Exp: Study of Various Commands used in Linux and Windows

21/7/2025

Aim: Study of Various networks used in Linux and windows.

Basic Networking Commands:

1) arp -a: ARP is short form for address resolution protocol, it will show the IP address of your Computer along with the IP address and MAC address of your router.

```
$ arp -a
? (172.16.72.1) at 75:5a:1C:f:
[other] on wlp20
```

2) hostname: Simplest of all TCP/IP commands $ hostname fedora.

3) ipconfig /all: displays detailed config info about your TCP/IP connection, incl router gateway, DNS, DHCP and type of ethernet adapter in your system.

```
$ ip a
1. lo: <LOOPBACK,UP,LOWER_UP> mtu65536
2. wlp20: <BROADCAST,MULTICAST,UP,LOWER_UP
```

4) nbtstat -a : Commands helps solve problems with NET BIOS name resolution.

$nmblookup fedora - linux
192.165.1.105 fedora - linux <00>

5) net stat - netstat displays a variety of statistics about a computer active TCP/ connections. It is a command line tool.

$netstat
Active internet connections (W/o servers)
proto recv - q send - q local address
proto recv - q send - q local address
tcp fedora : 47148
tcp 0 0 fedora : 40456
foreign address state
server - 108 - 159 - 10 : https time - wait

6) lookup : is a command that perform DNS lookups :

$ns lookup www - google com
server: 192 - 168. 1. 1
address : 192 - 168. 1. 1
Non - authoritative answer
name: www. google. com
address : 142. 250. 192. 68

7) pathpiping : pathpiping is a unique to windows and its basically a combination of the ping and tracert commands.

$ pathping www. google. com
My traceroute [v0.94]
hostname (192 - 168 - 1 - 105) → www. google com (142. 250. 192. 68)

Keys : help display mode restart statistics order of fields quit

Host	loss %	not	last	avgbst	wrst	stDev
1. 192.168.1.1	0.0 %	10	0.8	0.7	0.6	0.9	0.1
2. 10.20001	00 %	10	5.2	4.9	4.6	5.3	0.2
3. 142.150.192.168	0.0 %	10	20.5	19.9	19.5	20.5	0.3

8) ping - Packet internet groper command is the best way to test connectivity between two nodes. ping use IMCP to Communication to other devices.

$ ping 8.8.8.8
ping 8.8.8.8 (8.8.8.8) 56 (84 | bytes of data)

64 bytes from 8.8.8.8 using seq = 1, ttl = 115 time = 12.3 ms.

9) route print: route command is used to show or manipulate the IP routing tables.

usage: route [-nvee] [-FC] [<ip>]

list kernel routing tables

route {-V | --version} display version / auth and exit.

-v, verbose be verbose

-n --numeric don't resolve names

-e, --extend display other/more info

-C --cache instead of FIB.

Linux networking Commands:

1) show IP address

$ ip address show

w/p 250 ...

inet 172.16.75.17/21 ...

inet fe80::2725:6845:... :c5/64

2) Add an IP address:

$ sudo ip address add 192.168.1.254/24 dev w/p250

RTNETLINK answers : File exists

3) Delete an IP:

$ sudo ip address del 192.168.1.254/24 dev w/p250

4) Bring interface up:

$sudo ip link set w/p250 up

5) Bring interface down:

$sudo ip link set w/p250 down

6) Enable promiscous mode

$ sudo ip link set w/p250 promiscous

7) Add default route

$sudo ip address add 192.168.1.254/ dev...

