CS19541 - Computer Networks - Lab manual.

14/7/24

Practical 1

Aim:

Study of various network commands used in linux and windows:

Basic networking commands:

1) arp -a:

Interface : 192.168.100.1 ---0xd

Internet Address	Physical Address	Type
192.168.100.254	00-50-56-fc-56-76	dynamic
172.16.8.1	7c-5a-1c-cb-be-45	dynamic
224.0.0.2	01-00-5e-00-00-02	static
239.255.255.250	01-00-5e-76-bb-fa	static

2) Hostname

DESKTOP-HCVOANO

3) ipconfig /all

Windows IP configuration

Hostname . . . . . : DESKTOP-HCVOANO

Primary DNS suffix . . . . . :

Node Type . . . . . : Mixed

IP Routing Enabled . . . . : NO

WINS Proxy Enabled . . . . : NO

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . :

Description . . . . . : Realtek PCI e GBE

DNS Servers 172.16.8.1

NetBIOS Over TCPIP . . . . . Enabled.

4) nbtstat -a

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

RemoteName Remote host machine name

IP address Dotted decimal representation of IP addrs

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	HOCIDI7152:38881	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 answer

Name : www.google.com

Address : 2404 : 6800 : 4007 : 81e : 200e

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),

Max = 0ms, Max = 1ms, Avg = 0ms.

9) Route

Route [-6] [-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 (17.2.16.8.1) at 7c:5a:1c:cf:be:45 [ether] on enp2s0

2) Hostname

localhost.localdomain

3) ifconfig

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

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

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

4) nmblookup -A <ip address>

nmblookup -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-D3-13

5). nslookup www.google.com

Server : 172.16.8.1

Address : 172.16.8.1 # 53

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=35.2 ms

(iii) ping www.facebook.com

PING star-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=2.79 ms.

7) Route

kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	U
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 lo
valid_lft forever

lo : <LOOPBACK, UP, LOWER_UP> mtu 65536

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 a4:6a:6a:22:ca:fb

b) # ip address add 192.168.1.254/24 dev enp3s03

c) # ip address del 192.168.1.254/24 dev enp3s03

d) # ip link set etho up

e) # ip link set etho down

f) # ip link set etho promise on

g) # ip route add default via 192.168.1.254 dev etho

h) # ip route add 192.168.1.0/24 via 192.168.1.254

i) # ip route delete 192.168.1.0/24 via 192.168.1.254

j) # ip route add 192.168.1.0/24 dev etho

k) # ip route get 10.10.1.4

10.10.1.4 via 172.16.8.1 dev enp2s0 src 172.16.8.84 vid 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> hostname/ip

a) #mtr google.com

Host	Packets		Pings				
172.16.8.1	loss%	snt	Last	Avg	Best	Wrst	stD
	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 -c 3 google.com

e) #mtr -l google.com

1. tcpdump

tcpdump : 287 packets captured

1038 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 : 4.9.0-2.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

[...] output suppressed, use -v(v) -vv

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

11:31:24.519993 IP 172.16.9.164.51012 > 255.255.255.255

11:31:24.519998 IP localhost.localdomain.local > localdomain.local

12 packets captured, 328 packets received by filter

328 dropped.

a) # 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

258 packets received by filter

243 packets dropped by kernel

e) # tcpdump -i enp2s0 -c 4 host 8.8.8.8

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on enp2s0, link-type EN10MB (Ethernet)

0 packets captured

0 packets received by filter

0 packets received by kernel.

b) # tcpdum -i enp2s0 src host 8.8.8.8

tcpdump: verbose output suppressed, use -v (or -vv) for full protocol decode

0 packets captured

0 packets received by filter

0 packets dropped by kernel

nmcli connection show

NAME	UUID	TYPE	DEVICE
wired connection1	5af6dd98-3af4-3001-8551-defe0af2909e	ethernet	enp0s3

nmcli connection add con-name enp0s20 type ethernet

connection enp0s2 (6406f9c-6702-4761-9f63-048090aeb24d)

nmcli connection modify "wired connection 1" ipv4 method auto

nmcli connection modify "wired connection 1" ipv6.method auto

ip address show enp0s2

2: enp0s2: <BROADCAST, MULTICAST, PROMISC, UP, LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

link/ether 08:00:27:1f:01:4e brd ff:ff:ff:ff:ff:ff.

16/7/24