Networking & System Administration Lab

14-09-2021

Submitted by:

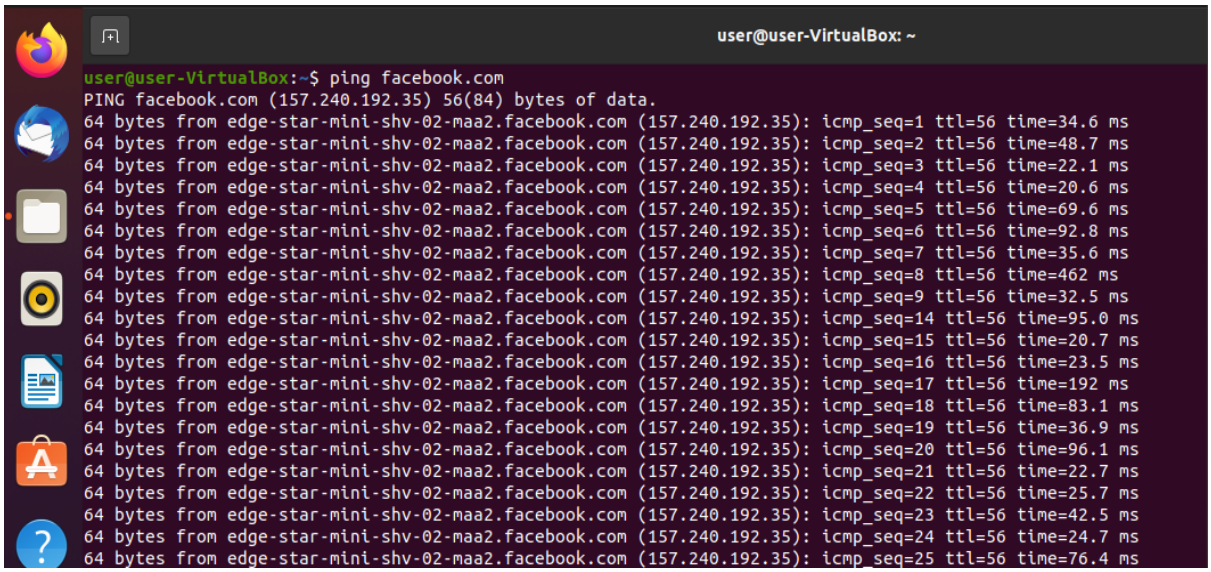
Amal Vijayan

Roll no: 10

S2 RMCA A

Ping Command

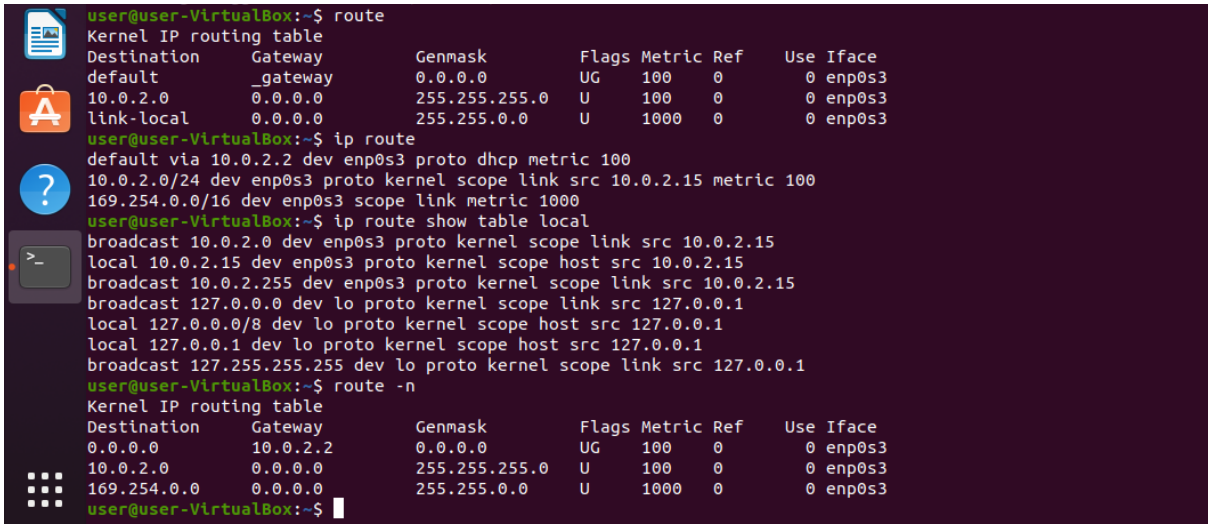
PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection.



```
user@user-VirtualBox: ~
user@user-VirtualBox:~$ ping facebook.com
PING facebook.com (157.240.192.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=1 ttl=56 time=34.6 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=2 ttl=56 time=48.7 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=3 ttl=56 time=22.1 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=4 ttl=56 time=20.6 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=5 ttl=56 time=69.6 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=6 ttl=56 time=92.8 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=7 ttl=56 time=35.6 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=8 ttl=56 time=462 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=9 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=14 ttl=56 time=95.0 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=15 ttl=56 time=20.7 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=16 ttl=56 time=23.5 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=17 ttl=56 time=192 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=18 ttl=56 time=83.1 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=19 ttl=56 time=36.9 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=20 ttl=56 time=96.1 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=21 ttl=56 time=22.7 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=22 ttl=56 time=25.7 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=23 ttl=56 time=42.5 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=24 ttl=56 time=24.7 ms
64 bytes from edge-star-mini-shv-02-maa2.facebook.com (157.240.192.35): icmp_seq=25 ttl=56 time=76.4 ms
```

