16/7/24

Experiment – 1

1. arp – a

2. hostname

3. ipconfig/all [ifconfig]

4. nbstat -a [nmblookup -A 192.168.1.1]

5. netstat

6. nslookup [nslookup google.com]

7. pathping [Unique to windows]

8. ping

9. Route

O/P

1. _gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
2. localhost - live
3. enp0s3: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
   inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255

   lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536
   inet 127.0.0.1 netmask 255.0.0.0
4. Looking up status of 192.168.1.1
   No reply from 192.168.1.1
5. Active Internet Connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	localhost-live:58446	166.188.117.34.bc:https	Established
tcp	0	0	43492	104.18.32.115:https	Established
udp	0	0	Bootpc	_gateway:bootps	Established

6. Server: 127.0.0.53
   Address: 127.0.0.53#53

   Non-authoritative answer:
   Name: google.com
   Address: 216.58.203.46
   Name: google.com
   Address: 2404:6800:4009:80f::200e

8. Limited to Windows

9. PING google.com (216.58.203.46) 56(84) bytes of data
   64 bytes from ~~216.58.~~hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=1 ttl= time=
   64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=2 ttl=59 time = 37.7 ms
   64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=3 ttl=59 time=36.6 ms

   --- google.com ping statistics ---
   3 packets ~~received~~ transmitted, 3 received, 0% packet loss, time 200 ms
   rtt min/avg/max/mdev = 36.582/43.447/56.041/8.917 ms

[enps03 → enp0s3]

1. ip

ip <options> <object> <command>

a. # ip address show

b. # ip address add 192.168.1.254/24 dev enps03

c. # ip address del 192.168.1.254/24 dev enps03

d. # ip link set eth0 ~~down~~ up

e. # ip link set eth0 down

f. # ip link set eth0 promisc on

g. # ip route add default via 192.168.1.254 dev eth0

h. # ip route add 192.168.1.0/24 ~~via~~ via 192.168.1.254

i. # ip route add 192.168.1.0/24 dev eth0

j. # ip route delete 192.168.1.0/24 via 192.168.1.254

k. # ip route get 10.10.1.4

ip address 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

2: enp0s3: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500
qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:1f:01:65 brd ff:ff:ff:ff:ff:ff

ip address add 192.168.1.254/24 dev enp0s3
RTNETLINK answers: File exists

ip address del 192.168.1.254/24 dev enp0s3

ip address add 192.168.1.254/24 dev enp0s3

ip address add 192.168.1.254/24 dev enp0s3

ip route get 10.10.1.4
10.10.1.4 via 10.0.2.2 dev enp0s3 src 10.0.2.15 uid 0
cache

ifconfig
enp0s3: flags = 4163 <UP, BROADCAST, RUNNING, MULTICAST>
mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast
10.0.2.255

lo: flags = 73 <UP, LOOPBACK, RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0

ip link set enp0s3 up

ip link set enp0s3 down

ip link set enp0s3 promisc on

ip route add 192.168.1.0/24 dev enp0s3
Error: Device for nexthop is not up.

2. mtr

mtr <options> hostname/IP

a. # mtr google.com

b. # mtr -g google.com

c. # mtr -b google.com

d. # mtr -c 10 google.com

localhost-live (2401:4900:1cc9:2ab:1cde:6de:ac1b:a2fe)
→ google.com (2404:6800:4009:811::200e)

Scale: .: 984 ms 1: 937 ms 2: 859 ms 3: 749 ms 9: 609 ms
b: 437 ms c: 234 ms

mtr -l google.com

x 0 338000
x 1 338001
x 2 338002
x 3 338003
x 4 33004

3. tcpdump

a. # dnf install -y tcpdump

b. # tcpdump -D

c. # tcpdump -i eth0

d. # tcpdump -i eth0 -c 10

e. # tcpdump -i eth0 -c 10 host 8.8.8.8

f. # tcpdump -i eth0 src host 8.8.8.8

g. # tcpdump -i eth0 dst host 8.8.8.8

h. # tcpdump -i eth0 net 10.1.0.0 mask 255.255.255.0

i. # tcpdump -i eth0 net 10.0.0.0/24

j. # tcpdump -i eth0 port 53

k. # tcpdump -i eth0 host 8.8.8.8 and port 53

l. # tcpdump -i eth0 -c 10 host www.google.com and port 443

```
#dnf install -y tcpdump
Last metadata expiration check: 0:43:06 ago on
                Thu 11 Jul 2024 03:48:46 PM EDT.
Package tcpdump-14:4.99.4-2.fc39.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
#tcpdump -D
1. enp0s3 [Up, Running, Connected]
2. lo [Up, Running, Loopback]
3. bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
#tcpdump -i enp0s3
dropped privs to tcpdump
tcpdump: verbose outpumpt suppressed, use -v[v]... for
full protocol decode
listening on enp0s3, link-type EN10MB(Ethernet), snapshot
length 262144 bytes
16:32:48.655388 ARP, Request who-has 192.168.1.12 tell _gateway,
length 46
16:32:50.761108 IP 192.168.1.10.6537 > 255.255.255.255.6537: UDP,
length 201
^C
361 ~~packets~~ packets captured
361 packets received by filter
0 packets dropped by kernel
#tcpdump -i enp0s3 host 8.8.8.8
~~tcpdump:~~
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full
protocol
listening on enp0s3, link-type EN10MB(Ethernet), snapshot
length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

```
#tcpdump -i enp0s3 -c 3
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]...
for full protocol decode
16:33:19.629767 IP localhost-live.49664 > mad05s23-in-f3.
1e100.net.https: Flags [P.], seq 4162835473:4162835512,
ack 26699339727, win 501, options [nop,nop,TS val
1893368936 ecr 3471518623], length 39
3 packets captured
3 packets received by filter
0 packets dropped by kernel

#tcpdump -i enp0s3 host google.com and port
443
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]...
for full protocol decode
listening on enp0s3, link-type EN10MB(Ethernet),
snapshot length 262144 bytes
^C
0 packets captured
4 packets received by filter
0 packets dropped by kernel
```

$nmcli connection show

NAME	UUID	TYPE	DEVICE
wired connection 1	598bdda8-3af4-3001-8651-defed43f2909e	ethernet	enp0s3
lo	01d710d2-4204-4c1e-9452-07fe9915ae60	loopback	lo

$nmcli connection add con-name cenp0s2 type ethernet
connection 'cenp0s2' (61,06 79c-6702-4761-afb3-04,8090aeb71,d) successfully added.

$nmcli connection modify "Wired connection 1" ipv4.method auto

$nmcli connection modify "Wired connection 1" ipv6.method auto

$ ip address show enp0s3
2: enp0s3 : <BROADCAST, MULTICAST, PROMISC, UP, LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:1f:01:65 brd ff:ff:ff:ff:ff:ff

$ ip route show default
default via 192.168.137.1 dev enp0s3 proto dhcp src 192.168.137.92 metric 1000

$ cat /etc/resolv.conf
nameserver 127.0.0.53
options edns0 trust-ad
search mshome.net

Student Observation

1. Which command is used to find the reachability of a host machine from your device?

Ping command

2. Which command will give the details of hops taken by a packet to reach its destination?

mtr (Matt's traceroute)

3. Which command displays the IP configuration of your machine?

IP <options> <object> <command>

4. Which command displays the TCP port status in your machine?

netstat

5. Write the modify ip configuration in a Linux machine

i.

address add 192.168.1.254/24 dev enp0s3

ii.

ip addres del 192.168.1.254/24 dev enp0s3

Result

Thus networking commands of both Linux & Windows are studied and executed successfully

16/7/24