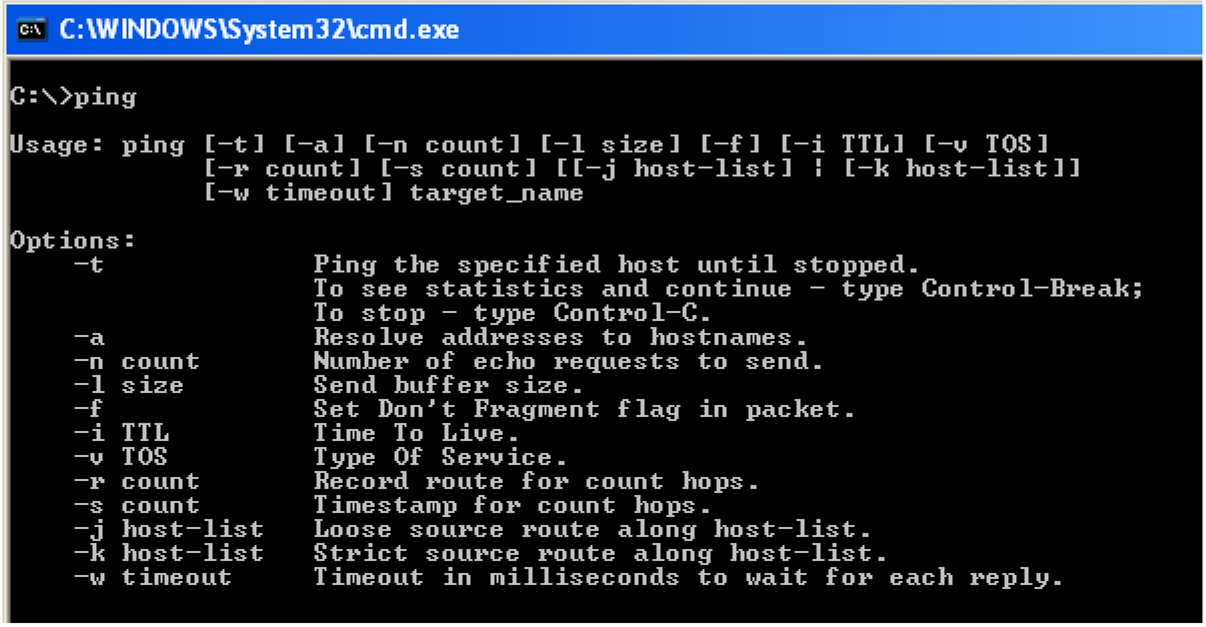
Module on DOS Network Tools and Commands

Prepared by: Dr. Natarajan Meghanathan

To go to the DOS promot, click Start-> Run-> Type cmd and Press enter. Type cd\ on the DOS window, it will take you to the root directory, commonly the C:\

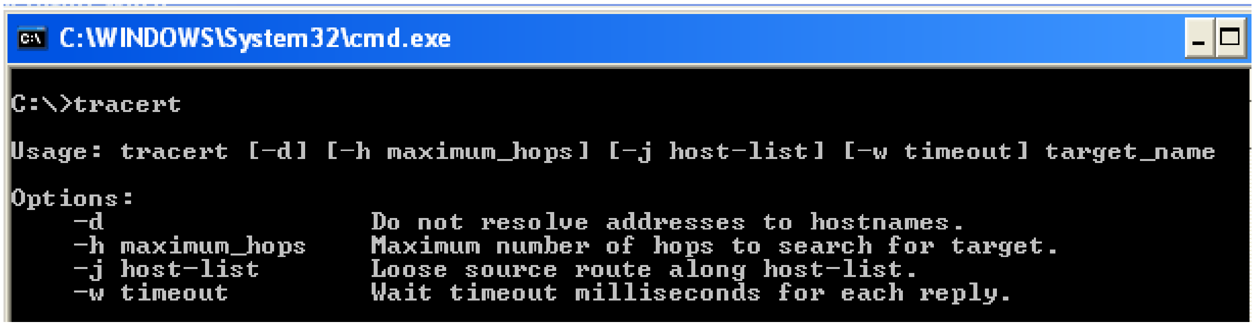
To get and idea of the commands, we will now see the primary utilities of each them.