$sudo ip route add default via 192.168.1.25... dev w/p250

8) Add a route to 192.168.1.0/24 via gateway 192.168.1.254

$sudo ip route add 192.168.1.0/24 Via 192.168.1.2.254

9) Add a route to 192.168.1.0/24 reachable on device w/p 250

$sudo ip route add 192.168.1.0/24 dev w/p 250

10) Delete route for 192.168.1.0/24 via gateway 192.168.1.254

$sudo ip route delete 192.168.1.0/24 Via 192.168.1.254

11) Display route taken to IP 10.10.1.4

$ ip route get 10.10.1.4

10.10.1.4 via 172.16.72.1 dev w/p 250 src 172.16.75.1

uid 1000 cache

12) ip config

$ip config

wlp 250: flags: 4163<up, BROADCAST, RUNNING, MULTICAST> mtu 0 050

inet 172.16.75.17 netmask 255.255.248.0 broadcast 172.16.79.255

ether 4c:82:a9:77:ff:19 ~~frequency~~ 1000 (ethernet)

TX packets 24436 bytes 11.3 MiB

13) mtr google.com

host	Loss%	Snt	Last	avg	Best	worst	stdev
1. 115.245.94.249	0.01	302	3.8	10.3	2.6	812.2	50.1
2. 72.14.217.252	0.01	321	6.5	15.5	3.9	368.8	28.3

(Packets)

14) mtr -b google.com

	Loss	Snt	Last	Avg	Best	Worst	st
172.16.12.122 (172.16.12.122)	0.01	83	6.2	14.2	5.8	281.2	
172.16.12.122 (172.16.12.122)	0.01	84	6.4	82.6	5.5	238.9	5

(Packets)

15) mtr -c google.com

	Loss%	Cnt	Last	Avg	Best	worst	st
115.245.93.249	0.01	8	23.1	57.6	2.3	361.0	117
	0.0	8	5.5	65.9	5.8	64.3	19

(Packets)

16) Capture traffic on your wifi interface wlp 250

$sudo tcpdump -i wlp 250

Listening on w/p 250

01:47:07 S1 172.16.75.140 > 230.0.0.1.wlp length 50

01:47:07 IP fedora > gateway PTR query

34 packets captured

732 packets received by filter.

17) Capture only 10 packets

$sudo tcpdump -i wlp 250 -c 10

dropped mins to tcp dump

snapshot length 262144 bytes

2323 .47 IP fedora 37165 > gateway domain

10 packets captured
244 packets received by filters
179 packets dropped by kernel.

18) To capture all port except port 80 and 53

$ sudo tcpdump -i wlp20 not port 53 and not port 25

23.36:18 IP fedora.44750 > 1100.net.https: length 2000

23:36: IP fedora.36976 > 1e100.net.https: Flags [S], seq ... win ... length 0

147 packets captured
2776 packets received by filters
2525 packets dropped by kernel.

19) Capture only Dns port 53 Traffic

$ sudo tcpdump -i wlp20 port 53

25:38:32 fedora > gateway domain: AAAA? ab.chatgpt.com
23:35:32 gateway domain > fedora: AAAA reply (0 records)

146 packets captured
146 packets received by filter
0 packets dropped by kernel.

20) For Traffic coming from 8.8.8.8 use:

$ sudo tcpdump -i wlp20 src host 8.8.8.8
dropped privs to tcpdump
tcpdump: Verbose output suppressed, use -v[v] for full protocol decode
listening on wlp20, link-type EN10MB (Ethernet), snapshot length 262144 bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel

21) To Capture HTTPS traffic:

sudo tcpdump -i wlp20 -c 10 host www.google.com and port 443

0 packets captured
4 packets received by filter
0 packets dropped by kernel

Students observation questions:

1) Which command is used to find reachability of a host from your device?

Ping command is used to test the reachability of a host.
It sends ICMP echo requests and awaits for replies from destination.

2) which command will be used to get the details of taken by a packet to reach its destination?

The traceroute command is used to display route packets state to a destination. It lists each I/P along the path and the response time each router.

3) which commands displays the I/P configuration of your machine.

The ifconfig command is used to view I/P configuration. These command show I/P addresses interfaces and other network details.

4) which command displays TCP post status in your machine?

The netstat -tulnp command is used to display TCP post status. Thus show active connection, listening ports and associated process.

5) Write modify I/P configuration in Linux machine.

The ip config or ip command is used to modify IP settings in Linux

Ex: sudo ip addr add 192.168.1.100/24 dev eth0

assigns an IP to an interface