

Lab 1: Network Commands & IP Addressing

Checking Physical (MAC) Address

1. What command shows all network details including the physical (MAC) address?
 - `ipconfig /all`

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ifconfig
enp0s31f6: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 18:db:f2:48:4e:03 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16 memory 0xec300000-ec320000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6862 bytes 990346 (990.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6862 bytes 990346 (990.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.12 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::e043:3792:179d:d24e prefixlen 64 scopeid 0x20<link>
    inet6 fdf4:e3fb:8ca0:7000:84b3:f9e4:3084:bf6c prefixlen 64 scopeid 0x0<global>
    inet6 fdf4:e3fb:8ca0:7000:79b5:472e:50b6:9a5a prefixlen 64 scopeid 0x0<global>
    ether b8:8a:60:f6:c4:44 txqueuelen 1000 (Ethernet)
    RX packets 1721539 bytes 1288892749 (1.2 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 305364 bytes 76411927 (76.4 MB)
    TX errors 0 dropped 7 overruns 0 carrier 0 collisions 0
```

2. How can you see your device's MAC address?
 - `Getmac`

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s31f6: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode DEFAULT group default
    link/ether 18:db:f2:48:4e:03 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default
    link/ether b8:8a:60:f6:c4:44 brd ff:ff:ff:ff:ff:ff
sayedmohamed@sayedmohamed-Precision-3510:~$
```

3. How can you show the MAC address with more details?

- `getmac /v`

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ip addr show
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: enp0s31f6: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 18:db:f2:48:4e:03 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b8:8a:60:f6:c4:44 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 86106sec preferred_lft 86106sec
    inet6 fdf4:e3fb:8ca0:7000:84b3:f9e4:3084:bf6c/64 scope global temporary dynamic
        valid_lft 6908sec preferred_lft 3308sec
    inet6 fdf4:e3fb:8ca0:7000:79b5:472e:50b6:9a5a/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 6908sec preferred_lft 3308sec
    inet6 fe80::e043:3792:179d:d24e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
sayedmohamed@sayedmohamed-Precision-3510:~$
```

APIPA & IP Configuration

4. What is the default APIPA address when the device fails to get an IP from DHCP?
 - Starts with: 169.254.x.x
 5. What command shows your current IP settings?
 - ipconfig
 6. How do you release your current IP address?
 - ipconfig /release
 7. How do you request a new IP address from DHCP?
 - ipconfig /renew
-

Ping Commands

9. How do you test connection to an IP address?

- ping [IP address]

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=6.00 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=5.28 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=5.58 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=5.64 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=8.72 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=5.30 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=5.03 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=4.50 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=2.00 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=5.25 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=4.24 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=7.10 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=4.74 ms
^C
--- 192.168.1.1 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12015ms
rtt min/avg/max/mdev = 1.997/5.336/8.724/1.485 ms
sayedmohamed@sayedmohamed-Precision-3510:~$
```

10. How do you test connection to a website (URL)?

- ping www.example.com

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ping www.google.com
PING www.google.com (142.251.37.228) 56(84) bytes of data.
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=1 ttl=119 time=47.6 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=2 ttl=119 time=50.2 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=3 ttl=119 time=49.3 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=4 ttl=119 time=51.6 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=5 ttl=119 time=51.7 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=6 ttl=119 time=48.1 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=7 ttl=119 time=46.9 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=8 ttl=119 time=50.1 ms
64 bytes from mrs09s16-in-f4.1e100.net (142.251.37.228): icmp_seq=9 ttl=119 time=47.5 ms
^C
--- www.google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 46.936/49.228/51.720/1.676 ms
sayedmohamed@sayedmohamed-Precision-3510:~$
```

11. How do you send a ping with a specific data size?

- ping [IP] -l [size]

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ping -s 100 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 100(128) bytes of data.
108 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=46.6 ms
108 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=46.0 ms
108 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=46.1 ms
108 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=46.2 ms
108 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=50.1 ms
108 bytes from 8.8.8.8: icmp_seq=6 ttl=119 time=46.6 ms
108 bytes from 8.8.8.8: icmp_seq=7 ttl=119 time=45.8 ms
108 bytes from 8.8.8.8: icmp_seq=8 ttl=119 time=46.0 ms
108 bytes from 8.8.8.8: icmp_seq=9 ttl=119 time=46.2 ms
108 bytes from 8.8.8.8: icmp_seq=10 ttl=119 time=46.6 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 901ms
rtt min/avg/max/mdev = 45.762/46.613/50.084/1.188 ms
sayedmohamed@sayedmohamed-Precision-3510:~$
```

12. How do you send a specific number of ping requests?

- ping [IP] -n [count]

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=46.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=48.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=45.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=48.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=46.4 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 45.619/46.913/48.186/1.038 ms
sayedmohamed@sayedmohamed-Precision-3510:~$
```

13. How do you send continuous ping requests until you stop it manually?
- ping [IP] -t

```
sayedmohamed@sayedmohamed-Precision-3510:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=49.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=46.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=46.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=46.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=47.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=119 time=47.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=119 time=46.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=119 time=47.6 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 46.197/47.316/49.787/1.119 ms
sayedmohamed@sayedmohamed-Precision-3510:~$
```

Netstat

19. How do you show all active connections?
 - netstat -a


