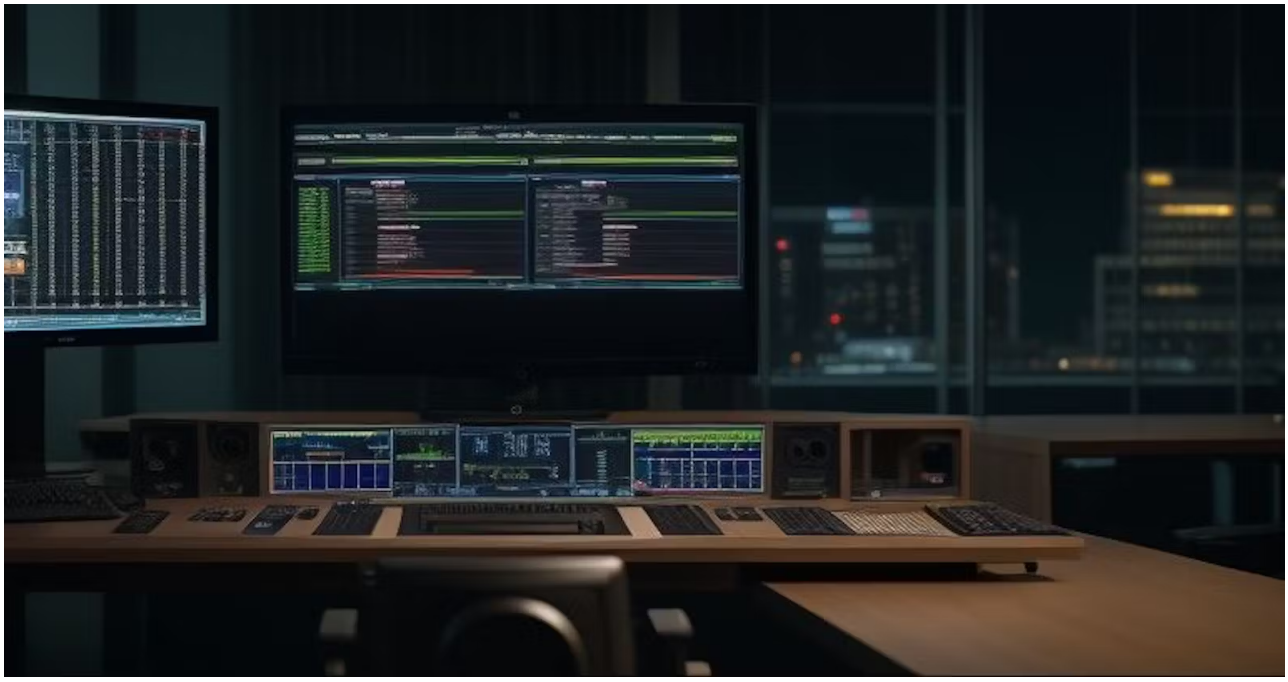
Sushan Shrestha

Following



17 Best Linux Networking and Troubleshooting Commands for Beginners

Sushan Shrestha

Dec 28, 2023 • 12 min read

Network configura troubleshooting are essential parts of system administration. Even for a developer who

works with Linux systems, knowledge of **Linux networking commands** is an added advantage.

Specifically, if you want to become a **DevOps engineer** or be part of SRE, it is essential to know all the **Linux troubleshooting commands** as they will be part of your day-to-day activities.

This post will cover the important **Linux networking and troubleshooting commands** that are natively available in Linux systems.

What are the best Linux Networking and Troubleshooting Commands?

Following is the list of natively available troubleshooting commands.

Command	Description
`hostname`	To check and set the hostname of the server.
`host`	To get host DNS details
`ping`	Checks if the remote server is reachable using ICMP protocol. It also shows the round trip time of packets.
`curl`	A cross-platform utility that is used to transfer data. It can be used for troubleshooting several network issues.
`wget`	Utility to download files. Can be used for troubleshooting proxy connections and connectivity.
`ip`	A replacement for `ifconfig`. Can be used to on about systems

Command	Description
`arp`	Utility to view and manage arp cache.
`ss/netstat`	Primarily used to check the connections and PID on ports and Unix sockets.
`tracerout` e	This utility uses the ICMP protocol and finds the hops involved in reading the destination server. It also shows the time it takes between hops.
`mtr`	mtr is a mix of `ping` and `traceroute`. It also provides additional information like intermediate hosts and responsiveness.
`dig`	Helps you get the DNS records associated with a domain name.
`nslookup`	Command similar to dig.
`nc`	utility to debug TCP/UDP sockets.
`telnet`	It can be used to test remote connectivity on ports
`route`	Helps you get all the route table information
`tcpdump`	This utility helps you to capture network packets and analyze them for network issues.
`lsof`	list all the open files and the process information that opened it

Let's understand each command and see how we can use it to troubleshoot Linux.

