Date : 3.7.25

Exp No: 1

AIM: Study of various network commands used in Linux and Windows

BASIC NETWORKING COMMANDS:

WINDOWS

1. arp-a : Displays IP address and MAC address of router and computer

```
Interface : 192.168.0.103 ---0x3
Internet Address      Physical Address      Type
192.168.0.1           98-25-4a-28-49-d2     dynamic
192.168.0.107         60-35-73-65-7d-31     dynamic
192.168.0.255         5c-22-da-3e-fa-f5     static
:                     :                     :
:                     :                     :
:                     :                     :
```

2. hostname : simply displays name of your computer

Output

Sanjana

3. ipconfig/all : Detailed configuration information about TCP/IP connection

output:

```
Windows IP configuration
    Host Name . . . . . : sanjana
    Primary DNS suffix . . . :

Wireless LAN adapter Wi Fi :
    Description . . . . : Intel(R) Wi Fi 6E
    Physical Address . . : 60-45-2E-3A-80-C7
```

4. Nbtstat

Nbt stands for NetBIOS over TCP/IP

→ nbtstat -a → Nbtstat -c

→ Nbtstat -n

Output

Node IpAddress : [192.168.0.103] Scope ID : [ ]

NetBIOS Local Name Table

Name	Type	Status
SANJANA	<00> UNIQUE	Registered
SANJANA	<20> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered

:

5. netstat : variety of statistics about a computers active TCP / IP connections

Output :

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49691	Kubernetes:49692	ESTABLISHED
TCP	127.0.0.1.49692	Kubernetes:49691	ESTABLISHED

:

6. nslookup : is a tool used to perform DNS lookup in Linux

Output

Default Server : 183.82.243.66.actcorp.in

Address : 183.82.243.66

:

7. pathping : combination of the ping and Tracert commands. Pathping traces the route to the destination address

pathping www.google.com

Output:

Tracing route to www.google.com

0 sanjana [2406:7400:bb:17c0:c9a4...

1 2406:7400:bb:17c0:9a25:4aff:fe28

2 2406:7400:b1::2

⋮ ⋮

8. ping : best way to test connectivity between two nodes

→ ping localhost

Output

Pinging sanjana [::1] with 32 bytes of data

Reply from ::1: time<1ms

Reply from ::1: time<1ms

⋮

Ping statistics

⋮

→ ping www.facebook.com

9. Route : used to show / manipulate the IP routing table

route print

→ Output :

Interface List

18...60. 45 2e 3a ..... Microsoft WiFi Direct..

11... 62 45 2e 3a .... Microsoft WiFi Direct Virtual

⋮

IPV4 Route Table

⋮

IPV6 Route Table

SOME IMPORTANT LINUX NETWORKING COMMANDS

1. ip : Basic command every administrator will need in daily work.

→ ip address show

- Output

1. lo : <LOOPBACK, UP, LOWER UP>
   ⋮
2. enp0s31f6 : .....
3. wlp2s0 .....
   inet 172.16.75.125/21

→ sudo ip address add 192.168.1.254/24 dev enp0s31f6

Output:

Connection established

You are now connected to enp0s31f6

→ sudo ip address del 192.168.1.254/24 dev enp0s31f6

→ sudo ip link set enp0s31f6 up

→ sudo ip link set enp0s31f6 down

→ sudo ip link set enp0s31f6 promisc on

→ sudo ip route add default via 192.168.1.254 dev enp0s13f6

2. ifconfig

The ifconfig command is a staple in many sysadmin's tool belt for configuring and troubleshooting networks.

⇒output

```
enp0s31f6: flags=4355<UP,BROADCAST..> mtu1500
        inet 192.168.1.100
          :
lo: flags=73<UP,LOOPBACK,RUNNING>
        inet 127.0.0.1
          :
wlp2s0: flags=4163<...>
        inet 172.16.75.125
          :
```

3. mtr

MTR (Matt's traceroute) is a program with a command line interface that serves as a network diagnostic and troubleshooting tool. This command combines the functionality of the ping and traceroute commands