Route command

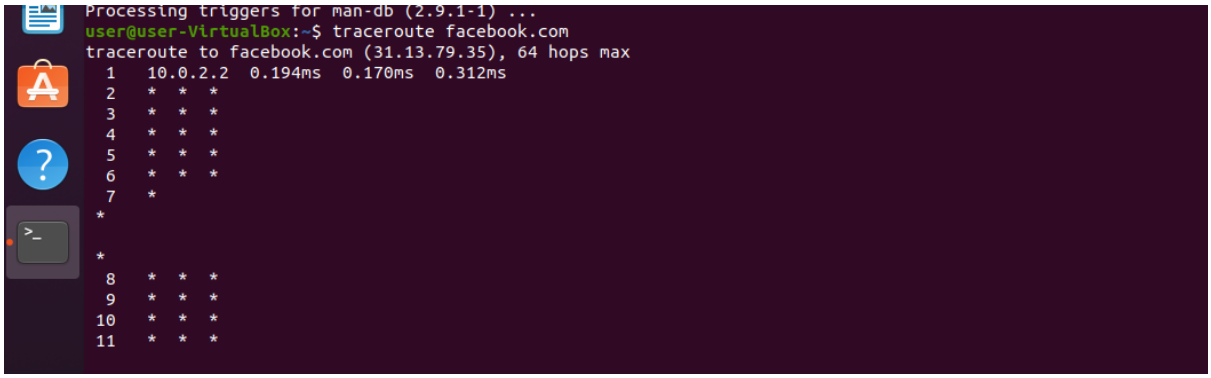
Route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.

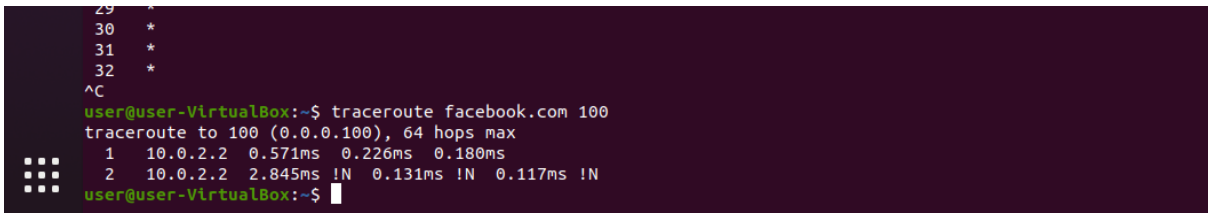


```
user@user-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
user@user-VirtualBox:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
user@user-VirtualBox:~$ ip route show table local
broadcast 10.0.2.0 dev enp0s3 proto kernel scope link src 10.0.2.15
local 10.0.2.15 dev enp0s3 proto kernel scope host src 10.0.2.15
broadcast 10.0.2.255 dev enp0s3 proto kernel scope link src 10.0.2.15
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
user@user-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
user@user-VirtualBox:~$
```