> ***Important Note:*** *Every command/utility mentioned in this post has many options and flags. Every command has a man page and you can use it to identify the flags and options that are required for your use case. For example, for* `ip` *command, you can just type it* `man ip` *in the terminal to get all the details about that command.*

1. hostname

Hostname command is used to view the hostname of the machine and to set the hostname.

COPY

```
hostname
```

You can use the hostname command to set a new hostname for the machine. For example,

COPY

```
sudo hostname temp.com
```

If you set the hostname using “ `hostname` ” command, when you restart the machine, the hostname will change to the name specified in the hostname file (eg: /etc/hostname).

So if you want to change the hostname permanently, you can use the `/etc/hosts` file or relevant hostname file present on the server.

1. For ubuntu machines, you can change it in the `/etc/hostname` file.
2. For RHEL, CentOS and Fedora you can change it in the `/etc/sysconfig/network` file.

2. host

Host command is for the reverse lookup of IP or a DNS name.

For example, If you an IP you can use the host commands as follows.

COPY

```
host 8.8.8.8
```

You can also do the reverse to find the IP address associated with the domain name. For example,

COPY

```
host blog.sushanstha.com
```

3. ping

The ping networking utility is used to check if the remote server is reachable or not. It is primarily used for checking the connectivity and troubleshooting the network.

It provides the following details.

1. Bytes sent and received
2. Packets sent, received, and lost
3. Approximate round-trip time (in milliseconds)

Ping command has the following syntax.

COPY

```
ping <IP or DNS>
```

For example,

COPY

```
ping blog.sushanstha.com
```

To ping IP address

COPY

```
ping 8.8.8.8
```

If you want to limit the ping output without using ctrl+c, then you can use the “-c” flag with a number as shown below.

COPY

```
ping -c 1 blog.sushanstha.com
```

4. curl

Curl utility is primarily used to transfer data from or to a server. However, you can use it for network troubleshooting.

For network troubleshooting, `curl` supports protocols such as `DICT`, `FILE`, `FTP`, `FTPS`, `GOPHER`, `HTTP`, `HTTPS`, `IMAP`, `IMAPS`, `LDAP`, `LDAPS`, `MQTT`, `POP3`, `POP3S`, `RTMP`, `RTMPS`, `RTSP`, `SCP`, `SFTP`, `SMB`, `SMBS`, `SMTP`, `SMTPS`, `TELNET` and `TFTP`

For example, `curl` can check connectivity on port 22 using telnet.

COPY

```
curl -v telnet://192.168.33.10:22
```

You can check the FTP connectivity using curl.

COPY

```
curl ftp://ftptest.net
```

You can troubleshoot web server connectivity as well.

COPY

```
curl http://blog.sushanstha.com -I
```

5. wget

The `wget` command is primarily used to fetch web pages.

You can use `wget` to troubleshoot network issues as well.

For example, you can troubleshoot proxy server connections using wget.

COPY

```
wget -e use_proxy=yes http_proxy=<proxy_host:port> http://externals
```

You can check if a website is up by fetching the files.

COPY

```
wget www.google.com
```

6. ip (ifconfig)

`ip` command is us s and network interfaces. **ip** command is the newer version of `ifconfig`. ifconfig works

in all the systems, but it is better to use ip command instead of ifconfig.

Let's have a look at a few examples of `ip` command.

Display network devices and configuration

COPY

```
ip addr
```

You can use this command with pipes and grep to get more granular output like the IP address of the eth0 interface. It is very useful when you work on automation tools that require IP to be fetched dynamically.

The following command gets the IP address of `eth0` network interface.

COPY

```
ip a | grep eth0  | grep "inet" | awk -F" " '{print $2}'
```

Get details of a specific interface

COPY

```
ip a show eth0
```

You can list the routing tables.

COPY

```
ip route
ip route list
```

7. arp

ARP (**Address Resolution Protocol**) shows the cache table of local networks' IP addresses and MAC addresses that the system interacted with.

COPY

```
arp
```

Example output,

COPY

```
vagrant@dcubelab:~$ arp
Address                  HWtype  HWaddress           Flags Mask
10.0.2.3                 ether   52:54:00:12:35:03   C
192.168.33.1             ether   0a:00:27:00:00:00   C
10.0.2.2                 ether   52:54:00:12:35:02   C
```

8. ss (netstat)

The `ss` command is a replacement for `netstat`. You can still use the `netstat` command on all systems.

