EX NO: 01
DATE: 21/7/25

NETWORK COMMANDS USING WINDOWS AND LINUX.

AIM:-

Study of various network commands used in Linux and windows commands.

Windows Commands:

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

OP:-

1. Interface : 192.168.1.5

Internet Address	Physical address	Type
192.168.1.1	00-1f-d0-af-ae-00	dynamic
192.168.1.10	58-2a-f1-12-3b-94	dynamic

2. Hostname : This is the simplest of all TCP/IP commands. It simply displays the name of yours computer.

host name.

KS03-113

3. ipconfig /all : This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP and type of Ethernet adapter in your systems.

ipconfig /all.

O/P:-

Windows IP configuration

Host name . . . . : KS03-113

Primary Dns Supplier :

Node type : Hybrid

IP routing Enabled : No

Ethernet adapter Ethernet : Intel(R) Ethernet.

Description . . . . :

Physical Address . . . . : A1-B2-C3-D4-E5-F6.

DHCP enabled . . . . : Yes

IPv Address . . . . : 192.168.1.5

4. nbstat -a : This command helps solve problems with Net BIOS name resolution. (Nbt stands for Net BIOS over T(P/IP).

nbstat -a KS03-113

Net BIOS Remote Machine Name Table

Name	Type	Status
Mycomputer <00>	unique	Registered.
Mycomputer <00>	unique	Registered.
Mycomputer <00>	unique	Registered.

MAC address = A1-B2-C3-D4-E5-F6.

5. netstat

Active Connections

Proto	Local Address	Foreign Address	State
Tcp	127.0.0.1:49679	LAPTOP-MMLRRFI:49683	Established
Tcp	127.0.0.1:49683	LAPTOP-MMLRRFL8:49679	Established
Tcp	192.168.1.126:53492	~~LAPTOP~~ a104-86-188-120:https	Established

6. nslookup :-

It is a tool used to perform DNS lookups in LINUX. It is used to display DNS details, such as the IP address of a particular computer.

Default Server: Unknown

Address: 192.168.1.1

7. Pathping :

Pathping is unique to Windows and is basically a combination of the Ping and Tracert commands.

Pathping [-g host-list] [-h maximum_hops] [-i address] [-n]

[-P Period] [-q num-queries]
[-w time Rout]
[-4] [-6] target-name.

Pathping google.com

Tracing route to google.com [142.251.222.206]
over a maximum of 30 hops:

0 LAPTOP-MMLRRF18 [192.168.1.126]
1 192.168.1.1
2
3 * 10.209.0.1
* * *

8. Ping :-

Command is the best way to test connectivity between two nodes. Ping use ICMP to communicate to other devices.

ping twitter.com.

Pinging twitter.com [162.159.140.229]
with 32 bytes of data.
Reply from 162.159.140.229 : bytes : 32
time : 4MS TTL : 58.
:
Ping statistics for 162.159.140.229:
Packets: Sent: 4, Received: 4, Lost 0 (0%

9. Route:

It is a command is used to show/ manipulate the IP routing table.

Manipulates network routing tables.

ROUTE [-f] [-p] [-4]/-6 command [destination]
[MASK netwask][gateway]
[METRIC metric] [IF interface]

LINUX NETWORKING COMMANDS

1) ip :-

The ip command is one of the basic commands every administrator will need in daily work, from setting up new systems and assigning IPs to troubleshooting existing systems.

(a) ip address show:

To show the IP addresses assigned to an interface on your server.

O/P:-

<LOOPBACK, UP, LOWER_UP> mtu 65536
qdisc noqueues state UNKNOWN
group default qlen 1000 link/loopback
00:00:00:00:00:00

00:00 link 00:00:00:00:00:00.
int 127.0.0.118 scope host lo.
valid_lft forever preferred_lft
forever.

(b) ip address add 192.168.1.254 my dev
wlp2s0:
To assign an IP to an interface.

(c) ip address del 192.168.1.254/24 dev
wlp2s0:
To delete an IP on an interface.

(d) ip link set wlp2s0 up :-
After the status of the interface by bringing the interface wlp2s0 online

(e) ip link set wlp2s0 down :-
After the status of the interface by bringing the interface wlp2s0 offline

(f) ip link set wlp2s0 promisc on:-
After the status of the interface by bringing the interface wlp2s0 offline.

