

DX  
20/1/24

Aim:

Study of Various Network Commands used in Linux and Windows.

### Basic Networking Commands

1) arp -a: It will show IP address of your computer  
 O/P Interface : 172.16.75.74 ... on 12

#### Internet Address

#### Physical Address

#### Type

172.16.72.1	7C-5A-1C-D-BE-41	dynamic
172.16.75.77	4C-82-99-78-8C-85	dynamic
172.16.79.255	ff-ff-ff-ff-ff-ff	Static
239.255.255.251	01-00-5E-7f-ff-fb	Static

2) Host name: It displays the name of computer

O/P DESKTOP - COIBH7D

3) ifconfig: The command display detailed configuration information

O/P: Windows IP configuration

Hostname - Desktop - COIBH7D

Primary Dns Suffix

Node Type - Hybrid

IP routing enabled - No

WINS proxy enabled - No

Ethernet Adapter Ethernet 3

Media State - Media disconnected

Connection - Specific DNS Suffix

Description - Intel(R) Ethernet Connection (7) I219-LU

Physical address - 20-88-0-86-C7-A6

DHCP Enabled - Yes

Auto configuration - Yes

4) nbstat -a: Displays protocol statistics and current TCP/IP connection using NBT

O/P:

Remote name - Remote host machine name

IP Address - Dotted decimal representation of IP address

Interval - Redisplays selected statistics, pausing interval seconds between each display, press Ctrl+C to stop redisplaying statistics

5) netstat: It displays a variety of statistics about computer active TCP/IP connections

O/P

Proto

TCP

TCP

TCP

TCP

TCP

Local Address

127.0.0.1:49678

172.16.75.74:5903

172.16.75.74:59499

172.16.75.74:59883

172.16.75.74:59885

Foreign Address

Desktop-C01BH7D:49679

204.79.197.222.https

ma9905328-in-fs:https

ma9905306-in-fs:https

172.16.72.1.domain

State

Established

Close-wait

Time-wait

Established

Time-wait

6) nslookup: [Name Server lookup] is a tool used to perform DNS lookups in Linux

O/P: nslookup www.google.com

Server: dns.google

Address: 8.8.8.8

Non-Authoritative Answer:

Name: www.google.com

Address: 2404:6800:4007:82d::2004

172.250.196.38

7) Ping: Command is the best way to test connectivity between two nodes

O/P

Ping www.Rajalakshmi.org

Pinging www.Rajalakshmi.org [14.99.10.232] with 32 bytes of data:

Reply from 14.99.10.232: bytes=32 time=9ms TTL=124

Reply from 14.99.10.232 bytes=32 time=9ms TTL=127

Ping statistics from 14.99.10.232

Packets: Sent=4, Received=4, Lost=0 (0% loss),

Approximate round trip times in Milli-seconds.

Minimum=4ms, Maximum=9ms, Average=6ms

8) Route : It is used to show/ Manipulate the IP routing table

O/P:

Command One of these:

Point Prints a route

Add Add a route

delete delete a route

destination Specifies the host

MASK - Specifies that the next parameter is net mask value

NETMASK - Specifies a subset mask value for this route entry if not specified, it defaults to 255.255.255.255

GATEWAY - Specifies gateway

INTERFACE - the interface number for specified route

METRIC - Specifies the metric ie cost for destination

9) Pathping: Pathping is unique to windows and is basically a combination of the Ping and tracert commands

# some important Linux Commands:

## 1) ip addr show

10: <loopback, up, lower-up> mtu 65536  
qdisc seq 0

State unknown group default qlen 1000

inet 127.0.0.1/8 brd 127.255.255.255 scope host 10

inet 6: 128.0.0.1/128 brd 128.0.0.1 scope host

## 2) ifconfig

### Output

enp250 flags=4163 <UP,BROADCAST,RUNNING>

Multicast MTU 1500

inet 172.16.8.118 netmask 255.255.252.0

Broadcast 172.16.11.255

inet 6 fe:80::47:15699:dc900 profile 69 scopeid 0x20<link>

Rx errors 0 dropped 37 overruns 0  
frame 0

10:

flags=73 <UP,LOOPBACK,RUNNING>

mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet 6:1 Prefix 10 128 scopeid 0a (10<host>)

loop txqueuelen 1000 (wlan0loopback)

3) > MTR Google.com

Output:

localhost.localdomain(0.0.0.0)

boys: Help Display mode

Restart Statistics Order of fields. quit

Host:

1) 172.16.8.1

2) static-41. 229.249 - Lataidco.in

3) 142.280. 171162

4) 142.251.72.215

5) 142.250. 288.1

6) Maas 05512 - in - t14. 1e1.00.net

4. # apt install -y tcpdump

Last metadata expiration check: 0 days ago on

Thu 11 Jul 2024 03:48:46 PM PDT

Package has no 'tcpdump' file installed. It is 86.66 kB.

Dependencies resolved.

Nothing to do.

Complete!

# tcpdump -D

1. enp0s3 [Up, running, connected]

2. lo [Up, running, Loopback]

3. bluetooth - monitor (Bluetooth Monitor)

# tcpdump -i enp0s3 [Wireless]

dropped privs to Tcpdump

Tcpdump: verbose

for full protocol output decade suppressed, use -v [VJ]

listening on enp0s3, link-type EN10MB (Ethernet),  
snapshot length 46.

16:32:50.761108 IP 192.168.1.10.6537 > 255.255.255.255.  
255.6537: UDP, length 201

nc

361 packets captured

361 packets received by filter

0 packets dropped by kernel

# tcpdump -i enp0s3 host 8.8.8.8

dropped owing to tcpdump

tcpdump verbose output suppressed, use -vLJ-- for  
full protocol.

listening on enp0s3, link-type EN10MB (Ethernet),  
snapshot length 262144 bytes

0 packets captured

0 packets received by filter

0 packets dropped by kernel.

# tcpcdump -i enp0s3 -c

dropped owing to tcpcdump

tcpdump verbose output suppressed use -vLJ--  
for full protocol details

16:33:19.629767 IP local host -> live. 49664

Macs 2s - in de 100.net.https: Flags [P],

Sseq 41628354 T3: 41628355 ack 2669933 9T2T, win 50,

Options [nop,nop] ts val 1893368936 ocr 3771518625J

length 39

3 packets captured

3 packets received by filter

0 packets dropped by kernel

4) Tcapdump -i enp0s3 host google.com and  
PIL3

dropped prior to tap clamp

tap clamp restrict output suppressed, use -v [V].  
for full protocol decode

listening on enp0s3, link-type EN10MB (Ethernet)  
Snapshot length: 262144 bytes

0 packets captured

4 packets received by filter

0 packets dropped by kernel

5) Ping:

PING google.com (216. 58. 200. 42)

64 bytes from mac ass10-int14. 12-100.net  
(216. 58. 200. 42)

ICMP seq = 1 TTL = 120 time = 3.31ms

64 bytes from mac ass10-int14. 12-100.net  
(216. 58. 200. 42)

ICMP seq = 2 TTL = 120 time = 3.31ms

(216. 58. 200. 42)

ICMP seq = 3 TTL = 120 time = 3.31ms

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

Ping <hostname>

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

traceroute <host name>

3) Which command display the IP configuration of your machine

IPConfig /if config

4) Which Commands display the IP configuration at your TCP port status of your machine

netstat -an

5) Write and Modity the IP configuration in linux Machine

- login as a root user and start terminal
- Input "ifconfig" command prompt
- input "ifconfig" followed by the network interface and your reasip address
- Press "Enter"

Result:

Thus the Network basic commands of windows & linux are studied.

24/3/24.