Using `ss` command, you can get more information than `netstat` command. ss command is fast because it gets all the information from the kernel userspace.

Now let's have a look at a few usages of `ss` command.

Listing all connecti

The “ `ss` ” command will list all the TCP, UDP, and Unix socket connections on your machine.

COPY

```
ubuntu@blog.sushanstha:~$ ss
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Adc
u_str  ESTAB      0      0                    * 7594
u_str  ESTAB      0      0      @/com/ubuntu/upstart 7605
u_str  ESTAB      0      0                    * 29701
u_str  ESTAB      0      0      /var/run/dbus/system_bus_socket 297
tcp    ESTAB      0      400      172.31.18.184:ssh         1.22.16
```

The output of the `ss` command will be big so you can use ” `ss | less` ” command to make the output scrollable.

Filtering out TCP, UDP and Unix sockets

If you want to filter out TCP , UDP or UNIX socket details, use “-t” “-u” and “-x” flag with the “ss” command. It will show all the established connections to the specific ports. If you want to list both connected and listening ports using “a” with the specific flag as shown below.

COPY

```
ss -ta
ss -ua
ss -xa
```

List all listening ports

To list all the listening ports, use “-l” flag with ss command. To list specific TCP, UDP o[illegible] “-x” flag with “-l” as shown below.

COPY

```
ubuntu@blog.sushanstha:~$ ss -lt
State      Recv-Q Send-Q      Local Address:Port          Peer Addr
LISTEN     0      128                     *:ssh
LISTEN     0      50                    :::http-alt
LISTEN     0      50                    :::55857
LISTEN     0      128                   :::ssh
LISTEN     0      50                    :::53285
ubuntu@blog.sushanstha:~$
```

List all established

To list all the established ports, use the `state established` flag as shown below.

COPY

```
ss -t -r state established
```

To list all sockets in listening state,

COPY

```
ss -t -r state listening
```

9. traceroute

If you do not have a `traceroute` utility in your system or server, you can install it from the native repository.

`traceroute` is a network troubleshooting utility. Using traceroute you can find the numbe packet to reach

the destination. You can essentially trace the path of the packet from your server to the remote host.

For example,

COPY

```
traceroute google.com
```

Here is the output.

COPY

```
traceroute to google.com (173.194.33.163), 30 hops max, 60 byte pac
 1  ec2-50-112-0-84.us-west-2.compute.amazonaws.com (50.112.0.84)
 2  100.64.1.247 (100.64.1.247)  1.414 ms 100.64.1.137 (100.64.1.13
 3  100.64.0.198 (100.64.0.198)  1.443 ms 100.64.0.62 (100.64.0.62)
10  66.249.94.214 (66.249.94.214)  6.313 ms  7.104 ms 209.85.249.34
11  209.85.244.65 (209.85.244.65)  6.157 ms  6.341 ms  6.574 m.
.
12  sea09s18-in-f3.1e100.net (173.194.33.163)  6.302 ms  6.517 ms
ubuntu@blog.sushanstha:~$
```

The above output shows the hop count (12) to reach google.com from blog.sushanstha AWS ec2 server.

This utiltity comes in handy when you want to troubleshoot issues related to network packets not reaching the host.

10. mtr

The `mtr` utility is a r shoot the network bottlenecks. It com ng and `traceroute`

For example, the following command shows the `traceroute` output in real-time.

COPY

```
mtr google.com
```

Here is the output.

mtr network diagnostic tool

mtr report

You can generate a report using the –report flag. When you run the mtr report, it sends 10 packets to the destination and creates the report.

COPY

```
mtr -n --report google.com
```

network troubleshooting with mtr report

11. dig

If you have any task related to DNS lookup, you can use "`dig`" command to query the DNS name servers.

Get all DNS records with dig

The following command returns all the DNS records and TTL information of a twitter.com

COPY

```
dig twiter.com A
```

all DNS records with dig

Use `+short` to get the output without verbose.

COPY

```
dig google.com ANY +short
```

Get Specific DNS Record with dig

For example, If you want to get the `A record` for the particular domain name, you can use the dig command. `+short` will provide the information without verbose

COPY

```
dig www.google.com A +short
```

Similarly, you can get the other record information separately using the following commands.

COPY

```
dig google.com CNAME +short
dig google.com MX +short
dig google.com TXT +short
dig google.com NS +short
```

Reverse DNS Lookup with dig

You can perform a reverse DNS lookup with dig using the following command. Replace `8.8.8.8` with the required IP

COPY

```
dig -x 8.8.8.8
```

12. nslookup

Nslookup (Name Server Lookup) utility is used to check the DNS entries. It is similar to dig command.

