GUJARAT TECHNOLOGICAL UNIVERSITY

Government Engineering College, Bhavnagar

Subject: **Computer Network**

B.E. C.E. Semester-5th

(Computer Branch)

Submitted By:

Name: Vankani Arjun BakulBhai
Enrollment: 180210107060

Prof. Chinmay Vyas
(Faculty Guide)

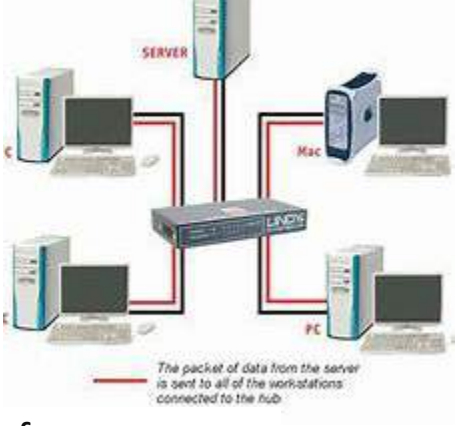
Prof. KARSHAN KANDORIYA
(Head of the Department)

Academic Year (2020-21)

Computer Network

Various Network devices:

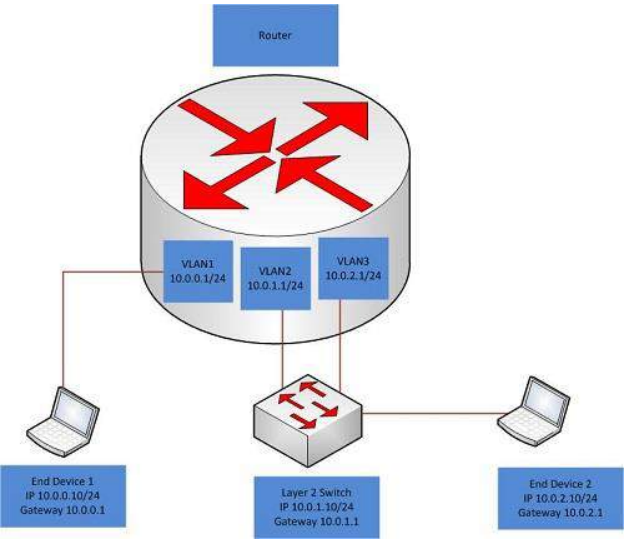
1) **NIC (Network Interface Card)**
    - NIC is hardware component used to connect a computer with another computer onto a network
    - The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).
    - It can support a transfer rate of 10,100 to 1000 Mb/s
    - There are two types of NIC:
        1) Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data
        2) Wireless NIC**:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.



2)HUB

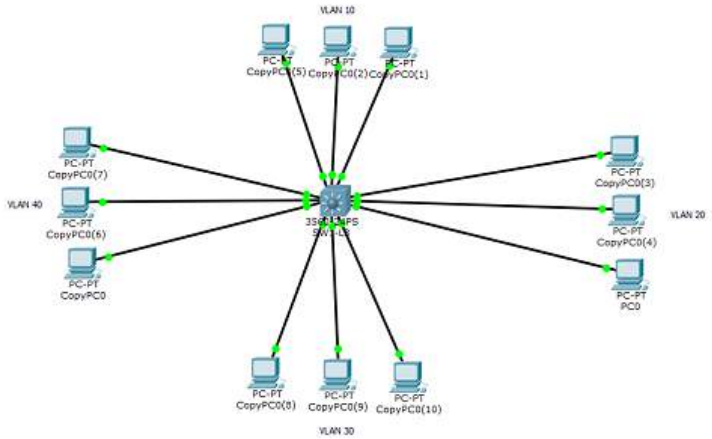
- Hubs are used to create small Home Networks.
- Hubs are used for monitoring the networks.
- Hubs are used in Organizations and Computer Labs for connectivity.
- It Makes one device or peripheral available throughout the whole network
- A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.
- The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

3) Layer 2 and Layer 3 Switches



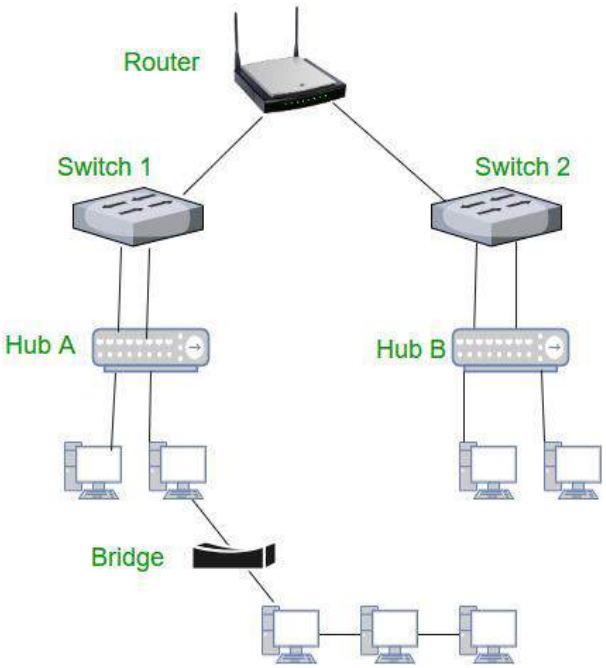
• Layer 2 switches basically do switch only, which means they operate using devices' MAC addresses to redirect the data packets from the source port to the destination port. It does that by maintaining a MAC address table to remember which ports have which MAC addresses assigned. A MAC address operates within the Layer 2 of the OSI reference model. A MAC address simply differentiates one device from another with

each device being assigned a unique MAC address. It utilizes hardware-based switching techniques to manage traffic in a LAN (Local Area Network). As switching occurs at Layer 2, the process is quite faster because all it does is sorting MAC addresses at a physical layer. In simple terms, a Layer 2 switch acts as a bridge between multiple devices.



- A Layer 3 switch is exactly the opposite of what a Layer 2 switch does. Layer 2 switches were not able to route data packets at layer 3. Unlike Layer 2 switches, Layer 3 does routing using IP addresses. It’s a specialized hardware device used in routing data packets. Layer 3 switches have fast switching capabilities and they have higher port density. They are significant upgrades over the traditional routers to provide better performance and the main advantage of using Layer 3 switches is that they can route data packets without making extra network hops, thus making it faster than routers. However, they lack some added functionalities of a router. Layer 3 switches are commonly used in large scale enterprises. Simply put, a Layer 3 switch is nothing but a high-speed router but without WAN connectivity.

4) Bridge



- A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments
- Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the OSI model, bridging is performed in the data link layer (layer 2).
- If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.
- The bridge is a networking device which is used to divide LAN into multiple segments.
- Bridge works under data link layer on OSI model.
- It stores the MAC address of PC available in a network.
- The bridge is used to reduce network traffic.

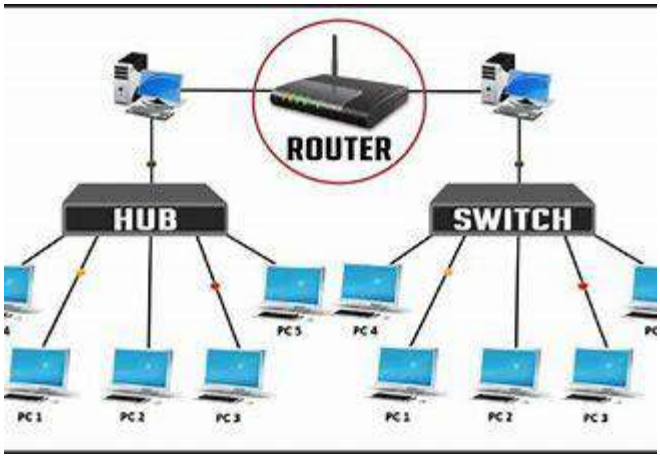
5)Wireless Access Point

- In computer networking, a wireless access point (WAP), or more generally just access point is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. The AP usually connects to a router as a standalone device, but it can also be an integral component of the router itself. An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available.

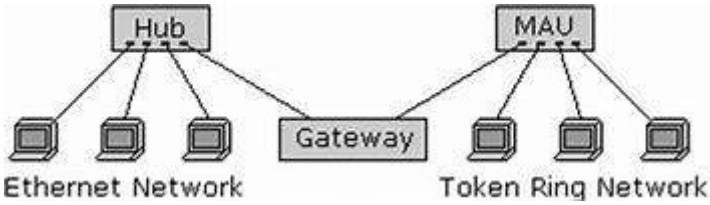
- A wireless access point is a network device that transmits and receives data over a wireless local area network (WLAN)

6)Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a Layer 3 of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.



7)Gateway



- A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect a bunch of networks and can operate at any of the seven layers of the open systems interconnection model.
- The term gateway can also loosely refer to a computer or computer program configured to perform the tasks of a gateway, such as a default gateway or router.

8)Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

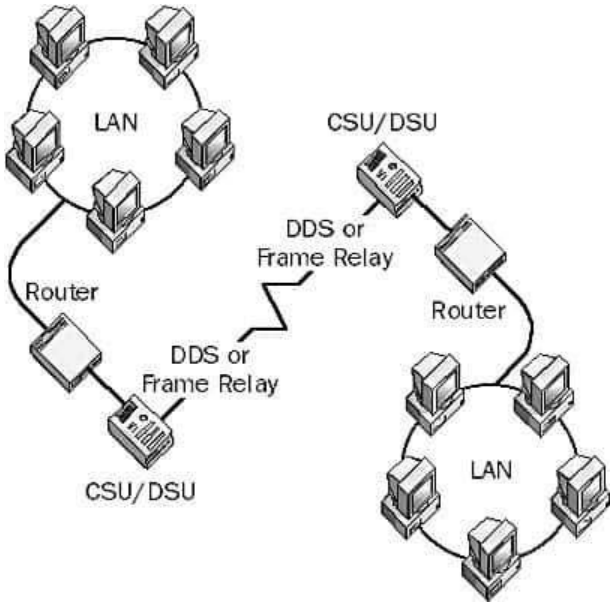
1)Standard PC modem or Dial-up modem

2)Cellular Modem

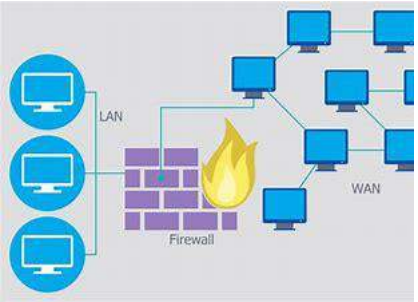
3)Cable Modem

9)CSU/DSU

- CSU/DSUs essentially function as the digital counterpart to analog modems. They are typically external units that look similar to an external modem, but they can also come in sizes that can be mounted in a rack. Unlike analog modems, CSU/DSUs do not perform signal conversion because the signal at both ends is already digital. CSU/DSUs package digital data into a format suitable for the particular digital transmission line they are servicing, and buffer and rate-adapt digital signals going to and from the telephone company network. CSU/DSUs ensure that data frames are properly formed and timed for the telephone company network and provide a protective barrier to electrical disturbances that can harm customer premises equipment.



- Digital lines usually terminate at customer premises with four-wire connections having various connector types, including RJ-45, four-screw terminal blocks, and M-block connectors (used for V.35 interfaces). The four-wire connection is joined to the appropriate connector on the CSU/DSU. The CSU/DSU typically adjusts itself to the line speed of the digital data service (DDS) line using an autosensing feature.

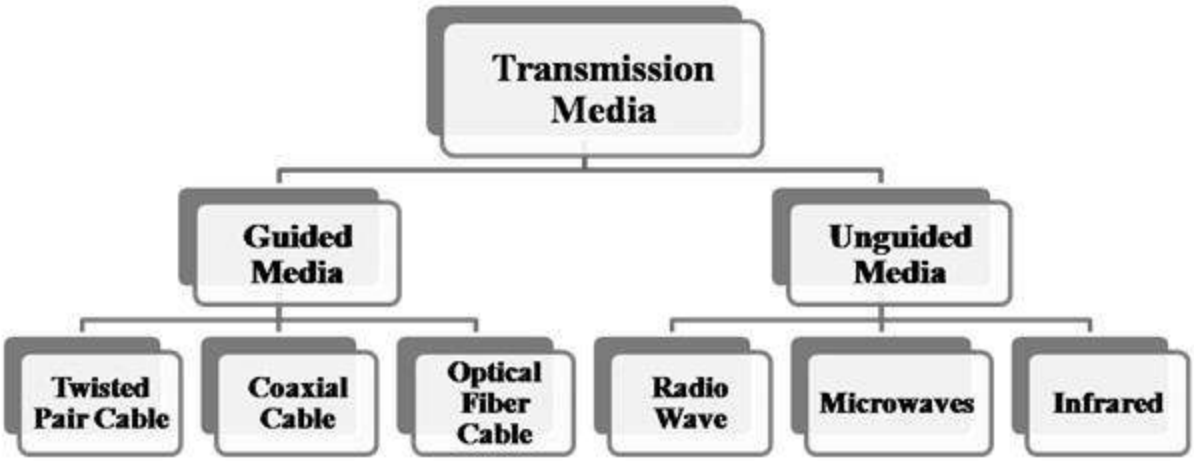


- **10)Firewall**
- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.
- Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
  From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
  Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type *code* instead of port number which identifies purpose of that packet.

Computer Networks LAB Session-2

Q.1) Transmission Media (Wireless and Wired)

- Communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media:(Wired Media)

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective

sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**
   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.
   Advantages:
   - Least expensive
   - Easy to install
   - High speed capacity

   Disadvantages:
   - Susceptible to external interference
   - Lower capacity and performance in comparison to STP
   - Short distance transmission due to attenuation
2. **Shielded Twisted Pair (STP):**
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
   Advantages:
   - Better performance at a higher data rate in comparison to UTP
   - Eliminates crosstalk
   - Comparatively faster

   Disadvantages:
   - Comparatively difficult to install and manufacture
   - More expensive
   - Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode (dedicated cable bandwidth) and Broadband mode (cable bandwidth is split into

separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fiber Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile
- unidirectional, i.e. will need another fiber, if we need bidirectional communication

2. Unguided Media: (Wireless)
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.
Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

(i) Radio waves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.
Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.
(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.
Don’t stop now and take your learning to the next level. Learn all the important concepts of Data Structures and Algorithms with the help of the most trusted course: DSA Self-Paced. Become industry ready at a student-friendly price.

(Q).2-A) What is packet tracer?

- Cisco Packet Tracer (CPT) is a powerful network simulator program developed by Cisco. With the simulator program by building complex network and improve your network knowledge. Cisco router switch server PC laptop is a free program that provides support for many more devices. And it is also very simple and easy to use. it is more conventional and faster than GNS3 because it does not force your computer over. Before developing a real network topology you can make a design in a packet tracer and create a more professional design.

