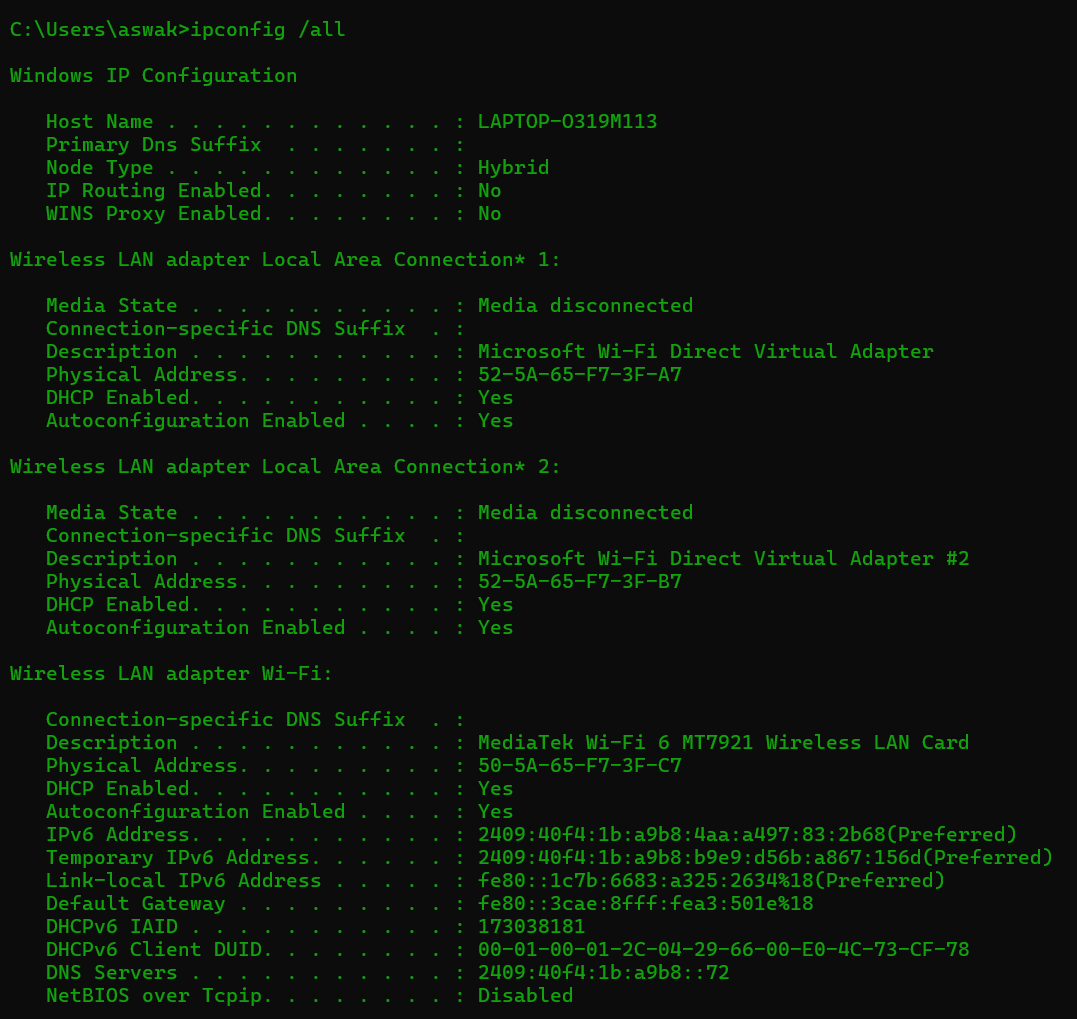
**SPIDER SOFTWARE TASK -1**

**COMMON TASK - COMPUTER NETWORKING**

**1.BASICS OF TERMINAL**

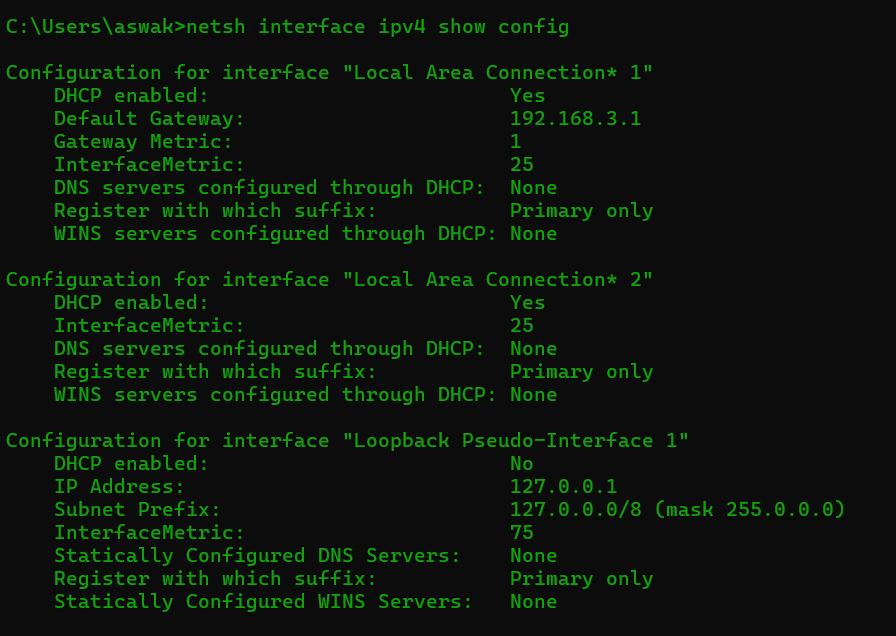
* **ipconfig /all** is the CLI command that displays all the network interfaces including ethernet interfaces, wi-fi interfaces, loopback interfaces or any virtual interfaces.

It also displays the detailed information about the network interfaces which includes IP address, MAC address (physical address) etc.



* To manually assign IP address, subnet masks, default gateways and DNS servers to a interface, you need to know the names of the network interfaces first.

**netsh interface ipv4 show config** is the command used to list all the names of the interfaces



Now you can assign the configuration using the command

**netsh interface ipv4 set address name=”<INTERFACE\_NAME>” static <IP\_ADDRESS> <SUBNET\_MASK> <GATEWAY>**

DNS servers can be set using the following command

**netsh interface ipv4 set dns name=”<INTERFACE\_NAME>” static <DNS\_SERVER>**

IP address conflicts occurs when two or more devices on the same network get assigned the same IP address, this will lead to communication problems and network connectivity issues. In order to avoid the conflicts you have to manage the IP addresses.