(g) ip route add default via 192.168.1.254 dev wlp2s0:

Add a default route via the local gateway 192.163.1.254 that can be reached on device wlp2s0

(h) ip route add 192.168.1.0/24 via 192.168.1.254.

Add a route to 192.168.1.0/24 via the gateway at 192.168.1.254.

(i) ip route ~~delete~~ add 192.168.1.0/24 dev wlp2s0:

Adds a route to 192.168.1.0/24 that can be reached on device wlp2s0.

(j) ip route delete 192.168.1.0/24 via 192.168.1.254:

Delete the route for 192.168.1.0/24 via the gateway at 192.168.1.254.

(k) ip route get 10.10.1.4:-

Display the route taken for 10.10.1.4.

O/p:-

10.10.1.4 dev wlp2s0 192.168.1.254 vid 0 cache.

2. ifconfig :-

This command was staple in many sysadmin's tool belt for configuring and troubleshooting networks.

O/P:-

lupos34s: flags = 4099<UP, BROADCAST, MULTICAST> mtu 1500

other 30:00:10:00:78:64 txqueuelan 1000 (ethernet

RX packets 0 bytes 0(0,0,B)

RX errors 0 dropped 0 overruns 0 frame 0.

fx packets 0 bytes 0(0,0,B)

(3) mtr :-

Matt's traceroute is a program with a command-line interface that serves as network diagnostic & troubleshoot tool

(a) mtr google.com :-

It shows the statistics including each hop with time and loss.

O/P:-

	MOST	PACKETS LOSS%	Snt	LAST	AVG	PINGS BEAT	WRST	stde
1.	JN 115.245.95.249	0.0%	302	3.8	12.3	2.6	812.2	50.1
2.	rs 72.14.217.252	0.0%	321	6.5	15.5	5.9	368.8	25.3

(b) mtr -b google.com

show the numeric IP addresses & hostnames too.

O/P:-

	PACKETS LOSS%	Snt	LAST	AVG	PING BEST	WRST
172.16.12.122	0.0%	83	6.2	14.2	5.8	20.2
172.16.12.122	0.0%	84	6.4	82.0	5.5	283.9

STDEV

24

59.8

4) tcpdump :-

This command is designed for capturing and displaying packets.

(a) tcpdump -i wlp2s0 :-

This command captures the traffic on wlp2s0.

O/P:-

dropped privs to tcpdump

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

listening on wlp2s0, link_type EN10MB (Ethernet), snapshot length 262144 bytes

23:15:48.819979 ARP, Request who-has [illegible] -ay-m-f3.

(b) tcpdump -i wlp2s0 -c 10 host 8.8.8.8:-

To capture traffic to and coming from one specific host.

O/P:-

dropped privs to tcpdump

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

listening on wlp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

- packets captured
- packets received by filter
- packets dropped by kernel.

c) tcpdump -i wlp2s0 ult 10.1.0.0 mask 255.255.255.0 :-

To capture traffic to and from a specific network.

O/P:-

dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode.
listening on wlp2s0, link-type EN10MB (Ethernet)

- packets captured
- packets received by filter.

(d) tcpdump -i wlp2s0 port 53:-

To capture traffic to and from port numbers.

O/P:-

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

- packets captured
- packets received by filter.

5) ping :-

It is used to troubleshoot connectivity, reachability and name resolution.

ping google.com :-

output :-

PING google.com (142.253.221.218)
56(84) bytes of data
from fedora (192.168.1.294)
icmp - seq = 1 Destination most unreachable.
from fedora (192.168.1.294) icmp seq = 2.
Destination most unreachable.

STUDENT OBS :-

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

A) ping <hostname or IP>

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

A) traceroute <hostname or IP>

3) Which command displays the ip configuration of your machine?

A) ifconfig (older systems)
ip addr (modern systems)

4) Which command displays the TCP port ~~syste~~ status in your machine?

A) netstat -tulpn (shows TCP/UDP ports and listening programs).

5) Write ~~the~~ to modify the ip configuration in a Linux machine.

A) ~~s~~ sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0.

(OR)

sudo ip addr add 192.168.1.100/24 dev eth0.

RESULT:-

Hence working in network commands in windows and Linux have been studied successfully

7/2/26