Workspace:

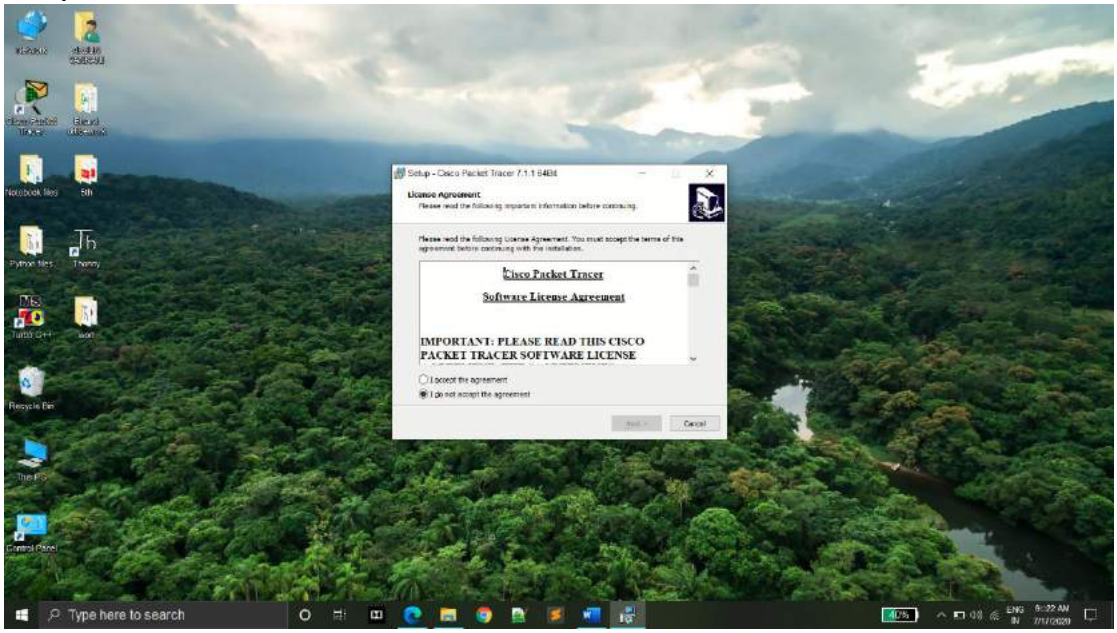
1. **Logical –**
   Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
2. **Physical –**
   Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

Key Features:

- Unlimited devices
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support
- Cross platform compatibility

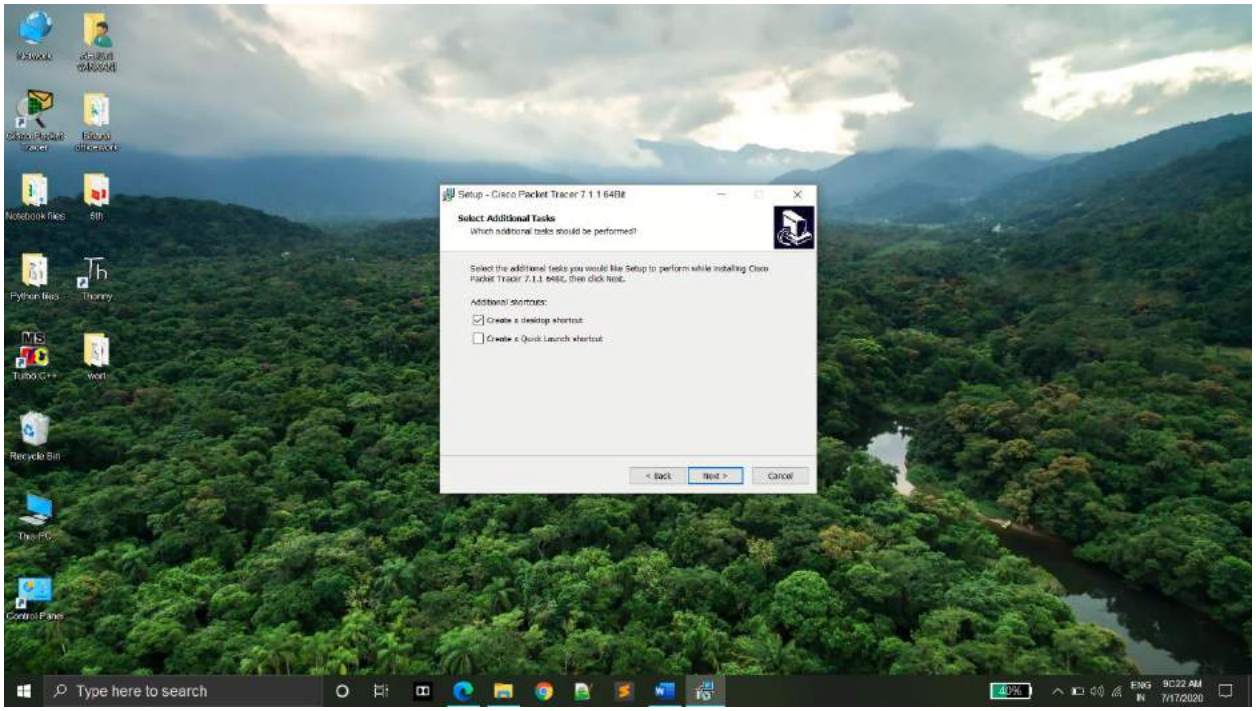
Q.(2-B) Installation Process with screenshot.

- Frist, we have to download Packet Tracer from Cisco site and enroll the course of understanding about packet tracer.
- Step-1



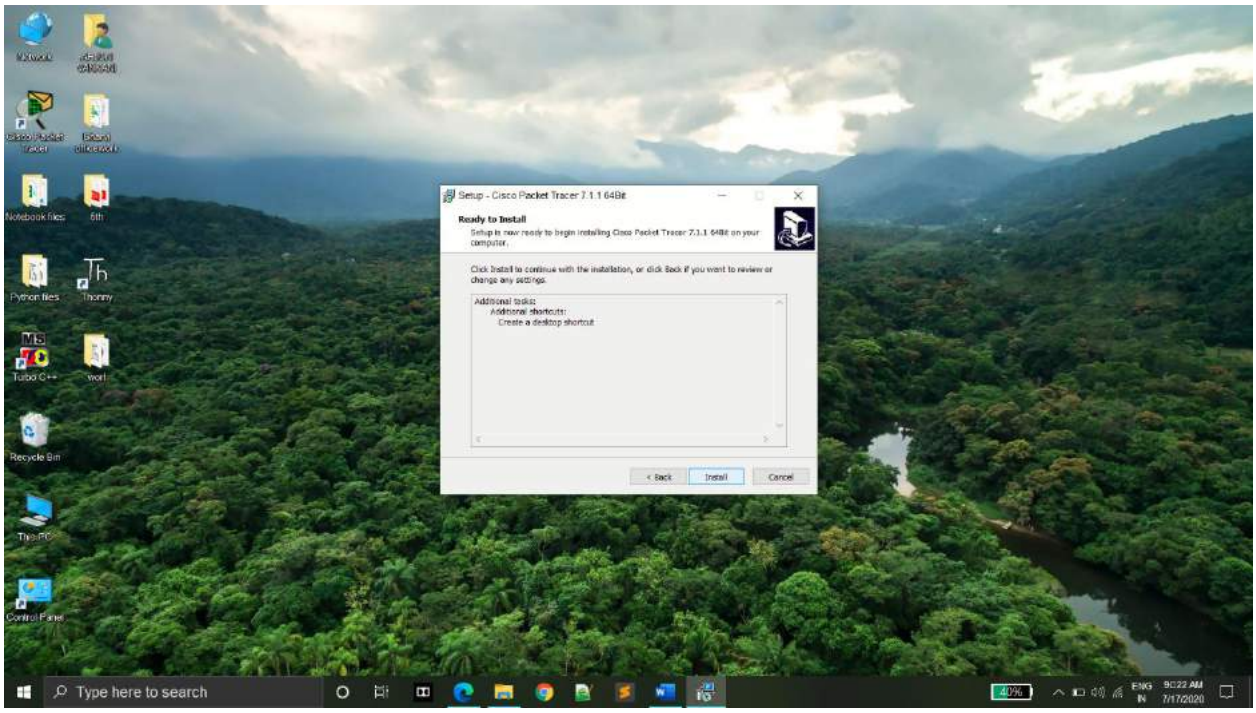
- Step-2

After install setup into our pc, And agree the condition



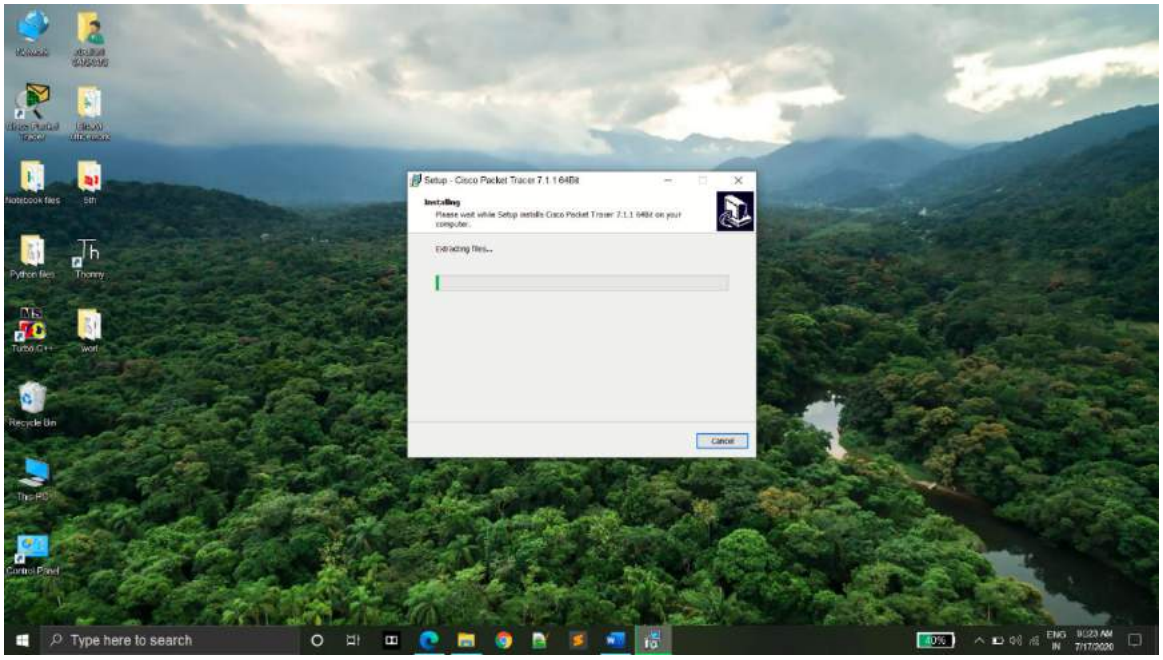
- Step-3

  if we want to create shortcut then select it and launch as quick shortcut.



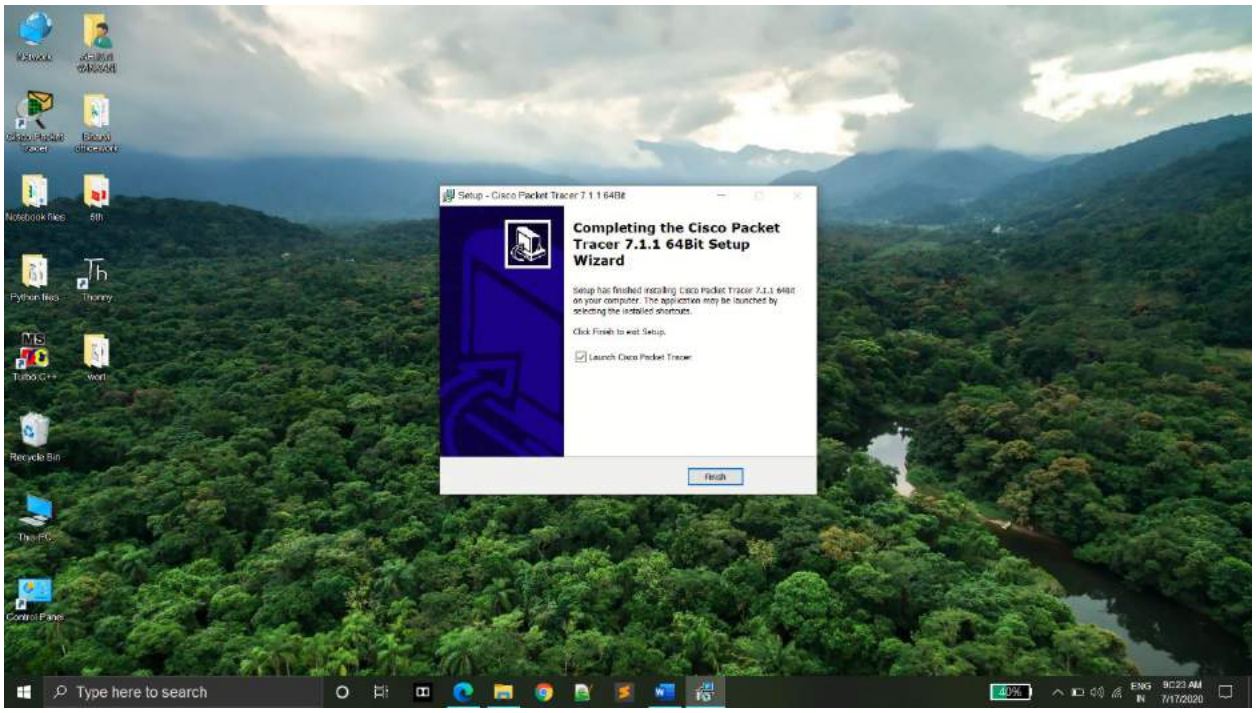
Step-4

- Push the install button to install that software



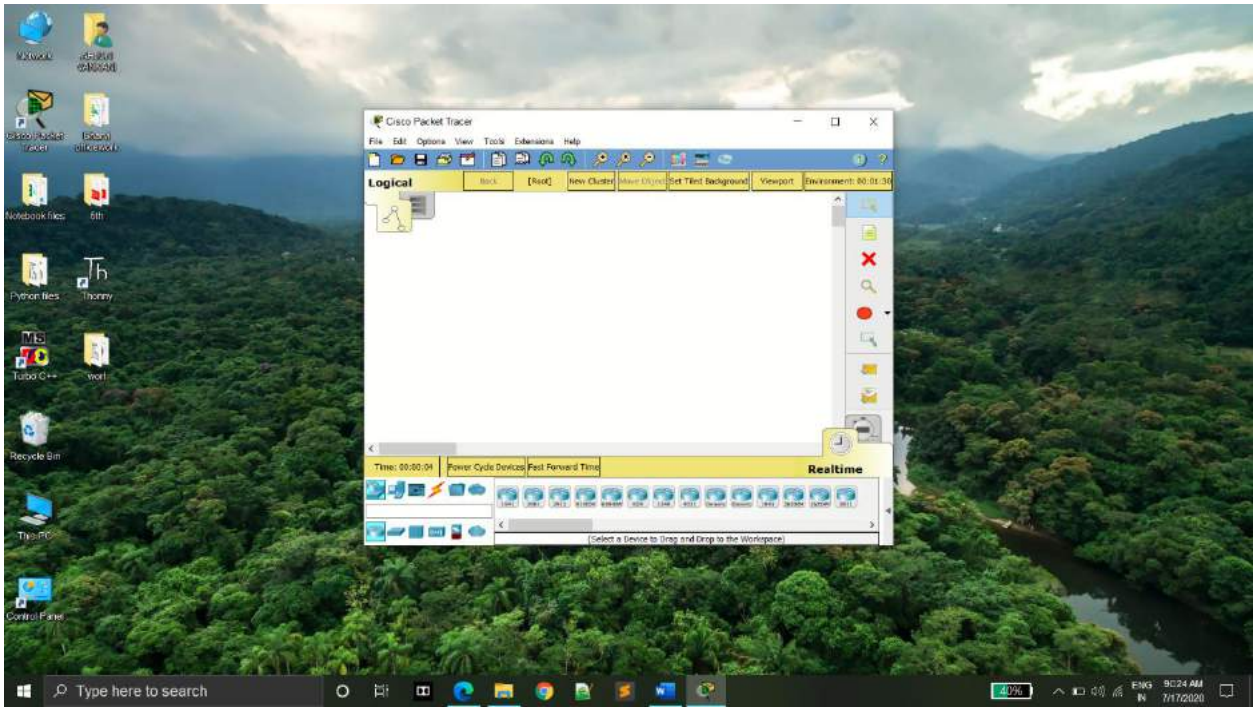
Step-5

- It works on extracting and installing setup.



