# MASTER OF COMPUTER APPLICATION

# (2024–26)



(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY)



**COMPUTER NETWORKS**

**LAB PRACTICAL FILE**

**Submitted to:**

Mrs. Rekha Saraswat

**Submitted by:**

VAISHALI MISHRA

(01811804424)

**INDEX**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **LAB PROGRAM** | **PAGE No.** | **SIGN** |
| 1. | Networking Lab 1 | 3-18 |  |
| 2. | Networking Lab 2 | 19-24 |  |
| 3. | Wireshark Lab 1 | 25-29 |  |

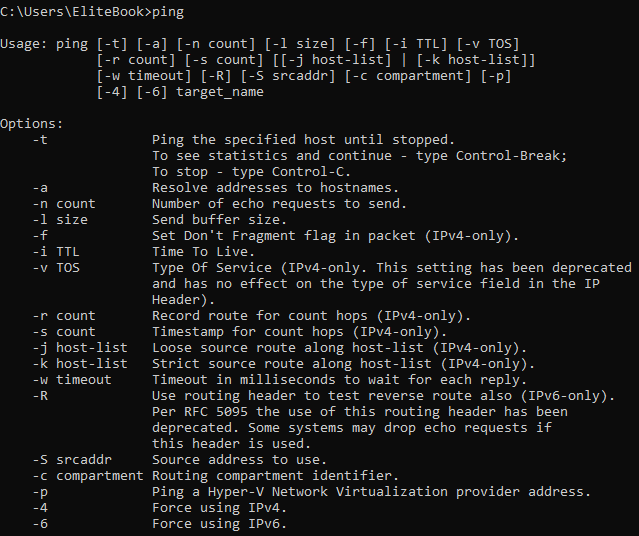
# 

# Networking Lab 1

# Basic networking commands:

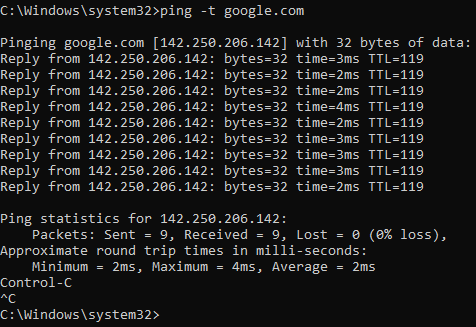
##### Ping

The ping command is a [Command Prompt command](https://www.lifewire.com/list-of-command-prompt-commands-4092302) used to test the ability of the source computer to reach a specified destination computer. It's a simple way to verify that a computer can communicate with another computer or network device.

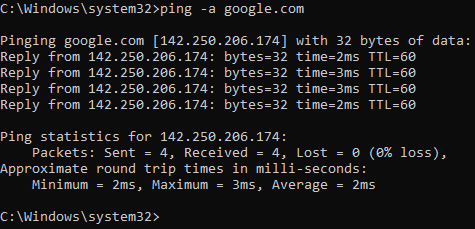


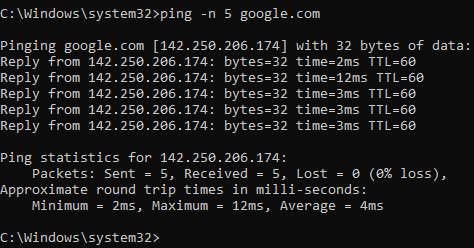
##### PING COMMAMND OPTIONS

* **-t :-** Using this option will ping the *target* until you force it to stop by using [Ctrl+C](https://www.lifewire.com/what-is-ctrl-c-used-for-2625834).



* **-a: -** This ping command option will resolve, if possible, the [hostname](https://www.lifewire.com/what-is-a-hostname-2625906) of an [IP address](https://www.lifewire.com/what-is-an-ip-address-2625920) *target*.

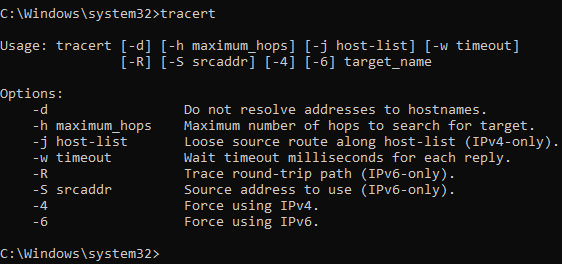


* **-n *count:-***This option sets the number of ICMP Echo Requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used.

##### Tracert

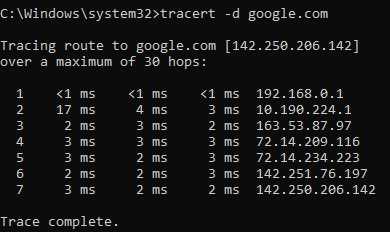
The Trace route command (Tracert on Windows) is a small network diagnostic software that you have built-in on your device and servers for tracing the route, hop by hop to a target.

Many network administrators use the Traceroute command daily. It is a convenient tool that you can use under different operation systems – Windows (Tracert), macOS, Linux (Traceroute), and even on mobile (Android and iOS).

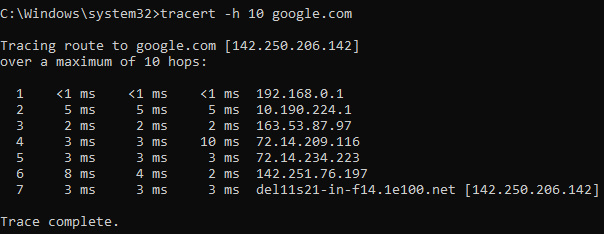


**Tracert Command Options**

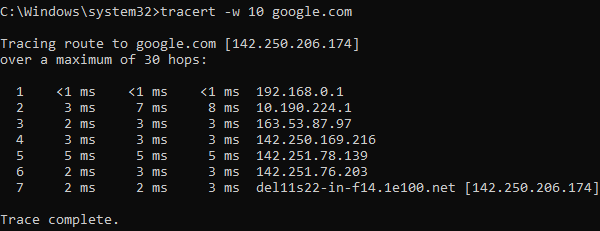
* **-d: -** Do not resolve addresses to hostnames.



