SOMNOG 8
Somali Network Operators Group
WORKSHOPS AND CONFERENCE
7 - 11 December, 2025

Inclusive Innovation: Enabling a Trusted and Collaborative Digital Economy in Somalia.

A DECADE OF KNOWLEDGE SHARING
10 YEARS
2015 — 2025

Basic network commands in Linux

Track 2: **Systems and Services**

Jazeera University

Day 2

- Ip addr

```
somnog@ss-track:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:db:0b:07:76:ff brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 172.31.39.223/20 metric 100 brd 172.31.47.255 scope global dynamic ens5
       valid_lft 3076sec preferred_lft 3076sec
    inet6 fe80::8db:bff:fe07:76ff/64 scope link
       valid_lft forever preferred_lft forever
somnog@ss-track:~$
```

- ping ip-address or domain
- ping 192.168.2.105 -c 4
- Hostname
- Hostname –I

```
somnog@ss-track:~$ ping google.com
PING google.com (192.178.223.100) 56(84) bytes of data.
64 bytes from yulhrs-in-f100.1e100.net (192.178.223.100): icmp_seq=1 ttl=105 time=1.62 ms
64 bytes from yulhrs-in-f100.1e100.net (192.178.223.100): icmp_seq=2 ttl=105 time=1.64 ms
64 bytes from yulhrs-in-f100.1e100.net (192.178.223.100): icmp_seq=3 ttl=105 time=1.64 ms
64 bytes from yulhrs-in-f100.1e100.net (192.178.223.100): icmp_seq=4 ttl=105 time=1.68 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.616/1.642/1.681/0.023 ms
somnog@ss-track:~$ ping google.com -c 4
PING google.com (192.178.223.113) 56(84) bytes of data.
64 bytes from yulhrs-in-f113.1e100.net (192.178.223.113): icmp_seq=1 ttl=105 time=1.79 ms
64 bytes from yulhrs-in-f113.1e100.net (192.178.223.113): icmp_seq=2 ttl=105 time=1.80 ms
64 bytes from yulhrs-in-f113.1e100.net (192.178.223.113): icmp_seq=3 ttl=105 time=1.82 ms
64 bytes from yulhrs-in-f113.1e100.net (192.178.223.113): icmp_seq=4 ttl=105 time=1.81 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.786/1.805/1.822/0.013 ms
somnog@ss-track:~$
```

Ss Command

- An abbreviation for "Socket Statistics", the `ss` command is a utility that displays UNIX socket connections. The command is an improved version of the old `netstat` command. It offers valuable insights into open ports, listening TCP and UDP sockets, active connections, routing tables, process statistics, and more.
- sudo ss –nltu
- man ss

```
somnog@ss-track:~$ sudo ss -nltu
Netid         State          Recv-Q         Send-Q                  Local Address:Port                  Peer Address:Port         Process
udp           UNCONN         0              0                          127.0.0.54:53                       0.0.0.0:*
udp           UNCONN         0              0                       127.0.0.53%lo:53                       0.0.0.0:*
udp           UNCONN         0              0                 172.31.39.223%ens5:68                       0.0.0.0:*
udp           UNCONN         0              0                         127.0.0.1:323                      0.0.0.0:*
udp           UNCONN         0              0                             [::1]:323                         [::]:*
tcp           LISTEN         0              4096                        0.0.0.0:22                       0.0.0.0:*
tcp           LISTEN         0              4096                    127.0.0.53%lo:53                       0.0.0.0:*
tcp           LISTEN         0              4096                       127.0.0.54:53                       0.0.0.0:*
tcp           LISTEN         0              4096                            [::]:22                         [::]:*
somnog@ss-track:~$
```

- **netstat command**

- network statistics', the `netstat` command is a valuable tool for displaying valuable network-related statistics. Although replaced by the `ss` command, the command-line utility still serves a useful role in displaying listening sockets (TCP and UDP) and open ports and port statistics.
- The following example displays all listening TCP ports, process name, and their PIDs.