Step-6

- This is shown Software was finish



- This is Main window of Packet tracer, now get started with work!!

(Q)(2-c) Explain uses and application of packet tracer?

- In this packet tracer we can make network model virtually like adding Pc& Laptop.
- We can assign IP address to computers, in which static or dynamic Ip and use VPN connection also run command in CMD or terminal windows
- Add switching network and set physical host
- Used cable network devices
- We can test ping between computers & add wireless router
- We create our special workspace and adding comment, notes

(Q)(2-d) List out Important modules /component of packet tracer.

- **1)Router devices emulated in Cisco Packet Tracer**

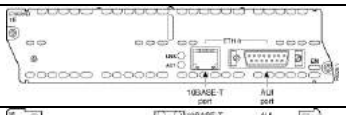
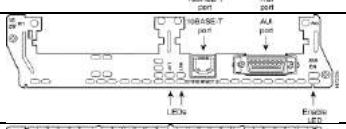
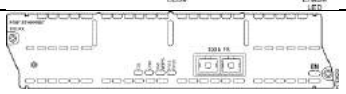
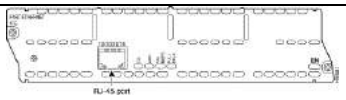
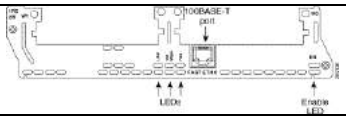
- Cisco 1841 ISR router
- Cisco 2620XM ISR router
- Cisco 2621XM ISR router
- Cisco 2811 ISR router
- Cisco 1941 ISR router
- Cisco 2901 ISR router
- Cisco 2911 ISR router
- Cisco 819 ISR router
- Cisco 829 ISR router
- Cisco CGR 1240 rugged router
- Cisco 4321 ISR router (added in Cisco Packet Tracer 7.1)

2)WIC modules

Module	*Photo*
WIC-1AM	

WIC-1ENET	
WIC-1T	
WIC-2AM	
WIC-2T	
HWIC-4ESW	
HWIC-8A	
WIC-Cover	

3)Network modules (NM)

Module	*Photo*
NM-1E	
NM-1E2W	
NM-1FE-FX	
NM-1FE-TX	
NM-1FE2W	
NM-2E2W	
NM-2FE2W	
NM-2W	
NM-4A/S	
NM-4E	
NM-8A/S	
NM-8AM	
NM-Cover	

Computer Network (LAB Session – 10)

- **Study of basic network command and Network configuration commands.**

1.Below is the list of some important network configuration command in Linux. Find the usage of the commands and also explore what is the equivalent command in windows for performing the similar task.

Explain the usage of the commands and observe the result of the command (Either windows or Linux)

A) Ping
B) Nslookup
C) Traceroute
D) Host
E) Netstat
F) Arp
G) Ifconfig /Ipconfig

- Here by, All the command is very useful for and needed to gathering information given below listed:

1) Ping = > (Send Test Packets)

It mostly used for Sending test packet in which our pc sends to 4 packets to server or website or another pc(target).

Ping URL or IPADDRESS to see if you reach an internet destination. If successfully reach then receive 4 packets other wise get lost 4 packets.

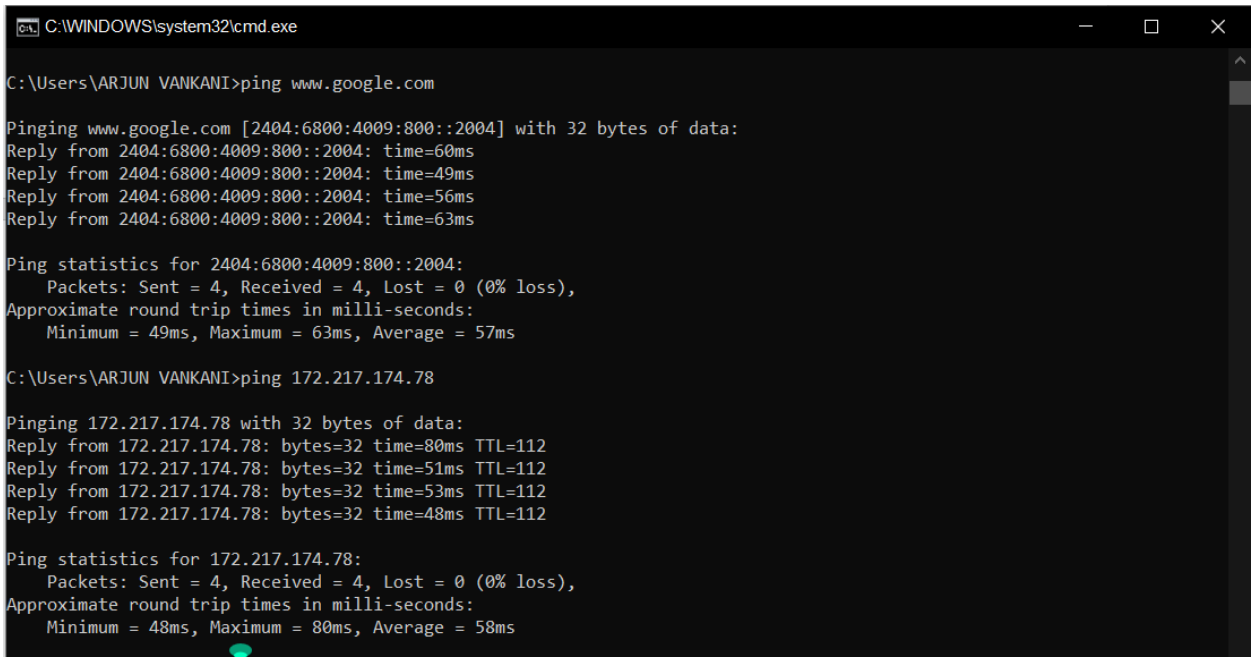


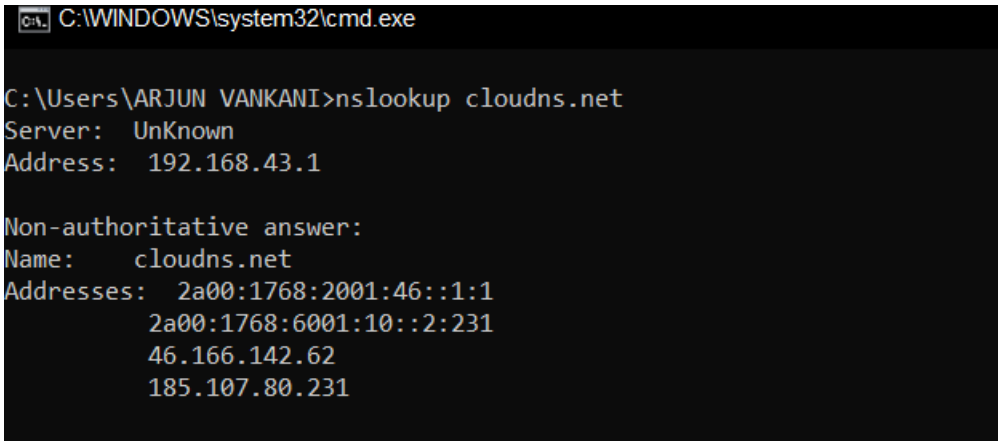
Figure (01)

In Figure (01), we sent the destination URL like google.com and see the result of Received: 4 packets in given time Otherwise its result is request timeout. And below Ping 172.217.174.78 is Ip address to send request.

2)Nslookup: (Network Administration Command-line Tool)

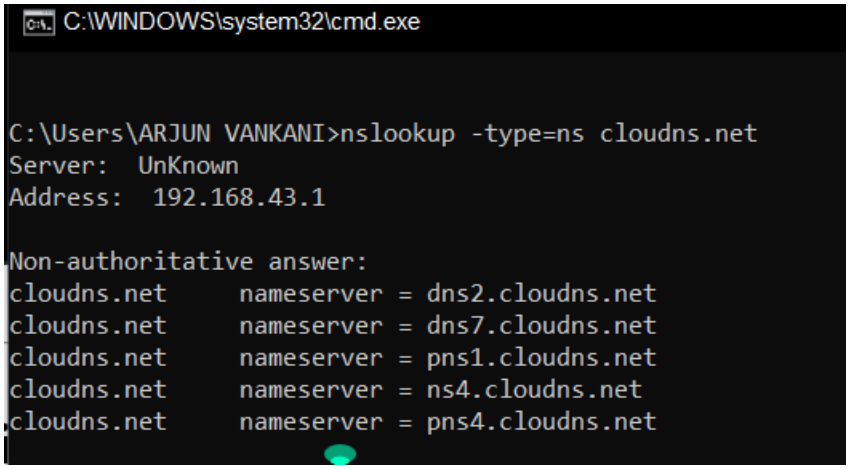
It's used for querying the Domain Name System to obtain name or Ip address mapping information. Main use of Nslookup is for troubleshooting DNS related problem. It can be use in interactive and non-interactive mode.

- To find a record of domain (How many records?)



```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    cloudns.net
Addresses:  2a00:1768:2001:46::1:1
          2a00:1768:6001:10::2:231
          46.166.142.62
          185.107.80.231
```

- To check NS record of domain (Name server for DNS Zone)



```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -type=ns cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
cloudns.net     nameserver = dns2.cloudns.net
cloudns.net     nameserver = dns7.cloudns.net
cloudns.net     nameserver = pns1.cloudns.net
cloudns.net     nameserver = ns4.cloudns.net
cloudns.net     nameserver = pns4.cloudns.net
```

- To query the SOA record (Start of Authority Record)

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -type=soa cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
cloudns.net
        primary name server = pns1.cloudns.net
        responsible mail addr = support.cloudns.net
        serial  = 2020090501
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 60 (1 min)
```

- To find the MX record responsible (Mail exchanger)

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -type=mx cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
cloudns.net     MX preference = 10, mail exchanger = ALT4.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 10, mail exchanger = ALT3.ASPMX.L.GOOGLE.COM
```

- To find all available DNS record

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -type=any cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
cloudns.net     internet address = 185.107.80.231
cloudns.net     internet address = 46.166.142.62
cloudns.net     AAAA IPv6 address = 2a00:1768:2001:46::1:1
cloudns.net     AAAA IPv6 address = 2a00:1768:6001:10::2:231
cloudns.net     MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 10, mail exchanger = ALT3.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 10, mail exchanger = ALT4.ASPMX.L.GOOGLE.COM
cloudns.net     MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
cloudns.net     nameserver = ns4.cloudns.net
cloudns.net     nameserver = pns4.cloudns.net
cloudns.net     nameserver = dns2.cloudns.net
cloudns.net     nameserver = dns7.cloudns.net
cloudns.net     nameserver = pns1.cloudns.net
```

- To check the specific DNS server

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup cloudns.net ns1.cloudns.net
(root)
        primary name server = undefined.cloudns.net
        responsible mail addr = support.cloudns.net
        serial  = 2020041401
        refresh = 7200 (2 hours)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 0 (0 secs)
Server:  UnKnown
Address:  2a00:1768:1001:9::1

Name:    cloudns.net
Addresses:  2a00:1768:2001:46::1:1
          2a00:1768:6001:10::2:231
          185.107.80.231
          46.166.142.62
```

- To check reverse DNS lookup

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Users\ARJUN VANKANI>nslookup 34.218.62.116
Server:  UnKnown
Address:  192.168.43.1

Name:    ec2-34-218-62-116.us-west-2.compute.amazonaws.com
Address:  34.218.62.116


C:\Users\ARJUN VANKANI>nslookup 185.136.96.96
Server:  UnKnown
Address:  192.168.43.1

Name:    pns21.cloudns.net
Address:  185.136.96.96


C:\Users\ARJUN VANKANI>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> geeksforgeeks.org
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    geeksforgeeks.org
Address:  34.218.62.116
```

- To change the port number for the Connection

```
C:\WINDOWS\system32\cmd.exe
C:\Users\ARJUN VANKANI>nslookup -port=56 cloudns.net
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    cloudns.net
Addresses:  2a00:1768:2001:46::1:1
          2a00:1768:6001:10::2:231
          46.166.142.62
          185.107.80.231
```

- To change the timeout interval for reply

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -timeout=10 google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:815::200e
          216.58.199.174
```

- To enable debug mode

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>nslookup -debug cloudns.net
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NXDOMAIN
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 0,  additional = 0

    QUESTIONS:
        1.43.168.192.in-addr.arpa, type = PTR, class = IN

------------
Server:  UnKnown
Address:  192.168.43.1

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 0,  additional = 0

    QUESTIONS:
        cloudns.net, type = A, class = IN
    ANSWERS:
    ->  cloudns.net
        internet address = 185.107.80.231
        ttl = 1800 (30 mins)
    ->  cloudns.net
        internet address = 46.166.142.62
        ttl = 1800 (30 mins)

------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 0,  additional = 0

    QUESTIONS:
        cloudns.net, type = AAAA, class = IN
    ANSWERS:
    ->  cloudns.net
        AAAA IPv6 address = 2a00:1768:6001:10::2:231
        ttl = 1800 (30 mins)
    ->  cloudns.net
        AAAA IPv6 address = 2a00:1768:2001:46::1:1
```

3)Traceroute (TRACERT)

- Traceroute and Tracert are computer network diagnostic commands for displaying possible(paths) and measuring transit delays of packets across an (IP) network.
- This command is a fascinating windows command to use, and curious to see the path of our internet traffic takes to get from our browser to remote system.

  This provide Three information

  1) Number of hops before getting to the destination

  2) Time it takes to get to each hop

  3) The IP and sometimes the name of hop

  ➔ (*) represent Time out -> that's why change path.

```
C:\WINDOWS\system32\cmd.exe

C:\Users\ARJUN VANKANI>tracert google.com

Tracing route to google.com [2404:6800:4009:805::200e]
over a maximum of 30 hops:

  1   532 ms     2 ms     2 ms  2405:204:8002:c9ff::14
  2     *        *        *     Request timed out.
  3    36 ms    35 ms    38 ms  2405:200:320:b::3
  4    40 ms    32 ms    52 ms  2405:200:801:b00::a9a
  5    34 ms    26 ms    27 ms  2405:200:801:b00::ab2
  6    57 ms    46 ms    48 ms  2405:200:801:200::31b
  7    75 ms    37 ms    46 ms  2405:200:802:760::1
  8    76 ms    46 ms    36 ms  2405:200:802:760::8
  9     *        *        *     Request timed out.
 10    74 ms    48 ms    56 ms  2001:4860:1:1::aac
 11     *        *        *     Request timed out.
 12    63 ms    42 ms    38 ms  2001:4860:0:1::1314
 13    97 ms    51 ms    45 ms  2001:4860:0:1::22c7
 14    71 ms    53 ms    75 ms  bom05s09-in-x0e.1e100.net [2404:6800:4009:805::200e]

Trace complete.
```

4) Host

It is used for DNS lookup operation in Linux, It finds particular domain name or IP address etc..