* **-h maximum\_hops: -** Maximum number of hops to search for target.

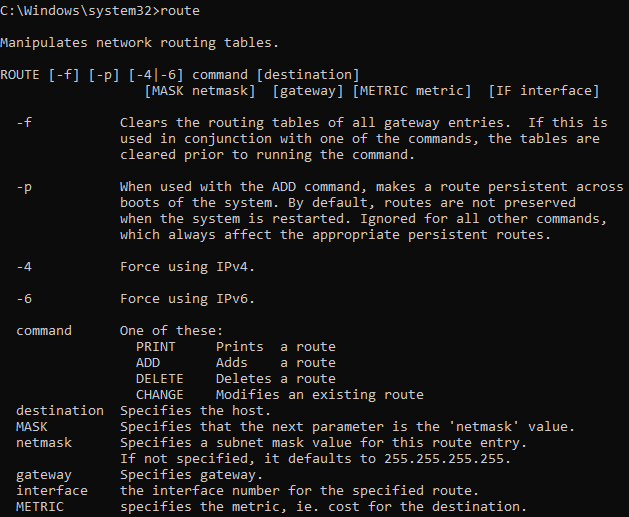


* + **-w timeout :-** Wait timeout milliseconds for each reply.



1. **Route Command**

The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the *Destination* variable, which can be specified either by symbolic name or numeric address. The route command resolves all symbolic names into addresses, using either the /etc/hosts file or the network name server.

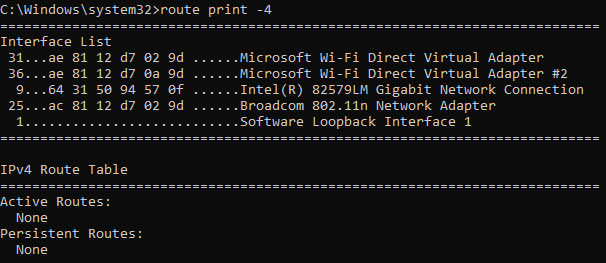


### Route Command Options

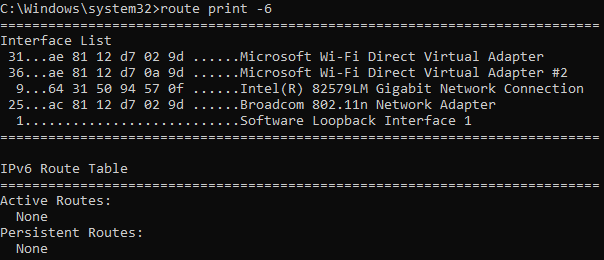
* + **-f : -** Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command

****

* + **-4: -** Force using IPv4.

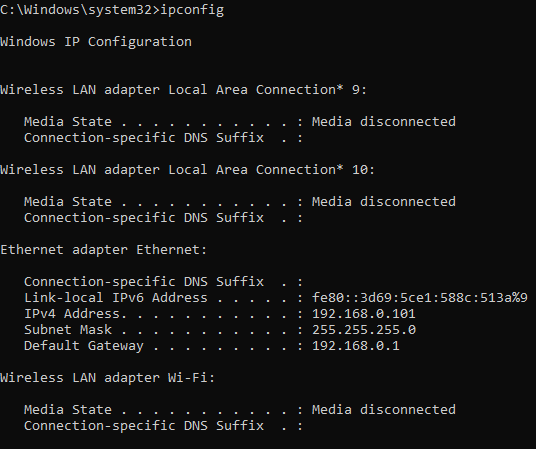


* + **-6: -**Force using IPv6.



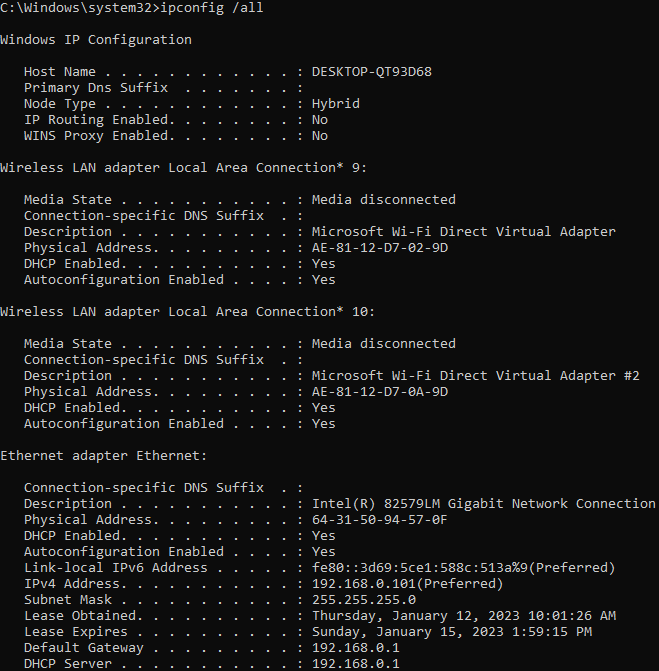
##### 4. Ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

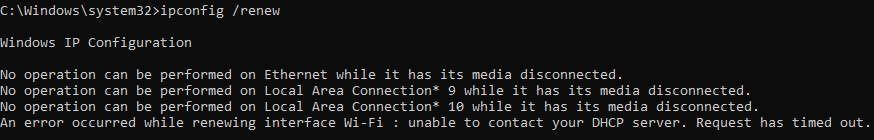


### Ipconfig Command Options

* + **/all: -** Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.



* + **/renew :-** renew all adapters

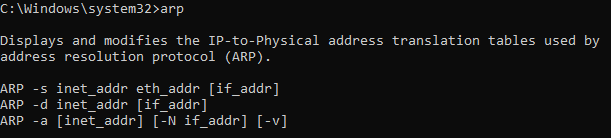


* + **/release: -** Release the IPv4 address for the specified adapter.



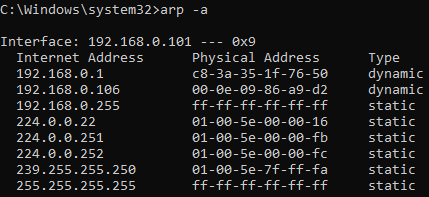
##### 5. ARP

Displays and modifies address resolution, including ATM (Asynchronous Transfer Mode) interfaces.

