

Exploratory Study of Various Commands used

21/7/2025

in Linux and Windows

Aim: Study of Various networks used
in Linux and Windows. (B.Tech CSE)

Objectives: To explore various protocols (TCP, UDP, ICMP, etc.)
Basic Networking Commands:

1) arp -a: ARP is a 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
8: ens3 : -gateway (172.16.72.1) at 75:5c:1c:c1:84:ff

2) host name: Simplest of all TCP/IP commands & host name fedora.

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

\$ ip a
1: ens3: <eno1> brd: no queueing discipline: mtu 1500 qdisc mq state UP qlen 1000

1. lo: <loopback, no queueing discipline: mtu 65536 qdisc noqueue state UNKNOWN qlen 1

2. ens3: <ethernet, broadcast, multicast, no queueing discipline: mtu 1500 qdisc mq state UP qlen 1000

3. ens3: <ethernet, broadcast, no queueing discipline: mtu 1500 qdisc mq state UP qlen 1000

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

\$ nslookup fedora -linux
192.168.1.105 fedora -linux <>

5) netstat - netstat displays a variety of statistics about active TCP connections. It is a command line

tool for displaying network statistics.

netstat -r for route table

Active Internet Connections (W/o servers)

proto recv -q send -q local address

proto recv -q send -q local address

tcp to (0.0.0.0) : fedora : 47148

tcp 0 0 0.0.0.0 fedora : 40456

foreign address state owner/prot (e.g. owner/prot)

server - 192.168.1.10 : https time-wait

6) nslookup: is a command that performs DNS lookups. It maps two

to the DNS server: 192.168.1.1 nslookup

\$ nslookup www.google.com

server: 192.168.1.1 nslookup

address: 192.168.1.1

Non-authoritative answer

www.google.com. 142.250.192.68

address: 142.250.192.68

7) Pathping: pathping is a utility to windows and its basically a combination of the ping and tracert commands.

\$ ping 192.168.1.105 www.google.com

addt. option /tracert My traceroute [v0.94]

trace hostname (192.168.1.105) to www.google.com (142.250.192.68)

Keys: help display mode netstat statistic
order of fields quit

Host loss% not last arg best wait etc

1. 192.168.1.105 0.0% 100.0% 0.7 0.6 0.9 0.1

2. 192.200.1 0.0% 10 5.2 4.9 4.6 5.3 0.2

3. 81.7.192.168 0.0% 10 20.5 12.9 19.5 20.5 0.3

8) ping - packet internet query command is the best way to test connectivity between two nodes. ping use ICMP to communicate 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 80=1.1ms
115ms = 12.3ms

a) route print; route [-v] - Version 3 display Version 1
 usage: route [-www] [-FC] [<sp>]
 list internal routing table
 [+.ov] traceset [?]

route { (V1) - Version 3 display Version 1
 (8d 11.02 17D) auth and exit.

enable type Virtual config file location
 type table for other

-u -- never forward don't resolve names

little known tools test - nasal tools

P.O d-d F.O E.S extend no. display other more info

E.C d-f P.F L.D 100 1000E.61.2

E.C E.P.P.M - cache instead of FIB

lungs) weighed twelve pounds - big (8
stinters) feet at post tied off in
at DMT ear plug. abdomen cut opened
- incised recto at sternum

~~(8.8.8.8) pig f
(8.8.8.8) pig~~

~~→ $\int f_1 \cdot f_2 = \text{vol } (\text{Ein } B \cdot \text{B} \cdot \text{g manf. auf } A)$~~

Linux networking commands:

- 1) show IP address
 $\$ ip address show$
 wlp250: -->
 i net 172.16.75.1/24 brd 172.16.75.255 mtu 1500
 i net fce:2725:6845 brd 172.16.75.255 mtu 64
 i brt brd 172.16.75.255 mtu 1500
 2) Add or IP address.
 $\$ sudo ip address add 192.168.1.254/24$
 $\$ sudo ip link set dev wlp250 up$
 RTNETLINK answers: File exists
 $\$$
- 3) Release an IP:
 $\$ sudo ip address del 192.168.1.254/24$
 $\$ sudo ip link set dev wlp250 down$
 Bring interface IP:
 $\$ sudo ip link set wlp250 up$
 Bring interface down:
 $\$ sudo ip link set wlp250 down$
 Enable promiscous mode
 ~~$\$ sudo ip link set wlp250 promisc$~~
 Add default route
 $\$ sudo ip address add 192.168.1.254/24$
 $\$ sudo ip route add default via 192.168.1.254$
 $\$$

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

via device wlp250

\$ sudo ip route add 192.168.1.0/24
dev wlp250

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 wlp250
qdisc pfifo_fast root 172.16.75.1
cpu 0.000000 watermark 0.000000