```
admin1@arjun: ~
File  Edit  View  Search  Terminal  Help
admin1@arjun:~$ host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] hostname [server]
       -a is equivalent to -v -t ANY
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -i IP6.INT reverse lookups
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
admin1@arjun:~$ host google.com
google.com has address 172.217.174.78
google.com has IPv6 address 2404:6800:4009:815::200e
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
admin1@arjun:~$
```

- -v used for verbose output

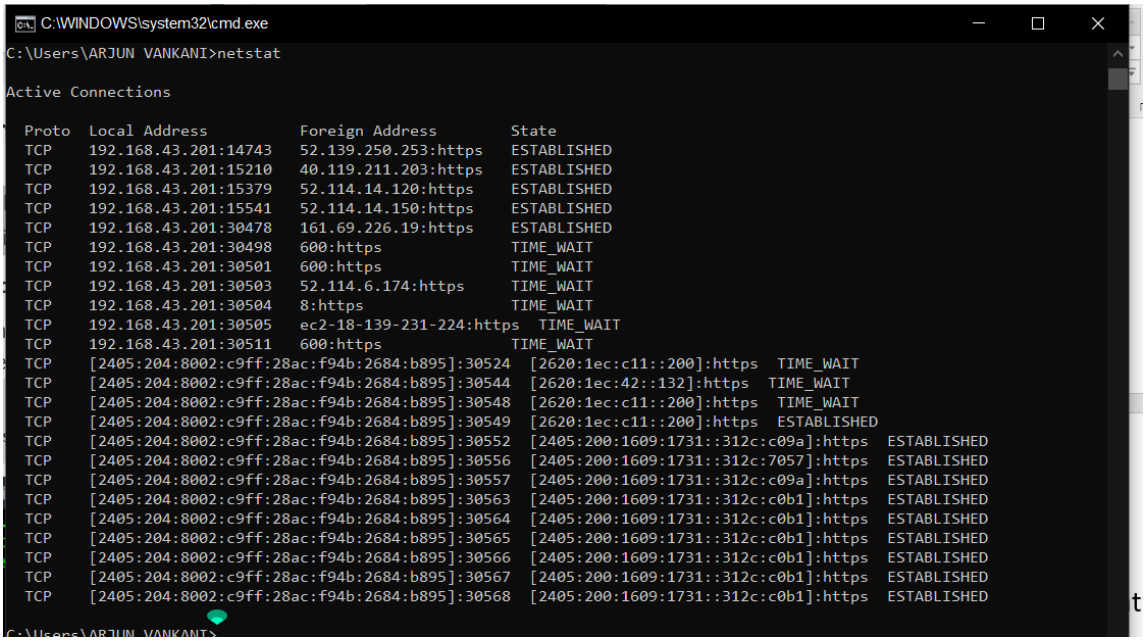
```
admin1@arjun: ~
File  Edit  View  Search  Terminal  Help
google.com mail is handled by 30 alt2.aspmx.l.google.com.
admin1@arjun:~$ host -v google.com
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8359
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             222     IN      A       172.217.174.78

Received 44 bytes from 127.0.0.53#53 in 70 ms
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4970
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      AAAA

;; ANSWER SECTION:
google.com.             120     IN      AAAA    2404:6800:4009:815::200e

Received 56 bytes from 127.0.0.53#53 in 0 ms
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15948
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             140     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             140     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             140     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             140     IN      MX      10 aspmx.l.google.com.
google.com.             140     IN      MX      30 alt2.aspmx.l.google.com.

Received 136 bytes from 127.0.0.53#53 in 0 ms
admin1@arjun:~$
```

```
admin1@arjun: ~
File  Edit  View  Search  Terminal  Help

admin1@arjun:~$ host -t ns  google.com
google.com name server ns4.google.com.
google.com name server ns2.google.com.
google.com name server ns3.google.com.
google.com name server ns1.google.com.
admin1@arjun:~$ host -t soa  google.com
google.com has SOA record ns1.google.com. dns-admin.google.com. 330353109 900 90
0 1800 60
admin1@arjun:~$ host -t txt  google.com
google.com descriptive text "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com descriptive text "facebook-domain-verification=22rm551cu4k0ab0bxsw536
tlds4h95"
google.com descriptive text "v=spf1 include:_spf.google.com ~all"
google.com descriptive text "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr
6c1l2BPvqKX8="
google.com descriptive text "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
admin1@arjun:~$ host -C txt  google.com
^Z
[1]+  Stopped                 host -C txt google.com
admin1@arjun:~$ host -C   google.com
Nameserver 216.239.32.10:
        google.com has SOA record ns1.google.com. dns-admin.google.com. 33035310
9 900 900 1800 60
Nameserver 216.239.34.10:
        google.com has SOA record ns1.google.com. dns-admin.google.com. 33035310
9 900 900 1800 60
Nameserver 216.239.36.10:
        google.com has SOA record ns1.google.com. dns-admin.google.com. 33035310
9 900 900 1800 60
Nameserver 216.239.38.10:
        google.com has SOA record ns1.google.com. dns-admin.google.com. 33035310
9 900 900 1800 60
admin1@arjun:~$ host -R 3   google.com
google.com has address 172.217.174.78
google.com has IPv6 address 2404:6800:4009:807::200e
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
admin1@arjun:~$ host -l  google.com
;; communications error to 127.0.0.53#53: end of file
;; communications error to 127.0.0.53#53: end of file
admin1@arjun:~$
```

- -t is used for specific type of query
- -t SOA is for record
- -t txt used for print txt record
- -c used for, in order to compare the SOA records on authoritative nameservers
- -r used for retries entry and try fails
- -l for list all hosts in domain

5)Netstat (Network Statistics)

- Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.



```
C:\WINDOWS\system32\cmd.exe
C:\Users\ARJUN VANKANI>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.43.201:14743   52.139.250.253:https   ESTABLISHED
  TCP    192.168.43.201:15210   40.119.211.203:https   ESTABLISHED
  TCP    192.168.43.201:15379   52.114.14.120:https    ESTABLISHED
  TCP    192.168.43.201:15541   52.114.14.150:https    ESTABLISHED
  TCP    192.168.43.201:30478   161.69.226.19:https    ESTABLISHED
  TCP    192.168.43.201:30498   600:https              TIME_WAIT
  TCP    192.168.43.201:30501   600:https              TIME_WAIT
  TCP    192.168.43.201:30503   52.114.6.174:https     TIME_WAIT
  TCP    192.168.43.201:30504   8:https                TIME_WAIT
  TCP    192.168.43.201:30505   ec2-18-139-231-224:https  TIME_WAIT
  TCP    192.168.43.201:30511   600:https              TIME_WAIT
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30524  [2620:1ec:c11::200]:https  TIME_WAIT
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30544  [2620:1ec:42::132]:https  TIME_WAIT
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30548  [2620:1ec:c11::200]:https  TIME_WAIT
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30549  [2620:1ec:c11::200]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30552  [2405:200:1609:1731::312c:c09a]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30556  [2405:200:1609:1731::312c:7057]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30557  [2405:200:1609:1731::312c:c09a]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30563  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30564  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30565  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30566  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30567  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
  TCP    [2405:204:8002:c9ff:28ac:f94b:2684:b895]:30568  [2405:200:1609:1731::312c:c0b1]:https  ESTABLISHED
```

- -a for list out all connection-> to show listening and non-listening socket
- -at for list out TCP port
- -au for list out UDP port
- -l list only listening port
- -lt for TCP listening and -lu for UDP listening

6)Arp (Address Resolution Protocol)

- Using the ARP command allows you to display and modify the Address Resolution Protocol (ARP) cache.
- An ARP cache is a simple mapping of IP addresses to MAC addresses. Each time a computer's TCP-Ip stack uses ARP to determine MAC address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster.

```
C:\WINDOWS\system32\cmd.exe
ARP: bad argument: google.com

C:\Users\ARJUN VANKANI>arp -a

Interface: 192.168.56.1 --- 0x2
  Internet Address      Physical Address      Type
  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: 169.254.183.78 --- 0x4
  Internet Address      Physical Address      Type
  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: 192.168.43.201 --- 0x28
  Internet Address      Physical Address      Type
  192.168.43.1          ce-36-57-57-30-cd     dynamic
  192.168.43.255        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
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

7) Ifconfig / Ipconfig

- Ipconfig in windows system used for gathering information about all IPv4 / IPv6 address and all connection given below.

```
C:\WINDOWS\system32\cmd.exe
*** UnKnown can't find c: Non-existent domain

C:\Users\ARJUN VANKANI>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ac3a:3361:63fc:b74e%4
   Autoconfiguration IPv4 Address. . : 169.254.183.78
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::59b8:df85:9602:fdd6%2
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:204:8002:c9ff:f125:edc1:70ac:a608
   Temporary IPv6 Address. . . . . . : 2405:204:8002:c9ff:28ac:f94b:2684:b895
   Link-local IPv6 Address . . . . . : fe80::f125:edc1:70ac:a608%40
   IPv4 Address. . . . . . . . . . . : 192.168.43.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::cc36:57ff:fe57:30cd%40
                                       192.168.43.1
```

Another indispensable and frequently used utility that is used for finding network information about your local machine-like IP addresses, DNS addresses etc.

1)Ipconfig/all -> display all network setup

2)Ipconfig/release -> release IP address

3)Ipconfig/renew -> renew ip address

4)Ipconfig/? -> shows help

5)Ipconfig/flushdns -> flush the dns cache

- **Assoc is used for Fix file associations**
- **Powercfg -> POWER configuration**
- **Systeminfo -> gives system information**
- **Tasklist -> all list out task running on our pc**
- **Taskkill -> kill or stop process.**
- **Cipher -> It used without any switches to quickly ascertain which files and folders in a given directory are encrypted.**

Computer Network(Lab session - 3)

1.Create a network topology in the packet tracer as shown below.

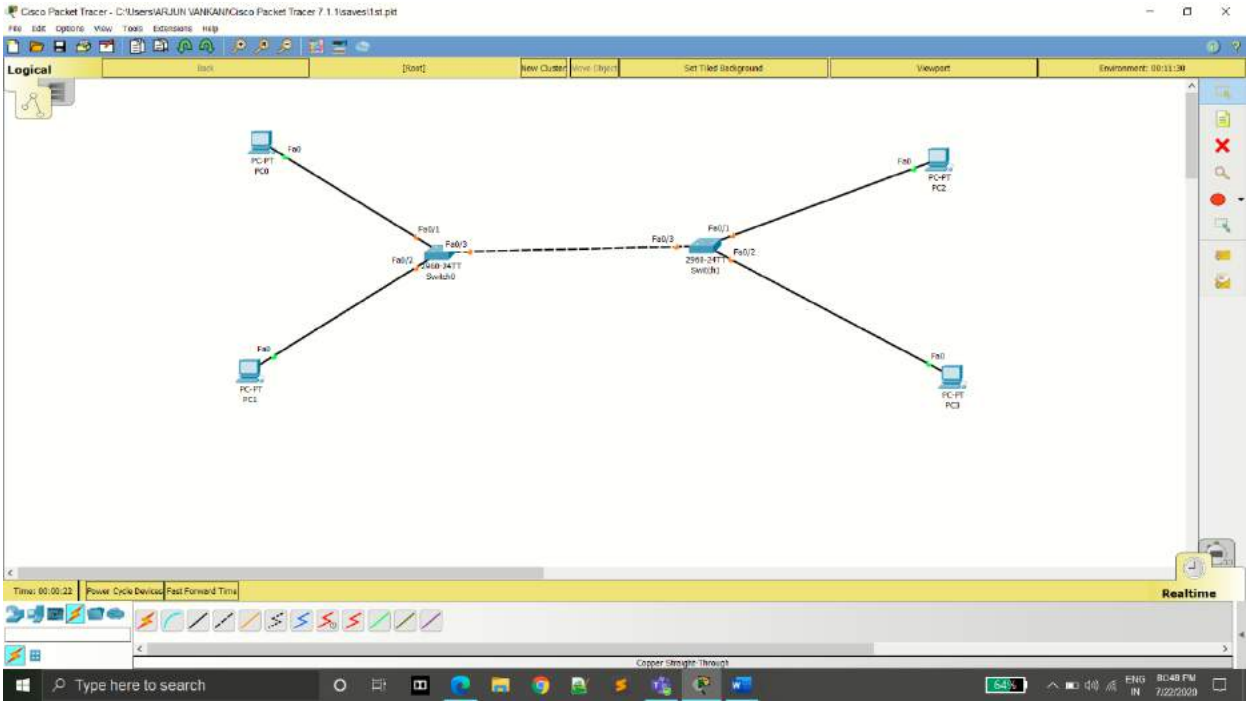
a). Configure all the PC devices by providing static IP addresses to them.

b). Verify the IP address in the command prompt using ipconfig /all command.

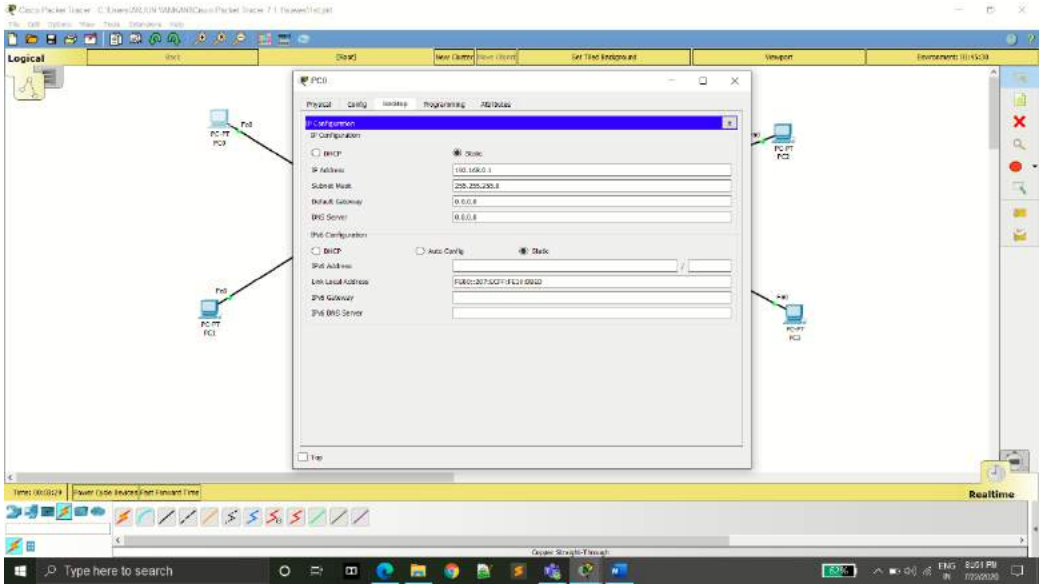
c). Ping any random PC from each PC and check the response.

d). Document the steps and command results

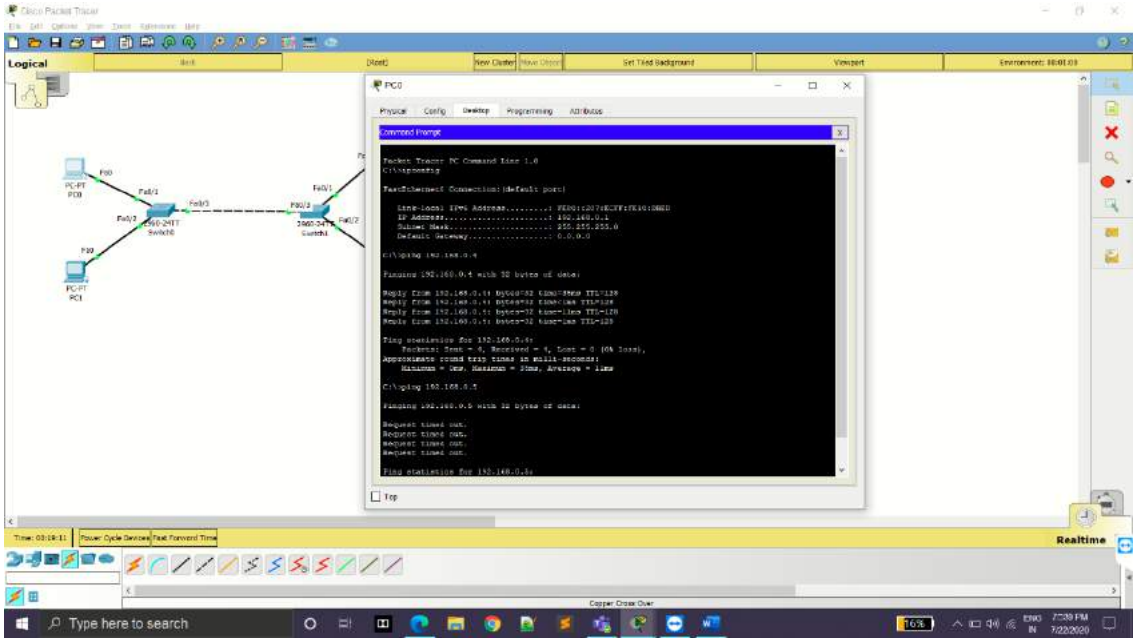
- create network topology with connect two pc with switch – 1, and another two pc with switch – 2.