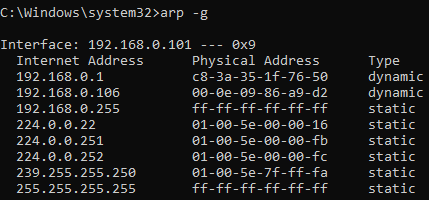


### ARP Command Options

* + **-a:** Displays current ARP entries by interrogating the current protocol data. If inet\_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

****

* + **-g:** This command works the same as the arp -a command.

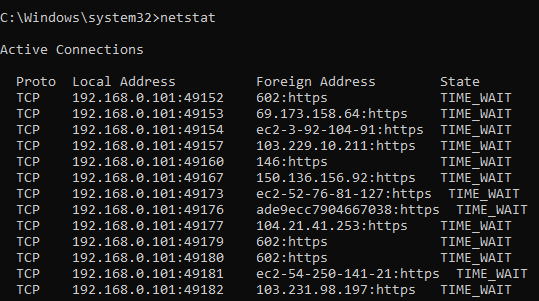


* + **-d:** This command is used when you want to delete an entry from the ARP table for a particular interface. To delete an entry, write arp -d command along with the IP address in a command prompt you want to delete.



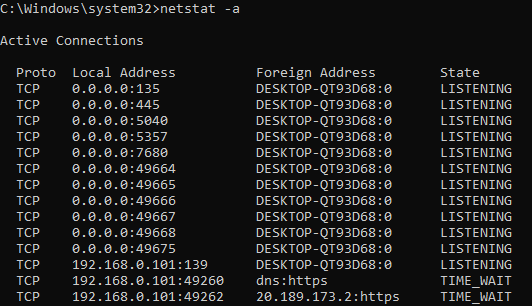
##### 6. Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

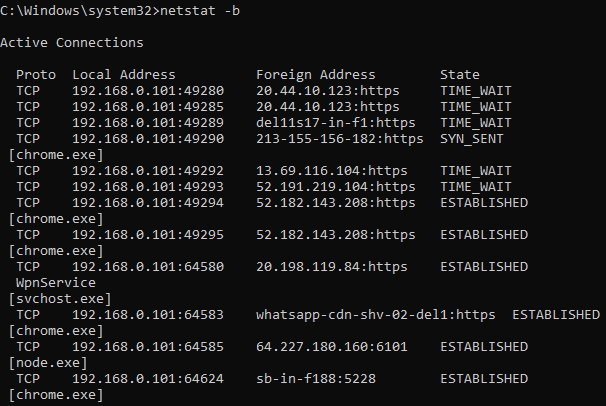


### Netstat Command Options

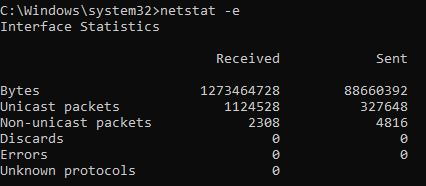
* + **-a: -** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

****

* + **-b :-** Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed.



* + **-e :-** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.



##### 7. Hostname

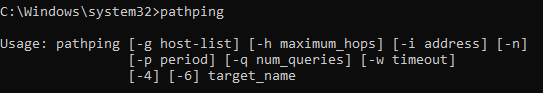
Your Computer Name (also known as the computer’s hostname) is used by our OIT Technicians to locate your computer’s physical location on campus, install software, and keep track of repairs that have been performed.



**8. Pathping**

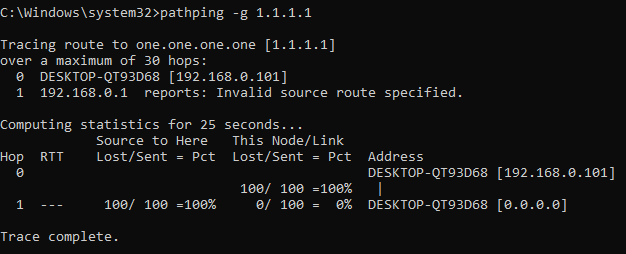
Provides information about network latency and network loss at intermediate hops between a source and destination. This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router. Because this command displays the degree of packet loss at any

given router or link, you can determine which routers or subnets might be having network problems. Used without parameters, this command displays help.

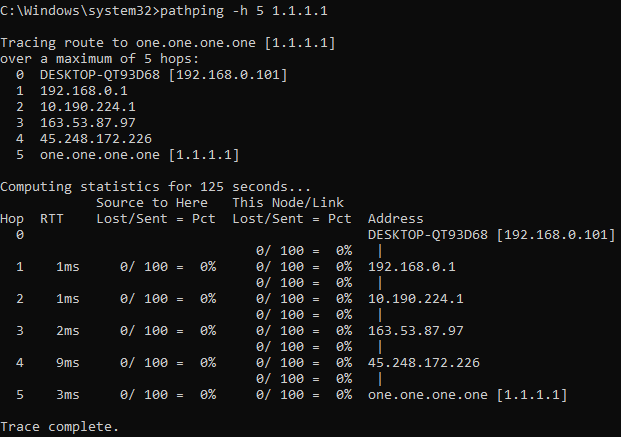


### Pathping Command Options

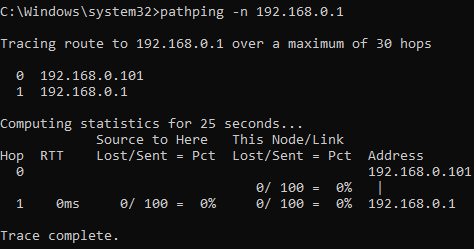
* + **-g host-list:-** Loose source route along host-list.



* + **-h maximum\_hops:-** Maximum number of hops to search for target.

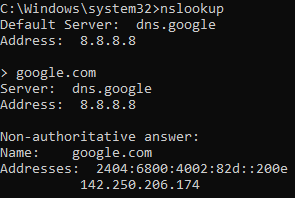


* + **-n: -** Do not resolve addresses to hostnames.



##### 9. Nslookup

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.