Ping: Used to check the availability of systems by using the ICMP Echo Request / Response messages.



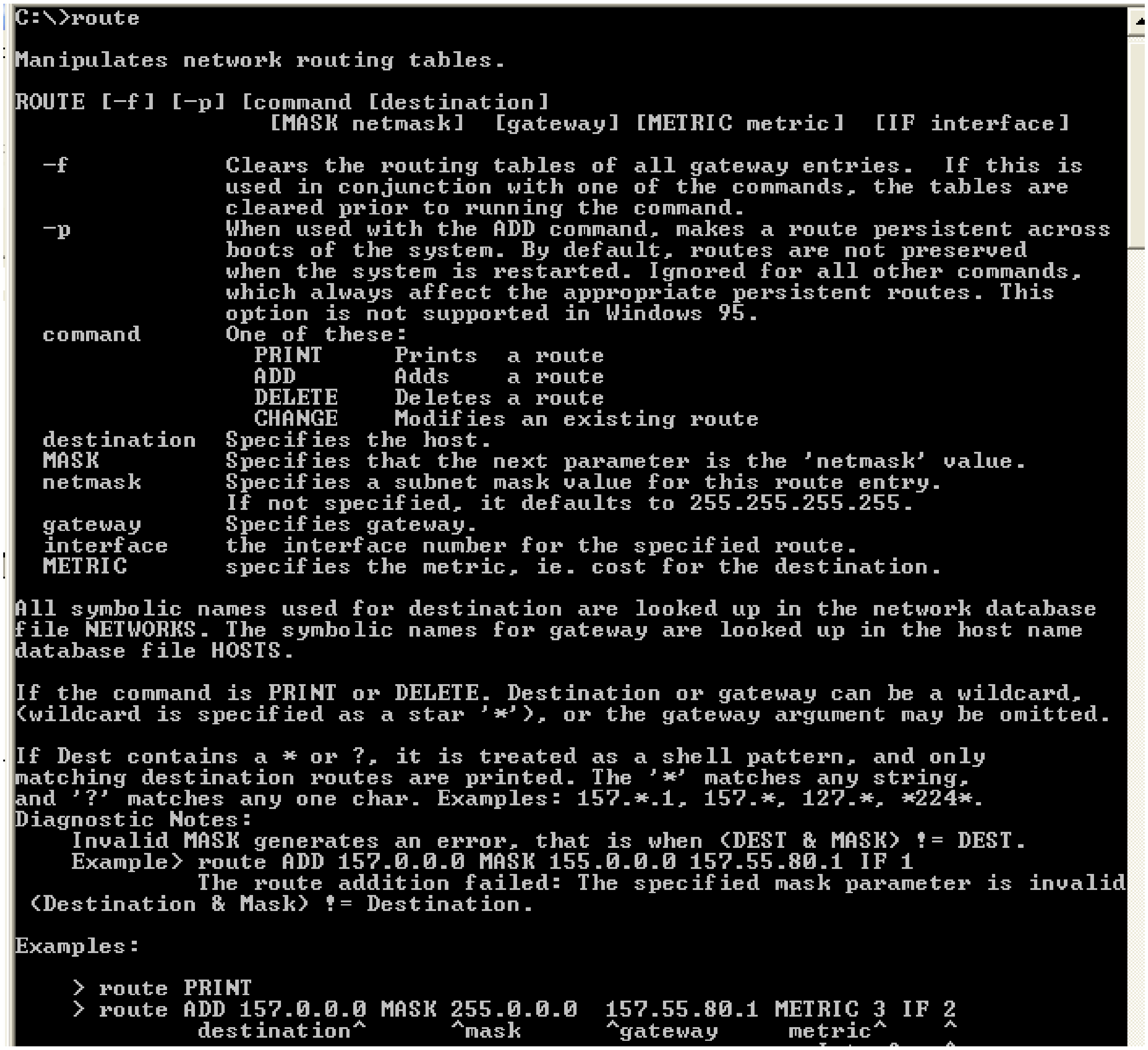
```
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

Tracert: The traceroute command is used to find the sequence of hops (i.e., the name of the intermediate hops/routers) from the source to a remote destination host.



