Ex: No: 1
14.07.25

Study of Various Network Commands Used in Linux and Windows

Aim: Study of various Network commands used in linux and windows.

Basic Networking Commands:

*arp -a:

ARP is 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 routes.

Output: Interface: 192.168.0.101 --- 0x5

Internet Address	physical Address	Type
192.168.0.1	f0-27-31-cb-89-30	Dynamic
192.168.0.100	48-46-c1-22-82-db	Dynamic
192.168.0.255	ff-ff-ff-ff-ff-ff	Static
224.0.0.22	01-00-5e-00-00-16	Static
224.0.0.251	01-00-5e-00-00-fb	Static

*hostname

This is the simplest of all TCP/IP Commands. It simply display the name of your computer.

output :- K303-83

*ipconfig/all

This command displays detailed configuration information about your TCP/IP connection including Routes, and type of ethernet adapters in your system.

output:- Windows Ip Configuration.

Host Name . . . . . :
Primary Dns Suffix . . . :

Node Type : Mixed
IP Routing enabled : No
WINS proxy enabled : No
Unknown adapter local area connection

Media State ..... Media Connected

* nbtstat -a :

This helps solve problem with NetBios name Resolution (Not stands for NetBios over TCP/IP)

output.

Displays protocol statistics and Current TCP/IP connections using NBT (NetBios over TCP/IP)

NBTSTAT [[-a Remote Name] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

-a (adapter status) Lists the Remote machine's name table given its name

-A (Adapter Status) Lists the Remote machine's name table given its IP address

-c (cache) Lists NBT's cache of Remote [machine] names and their IP address

* netstat : (network Statistics)

It displays a variety of statistics about a Computer active TCP/IP connections.

netstat -r

output :-

Interface list
13...00 00 27 00 00 dd ... VirtualBox Host-only Ethernet Adapter

3... 34 7d f6 af 69 94... Microsoft Wi-fi Direct Virtual Adapter

16... 86 7d f6 af 69 96... Microsoft Wi-fi Direct Virtual Adapter #2

5. 34 7d f6 af 69 96... Intel(R) Wi-fi 6A x201 160MHz

IPV4 Route Table

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331

*nslookup

combination of interactive and non-interactive

nslookup www.google.com

output:

Server: unknown

Address: 10.237.195.43

Non-authoritative answer:

Name: www.google.com

Address: 2404:6800:4007:81f::2004

142.250.67.68

*pathping:

Basically a combination of ping and Tracert Commands.

output:

Usage: pathping [-g host-list] [-h maximum hops]
[-i address] [-n] [-p period] [-q num.queries]
[-w timeout] [-4] [-6] target name

*Ping (Packet Internet Groper)

Best way to test Connectivity between two nodes.

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

Ping hostname

pinging hostname [fe80::a461:30ef:3baa:46b3%18]
with 32 bytes of data:

Reply from fe80::a461:30ef:3baa:46b3%18: time<1ms

:

Ping Statistics for fe80::a461:30ef:3baa:46b3%18:
Packet: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Avg = 0ms

*Route

Used to show the ip routing table

Route print

Output

IPv4 Route Table

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.56.0	255.255.255.0	On-link	192.168.56.1	281

Persistent Routes:

None

Some important linux networking Commands:

1. ip ip <OPTIONS> <OBJECT> <COMMANDS>

a. # ip address show

Output:

1. lo : <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue
   State UNKNOWN group default qlen 1000
2. enp0s31f6 : <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu
   1500 qdisc fq_codel State UP group default qlen 1000
3. wlp0s0 : <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500
   qdisc noqueue State UP group default qlen 1000

b. # sudo ip address add 192.168.1.25/24 dev enp0s31f6
   To assign an IP to an interface

c. # sudo ip address del 192.168.1.25/24 dev enp0s31f6
   To delete an IP on an interface

d. # sudo ip link set enp0s31f6 up
   Alter the status of the interface by
   bringing the interface online

e. # sudo ip link set enp0s31f6 down
   Alter the status of the interface by
   bringing the interface offline.

f. # sudo ip link set enp0s31f6 promisc on
   Alter the Status of the interface by
   enabling promiscuous mode for interface.

g. #sudo ip route add default via 192.168.1.254 dev enp0s31f6

Add a default route for all addresses via the local gateway 192.168.1.254 that can be reached on device enp0s31f6.