- sudo netstat -antpl

```
somnog@ss-track:~$ sudo netstat -antpl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1/init
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      327/systemd-resolve
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      327/systemd-resolve
tcp        0      0 172.31.39.223:22        154.73.27.2:9694        ESTABLISHED 1975/sshd: ubuntu [
tcp        0      0 172.31.39.223:42286     18.133.123.48:80        TIME_WAIT   -
tcp        0    412 172.31.39.223:22        154.73.27.2:57108       ESTABLISHED 1451/sshd: ubuntu [
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
somnog@ss-track:~$
```

traceroute command

The traceroute command keenly traces the path taken by data packets as they traverse from one router to another, a sequence known as hops. Loss of packets in a hop indicates that remediation measures should be taken to address packet loss and connection issues.

The traceroute command takes the following syntax.

Sudo apt install traceroute

traceroute ip-address

traceroute 8.8.8.8

```
somnog@ss-track:~$ traceroute google.com
traceroute to google.com (192.178.223.101), 30 hops max, 60 byte packets
 1  240.2.112.38 (240.2.112.38)  1.819 ms 240.2.112.37 (240.2.112.37)  1.299 ms  1.825 ms
 2  242.6.29.131 (242.6.29.131)  1.263 ms 242.6.28.1 (242.6.28.1)  1.116 ms 242.6.28.131 (242.6.28.131)  1.130 ms
 3  151.148.9.242 (151.148.9.242)  1.286 ms  2.023 ms 151.148.9.232 (151.148.9.232)  1.240 ms
 4  151.148.9.233 (151.148.9.233)  0.815 ms  0.804 ms  0.793 ms
 5  192.178.97.251 (192.178.97.251)  1.225 ms 192.178.97.43 (192.178.97.43)  1.822 ms  1.809 ms
 6  192.178.97.170 (192.178.97.170)  1.896 ms 192.178.97.94 (192.178.97.94)  1.655 ms 192.178.98.6 (192.178.98.6)  1.812 ms
 7  216.239.59.5 (216.239.59.5)  1.875 ms 142.251.236.52 (142.251.236.52)  3.369 ms 216.239.59.5 (216.239.59.5)  2.059 ms
 8  192.178.97.47 (192.178.97.47)  2.305 ms 142.251.197.133 (142.251.197.133)  2.422 ms 192.178.255.171 (192.178.255.171)  2.093 ms
 9  142.251.70.125 (142.251.70.125)  1.746 ms 142.251.230.139 (142.251.230.139)  1.836 ms 192.178.96.199 (192.178.96.199)  3.061 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  yulhrs-in-f101.1e100.net (192.178.223.101)  2.105 ms  2.301 ms  2.260 ms
somnog@ss-track:~$
```

mtr command

- Short for `My Traceroute`, the `mtr` command combines the functionality of traceroute and ping. It checks for the accessibility of a host target while also probing the path taken by data packets to the destination.

mtr google.com

```
                                                My traceroute  [v0.95]
ss-track (172.31.39.223) -> google.com (142.251.29.100)                                  2025-12-05T17:34:32+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                                  Packets               Pings
 Host                                                                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 240.2.112.39                                                                0.0%   161    1.6   1.5   1.3   3.2   0.2
 2. 242.6.28.5                                                                  0.0%   161    6.2   3.0   1.0  37.6   4.9
 3. 151.148.9.242                                                               0.0%   161    1.7   1.4   1.3   1.9   0.1
 4. 151.148.9.243                                                               0.0%   161    1.2   1.1   1.0   2.4   0.1
 5. 192.178.97.43                                                               0.0%   161    2.2   2.5   1.9  32.8   2.8
 6. 192.178.97.54                                                               0.0%   161    1.5   3.3   1.4  56.3   5.9
 7. 192.178.244.237                                                             0.0%   161    2.8   2.8   2.4   4.7   0.3
 8. 142.251.197.136                                                             0.0%   161    3.0   2.9   2.6   5.3   0.3
 9. (waiting for reply)
10. (waiting for reply)
11. (waiting for reply)
12. (waiting for reply)
13. (waiting for reply)
14. (waiting for reply)
15. uv-in-f100.1e100.net                                                        0.0%   160    2.2   2.2   2.2   3.3   0.1
```