Traceroute command

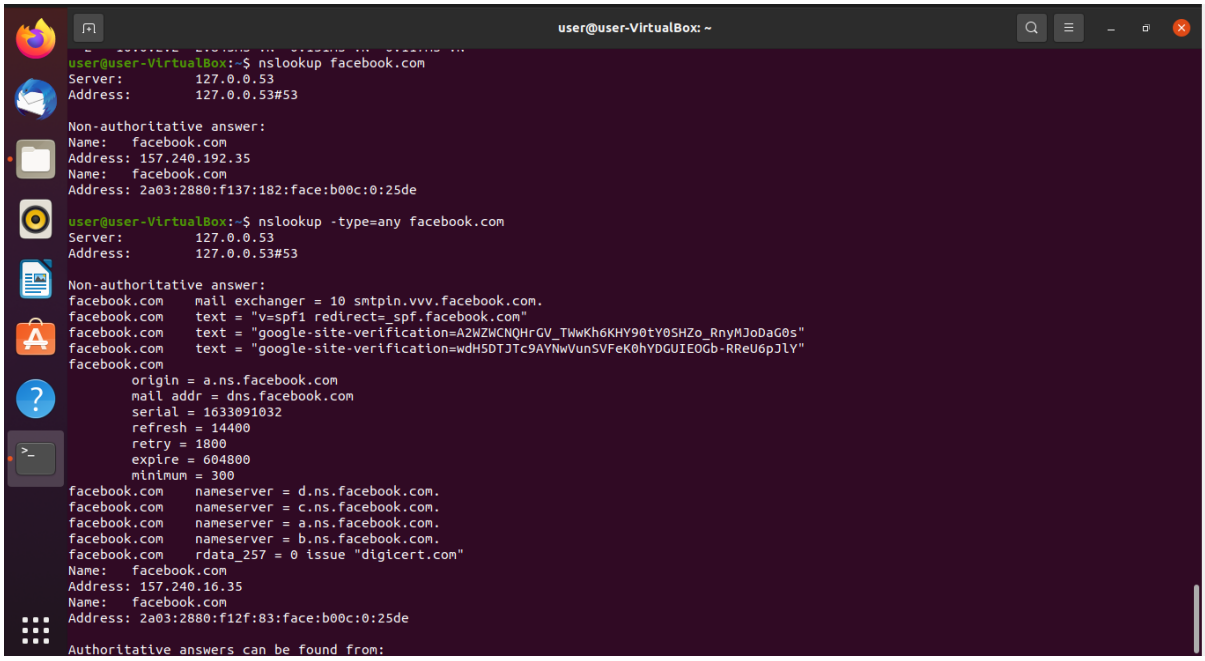
Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google (172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.