Syntax of the command

mtr <options> hostname / IP

Common use cases:

a. mtr google.com

Output

Host	Packets Loss%	Snt	Pings Last	Avg	Best	Wrst
1. -gateway	0.0%	85	2.4	7.5	1.7	79.0
2. static-41.229.249 ...	0.0%	85	66.9	14.0	4.4	132
⋮	⋮		⋮			

b. mtr -n google.com

Host	Packets Loss%	Snt	Pings Last	Avg	Best ...
1. 172.16.72.1	11.9%	63	8.3	28.2	2.4
2. 49.249.229.41	11.6%	66	6.7	41.6	4.9
⋮	⋮		⋮		

c. mtr -b google.com

d. mtr -c 10 google.com

Output:

Host	Packets Loss%	Snt	Pings Last	Avg	Best	Wrst
1. -gateway	0.0%	2	6.2	8.9	6.1	239.4
2. static-41.229.249.49..	0.0%	2	5.5	11.0	22.1	7.2
⋮	⋮		⋮			

4. tcdump

The tcpdump command is designed for capturing and displaying packets

→ Install tcpdump with the command:

1. sudo dnf install -y tcdump

Output:

⋮

Package tcpdump-14:4.99.4-2-fc39.x86 is already installed

Dependencies resolved

Nothing to do

Complete!

2. tcpdump -D

Output:

1. wlp2s0 [Up, Running, Wireless, Associated]
2. any
3. lo [Up, Running, Loopback]
4. enp0s31f6 [Up, Disconnected]

⋮

3. sudo tcpdump -i wlp2s0

⋮

listening on wlp2s0 ..

⋮

5 packets captured

481 packets received by filter

358 packets dropped by kernel

⋮

4. sudo tcpdump -i wlp2s0 -c 10

OUTPUT:

Listening on wlps2s0, link-type EN10MB

:

10 packets captured

34 packets received by filter

0 packets dropped by kernel

5. To find traffic coming from and going to 8.8.8.8, use the command:

tcpdump -i wlp2s0 -c 10 host 8.8.8.8

OUTPUT

01:43:22.402561 IP fedora > dns.google...

:

10 packets captured

10 packets received by filter

0 packets dropped by kernel

6. For traffic coming from 8.8.8.8,

sudo tcpdump -i wlp2s0 src host 8.8.8.8

OUTPUT

Listening on wlp2s0, link type EN10MB...

23:21:22.453708 IP dns.google > fedora...

23:21:23:479039 IP dns.google

:

7. For outbound traffic going to 8.8.8.8,

tcpdump -i wlp2s0 dst host 8.8.8.8

OUTPUT

:
Listening on wlp2s0, link-type EN10MB (Ethernet)..
23:22:26.469233 IP fedora > dns.google : ICMP echo request
23:22:27:469352 IP fedora > dns.google : ICMP echo request
:

8. To capture traffic to and from a specific network use the command below

tcpdump -i eth0 net 10.1.0.0 mask 255.255.255.0

OUTPUT:

Listening on eth0, link-type EN10MB (Ethernet)
11:21:23.696721 IP 172.25.141.91 > 10.1.0.0: ICMP ...
11:21:24.714039 IP 172.25.141.91 > 10.1.0.0: ICMP echo...
:

Capture traffic to and from Port numbers

9. Capture only DNS port 53 traffic

sudo tcpdump -i eth0 port 53

OUTPUT
:
01:15:10:456123 IP fedora.49821 > 8.8.8.8.domain..
01:15:10.445321 IP 8.8.8.8 domain > fedora.49821..
:

10. For a specific host

sudo tcpdump -i eth0 host 8.8.8.8 and port 53

OUTPUT:

Listening on eth0 ...

01:16:20.776543 IP fedora.5400

:

11. To capture only HTTPS traffic

sudo tcpdump -i eth0 -c 10 host www.google.com and port 443

OUTPUT

01:17:12.321456 IP fedora.55789 > www.google.com.443

01:17:12.421456 IP www.google.com ...

...

(10 packets captured)

12. To capture all ports except port 80 and 25

sudo tcpdump -i eth0 port not 80 and not 25

OUTPUT:

tcpdump: verbose output supressed ..

Listening on wlp2s0 ..

00:39:57.698207 IP 172.16.79.241.43369 > 239.0 ...

00:29:57.698208 IP6 :: > ff02::16: HBH ICMP6

...