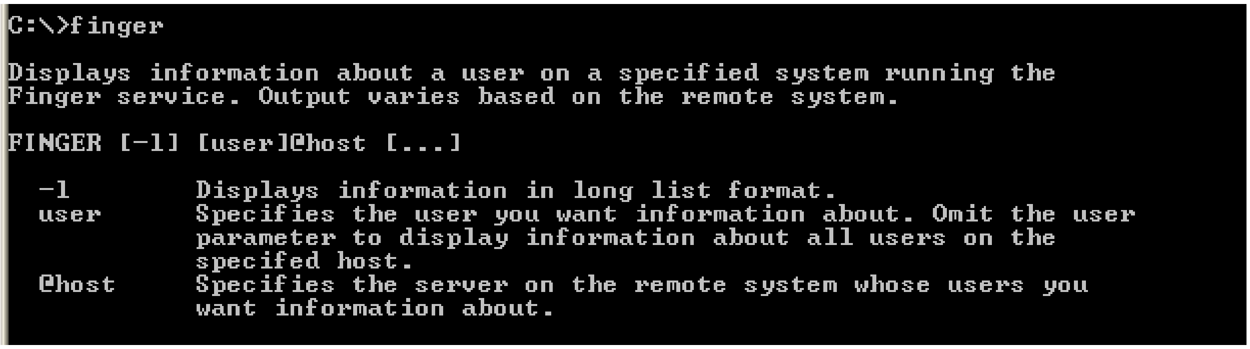
```
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list.
    -w timeout         Wait timeout milliseconds for each reply.
```

Route: The route command is used to display and modify the entries in the local routing table.



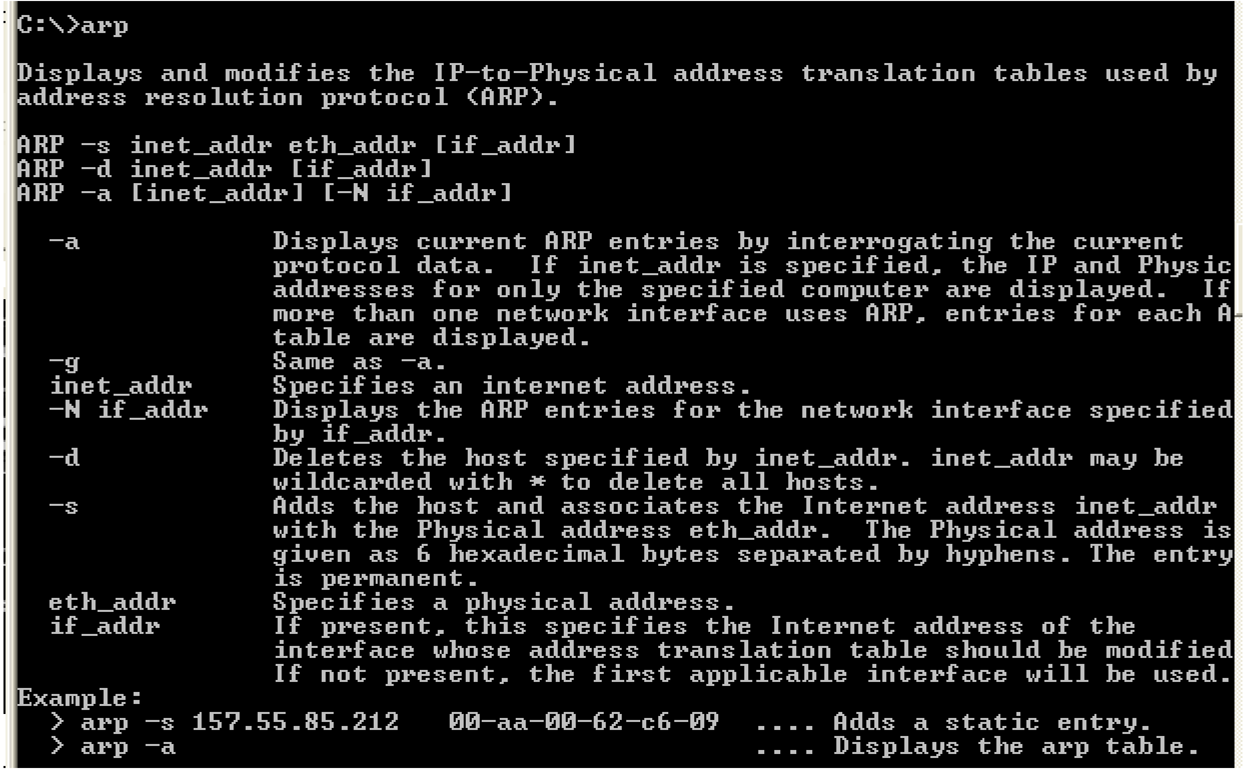
```
C:\>route