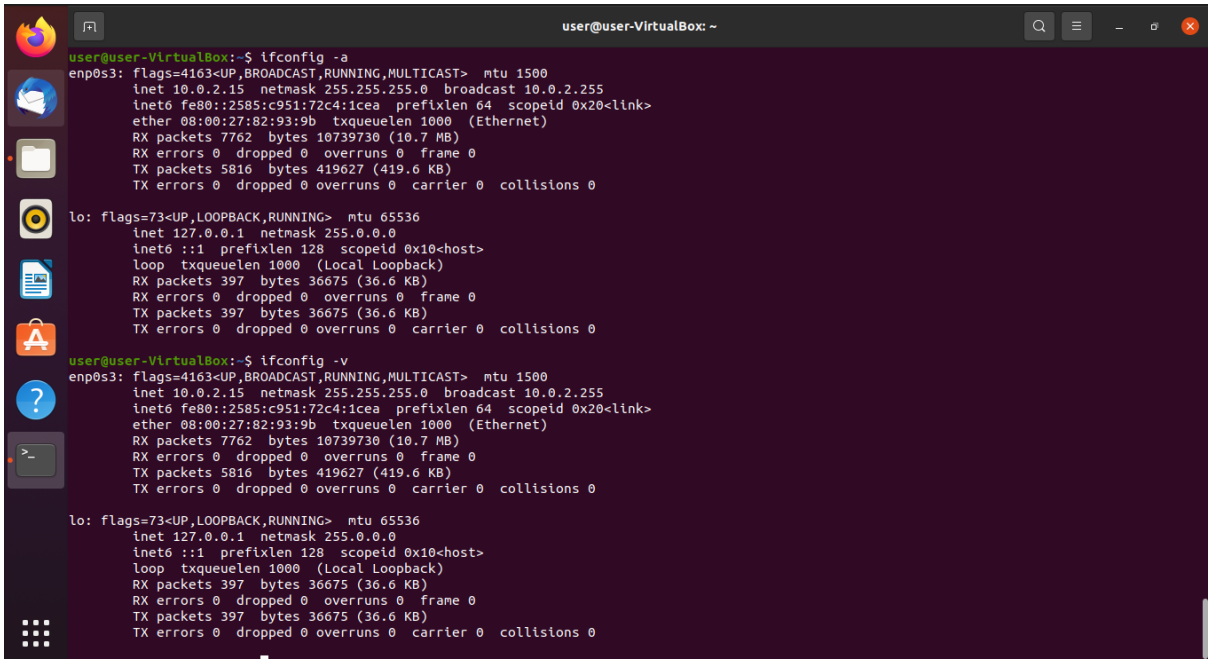
Nslookup command

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.



ifconfig(interface configuration) command

ifconfig(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.



Netstat command

Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

```
user@user-VirtualBox:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
user@user-VirtualBox:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:33852           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 user-VirtualBox:bootpc  _gateway:bootps         ESTABLISHED
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:38892              [::]:*
user@user-VirtualBox:~$
```

```
user@user-VirtualBox: ~
user@user-VirtualBox:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:33852           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 user-VirtualBox:bootpc  _gateway:bootps         ESTABLISHED
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:38892              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     28780    /tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    28471    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     26905    @/tmp/dbus-hSQVlAJE
unix  2      [ ACC ]     STREAM     LISTENING     28474    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     28483    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     26906    @/tmp/dbus-WabPD7y4
unix  2      [ ACC ]     STREAM     LISTENING     28484    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     28485    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     28486    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     28487    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     28488    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     28522    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     28858    /run/mysqld/mysqld.sock
unix  2      [ ACC ]     STREAM     LISTENING     28523    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     28524    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     31121    @/tmp/.ICE-unix/1305
unix  2      [ ACC ]     STREAM     LISTENING     28661    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     28779    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     30577    /tmp/ssh-edesjpgJ6Os4/agent.1183
unix  2      [ ACC ]     STREAM     LISTENING     31122    /tmp/.ICE-unix/1305
```

WINDOWS COMMANDS

1. Ping & traceroute tests

Ping and Trace Route tests can help to identify any connection issues between your network and a specified server (or website) address. PING test:

The PING command is used to test the connection and latency between two network connections.

The PING command sends packets of information to a specified IP Address and then measures the time it takes to get a response from the specified computer or device.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AMAL>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.192.35] with 32 bytes of data:
Reply from 157.240.192.35: bytes=32 time=18ms TTL=57
Reply from 157.240.192.35: bytes=32 time=20ms TTL=57
Reply from 157.240.192.35: bytes=32 time=21ms TTL=57
Reply from 157.240.192.35: bytes=32 time=19ms TTL=57

Ping statistics for 157.240.192.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 21ms, Average = 19ms

C:\Users\AMAL>
```

Trace Route test:

The TRACERT command is used to conduct a similar test to PING, but instead of displaying the time it takes to connect, it looks at the exact server hops required to connect your computer to the server. You should already have the CMD prompt dialogue box open, after performing the PING test above.

2. Nslookup

Microsoft Windows includes a tool called NSLOOKUP that you can use via the command prompt. This tool can be used to check DNS records propagation and resolution using different servers, and perform other troubleshooting steps.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AMAL>nslookup facebook.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f137:182:face:b00c:0:25de
          157.240.7.35


C:\Users\AMAL>
```

- Type nslookup -q=XX where XX is a type of a DNS record. Some of the available types are MX, A, CNAME, and TXT. The records are then displayed, to exit the tool type exit.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AMAL>nslookup facebook.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f137:182:face:b00c:0:25de
          157.240.7.35


C:\Users\AMAL>nslookup -type=ns facebook.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
facebook.com    nameserver = d.ns.facebook.com
facebook.com    nameserver = c.ns.facebook.com
facebook.com    nameserver = b.ns.facebook.com
facebook.com    nameserver = a.ns.facebook.com

C:\Users\AMAL>
```

- To use nslookup as a troubleshooting tool, you can set the specific type of record to lookup for a domain by using the - type=record_type where record_type is A, CNAME, MX, PTR, NS, ANY. Type nslookup -type=ns domain_name where domain_name is the domain for your query and hit Enter. Now the tool will display the name servers for the domain you specified.

3. **Netstat**

On Windows 10, netstat (network statistics) has been around for a long time, and it's a command-line tool that you can use in Command prompt to display statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for system or applications.