^C

7 packets captured

5. ping

Ping is a tool that verifies IP level connectivity to another TCP/IP computer by sending ICMP Echo message Requests.

→ 1. ping google.com

OUTPUT:

64 bytes from pnmaa-ar.in-f4.1e100.net ...

64 bytes from ... (142.251.43.46): icmp_seq=2 ...

⋮

^C

→ 2. ping -c 10 google.com

is used to ping a host 10 times

OUTPUT

PING google.com

64 bytes from ... (142.251.43.46): icmp_seq=1

64 bytes from ... icmp_seq=2 ttl=118 time=40.2ms

...

64 bytes from ... icmp_seq=10 ttl=118 time=10.9 ms

Configuring an Ethernet connection by using nmcli

If you connected a host to the network over Ethernet, you can manage the connection's settings on the cli the command line by using the nmcli utility

→ 1. List the NetworkManager connection profiles

nmcli connection show

NAME	UUID	TYPE	DEVICE
Wired connection 1	d5cb4fbc..	ethernet	enp1s0

→ nmcli connection add con-name my-wired ifname enp1s0 type ethernet

connection 'my-wired' successfully added

→ 3. nmcli connection modify "Wired connection 1" connection.id my-wired

(no-output, command executes)

→ 4. Display the current settings of connection profile

nmcli connection show "Wired connection 1"

...

connection.interface-name: enp1s0

connection.autoconnect: yes

ipv4.method: auto

...

→ 5. Configure the IPv4 settings

• To use a DHCP,

nmcli connection modify "Wired connection 1" ipv4.method auto

No output, command executes

- To set a static IPV4 address, network mask, default gateway, DNS servers,

nmcli connection modify "Wired connection 1"
ipv4.method manual ipv4.addresses
192.0.2.1/24 ipv4.gateway 192.0.2.254
ipv4.dns 192.0.2.200 ipv4.dns-search

No output, the command just executes

6. To configure the IPV6 settings

→ nmcli connection modify "Wired Connection 1"
ipv6.method auto

No output, command just executes

7. Activate the profile

nmcli connection up "Wired connection 1"

Connection successfully activated
No-output, command executes successfully.

VERIFICATION:

1. Display the IP settings of the NIC:

ip address show enp1s0

OUTPUT:

enp1s0: <BROADCAST, MULTICAST, UP ...> mtu 1500
state UP
:
:

2. Display the IPv4 default gateway:

ip route show default

OUTPUT:

...

default via 192.0.2.254 dev enp1s0 proto static metric 102

...

3. Display the IPv6 default gateway:

ip -6 route show default

OUTPUT:

default via 2001:db8:1:ffee dev enp1s0 proto static metric 102 pref

...

4. Display the DNS settings

cat /etc/resolv.conf

OUTPUT

...

nameserver 192.0.2.200

nameserver 2001:db8:1::ffb

...

5. Use the ping utility to verify that this host can packets to other hosts

ping google.com

OUTPUT:

64 bytes from pnmaa-av.in-f4.1e100.net...

64 bytes from ..... :icmp-seq=2

...

Student Observation :

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

- The ping command checks if a host is reachable over the network. It sends ICMP Echo Request and waits for a reply.

command: ping google.com

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

- The traceroute command shows the path packets take to reach a destination. It lists each router (hop) along the way.

Example, traceroute google.com

3. Which commands displays the ip configuration of your machine.

- ifconfig or ip a shows IP addresses, interfaces and network states.

ifconfig

enp0s31f6 : flags= 4355 <UP, BROADCAST, ...
inet 192.168.1.100
...

lo : flags = 73 <UP ... >
inet 127.0.0.1
...

wlp2s0 : flags = 4163 ...

4. Which command displays the TCP port status in your machine?

- netstat displays a variety of statistics about a computers active TCP / IP connections

netstat -tuln is used to view TCP/UDP port status.

5. Write the modify the ip configuration in a Linux machine

- ip addr add command is used to add a new IP. This requires root permisson

sudo ip addr add 192.168.1.254/24 dev enp0s31f6

OUTPUT :

connection established

You are now connected to enp0s31f6

RESULT :

The various linux and windows commands are executed and got the output

24/2/26