Manipulates network routing tables.

ROUTE [-f] [-p] [command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.
  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes. This
               option is not supported in Windows 95.
  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid
 (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
             destination^      ^mask      ^gateway     metric^    ^
```

Finger: The finger command is used to display information about users running in a specific host.



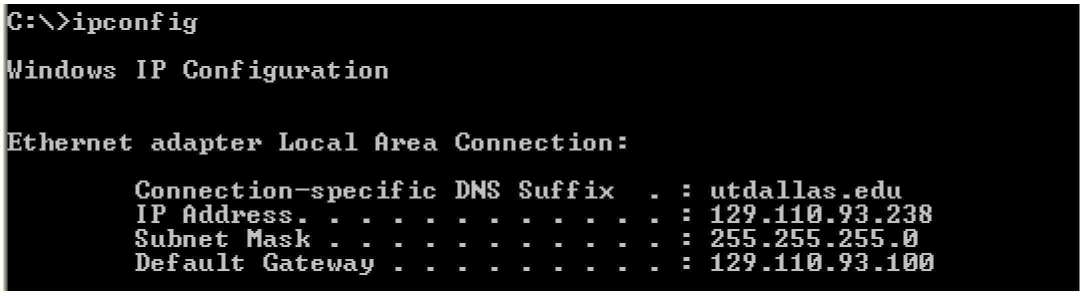
```
C:\>finger

Displays information about a user on a specified system running the
Finger service. Output varies based on the remote system.

FINGER [-l] [user]@host [...]

  -l        Displays information in long list format.
  user      Specifies the user you want information about. Omit the user
            parameter to display information about all users on the
            specifed host.
  @host     Specifies the server on the remote system whose users you
            want information about.
```

Arp: The arp command is used to display and modify the address resolution cache, which stores the mapping between the IP address of systems and their resolved physical addresses.



```
C:\>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physic
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each A
                table are displayed.
  -g            Same as -a.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

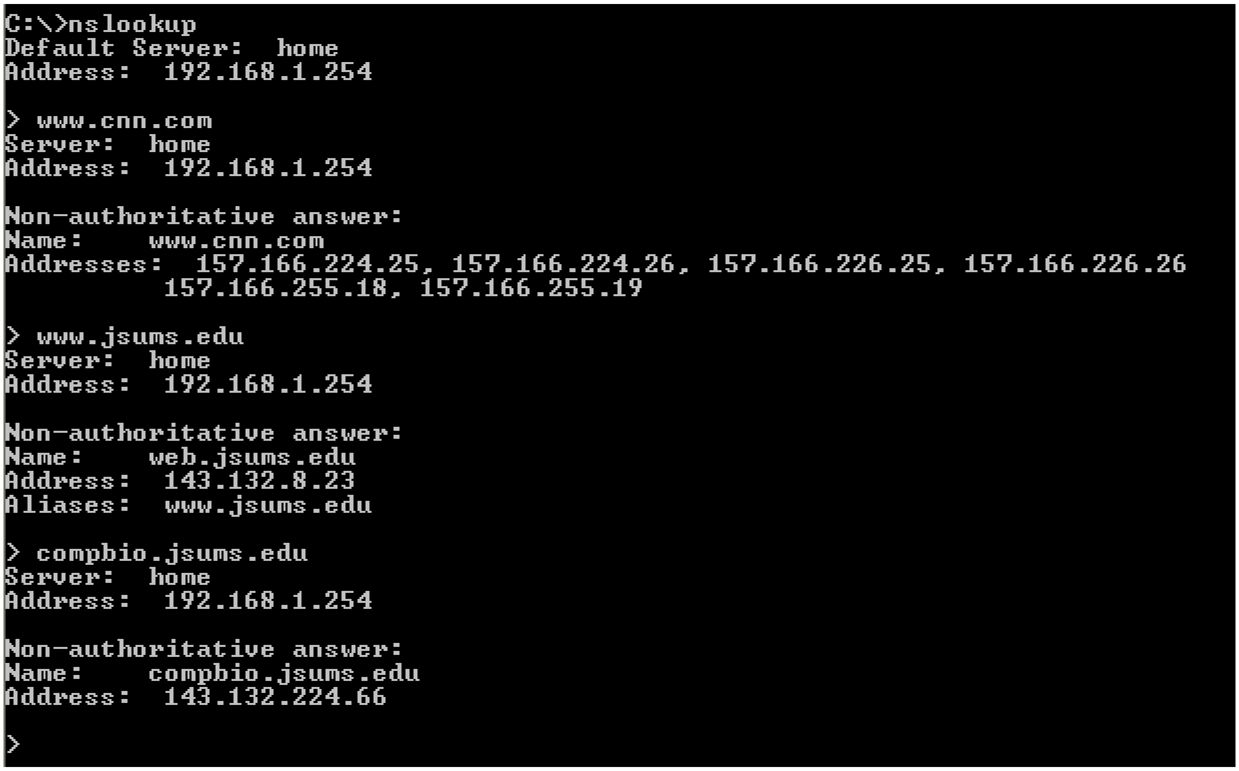
IPconfig: The ipconfig command is used to display the current TCP/IP network configurations. Also, try **IPconfig /all** to display full configuration information