To check the DNS records of a domain, you can use the following command.

COPY

```
nslookup google.com
```

You can also do a reverse lookup with the IP address.

COPY

```
nslookup 8.8.8.8
```

To get all the DNS records of a domain name, you can use the following.

COPY

```
nslookup -type=any google.com
```

Similarly, you can query for records like `mx`, `soa` etc

13. nc (netcat)

The `nc` (netcat) command is known as the swiss army of networking commands.

Using `nc`, you can check the connectivity of a service running on a specific port.

For example, to check if `ssh` port is open, you can use the following command.

COPY

```
nc -v -n 192.168.33.10 22
```

`netcat` can also be used for data transfer over TCP/UDP and port scanning.

Port scanning is not recommended in cloud environments. You need to request the cloud provider to perform port scanning operations in your environment.

14. telnet

The telnet command is used to troubleshoot the TCP connections on a port.

To check port connectivity using telnet, use the following command.

COPY

```
telnet 10.4.5.5 22
```

15. route

The “ `route` ” command is used to get the details of the route table for your system and to manipulate it. Let us look at a few examples for the route command.

Listing all routes

Execute the “ `route` ” command without any arguments to list all the existing routes in your system or server.

COPY

```
ubuntu@blog.sushanstha:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
default         ip-172-31-16-1. 0.0.0.0         UG    0      0
172.17.0.0      *               255.255.0.0     U     0      0
172.31.16.0     *               255.255.240.0   U     0      0
ubuntu@blog.sushanstha:~$
```

If you want to get the full output in numerical form without any hostname, you can use “-n” flag with the route command.

COPY

```
ubuntu@blog.sushanstha:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
0.0.0.0         172.31.16.1     0.0.0.0         UG    0      0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0
172.31.16.0     0.0.0.0         255.255.240.0   U     0      0
ubuntu@blog.sushanstha:~$
```

16. tcpdump

The `tcpdump` command is primarily used for troubleshooting network traffic.

> ***Note:** To analyze the output of `tcpdump` command requires some learning, so explaining it is out of the scope of this article.*

`tcpdump` command works with the network interfaces of the system. So you need to use administrative privileges to execute the command.

List all network interfaces

Use the following command to list all the interfaces.

COPY

```
sudo  tcpdump --list-interfaces
```

Capture Packets on Specific Interface

To get the dump of packets on a specific interface, you can use the following command.

> ***Note:** press `ctrl + c` to stop capturing the packets.*

COPY

```
sudo tcpdump -i eth0
```

To limit the packet capturing, you can use the `-c` flag with the number.

For example,

COPY

```
sudo tcpdump -i
```

Capture Packets on All Interfaces

To capture packets on all the interfaces, use the `any` flag as shown below.

COPY

```
sudo tcpdump -i any
```

17. lsof

`lsof` is a command that would used in day to day linux troubleshooting. This command is equally important for anyone working with Linux systems.

To list all open files, execute the `lsof` command.

COPY

```
lsof
```

One of the common error face by developers & DevOps engineers is "**Bind failed error: Address already in use**". You can find the process ID associated with a port using the following command. The you can kill the process to free up the port.

COPY

```
lsof -i :8080
```

Third-Party Network Troubleshooting Utilities

There are more networking troubleshooting command-line utilities available from third-party solutions.

You need to install them separately and use them for your troubleshooting purposes. Due to security compliance reasons, not every organisation will allow you to do it.

However, if you have to option to use third-party tools, you can explore them.

We have organized some tool information under different categories in the following table.

Category	Open-Source Tools
Network Scanners	Nmap, Zenmap (GUI for Nmap)
Packet Analyzers	Wireshark, Tcpdump
Bandwidth Monitors	BandwidthD, Cacti
Port Scanners	Nmap, Masscan
Ping/Traceroute Tools	MTR (My Traceroute)
Wireless Network Analyzers	Wireshark (for wireless), Kismet
Network Simulators	GNS3, Mininet
DNS Tools	DNSperf
Network Performance Testing	iperf

bestlinuxcommands Linux linux for beginners linux-basics linux-commands

Written by

Sushan Shrestha

I'm a DevOps Engineer, Open Source Enthusiast and a Technical Writer. I'm passionate about sharing knowledge, Concise documentations, and making it easy for others to understand technical concepts.

Following

MORE ARTICLES

Sushan Shrestha

Azure Synapse vs Databricks

Interested to learn the difference between Azure Synapse Analytics and Databricks? then you are at t...