Practical - 1

Aim:

Study of various network commands used in linux and windows.

Basic Networking commands:

windows commands:

1) arp - a

```
Interface : 192.168.100.1 ... 0xd
Internet Address      Physical Address        Type
192.168.100.254       00-50-56-f1-56-76       dynamic
172.16.8.1            7C-5a-1C-cb-b0-45       dynamic
224.0.0.2             01-00-5e-00-00-02       Static
239.255.255.250       01-00-5e-7f-ff-fa       static
```

2) Hostname

```
DESKTOP-HCVQAND
```

3) ipconfig/all

```
windows IP configuration
Host name . . . . . . . . . : DESKTOP-HCVQAND
Primary Dns Suffix . . . . . . . :
Node Type . . . . . . . . . : Mixed
IP Routing Enabled . . . . . . . : No
WINS Proxy Enabled . . . . . . . : No
Ethernet adapted Ethernet
connection - specific DNS suffix . . . . :
Description . . . . . . : Relatete PC Teable
                          Family Controller
DNS Servers . . . . . . : 172.16.81
```

NetBIOS over TCpip . . . . . . : Enabled

4) nbtstat - a

```
NBTSTAT [[-a Remote Name] [- A IP address] [-c] [-n]
    [-r] [-R] [-RR] [-s] [-S] [interval]]
```

Remote Name   Remote host machine name
IPaddress   Dotted decimal representation of IP address
interval   Redisplays selected statistics, pausing interval sec b/w each display

5) netstat

```
Active   connections
Proto    Local Add              Foreign Add             State

TCP   172.16.8.85:7680      172.16.8.179:55362      ESTABLISHED

TCP   172.16.8.85:7680      HDC1017152:38881        TIME-WAIT

TCP   172.16.8.85:62716     123:http                TIME-WAIT

TCP   172.16.8.85:62734     172:16.11.105:ms-do     SYN-SENT
```

6) nslookup

nslookup www.google.com

```
Server : unknown
Address : 172.16.8.1
Non-authoritative answers:
Name : www.google.com
Addresses : 2404:6800:4007:816:2004
            142.250.183.228
```

7) pathping

```
usage : pathping [-g host-list] [-h maximum-hops]
    [-i address] [-n] [-p period] [-q num-queries] ...
    [-w timeout] [-4] [-6] target-name
```

8) ping

Ping www.rajalakshmi.org

```
Pinging www.rajalakshmi.org [14.99.10.232] with 32
                              bytes of data

Reply from 14.99.10.232: bytes:32 time <1ms TTL
                                            =127

Reply from 14.99.10.232: bytes=32 time=1ms TTL
                                =127

Ping statics for 14.99.10.232
   Packets: Sent = 4 Received = 4, Lost = 0(0% loss),
   Min = 0ms. Max = 1ms. Avg = 0ms
```

9) Route

```
Route [-f] [-p] [-4] [-6] command [destination]
   [MASK netmask] [gateway] [METRIC metric] [IF
                                 Interface]
```

Command one of these:

PRINT   Prints a route
ADD   Adds a route
DELETE   Deletes a route
CHANGE   Modifies an existing route

LINUS COMMANDS:

1) arp - a

```
gateway (172.16.8.1) at 7c:50:1c:cf:b0:45 [ether]
                                    on enp2s0
```

2) Hostname

```
localhost: local domain
```

3) ifconfig

```
enp2s0: flag=4163<up, BROADCAST, RUNNING. MULTICAST
                                    mtu 1500
```

lo: flags = 73 <UP, LOOPBACK, RUNNING> mtu 65536

w1 p3s0: flags = 4099 <UP, BROADCAS. MULTICAST> mtu 1500

4) nmblook - A <ip address>

nmblookup - A 14.99.10.232

looking up status of 14.99.10.232

WORKGROUP <00> - <GROUP> B <ACTIVE>

DESKTOP - BQ498VC <00> - B <ACTIVE>

MAC Address - 50 - 9A - 4C - 34 - D3 - C3

5) nslookup www.google.com

Server : 172.16.8.1

Address : 172.16.8.153

Non - authorised answer

Name : www google.com

Address : 142.250.183.228

6) ping

(i) ping localhost

PING localhost (localhost (::1)) 56 data bytes

64 bytes from localhost (::1): icmp-seq = 1 ttl = 64 time = 0.077ms

(ii) ping 4.2.2.2

PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data

64 bytes from 4.2.2.2: icmp-seq = 1 ttl = 53 time = 35.2ms

(iii) ping www.facebook.com

PING star mini.cdr 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 = 59 time = 27.9 ms