dig command

- The dig command is a shorthand for Domain Information Groper. It's a DNS lookup network utility primarily used for verifying and diagnosing DNS issues. The dig command replaces the older `nslookup` and `host` commands.
- The command can return the following DNS records:
- **A record**: Maps a hostname directly to an IP address.
- **MX record**: Mail Exchange record. Specifies the email server for the domain.
- **SIG**: Signature record for encryption protocols.
- For instance, to perform a DNS lookup for **somnog.so**, run the command:
- dig somnog.so

```
somnog@ss-track:~$ dig somnog.so

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> somnog.so
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40218
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;somnog.so.                     IN      A

;; ANSWER SECTION:
somnog.so.              300     IN      A       216.172.184.215

;; Query time: 98 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Dec 05 17:35:06 UTC 2025
;; MSG SIZE  rcvd: 54

somnog@ss-track:~$
```

nslookup command

- A shorthand for ‘Name Server Lookup, the `nslookup` is another useful tool for performing DNS lookups. The command probes a DNS server for information such as the IP address, domain name mapping, and other DNS records. Despite being replaced by the dig command, the `nslookup` utility is a handy network diagnostic tool for troubleshooting DNS-related issues.
- The following command performs a DNS lookup for the domain `somnog.so`.

```
nslookup somnog.so
```

You can specify the type of record using the `type=` option and specify the record type. For example, to view the MX record for the domain, run the command:

nslookup -type=mx somnog.so

nslookup –type=ns google.com

```
somnog@ss-track:~$ nslookup -type=mx somnog.so
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
somnog.so       mail exchanger = 0 mail.somnog.so.

Authoritative answers can be found from:

somnog@ss-track:~$ nslookup -type=ns somnog.so
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
somnog.so       nameserver = ns8441.hostgator.com.
somnog.so       nameserver = ns8442.hostgator.com.

Authoritative answers can be found from:

somnog@ss-track:~$
```

host command

- The host command is a user-friendly DNS lookup tool that displays a domain’s IP and mail server(if one exists). To display a registered domain’s information, simply provide the domain name as the argument as shown.

- host domain
- host google.com

```
somnog@ss-track:~$ host google.com
google.com has address 142.251.30.139
google.com has address 142.251.30.102
google.com has address 142.251.30.138
google.com has address 142.251.30.101
google.com has address 142.251.30.113
google.com has address 142.251.30.100
google.com has IPv6 address 2a00:1450:4009:c15::71
google.com has IPv6 address 2a00:1450:4009:c15::8b
google.com has IPv6 address 2a00:1450:4009:c15::65
google.com has IPv6 address 2a00:1450:4009:c15::8a
google.com mail is handled by 10 smtp.google.com.
somnog@ss-track:~$
```

whois command

- The whois command is a protocol for performing domain lookups by querying a distributed database system. The protocol returns information about the domain, such as domain ownership, registration date, business contact information, etc.
- To run the command, provide the domain name after the `whois` directive.

```
somnog@ss-track:~$ whois somnog.so
Domain Name: somnog.so
Registry Domain ID: 30632-sonic
Updated Date: 2025-11-12T11:30:19Z
Creation Date: 2015-11-09T00:00:00Z
Registry Expiry Date: 2026-11-09T00:00:00Z
Registrar Registration Expiration Date: 2026-11-09T00:00:00Z
Registrar: Asal Solutions_LR
Registrar Street Address: A-6-3, TCC, Taleh, Hodan District,
Mogadishu
Benadir
Registrar Email: websolutions@asalsolutions.com
Registrar Abuse Contact Email: abuse@asalsolutions.com
Registrar Abuse Contact Phone: +252 616965458
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: 68063-sonic
Registrant Name: Abdullahi Bihi Hussein
Name Server: ns8442.hostgator.com
Name Server: ns8441.hostgator.com
DNSSEC: unsigned
>>> Last update of WHOIS database: 2025-12-05T17:40:05.176Z <<<

For more information on domain status codes, please visit https://icann.org/epp
```

wget command

- The wget command downloads files from the internet using the resource's URL. The tool takes the following syntax:

wget https://wordpress.org/latest.zip

wget -O wordpress.zip https://wordpress.org/latest.zip

wget -P /tmp https://wordpress.org/latest.zip

Save file to this links | apps.txt

```
https://www.python.org/ftp/python/3.13.0/Python-3.13.0.tgz

https://wordpress.org/latest.zip
wget -i sample.txt
```

```
somnog@ss-track:~$ wget https://www.python.org/ftp/python/3.13.0/Python-3.13.0.tgz
--2025-12-05 17:42:53--  https://www.python.org/ftp/python/3.13.0/Python-3.13.0.tgz
Resolving www.python.org (www.python.org)... 151.101.64.223, 151.101.0.223, 151.101.128.223, ...
Connecting to www.python.org (www.python.org)|151.101.64.223|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 29186321 (28M) [application/octet-stream]
Saving to: ‘Python-3.13.0.tgz’

Python-3.13.0.tgz                   100%[=============================================================================>]  27.83M  --.-KB/s    in 0.09s

2025-12-05 17:42:53 (316 MB/s) - ‘Python-3.13.0.tgz’ saved [29186321/29186321]

somnog@ss-track:~$
```

cURL command

- cuRL (client URL) is a networking CLI tool that transfers data to and from a server or host system by specifying the server's URL. It supports a range of protocols including HTTP, HTTPS, and FTP.
- The command uses the following syntax:

- curl example.com

- To download a resource, for example, the WordPress compressed file, run the following command. The `-O` option includes a download progress meter that measures download speed, data transfer rate, total time spent, and remaining download time.
- curl https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.4.tar.gz

ssh command

- The ssh command is used to connect to a remote host securely over a TCP/IP network. The command uses the following syntax:

- ssh username@ip- address
- Where: `username` is the user on the remote host
- `ip-address` represents the IP of the remote host. Additionally, a registered domain name can be provided instead.
- For example:
- ssh root@5.199.168.47
- By default, SSH listens on port 22. If not the case, the `-p` flag lets you specify the port number during connection. In this example, SSH on the remote host listens on port 5422. To connect to the host, we will run the command:
- ssh -p 5422 root@5.199.168.47

scp command

- The `scp` (Secure Copy) is a command-line tool that leverages SSH's strong encryption algorithms to copy files securely over a network.
- Here's the syntax:
- scp filename username@hostname_or_IP:/remote/path/
- The following command copies a file `sample_file.txt` to a remote server in the `/home/somnog` path which is the remote user's home directory.
- scp sample_file.txt root@5.199.168.47:/home/somnog
- To copy a directory, use the `-r` for recursive copying. This copies the directory and its entire contents to the remote server. Here, we are copying a directory named `data` to the remote server.
- scp -r data root@5.199.168.47:/home/cherry
- Conversely, you can copy files/directories from the remote server to the local system.
- `scp username@hostname_or_IP:/remote/file/ /local/path`
-
-

Nmap command

- Network Mapper, or Nmap for short, is a flexible and open-source utility mainly used for network scanning and reconnaissance. It is used to perform vulnerability assessments on host systems.
- In this example, nmap scans for all the hosts in the **192.168.2.0/24** subnet.
- To reveal more detailed or intricate information such as service versions pass the -A switch.
- nmap -A 192.168.2.0/24
- To scan a single host provide its IP address.
- nmap -A 192.168.2.1

- **arp command**

- The `arp` command manages the ARP cache on your system. It is used to display or modify ARP cache information. The ARP cache is simply a table that provides a mapping of IP addresses to their MAC addresses in the network. In addition to displaying the entries, you can modify and delete them from the cache.
- To display the entries, run:

- arp
- arp -D 192.168.2.103

- # nmcli command

- The nmcli is a versatile CLI tool for displaying, modifying activating, and deleting network connections. Without command flags, the `nmcli` provides a detailed summary of all network interfaces.

- nmcli
- nmcli device show enp0s3
- nmcli connection show

iftop command

- Short for Interface TOP, iftop is a command-line tool for monitoring bandwidth usage on a specific network interface. Run it as a sudo user or root to monitor all traffic flowing through the interface.
- By default, `iftop` is not installed. You can install it by running:
- **#On Ubuntu / Debian systems**
- sudo apt install iftop -y

bmon command

- The bmon command is a revamped alternative to `iftop`. it displays bandwidth statistics in an intuitive and human-readable format.
- Bmon is not installed out of the box, and you can do so by running:
- **#On Ubuntu / Debian systems**
- sudo apt install bmon –y
- To launch it and start monitoring bandwidth, simply run the command:
- bmon

Conclusion

- this round-up has offered a summary of some nifty commands you can leverage to troubleshoot network faults, monitor bandwidth, and retrieve salient information about network devices and registered domains.