PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641004

Department of Applied Mathematics and Computational Sciences

COMPUTER NETWORKS LAB

MSc Software Systems - Semester 4

**Explore/Test the following by using appropriate Linux commands:**

1. How would we check the IP address assigned to the system?

**ifconfig**

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001

inet 172.31.48.48 netmask 255.255.240.0 broadcast 172.31.63.255

inet6 fe80::41b:e4ff:febb:aeeb prefixlen 64 scopeid 0x20<link>

ether 06:1b:e4:bb:ae:eb txqueuelen 1000 (Ethernet)

RX packets 5501560 bytes 746505121 (746.5 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 6143332 bytes 2145998851 (2.1 GB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 3811 bytes 345044 (345.0 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 3811 bytes 345044 (345.0 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

1. If a host wants to know the route that the packets take to reach another host, how can it do so? For example, if a host wants to reach [www.google.com](http://www.google.com), how can we identify the route, that the packets take to reach the host?

**Windows:**

**tracert www.google.com**

Tracing route to www.google.com [172.217.31.196]

over a maximum of 30 hops:

1 1 ms 1 ms 1 ms dlinkrouter.Dlink [192.168.0.1]

2 1 ms 2 ms 3 ms 103.218.112.1

3 12 ms 10 ms 10 ms 103.194.240.1

**Linux: traceroute www.google.com**

1. How can Internet domain name servers be queried?

**LINUX**

**dig www.google.com**

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.google.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63051

;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;www.google.com. IN A

;; ANSWER SECTION:

www.google.com. 182 IN A 172.253.63.99

www.google.com. 182 IN A 172.253.63.147

www.google.com. 182 IN A 172.253.63.106

www.google.com. 182 IN A 172.253.63.105

www.google.com. 182 IN A 172.253.63.104

www.google.com. 182 IN A 172.253.63.103

;; Query time: 0 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Thu Feb 18 05:47:05 UTC 2021

;; MSG SIZE rcvd: 139

**WINDOWS:**

**nslookup www.google.com**

Server: UnKnown

Address: fe80::360a:33ff:fe91:2c6

Non-authoritative answer:

Name: www.google.com

Addresses: 2404:6800:4007:80a::2004

172.217.160.132

TO FIND OR DEBUG WHERE ISSUES ARE(linux)

**dig ns www.gmail.com**

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> ns www.gmail.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39737

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;www.gmail.com. IN NS

;; ANSWER SECTION:

www.gmail.com. 240 IN CNAME mail.google.com.

mail.google.com. 240 IN CNAME googlemail.l.google.com.

;; Query time: 0 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Thu Feb 18 05:55:02 UTC 2021

;; MSG SIZE rcvd: 95

1. Find a simple way to review each of your system’s network connections and open sockets.

netstat

netstat -nlp //gives process id

ss //gives info about sockets used(only tcp)

ss -ua udp

ss -xa unique sockets

1. How can we enable/disable the network interfaces?

ip up/down commands

**ip route**

default via 172.31.48.1 dev eth0 proto dhcp src 172.31.48.48 metric 100

172.31.48.0/20 dev eth0 proto kernel scope link src 172.31.48.48

172.31.48.1 dev eth0 proto dhcp scope link src 172.31.48.48 metric 100

packet sniffing tool in linux is tcpdump

in windows its wireshark (is like tcp+a user interface)

**Explore/Test the following by using appropriate Windows commands:**

1. How would we test the connectivity to a remote machine from our machine?

telnet <IP ADDRESS OF SERVER PC> <PORT>

1. Display the network connections (both incoming and outgoing), routing tables, and a network interface statistic of your machine.

Netstat -r //prints routing table info

Netstat -a //all connections

Netstat -o

1. Find the default gateway connected to your system. Analyse our Lab network architecture. How many switches/routers are used? What are these device capabilities?

Ipconfig

Ipconfig -all //includes dhcp servers, subnet mask, etc

1. How can we analyse DNS problems. How can we obtain IP address from hostname?
2. How can you obtain detailed information about the network you are connected to?

Address resolution protocol – does ip to mac conversion

**arp**

Address HWtype HWaddress Flags Mask Iface

ip-172-31-48-1.ec2.inte ether 06:93:ed:cc:ec:6f C

arp table - mapping btw ip and mac addresses

WINDOWS:

arp -a

Interface: 192.168.202.1 --- 0x5

Internet Address Physical Address Type

192.168.202.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

Interface: 192.168.56.1 --- 0x11

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

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

Interface: 192.168.0.178 --- 0x12

Internet Address Physical Address Type

192.168.0.1 34-0a-33-91-02-c6 dynamic

192.168.0.255 ff-ff-ff-ff-ff-ff static

224.0.0.2 01-00-5e-00-00-02 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 192.168.220.1 --- 0x15

Internet Address Physical Address Type

192.168.220.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

**SCAPY**