```
C:\Windows\System32\cmd.exe - netstat

C:\Users\AMAL>nslookup -type=ns facebook.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
facebook.com    nameserver = d.ns.facebook.com
facebook.com    nameserver = c.ns.facebook.com
facebook.com    nameserver = b.ns.facebook.com
facebook.com    nameserver = a.ns.facebook.com

C:\Users\AMAL>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:52246        LAPTOP-5GEAB7TG:64542  ESTABLISHED
  TCP    127.0.0.1:64536        LAPTOP-5GEAB7TG:65001  ESTABLISHED
  TCP    127.0.0.1:64542        LAPTOP-5GEAB7TG:52246  ESTABLISHED
  TCP    127.0.0.1:65001        LAPTOP-5GEAB7TG:64536  ESTABLISHED
  TCP    192.168.48.115:49653   13.68.168.63:https     ESTABLISHED
  TCP    192.168.48.115:53182   20.197.71.89:https     FIN_WAIT_1
  TCP    192.168.48.115:55103   11140-26803:751        ESTABLISHED
```

- **netstat –n:**

Command to display active connections showing numeric IP address and port number instead of trying to determine the names.

```
C:\Users\AMAL>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:52246        127.0.0.1:64542        ESTABLISHED
  TCP    127.0.0.1:64536        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:64542        127.0.0.1:52246        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:64536        ESTABLISHED
  TCP    192.168.48.115:49653   13.68.168.63:443       ESTABLISHED
  TCP    192.168.48.115:55103   185.25.50.237:751      ESTABLISHED
  TCP    192.168.48.115:55104   13.88.181.35:443       ESTABLISHED
  TCP    192.168.48.115:55116   20.198.162.78:443      ESTABLISHED
  TCP    192.168.48.115:55118   20.44.229.112:443      TIME_WAIT
  TCP    192.168.48.115:55121   20.44.229.112:443      ESTABLISHED
  TCP    192.168.48.115:55122   104.85.155.36:80       TIME_WAIT
  TCP    192.168.48.115:55123   49.44.194.58:80        TIME_WAIT
  TCP    192.168.48.115:55124   52.109.124.51:443      ESTABLISHED
  TCP    192.168.48.115:58096   52.98.63.34:443        ESTABLISHED

C:\Users\AMAL>
```

- **netstat –n:**

INTERVAL In the command, make sure to replace INTERVAL for the number (in seconds) you want to redisplay the information.

- **netstat –n:**

Command to display active connections showing numeric IP address and port number instead of trying to determine the names. netstat -n INTERVAL In the command, make sure to replace INTERVAL for the number (in seconds) you want to redisplay the information.

```
C:\Windows\System32\cmd.exe
  TCP    192.168.48.115:55124   52.109.124.51:443      ESTABLISHED
  TCP    192.168.48.115:58096   52.98.63.34:443        ESTABLISHED

C:\Users\AMAL>netstat -n 5

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:52246        127.0.0.1:64542        ESTABLISHED
  TCP    127.0.0.1:64536        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:64542        127.0.0.1:52246        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:64536        ESTABLISHED
  TCP    192.168.48.115:49653   13.68.168.63:443       ESTABLISHED
  TCP    192.168.48.115:55103   185.25.50.237:751      ESTABLISHED
  TCP    192.168.48.115:55104   13.88.181.35:443       ESTABLISHED
  TCP    192.168.48.115:55116   20.198.162.78:443      ESTABLISHED
  TCP    192.168.48.115:55121   20.44.229.112:443      TIME_WAIT
  TCP    192.168.48.115:55122   104.85.155.36:80       TIME_WAIT
  TCP    192.168.48.115:55123   49.44.194.58:80        TIME_WAIT
  TCP    192.168.48.115:58096   52.98.63.34:443        ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:52246        127.0.0.1:64542        ESTABLISHED
  TCP    127.0.0.1:64536        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:64542        127.0.0.1:52246        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:64536        ESTABLISHED
  TCP    192.168.48.115:49653   13.68.168.63:443       ESTABLISHED
  TCP    192.168.48.115:55103   185.25.50.237:751      ESTABLISHED
```

- **netstat -b**

The netstat -b command lists all the executables (applications) associated with each connection. Sometimes, applications may open multiple connections.

- **netstat -e**

The netstat -e command generates a statistic of the network interface, which shows information like the number of bytes, unicast and non-unicast sent and received packets. You can also see discarded packets and errors and unknown protocols, which can you troubleshoot networking problems.