```

sayedmohamed@sayedmohamed-Precision-3510:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 _localdnsstub:domain    0.0.0.0:*               LISTEN
tcp      0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp      0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp      0      0 localhost:33060         0.0.0.0:*               LISTEN
tcp      0      0 _localdnspoxy:domain    0.0.0.0:*               LISTEN
tcp      0      0 sayedmohamed-Prec:44450 104.18.32.47:https      ESTABLISHED
tcp      0      0 sayedmohamed-Prec:44464 104.18.32.47:https      ESTABLISHED
tcp      0      0 sayedmohamed-Prec:49580 104.18.39.21:https      ESTABLISHED
tcp      0      0 sayedmohamed-Prec:48392 ec2-3-233-158-26.:https ESTABLISHED
tcp      0      0 sayedmohamed-Prec:43176 wf-in-f188.1e100.n:5228 ESTABLISHED
tcp6     0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp      0      0 0.0.0.0:54037           0.0.0.0:*               *
udp      0      0 mdns.mcast.net:mdns     0.0.0.0:*               *
udp      0      0 mdns.mcast.net:mdns     0.0.0.0:*               *
udp      0      0 0.0.0.0:mdns           0.0.0.0:*               *
udp      0      0 _localdnspoxy:domain    0.0.0.0:*               *
udp      0      0 _localdnsstub:domain    0.0.0.0:*               *
udp      0      0 sayedmohamed-Prec:bootpc _gateway:bootps         ESTABLISHED
udp6     0      0 [::]:42738             [::]:*                  *
udp6     0      0 [::]:mdns               [::]:*                  *
udp6     0      0 sayedmoha:dhcpv6-client [::]:*                  *
raw6     0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node     Path
unix   3      [ ]       STREAM     CONNECTED   101078
unix   3      [ ]       STREAM     CONNECTED   77154

```

20. How do you show active connections with numbers only?

- netstat -n

```

sayedmohamed@sayedmohamed-Precision-3510:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp        0      0 192.168.1.12:44450      104.18.32.47:443        ESTABLISHED
tcp        0      0 192.168.1.12:44464      104.18.32.47:443        ESTABLISHED
tcp        0      0 192.168.1.12:49580      104.18.39.21:443        ESTABLISHED
tcp        25      0 192.168.1.12:48392      3.233.158.26:443        CLOSE_WAIT
tcp        0      0 192.168.1.12:43176      142.250.110.188:5228    ESTABLISHED
udp        0      0 192.168.1.12:57026      172.217.18.34:443      ESTABLISHED
udp        0      0 192.168.1.12:68         192.168.1.1:67         ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State       I-Node      Path
unix   3      [ ]         STREAM     CONNECTED   101078
unix   3      [ ]         STREAM     CONNECTED   77154
unix   3      [ ]         STREAM     CONNECTED   21895
unix   3      [ ]         STREAM     CONNECTED   24610      /run/user/1000/bus
unix   3      [ ]         STREAM     CONNECTED   18070      /run/systemd/journal/stdout
unix   2      [ ]         DGRAM      CONNECTED   10230
unix   3      [ ]         STREAM     CONNECTED   34964
unix   3      [ ]         STREAM     CONNECTED   24711      /run/user/1000/bus
unix   3      [ ]         STREAM     CONNECTED   18082      /run/systemd/journal/stdout
unix   2      [ ]         DGRAM      CONNECTED   4813
unix   3      [ ]         STREAM     CONNECTED   23665      /run/systemd/journal/stdout
unix   3      [ ]         STREAM     CONNECTED   4848
unix   3      [ ]         STREAM     CONNECTED   54156
unix   3      [ ]         STREAM     CONNECTED   23913      /run/systemd/journal/stdout
unix   3      [ ]         STREAM     CONNECTED   22872
unix   3      [ ]         STREAM     CONNECTED   15053      /run/systemd/journal/stdout
unix   3      [ ]         STREAM     CONNECTED   8171
unix   3      [ ]         STREAM     CONNECTED   55063      /run/user/1000/gvfsd/socket-Wfd5Azb0
unix   3      [ ]         STREAM     CONNECTED   20490
unix   3      [ ]         STREAM     CONNECTED   22919      /run/user/1000/bus
unix   3      [ ]         STREAM     CONNECTED   22708      @/tmp/.ICE-unix/2642
unix   2      [ ]         STREAM     CONNECTED   10014

```

21. What command shows MAC addresses of other devices on the network?

arp -a

```

sayedmohamed@sayedmohamed-Precision-3510:~$ arp -a
? (192.168.1.40) at f4:e3:fb:8c:a0:70 [ether] on wlp2s0
_gateway (192.168.1.1) at 24:d3:f2:b3:48:55 [ether] on wlp2s0
sayedmohamed@sayedmohamed-Precision-3510:~$ 

```

22. What command deletes the ARP cache?

arp -d

```
sayedmohamed@sayedmohamed-Precision-3510:~$ sudo arp -d 192.168.1.1
sayedmohamed@sayedmohamed-Precision-3510:~$
```

23. To know which IP address belongs to a domain name:

nslookup Domain_Name

Example:

nslookup Yahoo.com

```
sayedmohamed@sayedmohamed-Precision-3510:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.201.14
Name:   google.com
Address: 2a00:1450:4006:80e::200e

sayedmohamed@sayedmohamed-Precision-3510:~$
```

24. To know which domain name belongs to a specific IP address:

Type this command:

nslookup IP_address

Example:

nslookup 87.248.113.14

```
sayedmohamed@sayedmohamed-Precision-3510:~$ nslookup 172.0.0.53
53.0.0.172.in-addr.arpa name = 172-0-0-53.lightspeed.brhmal.sbcglobal.net.
```

Authoritative answers can be found from:

```
sayedmohamed@sayedmohamed-Precision-3510:~$
```