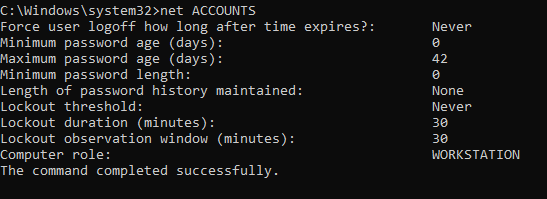


**10. Net Command**

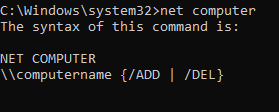
The **net** Command Prompt command manages almost any aspect of a network and its settings, including network shares, network print jobs, and network users.

### Net Command Options

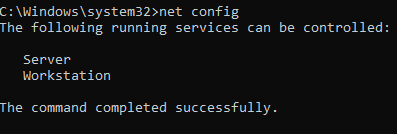
#### **Accounts: -** The net accounts command is used to set password and logon requirements for users. For example, the net accounts command can be used to set the minimum number of characters that users can set their password to.

****

* + **Computer:-** The net computer command is used to add or remove a computer from a domain.



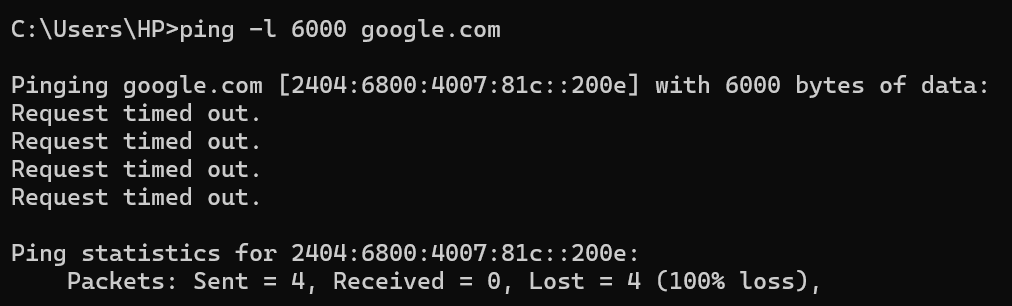
#### **Config: -** Use the net config command to show information about the configuration of the Server or Workstation service.

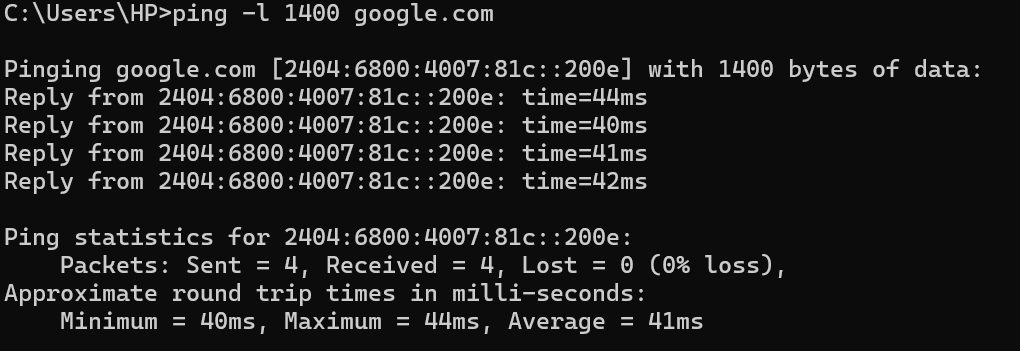


# Networking Lab 2

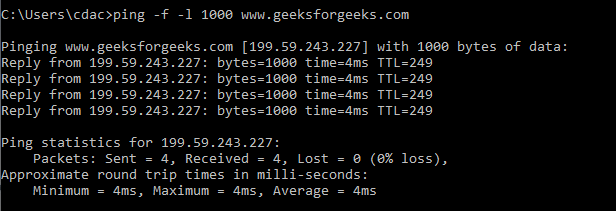
#### **Use the Networking commands, explored in lab1 to complete the following exercises.**

1. **Use any networking command you have studied,**
   * **In order to send a packet to a host (cdac. in) with the size of 60000 bytes each. We wish to send the packets repetitively.**

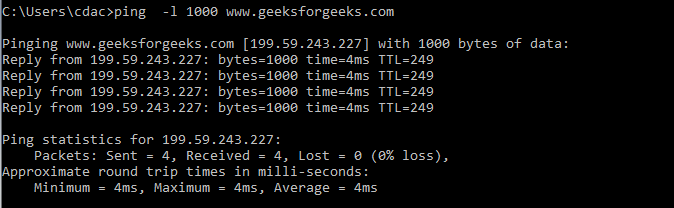


****

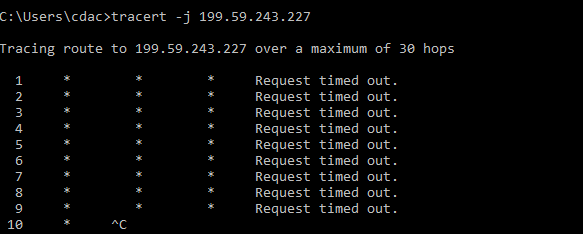
* + **In order to send a packet with a size of 1000 bytes and don’t permit fragmenting.**



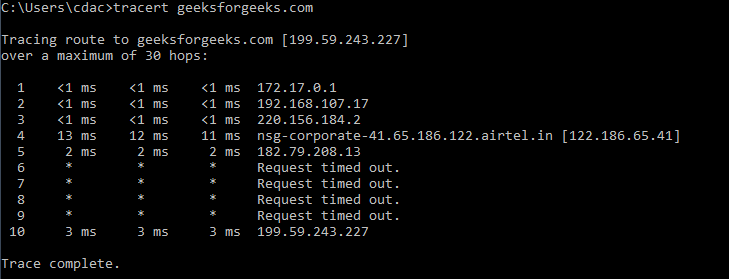
* + **In order to send a packet with a size of 1000 bytes and permit fragmenting.**



