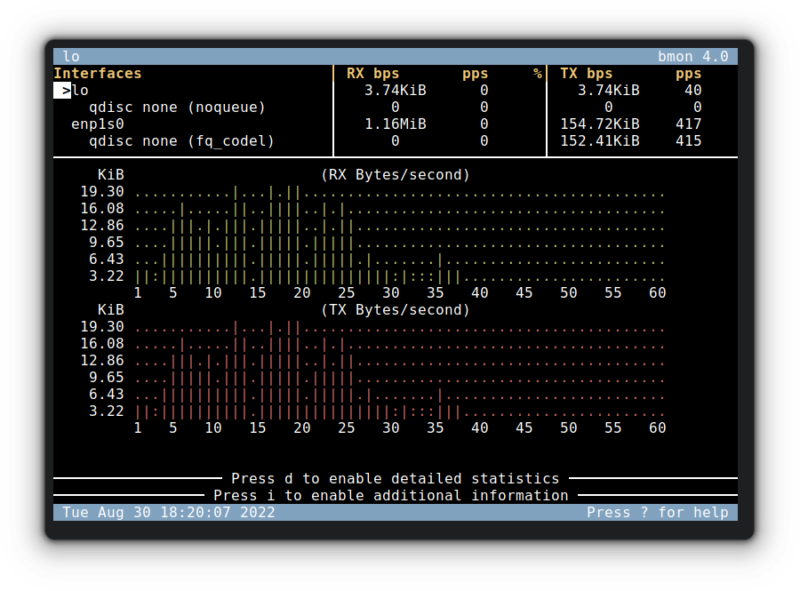
The bmon is an open-source utility to monitor real-time bandwidth and debug issues by presenting stats in a more human-friendly way. The best part of this tool is the graphical presentation and can even get your output in HTML!

Installation is quite simple as bmon is present in default repos of popular Linux distros and that also includes Ubuntu.

**apt install bmon**

Now, you just have to launch bmon and you’d be able to monitor bandwidth in eye pleasant way:

**bmon**

[](https://itsfoss.com/content/images/wordpress/2022/08/bmon-800x591.png)

**15. firewalld**

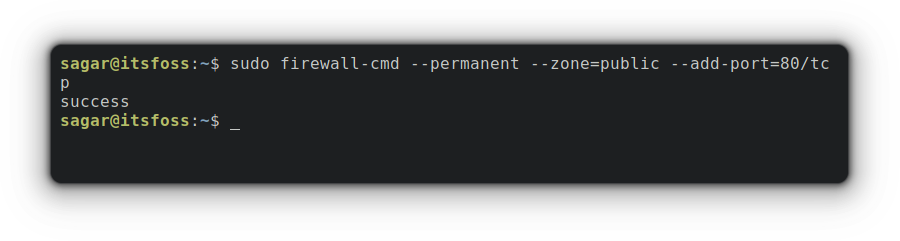
Managing firewalls can be considered the core part of network security and this tool allows you to add, configure and remove rules on firewall.

But the firewalld requires manual installation, and you can utilize the given command for installation if you’re using an Ubuntu-based distro:

**apt install firewalld**

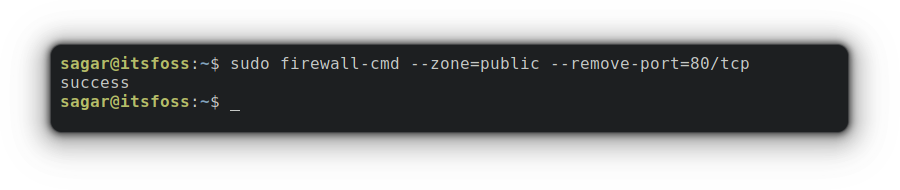
For example, I’d show you, how you can open port 80 permanently for the public zone:

**firewall-cmd --permanent --zone=public --add-port=80/tcp**

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-firewall-cmd-permanent-zonepublic.png)

Similarly, to remove the recently added rule, you have to use -remove option as shown below:

**firewall-cmd --zone=public --remove-port=80/tcp**

[](https://itsfoss.com/content/images/wordpress/2022/08/sudo-firewall-cmd-zonepublic-remove.png)

**16. iperf**

The iperf is an open-source utility written in C allowing users to perform network performance measurement and tuning.

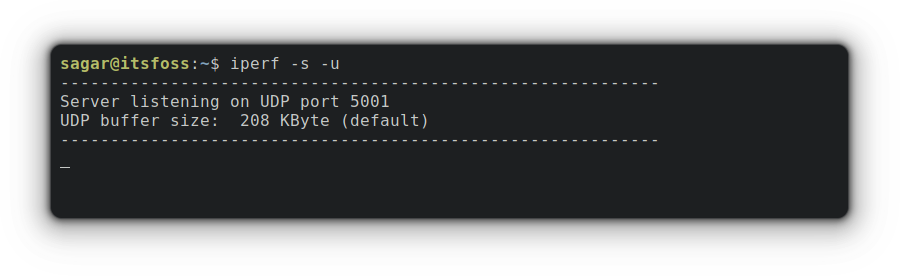
This tool is present in the default repository of Ubuntu and can be installed from the given command:

**apt install iperf**

To start monitoring the network, users must initiate this client on the server by given command:

