16/7/24

PRACTICAL - 1

AIM:

Study of various Network commands used in Linux and Windows.

BASIC NETWORKING COMMANDS:

WINDOWS COMMANDS:

1) arp -a

Interface: 192.168.100.1 --- 0xd

Internet Address	Physical Address	Type
192.168.100.254	00-50-56-fc-56-7b	dynamic
172.16.8.1	7c-5a-1c-cf-be-45	dynamic
224.0.0.2	01-00-5e-00-00-02	static
239.255.255.250	01-00-5e-7f-ff-fa	static

2) Hostname

DESKTOP-HCVQANO

3) ipconfig /all

Windows IP configuration

Host Name . . . . . : DESKTOP-HCVQANO

Primary Dns Suffix . . . . . :

Node Type . . . . . : Hixed.

IP Routing Enabled . . . . . : No

WINS Proxy Enabled . . . . . : No

Ethernet adapter Ethernet:

Connection-Specific DNS Suffix . . :

Description . . . . . : Realtek PCTe GbE
Family Controller

DNS Servers . . . . . : 172.16.8.1

NetBIOS over Tcpip . . . . . : Enabled

4) Nbtstat - a

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

RemoteName Remote host machine name

IP address Dotted decimal representation of IP address

interval Redisplays selected statistics, pausing interval sec b/w each display

5) Netstat

Active Connections

Proto	Local Add	Foreign Add	State
TCP	172.16.8.85:7680	172.16.8.179:55342	ESTABLISHED
TCP	172.16.8.85:7680	HDC101F152:38881	TIME-WAIT
TCP	172.16.8.85:62716	123:http	TIME-WAIT
TCP	172.16.8.85:62734	172:16.11.105:ms-do	SYN-SENT

6) Nslookup

Nslookup www.google.com

Server: Unknown

Address: 172.16.8.1

Non-authoritative answers:

Name: www.google.com

Addresses: 2404:6800:4007:81e:2004
142.250.183.228

7) Pathping

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

8) Ping

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<1ms TTL=127

Reply from 14.99.10.232: bytes=32 time=1ms TTL=127

Ping statistics for 14.99.10.232:

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

Min=0ms, Max=1ms, Avg=0ms

9) Route

Route [-f] [-p] [-4] [-6] command [destination]

[MASK netmask] [gateway] [METRIC metric] [IF Interface]

Command one of these:

PRINT Prints a route

ADD Adds a route

DELETE Deletes a route

CHANGE Modifies an existing route.

LINUX COMMANDS:

1) arp -a

gateway (172.16.8.1) at 7C:5a:1c:cf:be:45 [ether] on enp2s0

2) Hostname

localhost.localdomain

3) ifconfig

eup2so: flag = 4163 <UP, BROADCAST, RUNNING1, MULTICAST>
mtu 1500

lo : flags = 73 <UP, LOOPBACK, RUNNING1 > mtu 65536

wlp3so : flags = 4099 <UP, BROADCAS, MULTICAST > mtu 1500

4) nslookup -A <ip address>

nslookup -A 14.99.10.232

Looking up status of 14.99.10.232

WORKGROUP <00> - <GROUP> B <ACTIVE>

DESKTOP - BQ498VC <00> - B <ACTIVE>

MAC Address = 50 - 9A - 4C - 34 - D3 - C3

5) nslookup www.google.com

Server: 172.16.8.1

Address: 172.16.8.153

Non-authorised answer:

Name: www.google.com

Address: 142.250.183.228

6) Ping

(i) Ping localhost

PING localhost (localhost = (::1)) 56 data bytes

64 bytes from localhost (::1) : icmp_seq=1 ttl=64 time=0.077ms

(ii) Ping 4.2.2.2

PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data

64 bytes from 4.2.2.2 : icmp_seq=1 ttl=53 time = 35.2ms

(iii) Ping www.facebook.com

PING start-mini.clor.facebook.com (157.240.192.35) 56(84)
- bytes of data

64 bytes from edge-star-mini-shv-02-maa2.facebook.com
- (157.240.192.35) : icmp_seq=1 ttl=59 time=279 ms

7) Route

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use
default	gateway	0.0.0.0	UG	100	0	0
172.16.8.0	0.0.0.0	255.255.252.0	U	100	0	0

Some important Linux networking commands:

1) ip

ip <options> <object> <command>

a) # ip address show

1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536

inet 127.0.0.1/8 scope host to

valid_lft forever

inet6 ::1/128

2: enp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500

link/ether 50.9a:4c:34:d8:85

3: wlp3s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500

link/ether d4:6a:82:ca:fb

b) # ip address add 192.168.1.254/24 dev enps03

c) # ip address del 192.168.1.254/24 dev enps03

d) # ip link set etho up

e) # ip link set etho down

f) # ip link set eth0 promisc on

g) # ip route add default via 192.168.1.254 dev eth0

h) # ip route add 192.168.1.0/24 via 192.168.1.254

j) # ip route delete 192.168.1.0/24 via 192.168.1.254

j) # ip route add 192.168.1.0/24 dev eth0.

k) # ip route get 10.10.1.4

10.10.1.4 via 172.16.8.1 dev enp2s0 src 172.16.8.84 cd 0 cache

2) ifconfig

enp2s0: flags = 4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500

lo: flags = 73<UP, LOOPBACK, RUNNING> mtu 65536

wlp3s0: flags = 4099<UP, BROADCAST, MULTICAST> mtu 1500

3) mtr

mtr <options> host ie/ip

a) # mtr google.com

Host	Packets		Pings				
172.16.8.1	Loss%	Snt	Last	Avg	Best	Wrst	StDev
	52.2%	160	0.2	0.2	0.2	0.3	0.0
142.250.171.161	48.6%	181	0.9	3.6	2.6	43.8	4.2

b) # mtr -g google.com

c) # mtr -b google.com

d) # mtr -c3 google.com

e) # mtr -d google.com

4) tcpdump

tcpdump : 287 packets captured

1033 packets received by filter

740 packets dropped by kernel

a) #dnf install -y tcpdump

Last metadata expiration check : 2:50:40 ago on Tue 23 Jul 2024 08:23:12 AM IST

Package tcpdump-14:4.90-2.fc26.i686 is already installed. skipping

Dependencies resolved

Nothing to do

Complete!

b) # tcpdump -D

1. enp2s0 [up, Running; Loopback]
2. any (Pseudo-device that captures on all interfaces)
3. lo [up, Running, Loopback]
4. wlp3s0 [up]

c) #tcpdump -i eth0 [#tcpdump -i enp2s0]

tcpdump : eth0 : No device

[tcpdump : verbose output suppressed, use -v (or) -vv

listening on enp2s0, link-type EN10MB (ethernet), capture

11:31.24.547943. IP 172.16.9.164.51012 > 239.255.255.250

11:31:24.518748 IP localhost.localdomain.localdomain

45156 18 packets captured, 328 packets received, 328 dropped.

d) #tcpdump -i enp2s0 -c 4

listening on enp2s0, link-type EN10MB (Ethernet)

11:36:56.347974 IP 172.16.9.46.mdns > 224.0.0.251.mdns

4 packets captured

252 packets received by filter

243 packets dropped by kernel.

26/7/24

Result:

Various Network commands used in Linux and Windows have been studied.