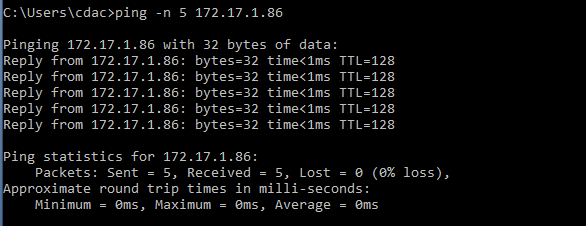
* + **In order to use loose route to a destination.**



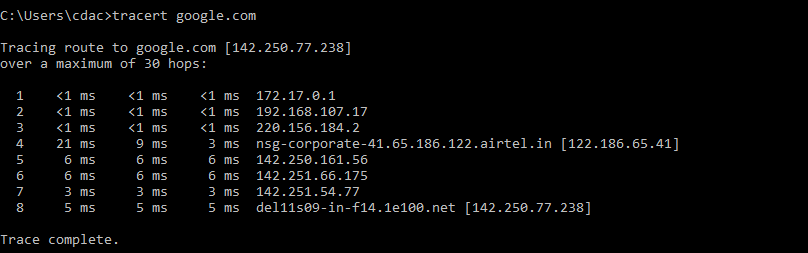
* + **In order to use a strict route to a destination.**



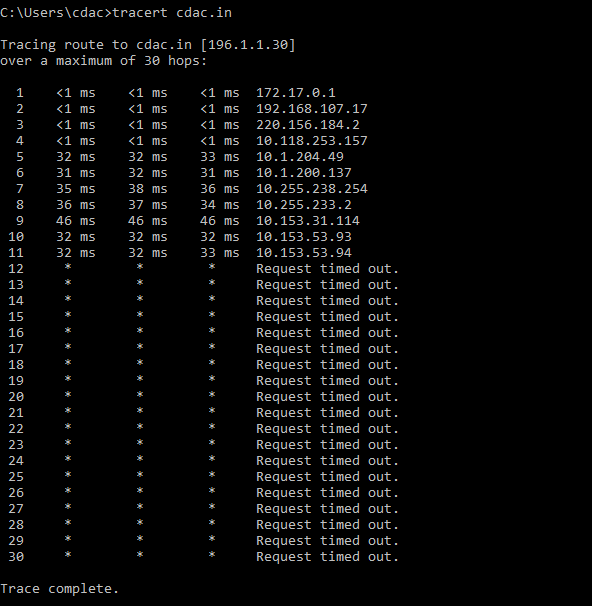
* **Test the reach ability towards a PC [192.168.230.4] with the fragmenting option enabled and limit the number of echoes to 5.**



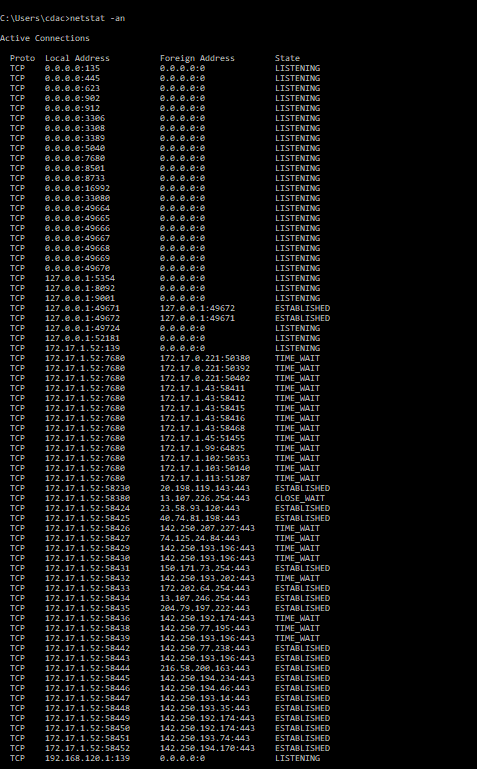
1. **Find the route from your PC to ITC [itc.kfupm.edu.sa OR 10.140.3.171].**



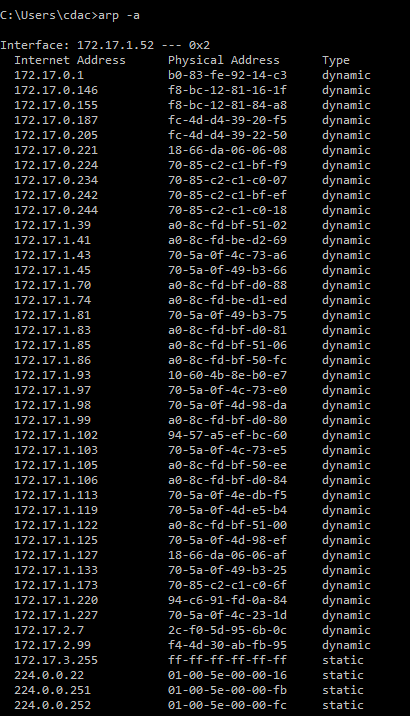
1. **Find the route from your PC to a CCSE server [vlsi.ccse.kfupm.edu.sa OR 196.1.64.70]**



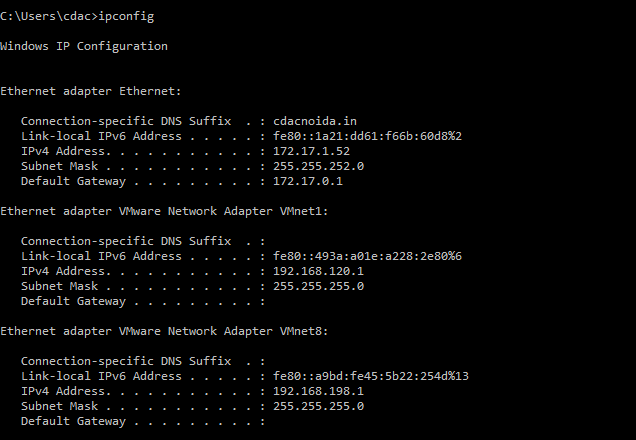
1. **Using the answers above, determine what is the first device your packet reaches to move from our network lab.**
   * + 1. **(Gateway) is the first device to which the packet reaches from the lab.**
2. **Open a browser connection to http server** [**[w**](http://www.kfupm.edu.sa/)**w**[**w.kfupm.edu.sa]**](http://www.kfupm.edu.sa/) **and write down the outcome of the command 'netstat -an'.**