- After add Ip address in every pc in static Ip



- Now check ping with pc – 1 with pc – 4 , and with random pc – 5 still it's output given below
  - Ping 192.168.0.4 share 4 packet received



  - And check if we check for 192.168.0.5 then can't receive packet.

Q -2) Create a network topology in the packet tracer as shown below.

a) Configure the router's DHCP server setting to accept maximum 5 users and give starting IP address as 192.168.1.120

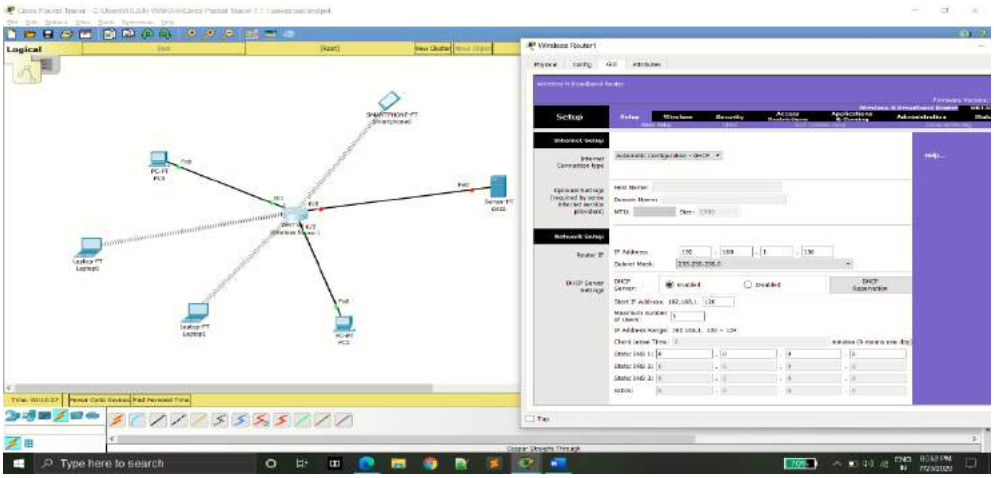
b) Configure all client-side end devices to connect to the router and receive the IP address by selecting DHCP in the IP configuration setting.

c) Configure the server by providing a static IP address 192.168.1.150.

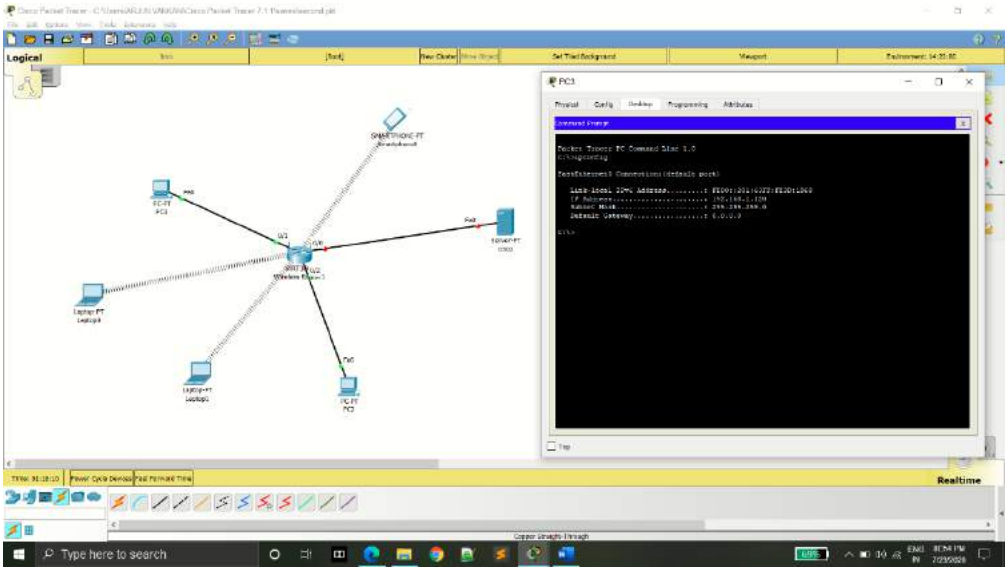
d) From all client-side devices, record the response for ipconfig /all command and ping any random device in the network and record the response

e) Open the browser from any client-side device and access the server by giving the IP address in the URL. Capture the response

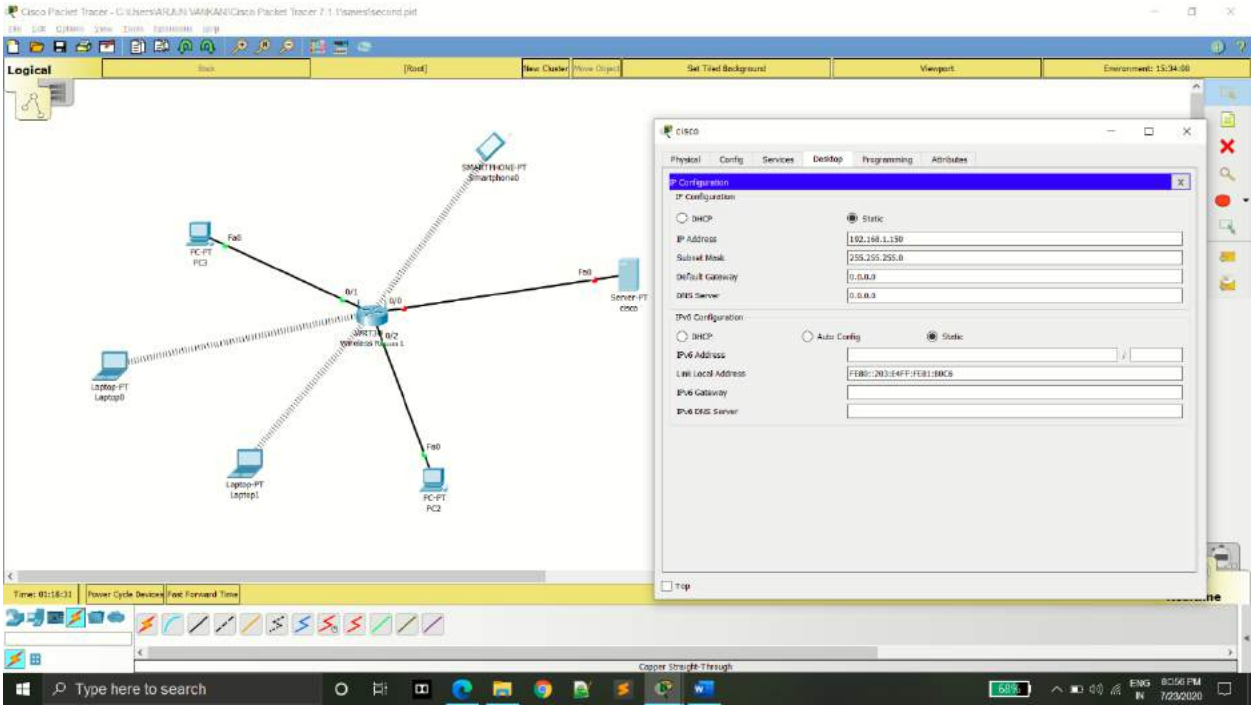
- Here, firstly we connect two pc with wired connection and two laptop in wireless connection with one smart phone all this devices connected in DHCP server with Router at starting ip as 192.168.1.120-124



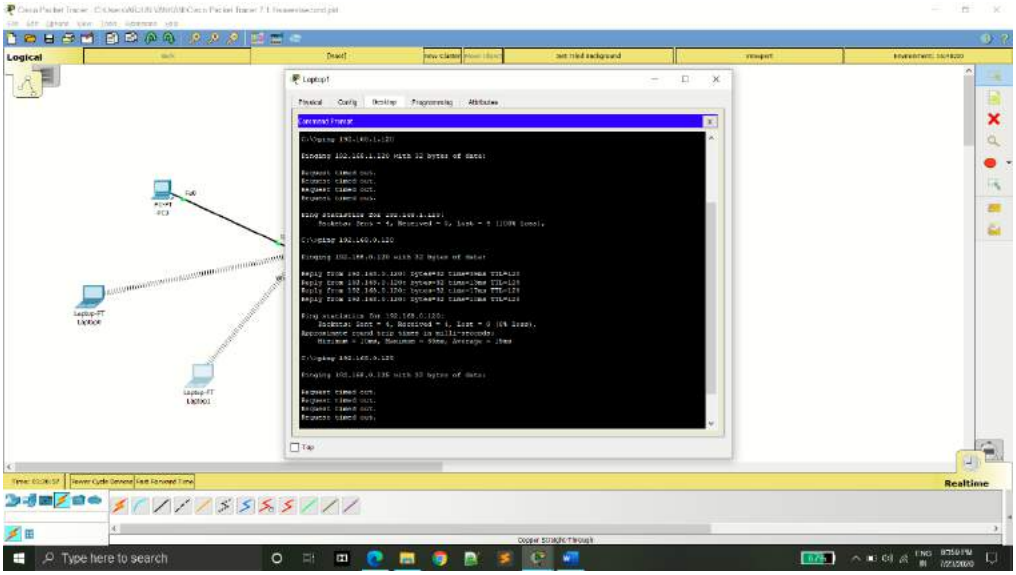
- After we config ip in every connected device.



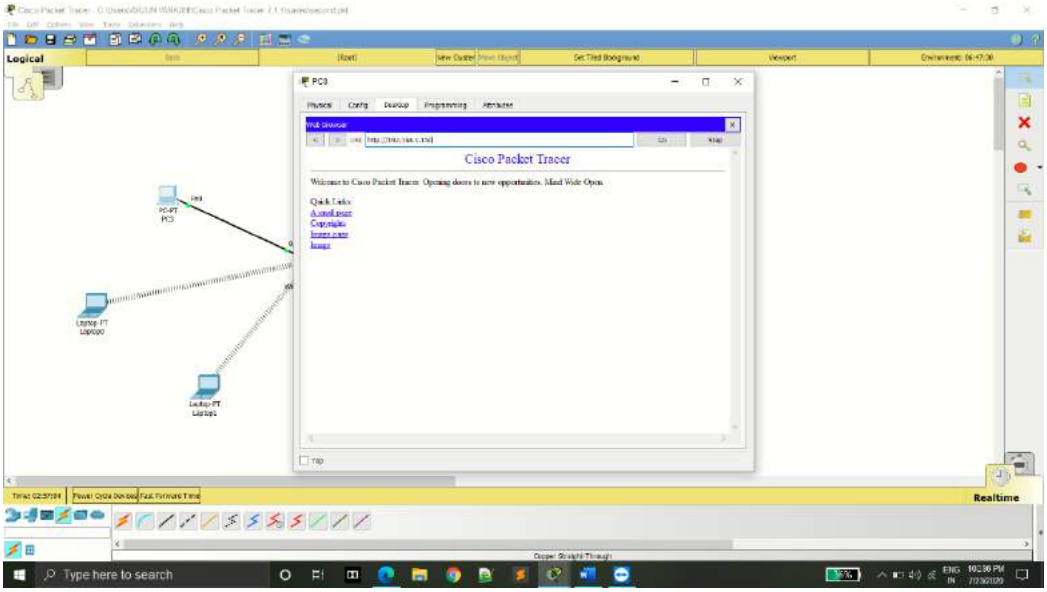
- Now third step we set ip as 192.168.1.150 in server side



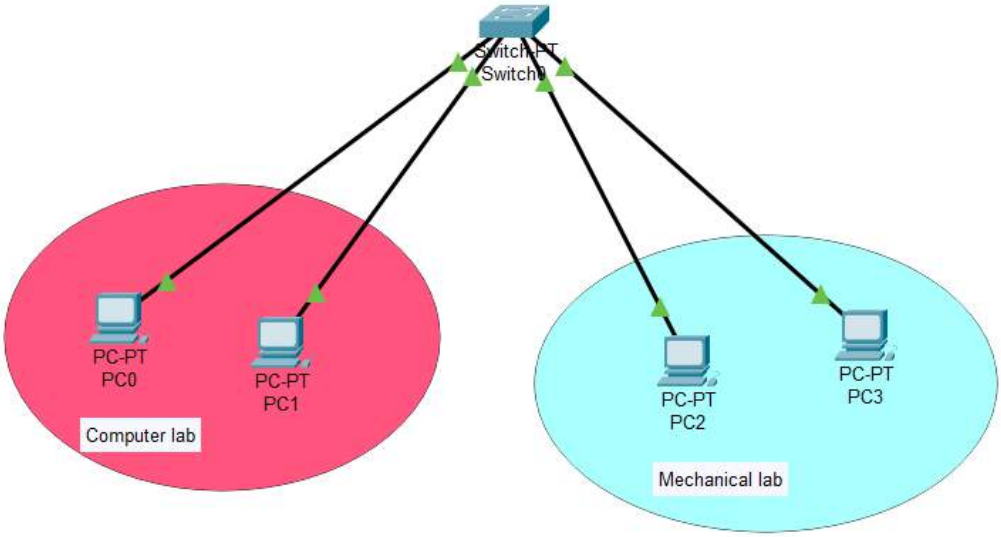
- Now check ping with random device to connected with router is or isn't



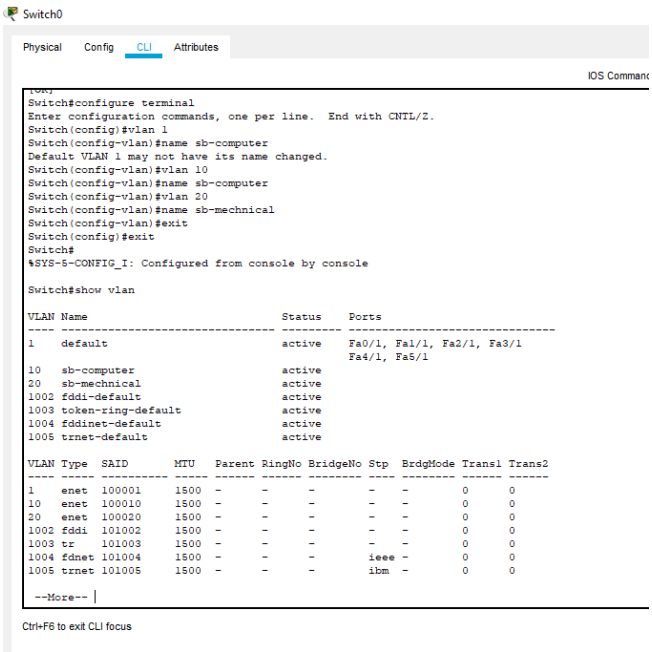
- Now set server set in ip and gateway after set cisco.com and check for pc in this side to show site from server



Q-5) Implement the concept of VLAN using Network Simulator. Create a small network topology and implement at least 2 different VLAN. The data communication is possible only between the machines of same VLAN.