7) Route

```
Kernel IP routing table
Destination  Gateway  Genmask        Flags  Metric  Ref  use
default      gateway  0.0.0.0        UG     100     0    0
172.16.8.0   0.0.0.0  255.255.258.0  U      100     0    0
```

Some important Linux networking commands

1) ip

ip <options> <object> <command>

a) # ip address show

1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536

inet 127.0.0.1/8 scope host lo

valid - lft forever

inet 6 ::1/129

2: enp 2s0: <BROADCAST, MULTICAST, UP, LOWER-UP> mtu 1500

link/ether 50.9a:4c:34:d8:85

3: wlp3s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500

link/ether d4:6a:82:ca:fb

b) # ip address add 192.168.1.254/24 dev enp5o3

c) # ip address del 192.168.1.254/26 dev enp5o3

d) # ip link set eth0 up

e) # ip link set eth0 down

f) # ip link set eth0 promise on

g) # ip route add default via 192.168.1.254 dev eth0

h) # ip route add 192.168.1.0/24 via 192.168.1.254

i) # ip route delete 192.168.1.0/24 via 192.168.1.254

j) # ip route add 192.168.1.0/26 dev etho

k) # ip route get 10.10.1.4

10.10.1.4 via 172.16.8.1 dev enp0 src
172.16.8.84 uid 0 cache

2) ifconfig

enps0: flags=4163<up, BROADCAST, RUNNING,
MULTICAST> mtu 1500

lo: flags=73<UP, LOOPBACK, RUNNING> mtu
65536

wlp3s0: flags=4099<UP, BROADCAST, MULTICAST
mtu 1500

3) mtr

mtr <options> host ie/ip

a) # mtr google.com

Host Packets Pings

172.16.8.1 host % snt last dog Best wost std

52.2%. 160 0.2 0.2 0.2 0.3 0.0

48.6%. 181 0.d 3.6 2.6 43%. 4.2

142.250.71.161

b) # mtr .g google.com

c) # mtr -b google.com

d) # mtr - c 3 google.com

e) # mtr - l google.com

4) tcp dump

tcp dump: 287 packets captured
1033 packets recieved by filter
740 packets dropped by kernel

a) # dnf install -y tcpdump

last meta data expiration check: 2:50:40 ago
on tue 23 Jul 2024 08:23:12 AM IST

package tcpdump - 14:4:9.0.2 fc26.i686
is already installed, skipping.
Dependencies resolved
nothing to do
Complete;

b) # tcpdump - D

1. enp2s0 [up, Running; loopback]

2. any (Pseudo. device that captures on all interface)

3. lo [up, Running, loopback]

4. wlp3s0 [up]

c) # tcpdump - i etho [# tcpdump - i enp2s0]

tcpdump: etho: No device

(tcp dump: verbose output suppressed, use -v (or)
-vv listening on enp2s0, link - type EN10MB
(ethernet), capture 11:31:24.517943. IP 172.
16.9.164.5102 > 239.256.255.250.
11:31:24.518748 IP local host. local domain. total
domain. 45156, 18 packets captured, 328 packets
recieved, 328 dropped,

d) # tcpdump - i enp2s0 - c 4

listening on enp2s0, link - type EN10MB (Ethernet)

```
11:36:56.347974 IP 172.16.9.46 mdns>
224.0.0.251.mdns
4 packets captured
252 packet recived by filter
243 packets dropped by kernel
```

e)
```
# tcpdump -i enp2s0 -c 4 host 88.88
tcpdump: Verbose output suppressed (Ethernet)
0 packets recived by filter
0 packets captured
0 packets dropped by kernel
```

```
nmcli connection show
Name        UUID                          TYPE
wired       59afbdda8-3bf4-3001           ethernet
connection  -8551-defed4fb29090c

                                          DEVICE
                                          enp0S3
```

```
# nmcli connection add con-name enp0s2
type ethernet
connection enp0s2 (640679c-6702-4761-
               af63-948090a0b74d)
# nmcli connection modify "wired connection
, ipv4: method auto
# nmcli connection modify "wired connection
"" ipv6.method auto.
# ip address show enp0s2
2: enp0s2: <BROADCAST,MULTICAST,PROMISE
UP,LOWER UP> mtu
1500 qdisc fq-codel state up group default qlen
1000
link/ether 08:00:27:cb:01:45 brd ff:ff:
          ff:ff:ff
```

```
# ip route show default
default via 192.168.137.1 dev enp0s2 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
```

8
14/7/24

Result:

Various Network commands used in Linux and windows have been studied.