12) ip config in the terminal

\$ ip config shows connection id 10

WIFI: flags: 4163<up, BROADCAST, RUNNING,
MULTICAST mtu 0 qdisc noqueue

inet 172.16.76.17 brd 172.16.76.255
netmask 255.255.252.0

ether 00:0c:29:6a:9f:7f brd 172.16.76.255
MACv4 00:0c:29:6a:9f:7f media 1000baseT
Tx packets 24436 bytes 11.3 kB

13) traceroute google.com Packets
host 1 Loss=0% Lost=0% Avg=Best Worst st

1 115.245.94.249 0.01 321 3.8 103 3.6 817.2 501

2 172.14.217.262 0.01 321 6.5 155 3.9 308.8 283

3 172.16.12.122 (172.16.12.122) 0.01 83 6.2 14.2 5.8 281.2

4 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

5 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

6 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

7 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

8 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

9 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

10 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

11 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

12 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

13 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

14) traceroute google.com Packets

host 1 Loss=0% Lost=0% Avg=Best Worst st

1 172.16.12.122 (172.16.12.122) 0.01 83 6.2 14.2 5.8 281.2

2 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

3 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

4 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

5 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

6 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

7 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

8 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

9 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

10 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

11 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

12 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

13 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

14) traceroute google.com Packets

host 1 Loss=0% Lost=0% Avg=Best Worst st

1 172.16.12.122 (172.16.12.122) 0.01 83 6.2 14.2 5.8 281.2

2 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

3 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

4 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

5 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

6 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

7 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

8 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

9 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

10 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

11 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

12 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

13 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

14 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

15) traceroute google.com Packets

host 1 Loss=0% Lost=0% Avg=Best Worst st

1 172.16.12.122 (172.16.12.122) 0.01 83 6.2 14.2 5.8 281.2

2 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

3 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

4 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

5 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

6 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

7 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

8 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

9 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

10 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

11 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

12 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

13 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

14 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

15 172.16.12.122 (172.16.12.122) 0.01 84 6.4 22.6 5.5 281.9

16) Capture traffic on your interface

\$ sudo tapdump -i wlp250

listening on wlp250

01:47:07.517172.16.75.14 > 23.52.0.1. wlp250

length 50

01:47:07.517172.16.75.14 > gateway PTR

01:47:07.517172.16.75.14 > gateway

32. Packets captured

32. Packets received by filter.

732 Packets dropped by filter.

17) Capture only 10 packets.

\$ sudo tapdump -i wlp250 -c 10

dropped max to tapdump

snapshot length 26244 bytes

2323 at 1 IP feedba 3716 > gateway domain

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

18) To capture all port except port 80 and port 25
\$ sudo tcpdump -i wlp2s0 not port 80 and
not port 25

23:36:18 IP fedora -> 1.1.1.1. Port 443
HTTP/1.1 GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 2000
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US, en;q=0.9
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

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

19) Capture only on port 53. Traffic
\$ sudo tcpdump -i wlp2s0 port 53
23:38:32 fedora -> gateway domain: AAAA
23:38:32 gateway domain -> fedora domain: AAAA
146 packets captured
146 packets received by filter
0 packets dropped by kernel.

20) Filter traffic coming from 8.8.8.8
\$ sudo tcpdump -i wlp2s0 src host 8.8.8.8
dropped previous to tcpdump
tcpdump: Verbose traces at interface
for full protocol decode
listening on wlp2s0, link type EN10MB
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 wlp2s0 -c 10 host
www.google.com
21) To capture https traffic
\$ sudo tcpdump -i wlp2s0 -c 10 host
www.google.com
0 packets captured
0 packets received by filter
0 packets dropped by kernel

Students observation questions:
1) Which command is used to test the
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 replies from destination.

- 2) Which command will give the details of taken by a packet to each router along its path to its destination?
- [v] - The traceroute command is used to display route packets state to a destination. It lists each IP along the path and the response time each router.
- 3) Which command displays the IP configuration of your machine?
- The ifconfig command is used to view IP configuration. These command shows IP addresses, interfaces, and other network details.
- 4) Which command displays TCP port status in your machine?
- The netstat -tln command is used to display TCP port status. Thus shows active connection, listening ports and associated process.
- 5) Write modify TCP configuration in Linux
- In Linux ipconfig or ifconfig command is used to modify TCP settings in Linux.

Ex: Sends IP address add
192.168.1.100/24 dev eth0

assigns an IP to an interface.

also creates IP configuration file for which

hosting to config traffic. (hosted on
host to config traffic. (hosted on)

host to config traffic. (hosted on)

also (450) using config traffic. (hosted on)

also (452) using config traffic. (hosted on)

also using config traffic. (hosted on)

Protocol	Host A	Host B	Expected Result
TCP	port 8080	port 8080	Established connection
Telnet	port 23	port 23	Established connection
HTTP	port 80	port 80	Established connection
FTP	port 21	port 21	Established connection
Telnet	port 23	port 23	Established connection
HTTP	port 80	port 80	Established connection
FTP	port 21	port 21	Established connection

Result:
Thus the study of various
networks in Linux and windows
was successfully.

Result:

Thus the study of various
networks in Linux and windows
was successfully.