- Creating the VLAN:



Switch0

Physical Config CLI Attributes

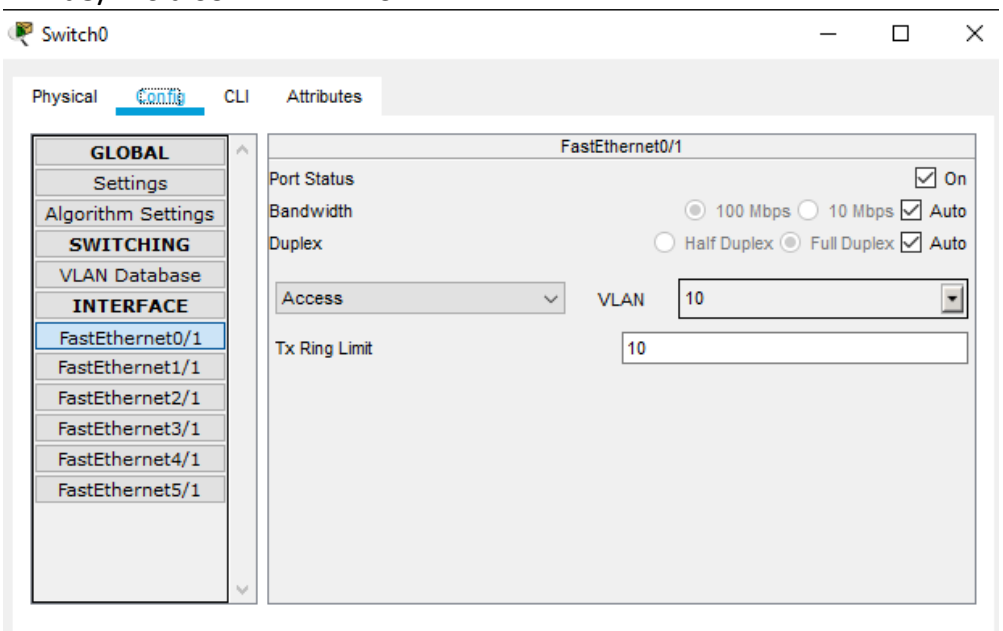
IOS Commanc

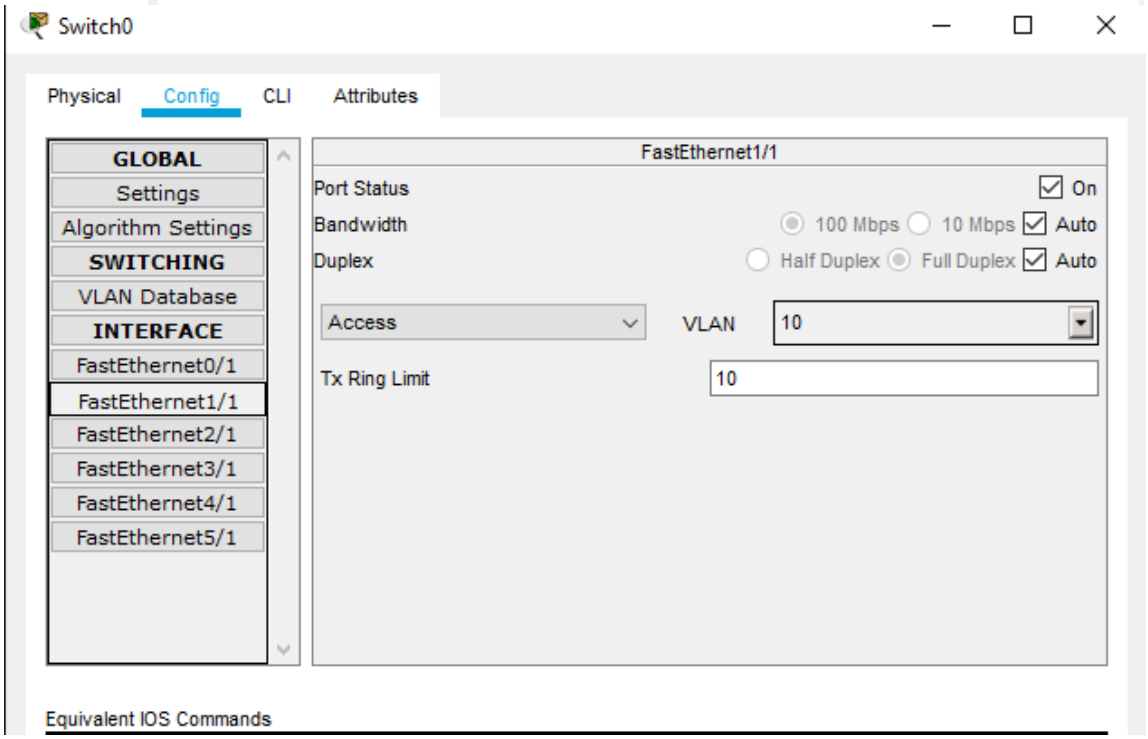
```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#name sb-computer
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name sb-computer
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name sb-mechnical
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                Fa4/1, Fa5/1
10   sb-computer                      active
20   sb-mechnical                     active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

 --More--
```

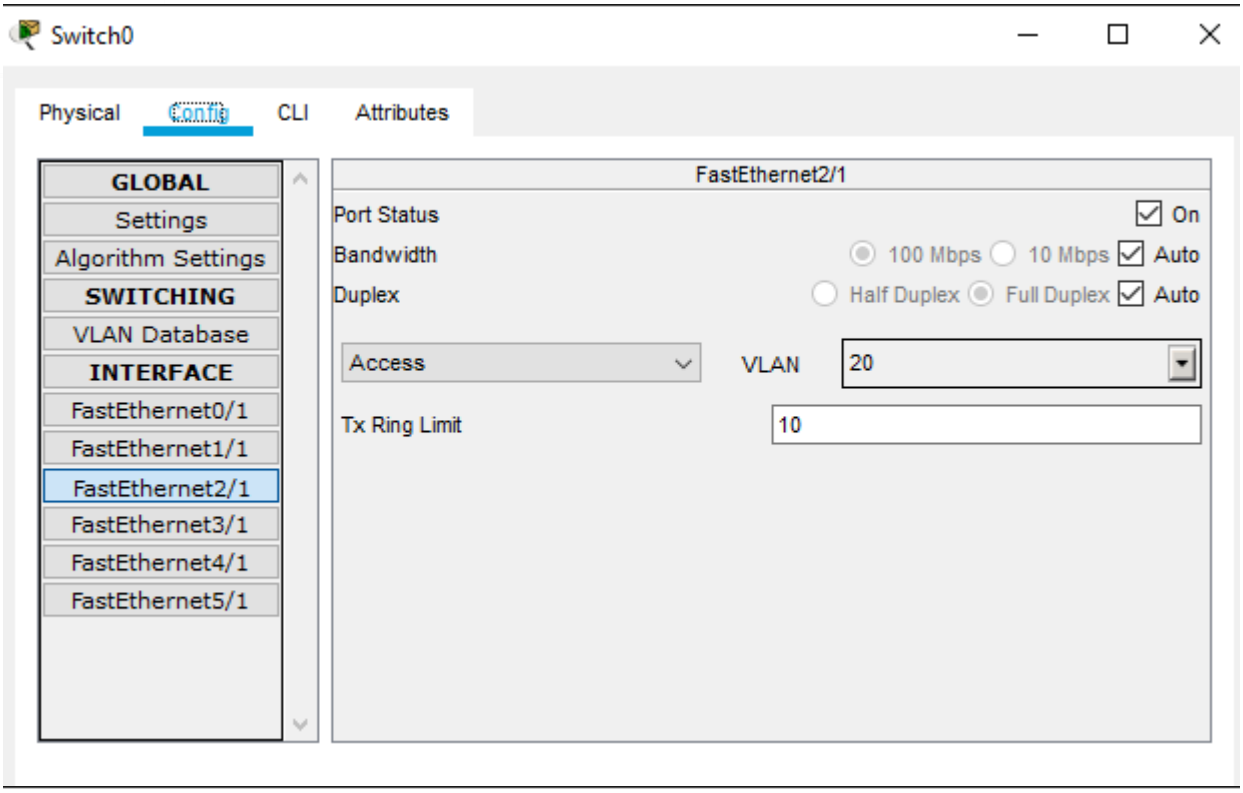
Ctrl+F6 to exit CLI focus

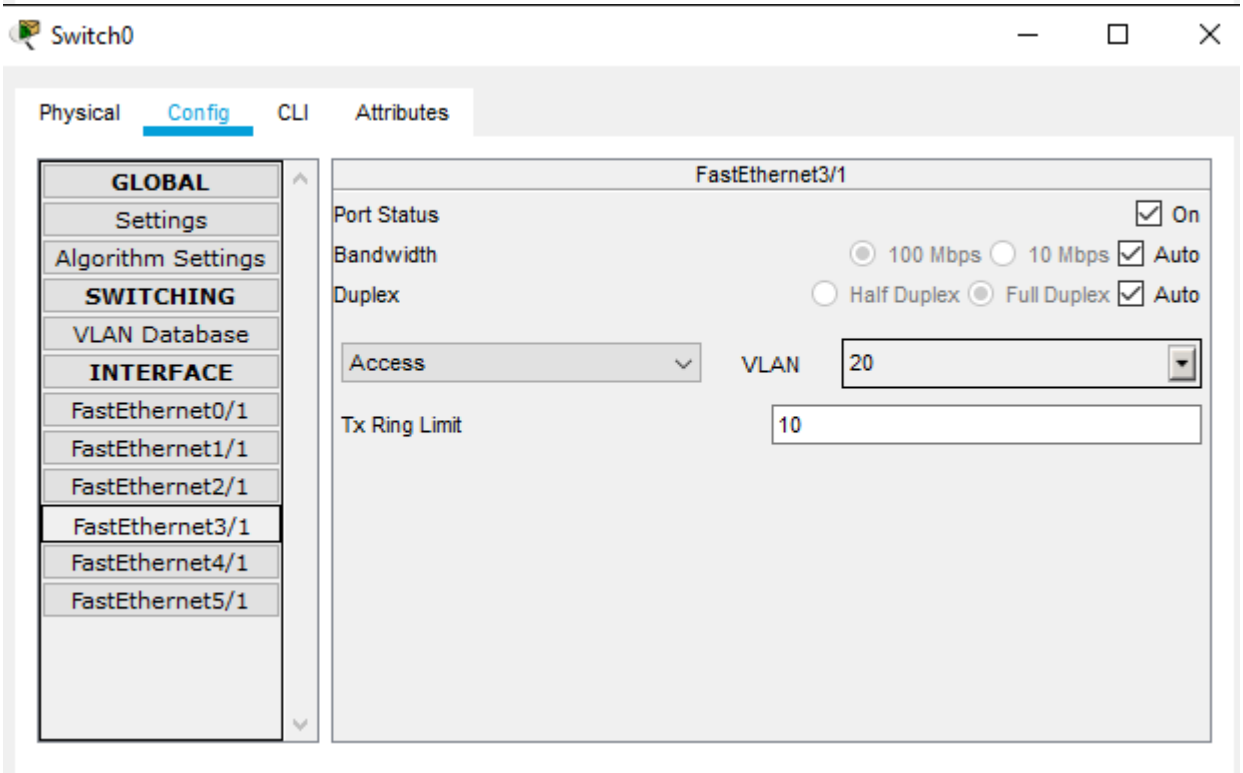
(“vlan 10” create vlan 10 and for give name you can use “name <any_name>”. For see how many vlan is created in switch you can write “show vlan” command.)
After creating VLAN set interfaces to particular VLAN.

- Here, fa0/1 is in VLAN 10
  fa1/1 is also in VLAN 10
  fa2/1 is in VLAN 20
  fa3/1 is also in VLAN 20

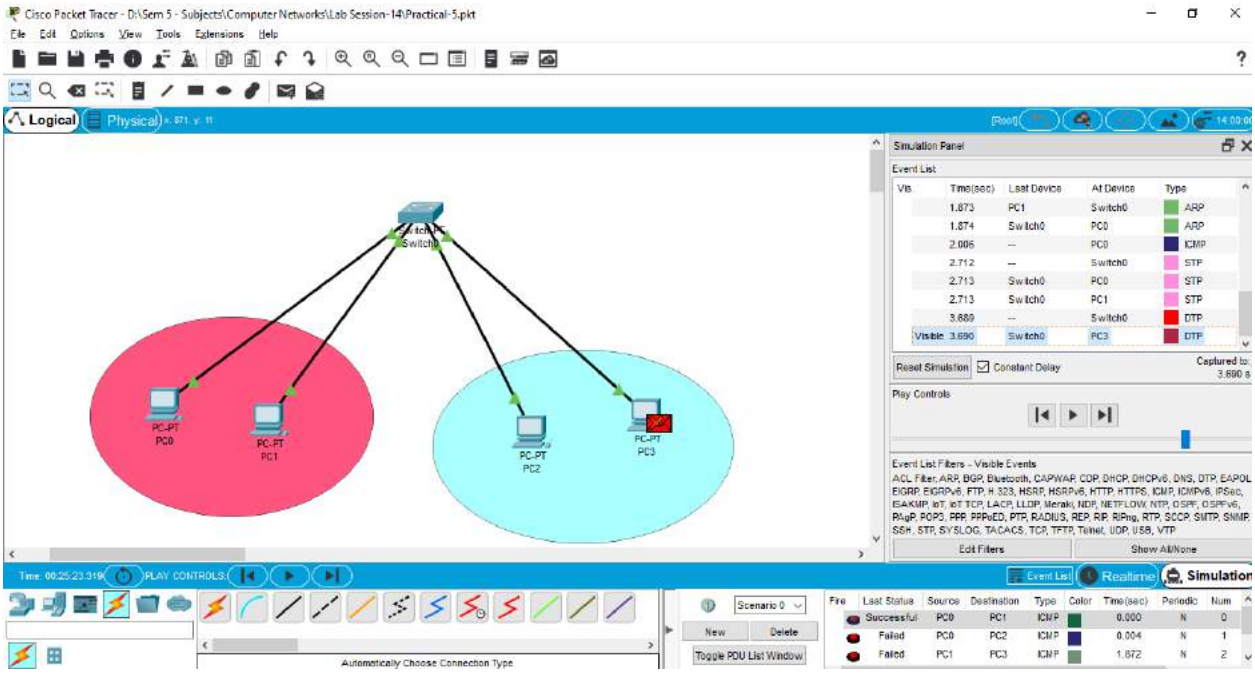





Switch0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet1/1
FastEthernet2/1
FastEthernet3/1
FastEthernet4/1
FastEthernet5/1
FastEthernet2/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
Access
VLAN
20
Tx Ring Limit
10


Switch0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet1/1
FastEthernet2/1
FastEthernet3/1
FastEthernet4/1
FastEthernet5/1
FastEthernet3/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
Access
VLAN
20
Tx Ring Limit
10

- After you can see below packet sending results….