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. #sudo ip route add 192.168.1.0/24 dev enp0s31f6

Add a route to 192.168.1.0/24 that can be reached on device enp0s31f6.

j. #sudo 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. #sudo ip route get 10.10.1.4

Display the route taken for IP 10.10.1.4

(2) ifconfig

The ifconfig command was is a staple in many Sys admin's tool belt for configuring and trouble shooting networks.

output:

enp0s31f6: flags=4355<UP, BROADCAST, PROMISC, MULTICAST> mtu 1500

inet: 192.168.1.254 netmask 255.255.255.0 broadcast 0.0.0.0

ether 20:88:10:86:79:89 txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

⋮

3. mtr

MTR (Matt's traceroute) is a program with a Command-line interface that serves as a network diagnostic and trouble shooting tool.

Syntax of the command is as follows:

mtr <options> hostname/Ip

(a) Basic mtr command shows you the statistics:

#mtr google.com

output: My traceroute [v0.95]

fedora (172.16.75.85) → google.com (142.251.221.206)

2025-07-14T13:42:07-0400

Keys:

	Host	Packet Loss%	Pings Snt	Last	Avg	Best	Wrst	StDev
1.	IN 115.245.95.245	0.0%	8.3	16.2	14.2	5.8	20.2	24
2.	IN 72.14.217.252	0.0%	8.4	6.4	82.8	5.5	283.9	528

(b) mtr -b google.com

Shows the numeric Ip addresses & hostname too

output:

	Packet loss%	Pings Snt	Last	Avg	Best	Wrst	StDev
172.16.12.122	0.0%	302	3.8	12.3	2.6	412.5	50.1
172.16.12.122	0.0%	321	6.5	15.5	5.9	368.8	25.3

(4) tcpdump

This command is designed for capturing and displaying packets.

(a) tcpdump -i wlp2s0:

This command captures the traffic on wlp2s0.

output:

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 48:879979 ARP Request who-has linca.g
a.rfa

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

To capture traffic to and coming from one specific host

output:

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.

- 0 packets captured.
- 0 packets received by filter.
- 0 packets dropped by Kernel.

(c) tcpdump -i wlp2s0 net 10.1.0.0 mask 255.255.255.0

To capture traffic to and from a specific network.

output:

dropped privs to tcpdump

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

listening on wlp2s0 link-type EN10MB (Ethernet)

- 0 packets captured
- 0 packets received by filter
- 0 packets dropped by Kernel.

(d) tcpdump -i wlp2s0 port 53

To capture traffic to and from port number

output:

dropped privs to tcpdump

tcpdump : verbose output Suppress it, 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 (142.253.221.206) 56(84) bytes of data.

From fedora (192.168.1.294) icmp_seq=1 Destination Host Unreachable

From fedora (192.168.1.294) icmp_seq=2 Destination Host unreachable.

Student observation:

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

ping <hostname or IP address>

Eg: ping google.com

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

mtr <hostname>

Eg: mtr google.com

(3) which Command displays the ip configuration of your machine.

On Linux: ipconfig or ip addr
On windows: ipconfig

Eg: ipconfig
ip addr show

(4) which Command displays the TCP port status in your machine?

On Linux: netstat
Ej: netstat -r

(5) Write the modify the ip configuration in a Linux Machine.

To add: Sudo ip address add 192.168.1.100/24 dev enp503sf6

to delete: Sudo ip address del 192.168.1.100/24 dev enp503if6

Result:
The Networking Commads in windows and Linux have been executed Successfully.

4/8/26