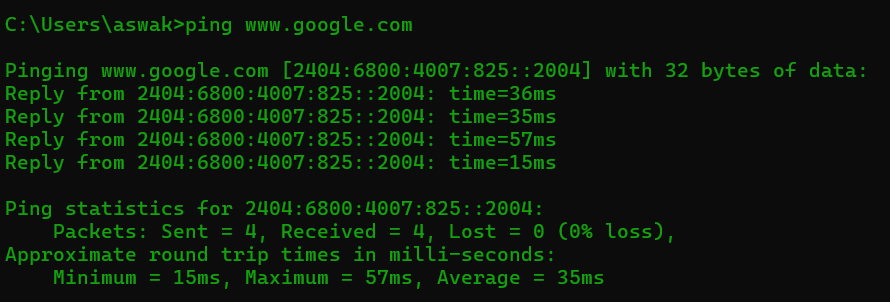
1. Manually assign unique addresses that are outside the range assigned by the DHCP server
2. Reserves IPs for certain devices to ensure they receive the same IPs from the DHCP server

Finally, use the command **ipconfig /all** to configure the static IP address, subnet mask, gateway and DNS server so that no connectivity problems occur.

* Data instead of transmitted as single block gets transferred as multiple smaller units to improve the transferring rate.

Packets are these smaller units of data that is transmitted over a network from a source to a desired destination. Packet loss occurs when a packet fails to reach the destination which results in information loss

The **ping** command is used to check if the desired source and destination are reachable or not, it sends 4 packets of data from source to destination and checks for packet loss, if there is no packet loss then they are reachable



Round Trip Time (RTT) is the time that takes for a signal to travel from the source to the destination and get back to the source.

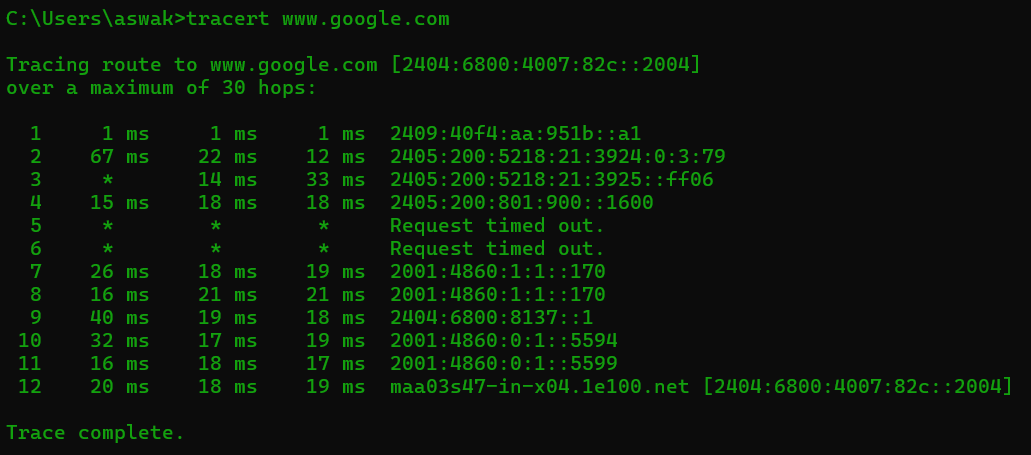
1. **Minimum RTT**: The shortest time taken for a round trip during the measurement period. It represents the best-case scenario under ideal conditions.