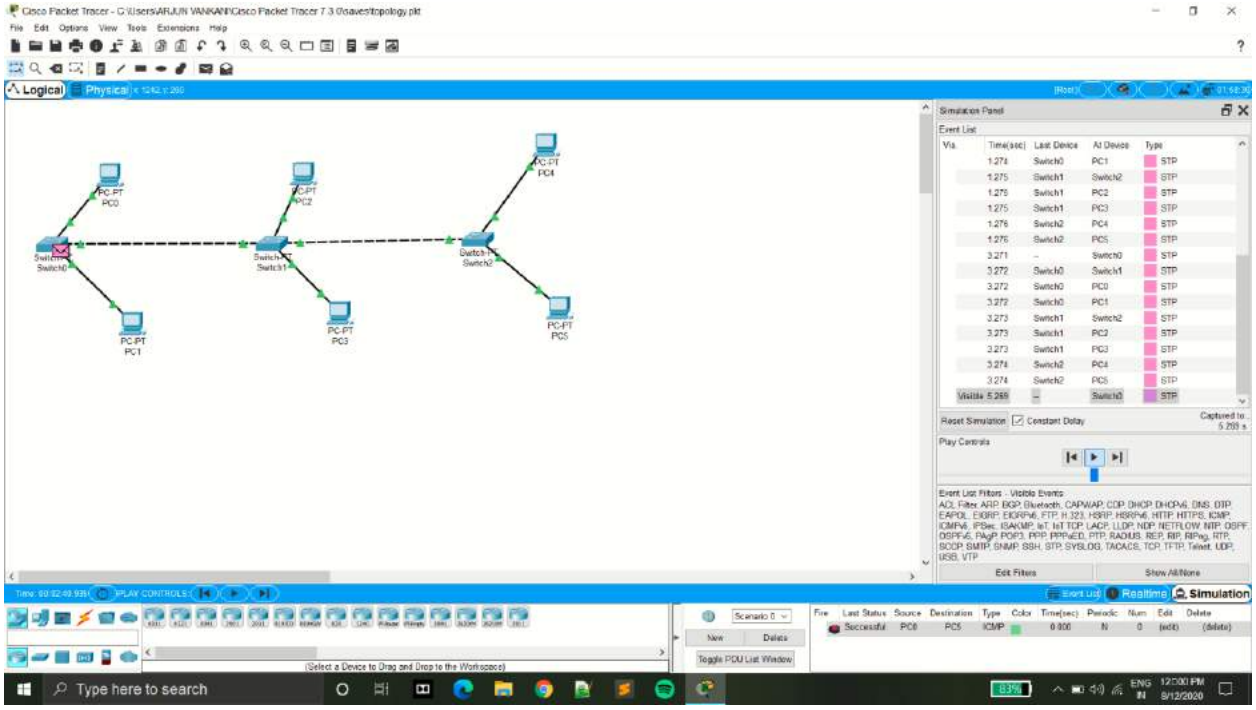


(Here, you can see PC0 to PC1 packet is successfully transfer because both pc are in same VLAN and PC0 to PC2 is failed because those both pc are in different VLAN, and same for PC1 to PC3)

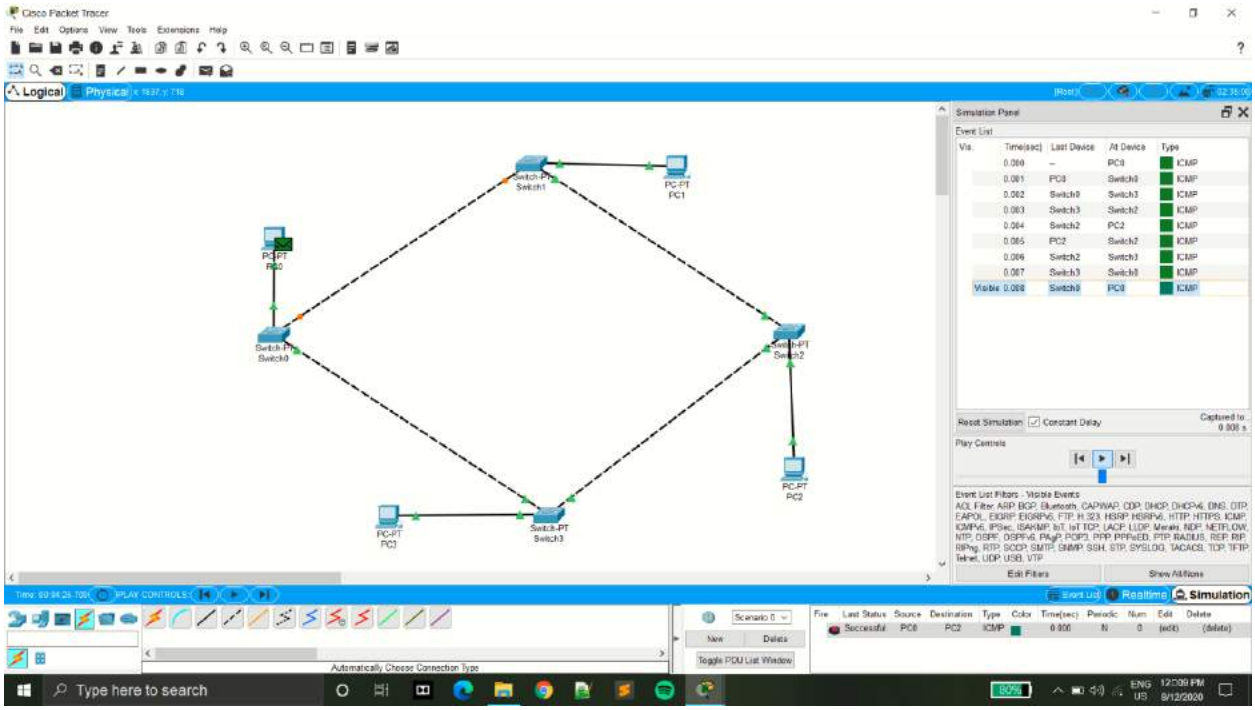
Computer Network (LAB Session-5)

- Implement different LAN topologies using CISCO Packet Tracer
- Create below network topologies in CISCO packet tracer. (Verify the connection by passing a sample message between any two devices.)