```
C:\Windows\System32\cmd.exe
  TCP    127.0.0.1:65001        127.0.0.1:64536        ESTABLISHED
  TCP    192.168.48.115:49653   13.68.168.63:443       ESTABLISHED
  TCP    192.168.48.115:55103   185.25.50.237:751      ESTABLISHED
  TCP    192.168.48.115:55116   20.198.162.78:443      ESTABLISHED
  TCP    192.168.48.115:55121   20.44.229.112:443      TIME_WAIT
  TCP    192.168.48.115:55122   104.85.155.36:80       TIME_WAIT
  TCP    192.168.48.115:55123   49.44.194.58:80        TIME_WAIT
  TCP    192.168.48.115:58096   52.98.63.34:443        ESTABLISHED
^C
C:\Users\AMAL>netstat -b
The requested operation requires elevation.

C:\Users\AMAL>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     550926286       350735168
Unicast packets             1216795          666709
Non-unicast packets            2574            7792
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\AMAL>
```

4. ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

```
C:\Windows\System32\cmd.exe
  TCP    192.168.48.115:55116   20.198.162.78:https    ESTABLISHED
^C
C:\Users\AMAL>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6ccc:e1ce:b996:7871%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7485:728a:fddd:4ae0%17
```

- **/all:**

Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

```
C:\Windows\System32\cmd.exe
^C
C:\Users\AMAL>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6ccc:e1ce:b996:7871%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7485:728a:fddd:4ae0%17
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

- **/registerdns:**

Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

- **/displaydns:**

Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

```
C:\Windows\System32\cmd.exe

C:\Users\AMAL>ipconfig /displaydns

Windows IP Configuration

    203.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 203.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 3243
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : LAPTOP-OF9SBL90.mshome.net


    ucmetrixa.info
    ----------------------------------------
    Record Name . . . . . : ucmetrixa.info
    Record Type . . . . . : 1
    Time To Live  . . . . : 1176
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 194.180.158.55


    ucmetrixb.info
    ----------------------------------------
    Record Name . . . . . : ucmetrixb.info
    Record Type . . . . . : 1
    Time To Live  . . . . : 754
```

- **/flushdns:**

Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

```
C:\Windows\System32\cmd.exe

C:\Users\AMAL>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\AMAL>
```

Other Networking Commands

1. **Hostname Command**

   A very simple command that displays the host name of your machine. This is much quicker than going to the control panel>system route.

2. **getmac Command**

   Another very simple command that shows the MAC address of your network interfaces

3. **arp Command**

   This is used for showing the address resolution cache. This command must be used with a command line switch arp -a is the most common.

4. **Nbtstat**

   Diagnostic tool for troubleshooting NetBIOS problems. 5. Net Command Used for managing users, service, shares etc.

5. **Net Command**

   Used for managing users, service, shares etc.

```
C:\Windows\System32\cmd.exe

C:\Users\AMAL>hostname
LAPTOP-5GEAB7TG

C:\Users\AMAL>getmac

Physical Address    Transport Name
=================== ==========================================================
08-97-98-BD-91-D0   Media disconnected
62-47-E7-44-3B-99   \Device\Tcpip_{05C2EF50-39C6-4AE2-B9CA-75248A053EFA}
CA-E2-65-9E-66-D7   \Device\Tcpip_{C34D272F-3434-400A-A959-A603B0A9E2B1}
0A-00-27-00-00-0A   \Device\Tcpip_{8645ADE5-D08B-4462-91DB-4F473BC63589}

C:\Users\AMAL>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
```