2. **Average RTT**: The mean time taken for all round trips during the measurement period. It provides a general sense of network performance over time.

3. **Maximum RTT**: The longest time taken for a round trip during the measurement period. It represents the worst-case scenario, indicating issues.

Running **ping** command in macOS gives the standard deviation of RTT directly as **stddev**, to check the standard deviation in others we can add a **pingstat** plugin or write a dedicated code to check for standard deviation in the terminal using the ‘Test-Connection’ cmdlet to ping a target host multiple times, collecting the RTT data, and then calculating the standard deviation from the collected data.

* To Traceroute to a server we use **tracert** command which tracks the path that packets take from the source to the destination. It records the number of hops along the way and also measures the time taken for each hop



**Hops** refers to the networking devices (usually a **router**) that is dealt by a packet when it goes from source to a destination, **Hop Count** refers to the number of these devices in the path.

**Hop-by-Hop information** refers to the details gathered at each hop along the path that data packets travel from the source to the destination in a network.

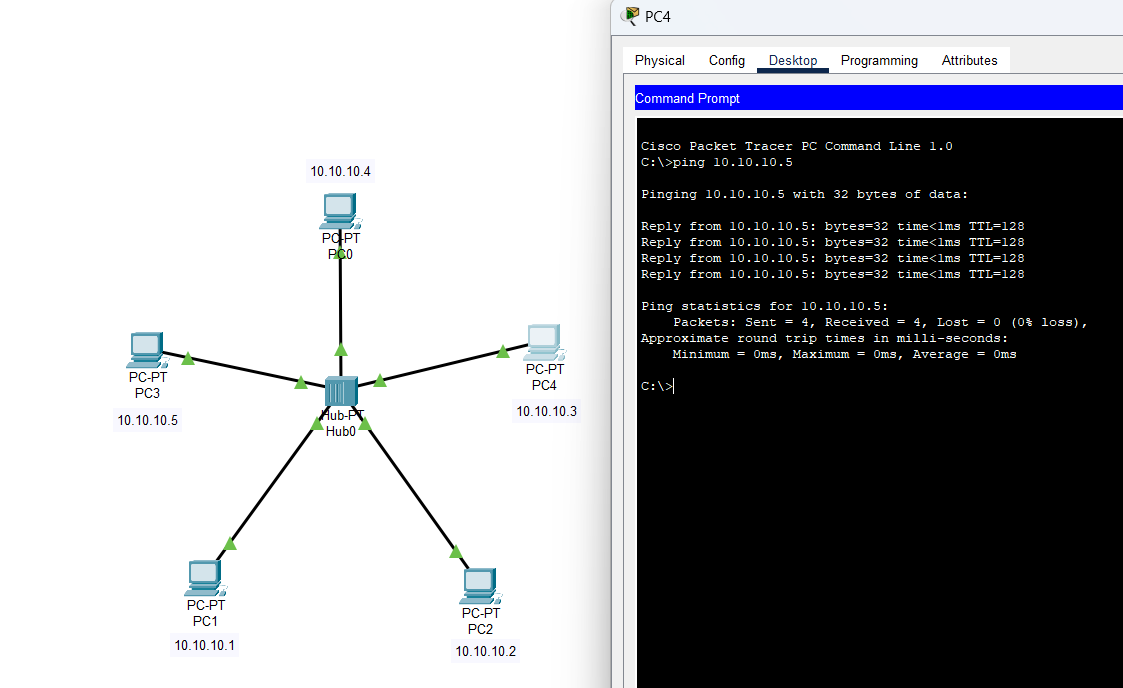
In the above image of tracing route to the Google server, the packets dealt with 12 hops and their hop by hop information is displayed sequentially.

A Hop by Hop information generally contains the Round Trip Time (RTT) and the IP address of the hop, this is generally used to help the network administrators to identify where delays or issues may be occurring along the path.

