Study of various Network commands used in Linux

1) arp -a

gateway (172.16.8.1) at 7c:5a:1c:cf:be:45 [ether] on wlp3s0
gateway (172.16.8.1) at 7c:5a:1c:cf:be:45 [ether] on enp2s0

2) hostname

localhost.localdomain

3) ifconfig

enp2s0 : flags = 4163<UP, BROADCAST, RUNNING, MULTICAST > mtu 1500
    inet 172.16.11.3 netmask 255.255.252.0 broadcast

wlp3s0 : flags = 4163<UP, BROADCAST, RUNNING, MULTICAST > mtu 1500
    inet 172.11.16 5 netmask 255.255.252.0 broadcast

3) nmblookup -A 192.168.1.1

looking up status of 192.168.1.1
No reply from 192.168.1.1

4) netstat -r

Kernal IP routing table

Destination	Gateway	Genmask	Flags	MSS window	irtt	Iface
default	gateway	0.0.0.0	UG	0	0	enp2s0
172.16.8.0	0.0.0.0	255.255.252.0	U	0	0	wlp3s0

5) nslookup www.google.com

Server : 172.16.8.1

Address : 172.16.8.1#53

Study of various Network commands used in Windows

1) arp -a;

    Interface : 192.168.26.1 --- 0xe

Internet Address	Physical Address	Type
192.168.26.255	ff-ff-ff-ff-ff	Static
224.0.0.22	01-00-5e-00-00-16	static

    Interface : 172.16.8.113 --- 0xf

Internet Address	Physical Address	Type
172.16.8.1	f8-bc-12-90-42-d8	dynamic
172.16.11.255	ff-ff-ff-ff-ff	static

2) hostname

    DESKTOP-A7IULD8

3) ipconfig:-

    Windows IP Configuration

    Ethernet adapter Ethernet:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address....: fe80:: d29a: 90f8: b093:115a/15
    IPv4 Address............: 172.16.8.113
    Subnet Mask.............: 255.255.252.0
    Default Gateway.........: 172.16.8.1

    Wireless LAN adapter Local-Area Connection * 1:

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

4) nbtstat -a (hostname)

    <u>Input</u>: nbtstat -a DESKTOP-ATIULD8

    <u>Output</u>:- Ethernet:

        Node Ip Address: [172.16.8.113] Scope ID: []

        Host Not fount

        VMware Network Adapter V.Hnet 8:

        Node IPAddress: [192.168.186.1] Scope Id: []

5) nbtstat -a :-

    Display protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP)

    NBTSTAT [[-a RemoteName] [-A IP Address] [-c] [-n]

        [-r] [-R] [-RR] [-s] [-S] [interval]]

-a — lists the remote machine's name table given its name

-A — lists the remote machine's name table given its IP Address

-c — List NBT's cache of remote names and their IP addresses

-n — Lists local NetBIOS names.

-r — Lists names resolved by broadcast and via WINS

-R — Purges and reloads the remote names.

-S — List sessions table with the destination IP address

-s — Lists sessions table converting destination IP address to computer NETBIOS names

-RR — Sends Name Release packets to WINS and then, starts Refresh

11) ping

ping [-t][-a] [-n count] [-l size] [-f] [-i TTL]
     [-v TOS] [-r count] [-s count] [-j host-list]
     [-k host-list] [-w timeout] [-R][-S srcaddr]
     [-c compartment] [-p] [-4] [-6] target_name

ping -t 172.16.8.1

Pinging 172.16.8.1 with 32 bytes of data:
Reply from 172.16.8.1 : bytes = 32   time < 1ms   TTL = 64
Reply from 172.16.8.1 : bytes = 32   time < 1ms   TTL = 64

ping 172 172.16.8.1

Ping statistics for 172.16.8.1:
    Packets: Sent = 26, Received = 26, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds.
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Some important linux networking commands

1. ip

Eg: ip address show

1) lo : <LOOP BACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link /loopback 00:00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo

2) enp2s0 : <NO_CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
link /ether 50:9a:4c:34:d3:b5 brd ff:ff:ff:ff:ff

3) wlp3s0 : <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
link /ether d4:6a:6a:82:cd:0b brd ff:ff:ff:ff:ff:ff

2) ifconfig

enp2s0: flags=4049 <UP, BROADCAST, MULTICAST > mtu 1500
ether 50:9a:4c:34:d3:b5 txqueuelen 1000 [Ethernet]
RX packets 0 bytes 0 (0.0 B)

lo : flags = 73 <UP, LOOPBACK, RUNNING > mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 128 stepid 0x10 <host>

wlp3s0: flags = 4163 <UP, BROADCAST, RUNNING, MULTICAST > mtu 1500
inet 172.16.11.78 netmask 255.255.252.0 broadcast
172.16.11.255
inet6 fe80 :: fdfo : b6ce :2ea6 :bd02 prefixlen 64 stepid
0x20 < link>
ether d4:6a:6a:82:cb:0b txqueuelen 1000 (Ethernet)
RX packets 32,323 bytes 3291155 (3.1 MiB)

3) mtr

ey: mtr google.com

	Packets				Pings			
Loss%	Snt	Last	Avg	Best	Wrst	StDev		
28.0%	78	156	71.6	4.5	489.5	93.9		
25.7%	92	188.3	100.7	7.5	1292	200.7		
26.1%	96	248.0	191.7	9.5	2003	327.5		

4) tcpdump.

eg: tcpdump -D

1) wlp3s0 [UP, Running]

2) any (Pseudo-device that captures on all iterfaces)

3) lo [UP, Running, loopback]

4) enp2s0 [Up]

5) bluetooth - moniter (Bluetooth linux Moniter

6) bluetooth [Bluetooth adapter number 0)

7) n flog (Linux netfilter log (NFLOG) interface)

8) nfqueue (Linux netfilter queue (NFQUEUE) interface)

9) usbmon1 (USB bus number 1)

10) usbmon2 (USB bus number 2)

Result:-

Thus, the various Network commands used
in Linux and Windows are successfully executed
and the output is verified