EXP NO: 01 | Study of various network commands used in Linux and Windows

DATE: 24.07.2025

Aim: TO study various networking commands used in Linux and windows.

Basic networking commands:

1. arp -a:

ARP is short form of address resolution protocol. It will show the IP address of your computer along with IP address and MAC address of your router.

Output:

Interface: 192.168.29.99 --- 0x9

Internet address	Physical address	Type
192.168.29.1	04-ab-08-2a-b3-61	dynamic
192.168.29.255	ff-ff-ff-ff-ff-ff	static

2. hostname:

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

Output:

K303-09

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 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 . . . . . : Medic disconnected

Connection specific DNS suffix . . . :

Description . . . . . : Expres VPN TUN Driver

Physical address . . . . . :

DHCP enabled . . . . . : No

Autoconfiguration enabled . . . : Yes

4. nbstat -a:

This command helps solve problem with NetBIOS name resolution.

Output:

Displays protocol statistics and current TCP/IP connections using NBT

[NetBIOS over TCP/IP]

NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR]

[-s] [-S] [interval]]

-a (adapter status) List the remote machine's name table given its name

-A (adapter status) List's the remote machine's name given its IP address

-c (cache) List's NBT's cache of remote [machine] names and their IP addresses

-n (names) Lists local NetBIOS names.

5. netstat (network statistics)

It displays a variety of statistics about a computer's active TCP/IP connections. It is a command line tool for monitoring network connections both incoming and outgoing.

Output:

Active connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:2020	LAPTOP-Q9HGLHN4:499	ESTABLISHED
TCP	127.0.0.1:2021	LAPTOP-Q9HGLHN4:499	ESTABLISHED

6. nslookup : (name server lookup)

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

Output:

Default Server: Unknown

Address: 172.16.72.1

7. pathping:

It is unique to windows and is basically a combination of the ping and tracert commands. Pathping trace the route to the destination address then launches a 25 second test of each router along the way.

Output:

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-h] [-6] target_name

options:

-g host-list : Loose source route along host-list

-h max_hops Maximum number of hops to search for target

-i address use the specified source address

-n Do not resolve addresses to hostnames

8. ping: (Packet Internet Grouper)

It is the best way to test connectivity between two nodes. It uses ICMP (Internet control Message Protocol).

Output:

ping 1.2.2.2

pinging 1.2.2.2 with 32 bytes of data:

Reply from 1.2.2.2 : bytes = 32 time = 38 ms TTL = 50

Reply from 1.2.2.2 : bytes = 32 time = 39 ms TTL = 50

Ping statistics for 1.2.2.2:

Packets : Sent = 2 Received = 2, Lost = 0 (0% loss)

Approximate round trip times in milliseconds:

Minimum = 38 ms Maximum = 39 ms, Average = 38 ms

9. Route:

It is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host / networks to an interface.

Output:

route PRINT

Interface List

6 ..... ExpressVPN TUN Driver

7...38 bf 24 2d b5 a5 ... Microsoft Wifi Direct virtual Adapter

IPv4 Route Table

Active Routes

Network Destination	Network	Gateway	Interface	Metrics
0.0.0.0	0.0.0.0	192.168.29.6	192.168.29.6	35
127.0.0.0	255.0.0.0	On-Link	127.0.0.1	331

Persistent Routes:

None

Linux Networking Commands:

1. ip:

The ip command show address information, manipulative routing plus display network various devices, interfaces and tunnels.

a) ip address show:

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

Output:

lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo

b) ip address add 192.168.1.254/24 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:

Alter the status of the interface by bringing the interface wlp2s0 online.

e) ip link set wlp2s0 down:

Alter the status of the interface by bringing the interface wlp2s0 offline.

f) ip link set wlp2s0 promisc on:

Alter the status of the interface by enabling promisc mode for wlp2s0.

g) ip route add default via 192.168.1.254 dev wlp2s0:

Add a default route via the local gateway 192.168.1.254 that can be reached on device wlp2s0.

h) ip route add 192.168.1.0/24 via 192.168.1.254:

Add a route 192.168.1.0/24 via the gateway at 192.168.1.25

i) ip route 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 IP 10.10.1.4

output:

10.10.1.4 dev wlp2s0 src 192.168.1.254 uid 0 cache

2. ipconfig:

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

Output:

```
enp0s31f6: flags=4099<UP, BROADCAST, MULTICAST> mtu 1500
        ether 30:00:10:00:78:b4  txqueuelen 1000 (Ethernet
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX 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 & troubleshooting tool.

a) mtr google.com:

It shows the statistics including hop (hostnames) with time and loss %.

Output:

Host	Packets Loss %	Snt	Last	Avg	Pings Best	Wrst	Stdev
1. EN 115.215.95.249	0.0%.1	302	3.8	12.3	2.6	813.8	50.1
2. IN 72.14.217.252	0.0 %.	321	6.5	15.5	5.9	368.8	26.3

b) mtr -b google.com

Shows the numeric IP addresses & hostnames too.

Output:

	Packets	Pings				
172.16.12.122	Loss %. 0.0%.	Snt 83	Last 6.2	Avg 14.2	Best 5.8	Wrst 90.2	Stdev 24
172.16.12.122	0.0%.	84	6.4	82.6	5.5	283.7	51.8

1. 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
23:15:48.819979 ARP, Request who has Sinan-ay-a-f3

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 bytes EN10MB(Ethernet), snapshot length 262214 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

d) tcpdump -i wlp2s0 port 53:

To capture traffic to and from port numbers

Output:

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

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

Student observation:

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

Ans: ping <hostname or IP> command is used.

Example: ping google.com

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

Ans: The traceroute <hostname or IP> command is used to display the route packets taken to a destination.

3. Which command displays the IP configuration of your machine?

Ans: On windows: ipconfig

On Linux: ipconfig or ip address show

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

Ans: The netstat -tuln lists all TCP/UDP listening ports. They show active connections, listening ports and associated processes.

5. Write the command to modify the IP configuration in a Linux machine

Ans: To assign an new IP address temporarily

sudo ip addr add 192.168.1.[illegible] dev wlp2s0

sudo ip add default via 192.168.1.1

Result:

Thus the study of network commands used in Linux and Windows is done successfully.

21/8/20