**2.BASIC NETWORK TOPLOGY MODULE**

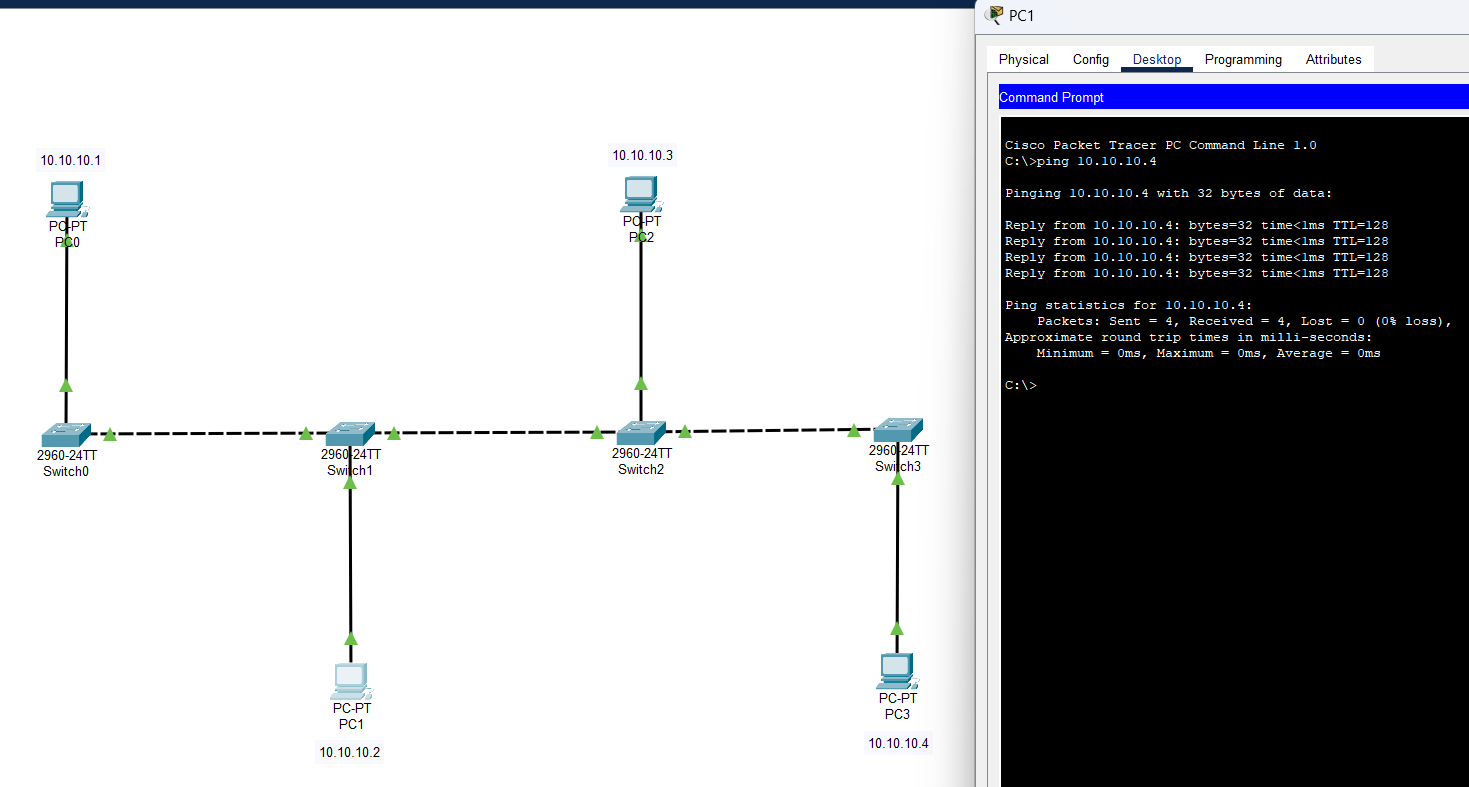
**Star Topology:**

A star topology is implemented by connecting all the individual nodes to a central connection point (usually a hub). A huge advantage of this topology is that if one cable fails only one device will be brought down but it has its own disadvantages as well, one device has to send data to another device by sending it to the hub first and only then it goes to the designated device.



**Bus Topology:**

In a bus topology all the devices are linked together by a single cable named “bus”, data is transmitted through this cable. This cable serves as a shared communication medium allowing all devices in the network to receive the same signal simultaneously. It is very much efficient for small networks. The main disadvantage is if the main cable gets damaged then the whole network fails.



**Ring topology:**

Ring topology is a type of network topology where devices are connected in a circular manner, forming a closed loop. In this setup, each device is connected to exactly two other devices, creating a continuous pathway for data transmission. This means that data travels in only one direction around the ring, passing through each device until it reaches its destination. The disadvantages are to communicate between devices all the devices must be turned on and the data packet has to go through all the nodes.