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : utdallas.edu
        IP Address. . . . . . . . . . . . : 129.110.93.238
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 129.110.93.100
```

Netstat: When used without parameters, ***netstat*** displays active TCP connections.
Use netstat -e option to learn about the statistics of the Ethernet.
netstat –a option to learn about the active TCP connections and also the ports on which the computer is waiting for incoming TCP/UDP messages.
netstat –n option to learn about the numerical values of the IP addresses and ports used for active TCP connections.
netstat –p <protocol> to learn about the statistics for a specific protocol. The valid values for <protocol> include tcp, udp, ip, icmp.

nslookup: The nslookup command is used to study the DNS infrastructure.



```
C:\>nslookup
Default Server:  home
Address:  192.168.1.254

> www.cnn.com
Server:  home
Address:  192.168.1.254

Non-authoritative answer:
Name:    www.cnn.com
Addresses:  157.166.224.25, 157.166.224.26, 157.166.226.25, 157.166.226.26
          157.166.255.18, 157.166.255.19

> www.jsums.edu
Server:  home
Address:  192.168.1.254

Non-authoritative answer:
Name:    web.jsums.edu
Address:  143.132.8.23
Aliases:  www.jsums.edu

> compbio.jsums.edu
Server:  home
Address:  192.168.1.254

Non-authoritative answer:
Name:    compbio.jsums.edu
Address:  143.132.224.66

>
```

<u>Sample Questions</u>

1. Use an efficient algorithm and any one of the above command tools to find the maximum data size that can be handled by the physical network to which your computer is attached.

2. Use the ping command to determine how long it takes for a request packet with data size 50 bytes to reach a website operated from India: www.sify.com. Try sending another request packet of data size 1200 bytes to the same website and observe the delay it takes this time. Compare the delays you observed in the two cases. Are they significantly different? If so, why? If not, why there is no significant difference?

3. Find the number of hops and the corresponding delay it takes to reach www.abc.com and www.eduaustralia.co.kr. What is the percentage increase in the number of hops and delay to reach the site in Korea compared to reaching www.abc.com, a website in California? If you observe that the increase in the delay is not proportional to the increase in the number of hops, comment?

4. Find the domain name of the machine with IP address 74.125.45.99?

5. Find the number of unicast Ethernet frames sent and received by each of the network interfaces of your PC?

6. What is the physical address of the Ethernet adapter of the PC in which you are working?

7. Find whether port number 4123 is part of an active connection?

8. What is the IP address and physical address of the default router to which your machine forwards a packet for which it has no other next-hop forwarding router information in its local routing table?