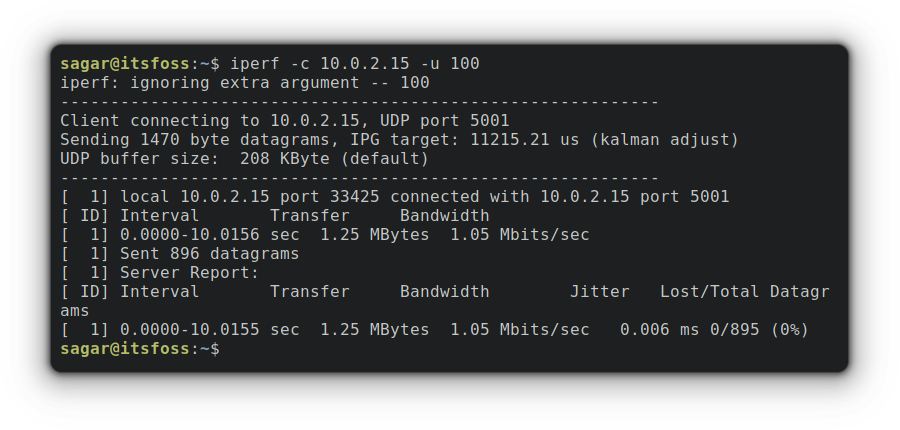
**iperf -s -u**

Where, -s option indicates server and -u option is for UDP format.

[](https://itsfoss.com/content/images/wordpress/2022/08/iperf-s-u.png)

Now, you can connect to your server (using -c option indicating client side) by providing an IP address payload for the preferred protocol. For this example, I went with UDP (using -u option) with a payload of 100.

**iperf -c 10.0.2.15 -u 100**

[](https://itsfoss.com/content/images/wordpress/2022/08/iperf-c-.png)

**17. speedtest-cli**

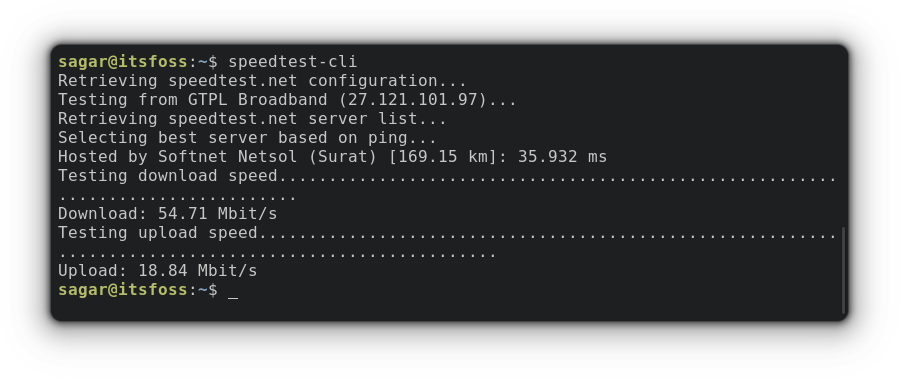
As the name suggests, this is the CLI utility for the speedtest.net website. This open-source utility released under Apache 2.0 license can be quite helpful when you want a reliable source for [checking internet speeds](https://itsfoss.com/network-speed-monitor-linux/) from cli.

Installation is quite straightforward and can easily be installed utilizing the given command if you’re on an Ubuntu base:

**apt install speedtest-cli**

Once you’re done with the installation part, you just have to use a single command to get your speeds tested:

**speedtest-cli**

[](https://itsfoss.com/content/images/wordpress/2022/08/speedtest-cli.png)

**18. vnstat**

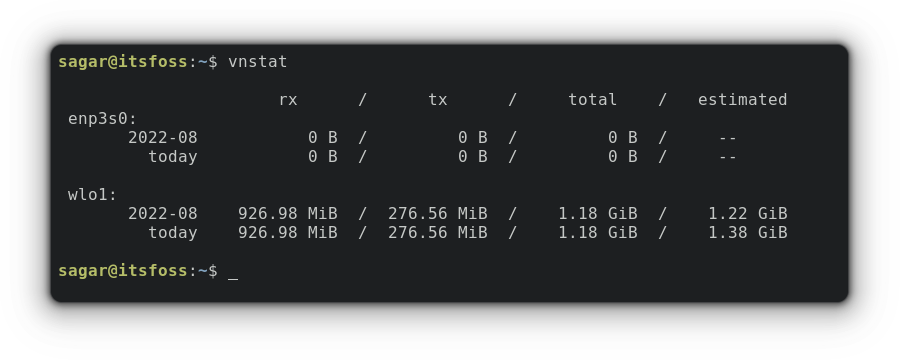
The vnstat utility is mostly used by sysadmins to monitor network traffic and bandwidth consumption (for the most part) as this tool monitors traffic on network interfaces of your system.

As with any other networking tool, you can find vnstat in the default repositories, and if you’re on Ubuntu, the installation can be done through the given command:

**apt install vnstat**

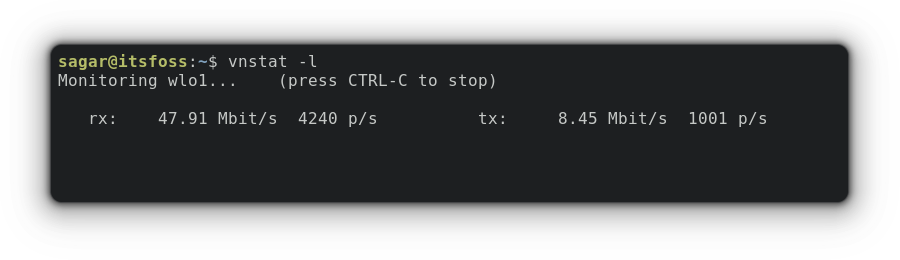
You can use vnstat command without any options, and it will bring basic stats of all available interfaces of your system:

**vnstat**

[](https://itsfoss.com/content/images/wordpress/2022/08/vnstat.png)

For live monitoring, you can pair vnstat command with -l option:

how to get the most out of man pages

[](https://itsfoss.com/content/images/wordpress/2022/08/vnstat-l.png)