EXP. NO: 01

DATE: 16-07-2024

STUDY OF VARIOUS COMMANDS USED IN LINUX & WINDOWS

BASIC NETWORK COMMANDS

AIM:

Study of various Network commands used in Linux & Windows.

arp -a:

```
Interface : 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static

Interface : 192.168.1.9 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.9           60-bd-2c-48-d9-00     dynamic
  192.168.1.110         44-03-77-51-87-71     dynamic
```

host_name:

```
DESKTOP-BI7A91G
```

ipconfig /all:

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (10) I219-V
   Physical Address . . . . . . . . : 00-2B-67-E1-D4-10
```

DCHP Enabled . . . . . : Yes

Auto configuration Enabled . . . . : Yes

nbtstat -a:

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 it's n

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

-n (names) Lists local NetBios names

-r (resolved) Lists names resolved by broadcast and via WINS

-s (sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names.

netstat -a:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-BI7A91G:0	LISTENING
TCP	192.168.1.9:53049	4.153.25.230:https	CLOSE_WAIT
TCP	192.168.1.9:54811	20.198.118.190:https	ESTABLISHED
TCP	[::1]:49669	DESKTOP-BI7A91G:0	LISTENING
UDP	0.0.0.0:63863	*:*	
UDP	[fe80::6873:fa26:66bb:b683%16]:1900	*:*	

nslookup :

nslookup www.google.com

Server : Unknown

Address : fe80::1

Non-authoritative answer:

Name : www.google.com

Addresses : 2404:6800:4009:823::2004

172.217.166.4

pathping :

Usage : pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
[-p period] [-q num-queries] [-w timeout]
[-4] [-6] target_name

Options :

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

-h maximum_hops Maximum number of hops to search for target

~~ping~~ :

ping :

Usage : ping [-a AbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
[-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
[-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
[-w deadline] [-W timeout] [hop1 ...] destination

Route:

Kernel IP Routing table

Destination	Gateway	Genmask	Flags	Metrics	Ref	Use	Iface
default	gateway	0.0.0.0	UG	100	0	0	enp2s0
172.16.8.0	0.0.0.0	255.255.252.0	U	100	0	0	enp2s0

LINUX NETWORKING COMMANDS:

1. ip:

a) ip address show:

```
1: 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
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
```

b) ip address add 192.168.1.254/24 dev enp503:

RT NETLINK answers: Operation not permitted

c) To delete an IP on an interface:

ip address del 192.168.1.254/24 dev enp230.

d) To alter the states of the interface by bringing the interface eth0 online & offline:

Online: ip link set eth0 up

Offline: ip link set eth0 down

e) Alter the status by enabling promiscuous mode of eth0:

ip link set eth0 promisc on.

f) Add a default route:

ip route add default via 192.168.1.254 dev eth0

g) Add a route:

ip route add 192.168.1.0/24 via 192.168.1.254

h) Display the route:

ip route get 10.10.1.4

2. mtr:

Hosts	Packets			Pings			
	Loss	Snt	Last	Avg	Best	Worst	StDev
1::1	0.01.	57	0.1	0.1	0.1	0.2	0.0

i) Show numeric IP Address:

mtr -b google.com

ii) Set no. of pings:

mtr -c 10 google.com

3. tcpdump:

dnf install -y tcpdump

i) tcpdump -D

1. ~~enp~~ enp2s0 [up, Running]
2. any (Pseudo-device that captures on all interfaces) [up. Running]
3. lo [Up, Running, Loopback]
4. wlp3s0
5. bluetooth 0 (Bluetooth adapter number 0)
6. usbmon1 (USB bus number 1)

ii) tcpdump -i enp0s3

verbose ~~of~~ output suppressed, use -v[v] ... for full protocol decode

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

16:32:48.655388 ARP, Request who has 192.168.1.12 tell gateway

iii) tcpdump -i enp0s3 host 8.8.8.8

dropped privs to tcpdump

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

^C

0 packet captured

0 packet received by filter

0 packet dropped by Kernel

iv) tcpdump -i enp0s3 -c

dropped privs to tcpdump

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

16:33:19.629767 IP localhost-live.49664 > ~~maa~~ maa05s23-in-f3.1e100.net.https: Flags [P.], seq 416 2835473.41.6.2883551 2 ack 2669933 9727, win 501 option [nop, nop, TS val 189 33689 36 ecr 3471518263], length 39

3 packet captured

3 packet received on filter

0 packet dropped by Kernel

v) tcpdump -i enp0s3 host google.com and port 43

dropped privs to tcpdump

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

listening on enp0s3, link-type EN10MB snapshot length 43

RESULT:

Thus the given Windows & Linux commands is executed successfully & output is verified.

16/7/24