1. **Find out the entries on your system regarding ip addresses and their matching physical addresses.**



1. **Find out the TCP/IP configuration of your system.**

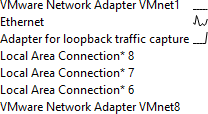


# Wireshark Lab 1

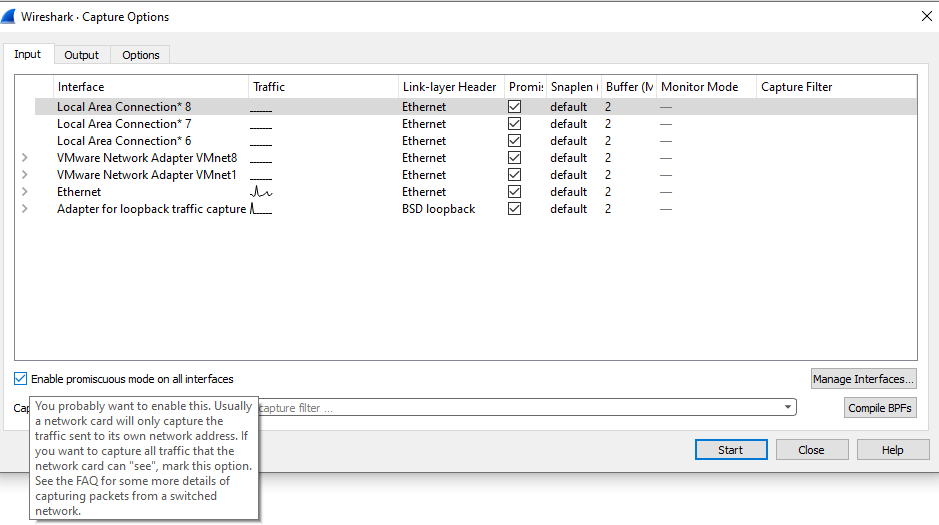
**Objective: Network Traffic Analysis Tool Used: Wireshark**

**Wireshark is a network packet analyzer tool that captures network packets and displays the packet details.**

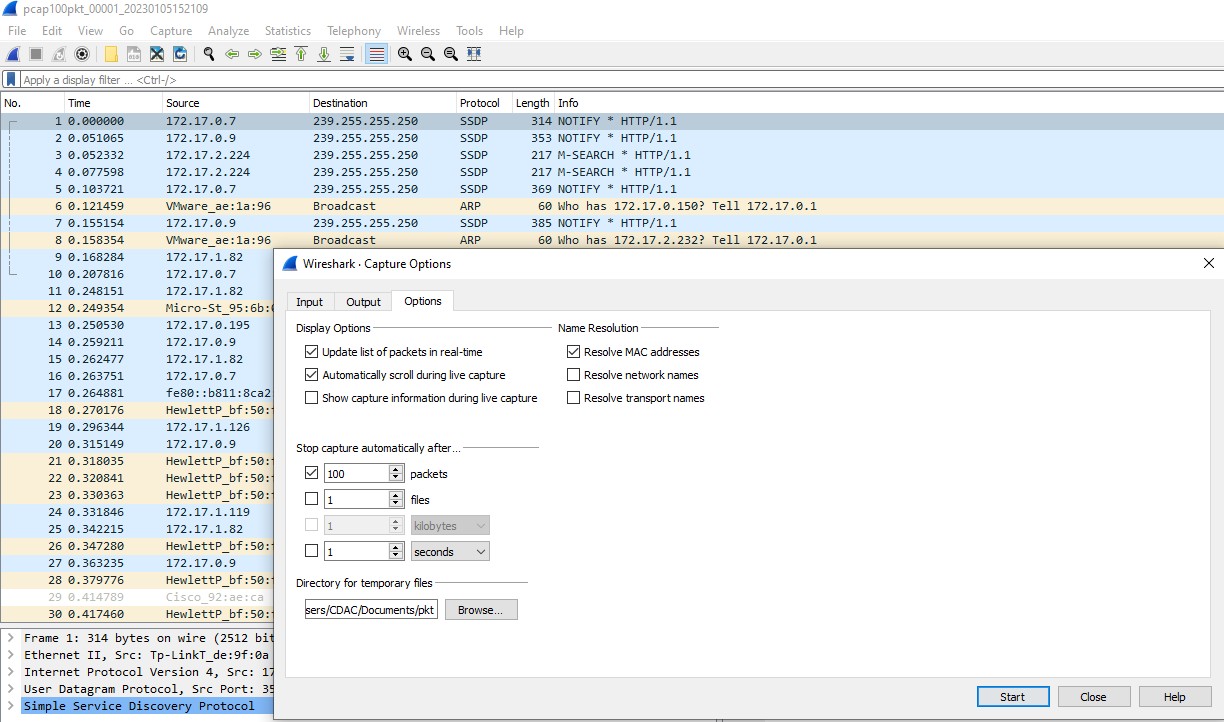
1. **List down the network interfaces connected to your host. Identify the Ethernet interface.**

****

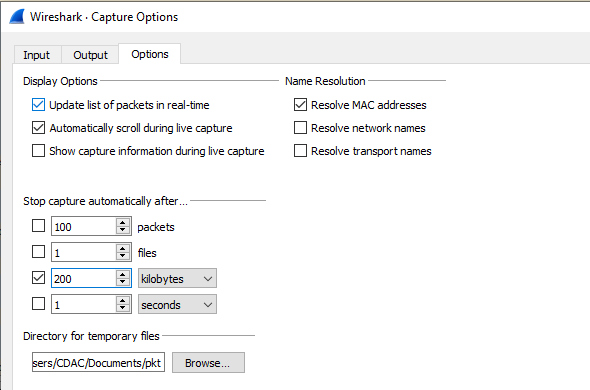
1. **Check whether the network interface of your machine is in Promiscuous mode. If it is not in promiscuous mode, change it to promiscuous mode.**

