

Expt no: 01
Date: 16/07/24

Practical-01

Aim:

Study of various command used in linux and windows

Basic Networking command in windows

1) arp -a

Interface : 192.168.261----- 0xd

Internet Address	Physical Address	Type
192.168.26.254	00-50-56-F9-66-27	Dynamic
192.168.26.254	FF-FE-FF-FF-FF-FF	Static
224.0.0.2	01-00-5e-00-00-02	Static

2) hostname

Desktop DESKTOP-ATIULDB

3) ipconfig /all

Windows IP configuration

Host Name DESKTOP-ATIULDB

Primary DNS suffix

Node Type Mixed

IP Routing Enabled No

WINS Proxy enabled No

4) ~~ipconfig~~ netstat -a

netstat -a DESKTOP-ATIULDB

Ethernet 3:

Node IP Address: [0.0.0.0] Scope Id: []

Host Not found

Bluetooth network configuration 2:

Node IP Address: [0.0.0.0] Scope Id: []

Host not found

5) netstat

Active communication	Foreign Address	State
proto	Local Address	
TCP	127.0.0.1:49678	ESTABLISHED
TCP	127.0.0.1:49679	ESTABLISHED
TCP	172.16.75.28:62144	20.42.73.26:80 [HTTP] CLOSE_WAIT

6) nslookup www.google.com

server: unknown

Address: 172.16.72.1

Non-authoritative answer

Name: www.google.com

Address: 2404:6800:4007:810:2004
142.250.163.228

7) pathping

Usage: pathping [-g host-list] [-h maximum-hops]
[-i address] [-n] [-p period] [-q num-queries]
[-w timeout] [-u] [-b] target-name

Options:

- g host-list Trace source route along host-list.
- h maximum-hops Maximum number of hops to search for target
- i address Use the specified source address
- n Do not resolve addresses to hostname
- p period Wait period milliseconds between pings
- q num-queries Number of queries per hop

8) ping

Usage: 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

Options:

- t Ping the specified host until stopped
To see statistics and continue - type Control-Break;
To stop - type Control-C.
- a Resolve addresses to host name
- n count Number of ~~each~~ requests to send
- l size Send buffer size
- f Set Don't Fragment flag in packet (IPv4-only)
- i TTL Time to Live
- V TOS Type of Service
- r count Record route for count hops (IPv4-only)
- s count Timestamp for count hops (IPv4-only)
- w timeout Timeout in milliseconds to wait for each reply.

9) Route

Kernel IP Routing Table

Destination	Gateway	Genmask	Flag	Metric	Ref	Use
default	gateway	0.0.0.0	UG	100	0	0
172.16.8.0	0.0.0.0	255.255.255.0	U	100	0	0

Interface
enp2s0
enp2s0

Linux Networking Command

1) ip:

a) ip address show

1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noop
state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd
00:00:00:00:00:00
inet6 ::1/128 scope host
valid-lft forever preferred-lft forever

b) ip address add 192.168.1.254/24 dev enp2s0
RTNETLINK answers: Operation not permitted.

c) ip address del 192.168.1.254/24 dev enp2s0
RTNETLINK answers: Operation not permitted

d) To alter the states of interface by bringing the interface
eth0 online & offline

Online: ip link set eth0 up

Offline: ip link set eth0 down

e) ~~Alter~~ Alter the status by enabling promiscuous
ip link set eth0 promiscuous

f) Add a default route:

ip route add default via 192.168.1.254 dev eth0

g) Add a route

ip route add 192.168.1.0/24 via 192.168.1.254

2) mtr:

Host	Loss%	Packets Snt	Packets Last	Avg	Pings Best	Worst	StDev
1.1.1.1	0.0%	41	0.1	0.1	0.0	0.1	0.0

i) show numeric IP address

mtr -b google.com

ii) set no. of pings:

mtr -c 10 google.com

3) tcpdump:

dnf install -y tcpdump

i) tcpdump -D

1) enp2s0 [up, Running]

2) any [Pseudo-device that captures all interfaces]
[up, Running]

3) la [up, Running, Loopback]

4) wlp3s0

5) bluetooth 0

6) bluetooth 1

ii) tcpdump -i enp0s3

userbase output suppressed, use -u[ui]... for

full protocol decode

listening on enp0s3, link-type EN10MB (Ethernet),
snapshot length 262144 bytes

16:32:48.655388 ARP, request from 192.168.1.12
Toll - gateway length

(iii) `tcpdump -i enp0s3 host 8.8.8.8`

dropped prior to `tcpdump`

`tcpdump`: verbose output suppressed, use `-u[u]`...
for full protocol

^C

0 packet captured

0 packet received by filter

0 packet dropped by kernel

(iv) `tcpdump -i enp0s3 -c`

dropped prior to `tcpdump`

`tcpdump`: verbose output suppressed, use `-v[v]`... for
full protocol decode

16:33:19.1629767 IP localhost -> live.49664>

maao 5523-in.f3.le100.net.https:-flags[p],

seq 416 2835473.41.6.28835512 ack

266 9933 9727, win 501 option [nop, nop, TS val

189 3368936 ack 3471518263], length 39

~~3 packet captured~~

~~3 packet received on filter~~

~~0 packet dropped by kernel~~

Result:

Thus the output is verified successfully.