****

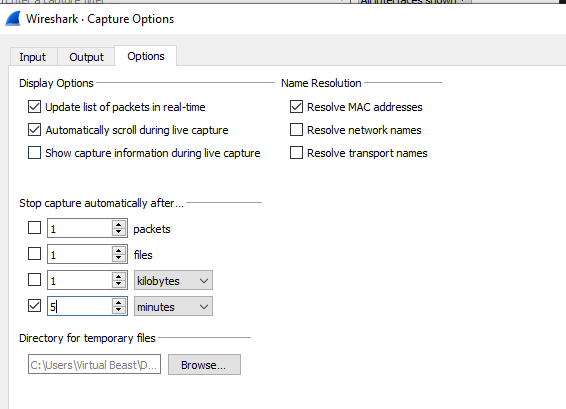
1. **Configure the capture stop option of the Wireshark in the following settings**
2. **Stop after 100 packets and store into a file “pcap100pkt”.**

****

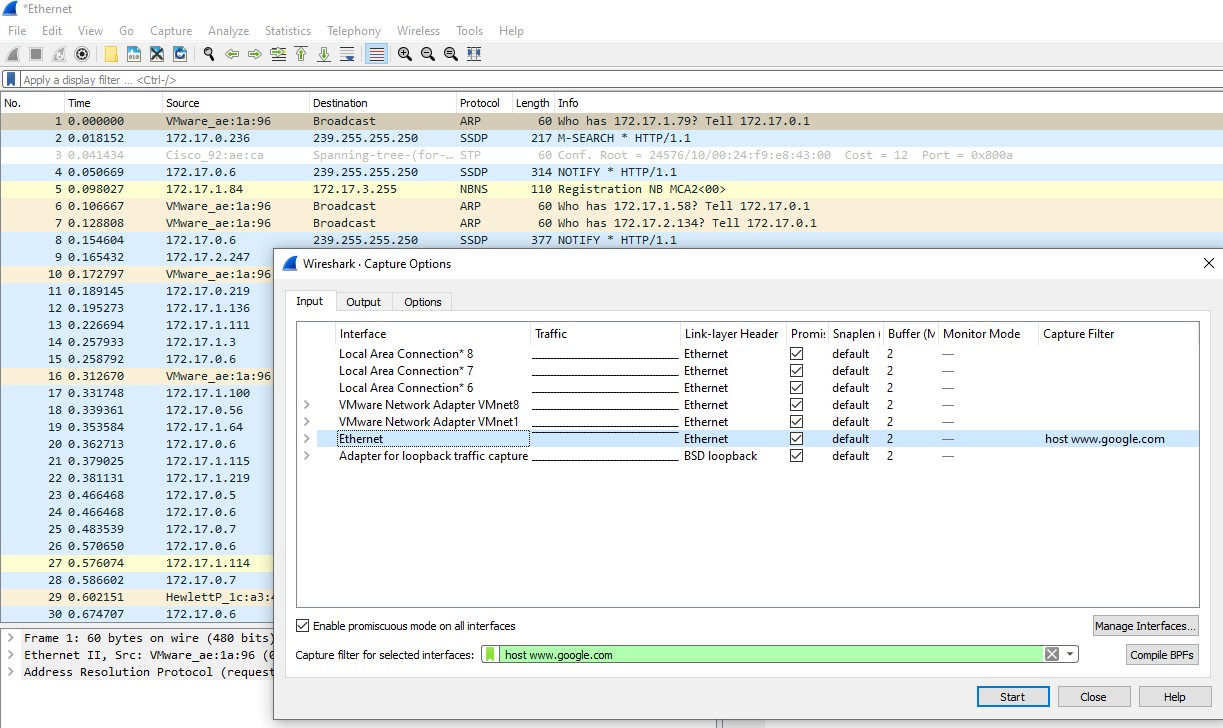
1. **Stop after 200 Kb and store into a file “pcap200kb”.**

****

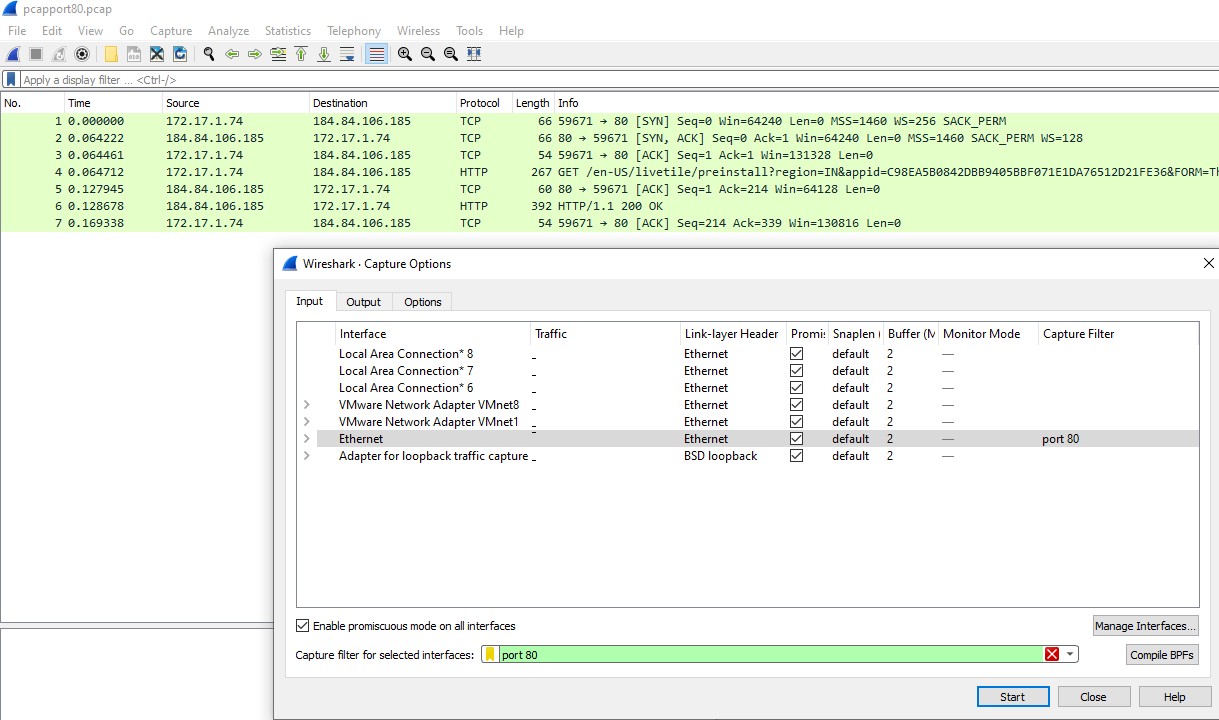
1. **Stop after 5 minutes and store into a file “pcap5min”.**

****

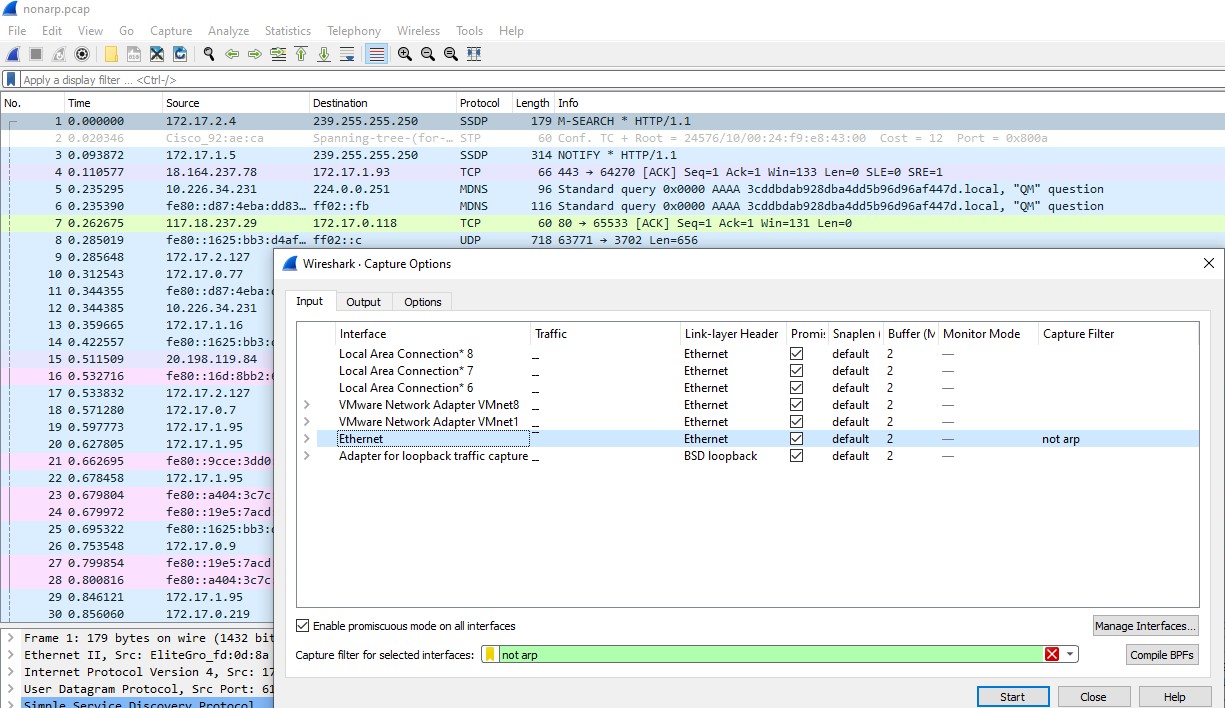
1. **Capture live traffic from** [**www.google.com**](http://www.google.com/) **and store the captured file as “pcaphost. pcap”.**

****

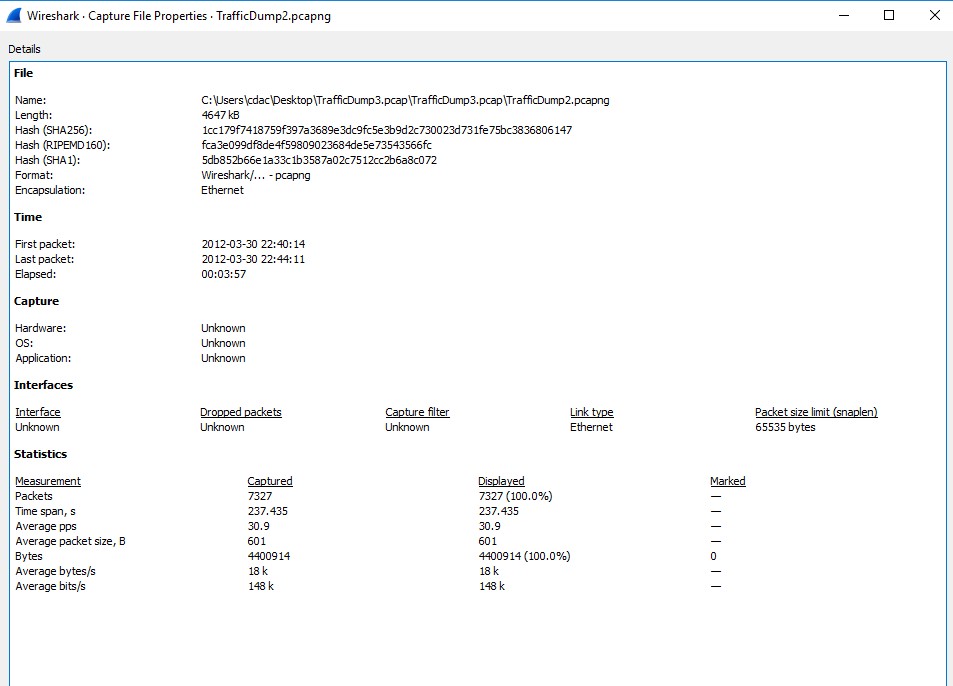
1. **Capture live traffic from port 80 and store the captured file as “pcapport80.pcap”.**

****

1. **Capture all non-ARP traffic using capturing filter operators and store the captured file as “nonarp. pcap”.**

****

1. **Display the summary of the following**
2. **No. of a packet captured, total bytes transferred**
3. **Average packets/sec, average packet size**
4. **Bandwidth usage (Average bytes/ sec)**

****