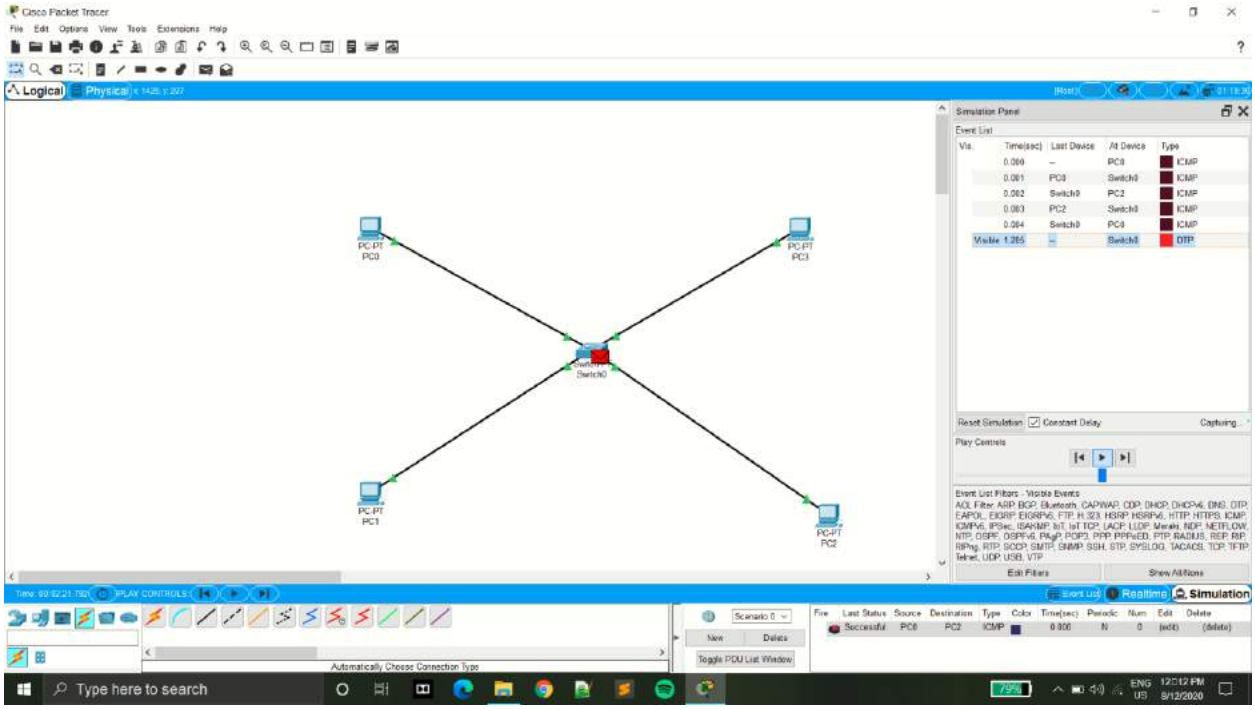
1) Bus Topology



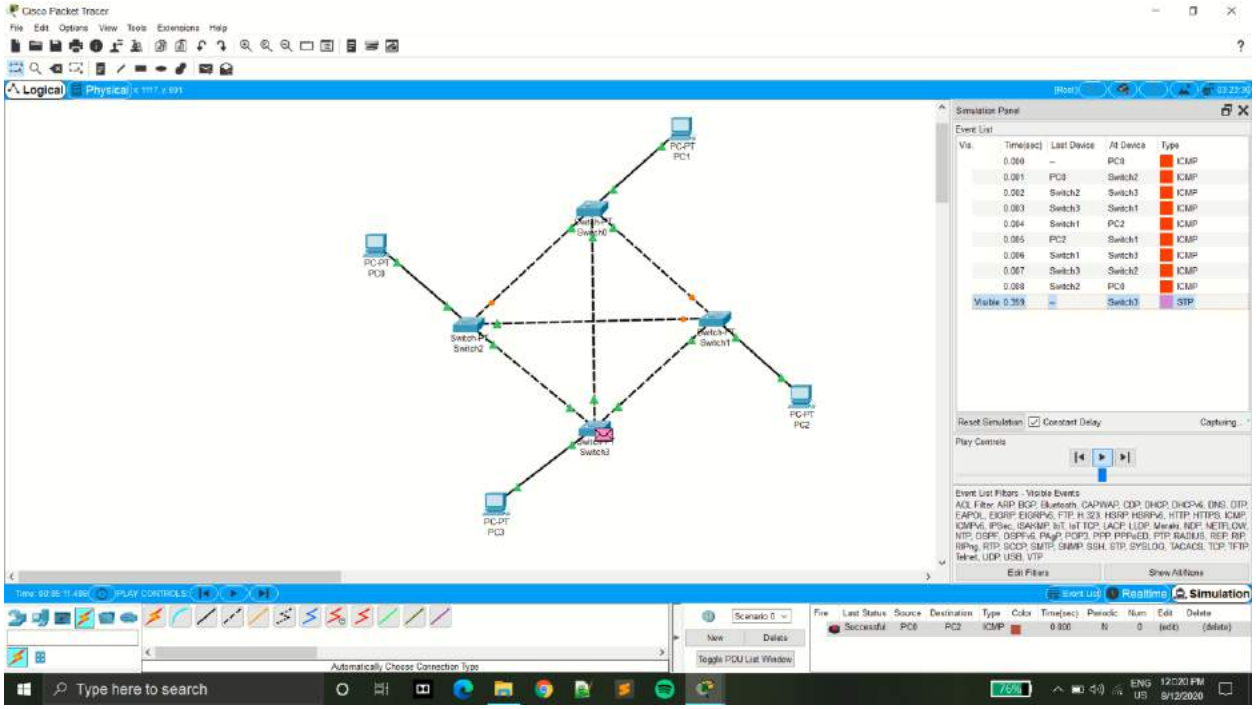
2) Ring Topology



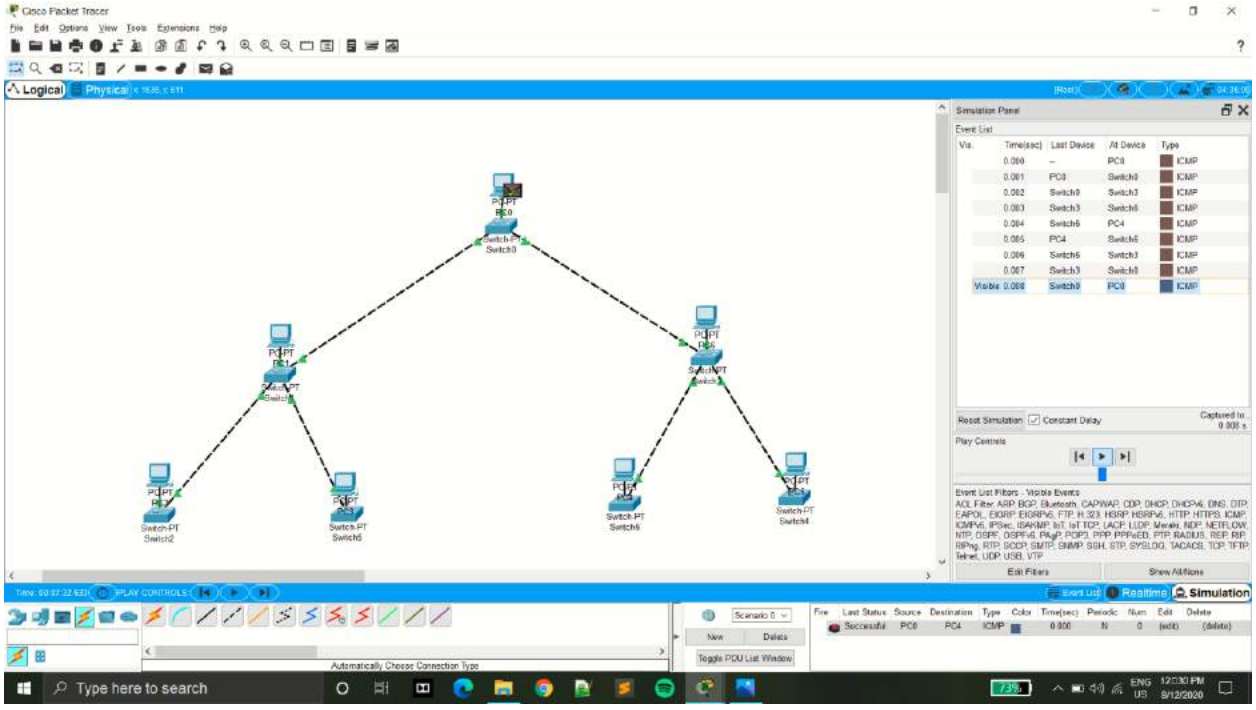
3) Star Topology



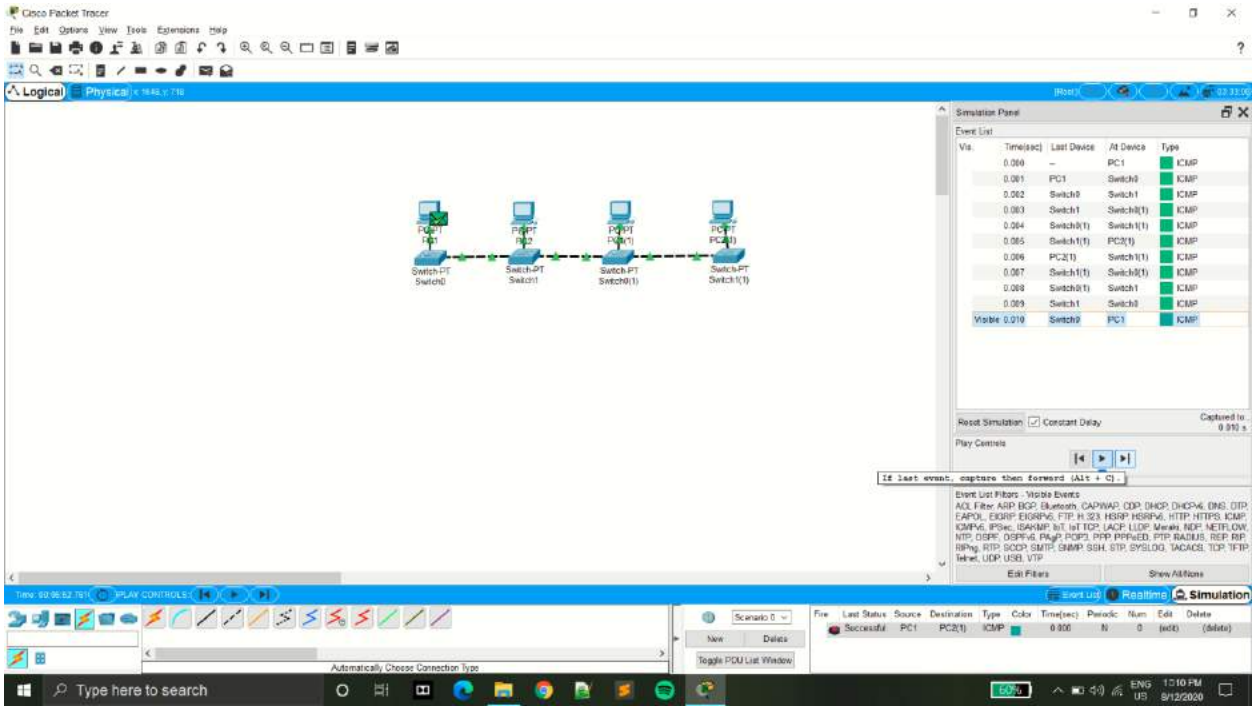
4) Mesh Topology



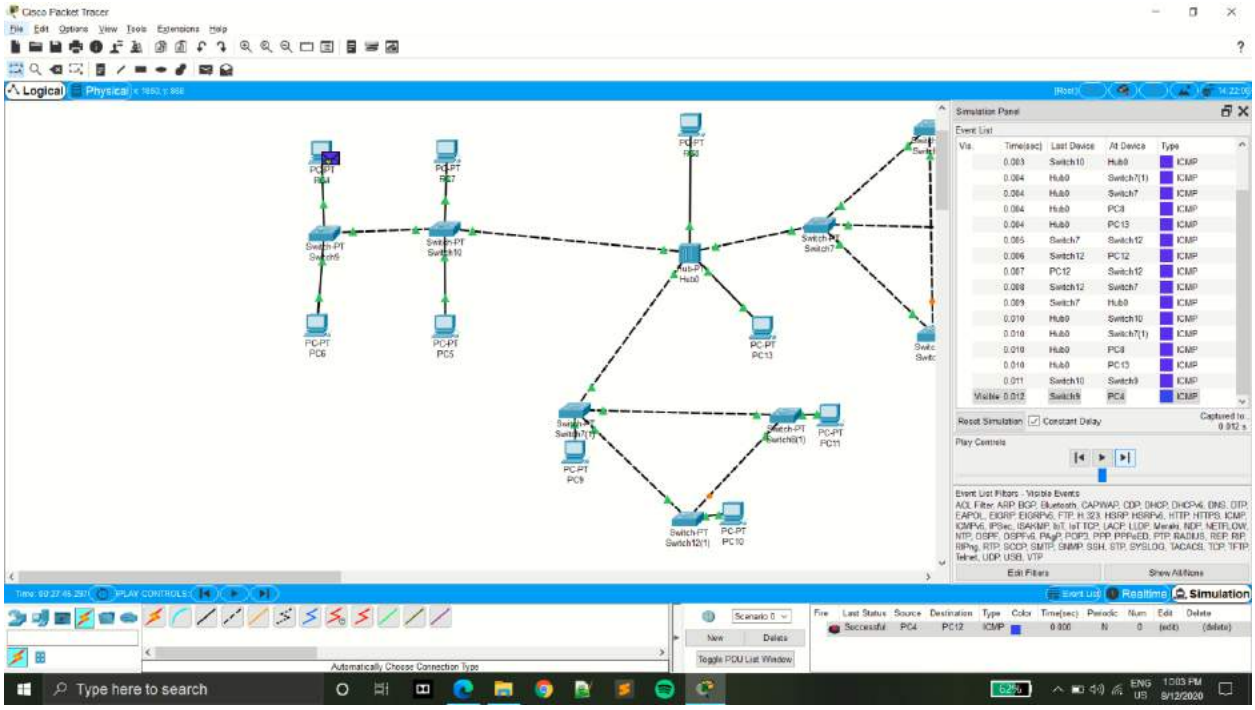
5) Tree Topology



6) Daisy Chain



7) Hybrid Topology



Computer Network (Practical list -4)

1.You have a server that stores the data of the employees of a company. The data is in the below format. EMP. ID FirstName Last Name Department Experience(years)Employee can query the server for the data by giving the employee ID and can receive the details in return. Server will return error message if it does not have the details for any employee ID. Using Socket programming, write a client program and server program that performs the required operations. You can write the coed in any language of your choice. (No need to create actual Database on server side, you can use collections like Map in Java or Dictionary in Python. You can also choose any other data structure to store the data.)

a.) Explain the difference between TCP and UDP protocol.

	TCP	**UDP**
Full form	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	Transmission Control Protocol is a connection-oriented protocol.	User Datagram Protocol is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol.

Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection.	UDP does not have an option for flow control

b.) Write the socket program that connects client and server using UDP protocol.

- **UDP for server Program:**

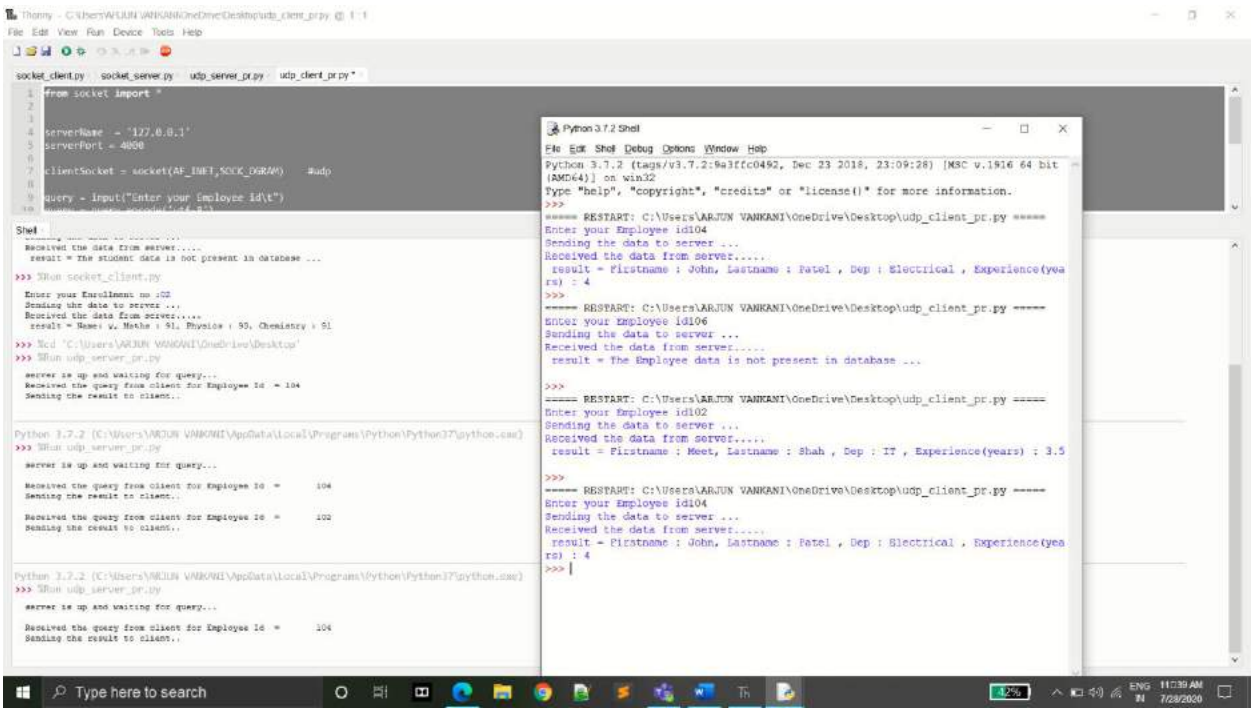
```
from socket import *


DataEmployy = {
        "101":"Firstname : Ved, Lastname : Shukla , Dep : Mechnical , Experience(years) : 2 ",
        "102":"Firstname : Meet, Lastname : Shah , Dep : IT , Experience(years) : 3.5 ",
        "103":"Firstname : Sujit, Lastname : Maniya , Dep : Computer , Experience(years) : 1.5 ",
        "104":"Firstname : John, Lastname : Patel , Dep : Electrical , Experience(years) : 4 ",
        "105":"Firstname : Kaushal, Lastname : Jani , Dep : Mechnical , Experience(years) : 4.5 "
        }
serverPort = 4000


serverSocket = socket(AF_INET,SOCK_DGRAM)  # udp


serverSocket.bind(('', serverPort))


print("server is up and waiting for query...\n")
```

```
while True:
    query, clientAddress = serverSocket.recvfrom(2048)
    query = query.decode('utf-8')

    print("Received the query from client for Employee Id  = \t{}".format(query))

    res = DataEmployy.get(str(query),"The Employee data is not present in database ...\n")
    res = res.encode('utf-8')

    print("Sending the result to client..\n")
    serverSocket.sendto(res,clientAddress)
```

- **UDP for client Program:**

```
from socket import *



serverName  = '127.0.0.1'
serverPort = 4000

clientSocket = socket(AF_INET,SOCK_DGRAM)    #udp

query = input("Enter your Employee id\t")
query = query.encode('utf-8')

print("Sending the data to server ...\n")
clientSocket.sendto(query,(serverName,serverPort))
```

```
result, serverAddress =  clientSocket.recvfrom(2048)

result = result.decode('utf-8')


print("Received the data from server.....\n result => \n{}".format(result))



clientSocket.close()
```



c.) Write the socket program that connects client and server using TCP protocol

- **TCP for server Program:**

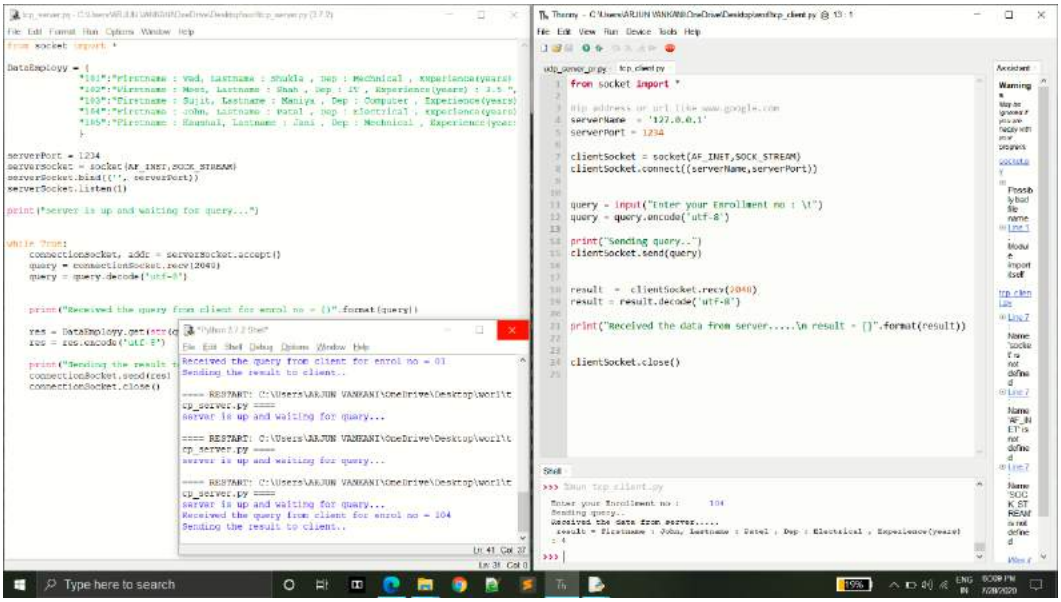
```
from socket import *

DataEmploy = {
        "101":"Firstname : Ved, Lastname : Shukla , Dep : Mechnical , Experience(years) : 2 ",
        "102":"Firstname : Meet, Lastname : Shah , Dep : IT , Experience(years) : 3.5 ",
        "103":"Firstname : Sujit, Lastname : Maniya , Dep : Computer , Experience(years) : 1.5 ",
```

```
        "104":"Firstname : John, Lastname : Patel , Dep : Electrical , Experience(years) : 4
",
        "105":"Firstname : Kaushal, Lastname : Jani , Dep : Mechnical , Experience(years)
: 4.5 "
        }

serverPort = 1234
serverSocket = socket(AF_INET,SOCK_STREAM)
serverSocket.bind(('', serverPort))
serverSocket.listen(1)

print("server is up and waiting for query...")


while True:
  connectionSocket, addr = serverSocket.accept()
  query = connectionSocket.recv(2048)
  query = query.decode('utf-8')


  print("Received the query from client for enrol no = {}".format(query))

  res = DataEmployy.get(str(query),"The student data is not present in database ...")
  res = res.encode('utf-8')

  print("Sending the result to client..")
  connectionSocket.send(res)
  connectionSocket.close()
```

- **TCP for client Program:**

```
from socket import *


#ip address or url like www.google.com

serverName  = '127.0.0.1'

serverPort = 1234
```

```
clientSocket = socket(AF_INET,SOCK_STREAM)
clientSocket.connect((serverName,serverPort))


query = input("Enter your Enrollment no : \t")
query = query.encode('utf-8')

print("Sending query..")
clientSocket.send(query)


result  =  clientSocket.recv(2048)
result = result.decode('utf-8')

print("Received the data from server.....\n result = {}".format(result))

clientSocket.close()
```



Computer Network (LAB-SESSION 9)

Q-1) UDP Pinger

A) Create a UDP Client and a UDP Server. UDP client will ping UDP server 10 times. UDP Server will reply to the ping message as soon as it receives it. If the reply for the ping message does not come within one second, you can consider the packet as a lost packet (you can implement this scenario by not sending a reply for some random client ping)

B) After receiving reply from server for each ping message, UDP client will calculate and print the RTT time (time between sending the ping and receiving the reply) for each response.

C) After the cycle of 10 pings, client will analyze all 10 response times and will print maximum RTT, minimum RTT and average RTT.

➢

UDP Server

```
from socket import *
from time import sleep

host = 'localhost'
port = 4444

socketserver = socket(AF_INET,SOCK_DGRAM)  #UDP
socketserver.bind((host,port))

data = []

for i in range(10):
   value = socketserver.recvfrom(1024)
   ip = value[1]

   data.append(value[0].decode())
   if data[i] == "3" or data[i] == "6":
      sleep(3)
   send = socketserver.sendto(data[i].encode(),ip)
   sleep(2)
print("Connection Address of server:",ip)
```

Output:

```
Connection Address of server: ('127.0.0.1', 51280)
```

UDP Client

```
from socket import *
from time import *

host = 'localhost'
port = 4444

socketserver = socket(AF_INET,SOCK_DGRAM) # UDP
ip = (host,port)
lst = []
seq = 10
i = 0
while i < seq:
   i += 1
   srttime = time()
   socketserver.sendto(str(i).encode("utf-8"),ip)
   rec = socketserver.recvfrom(1024)
   rtt = time() - srttime
   tm = localtime(rtt)
   lst.append(tm.tm_sec)
   if(tm.tm_sec <=1):
      print("Responce from server with in.....",tm.tm_sec)
   else:
      print("Responce time out.....")
   sleep(0.5)
print("All timing for response",lst)
n1 = sum(lst)
n2 = len(lst)
avg = n1/n2
print("Total RTT Time",str(n1))
print("Maximum RTT Time",str(max(lst)))
print("Minimum RTT Time",str(min(lst)))
print("Average RTT Time",str(avg))
```

Output:

```
Responce from server with in..... 0

Responce from server with in..... 1

Responce time out.....

Responce from server with in..... 1

Responce from server with in..... 1

Responce time out.....

Responce from server with in..... 1
```

Responce from server with in..... 1

Responce from server with in..... 1

Responce from server with in..... 1

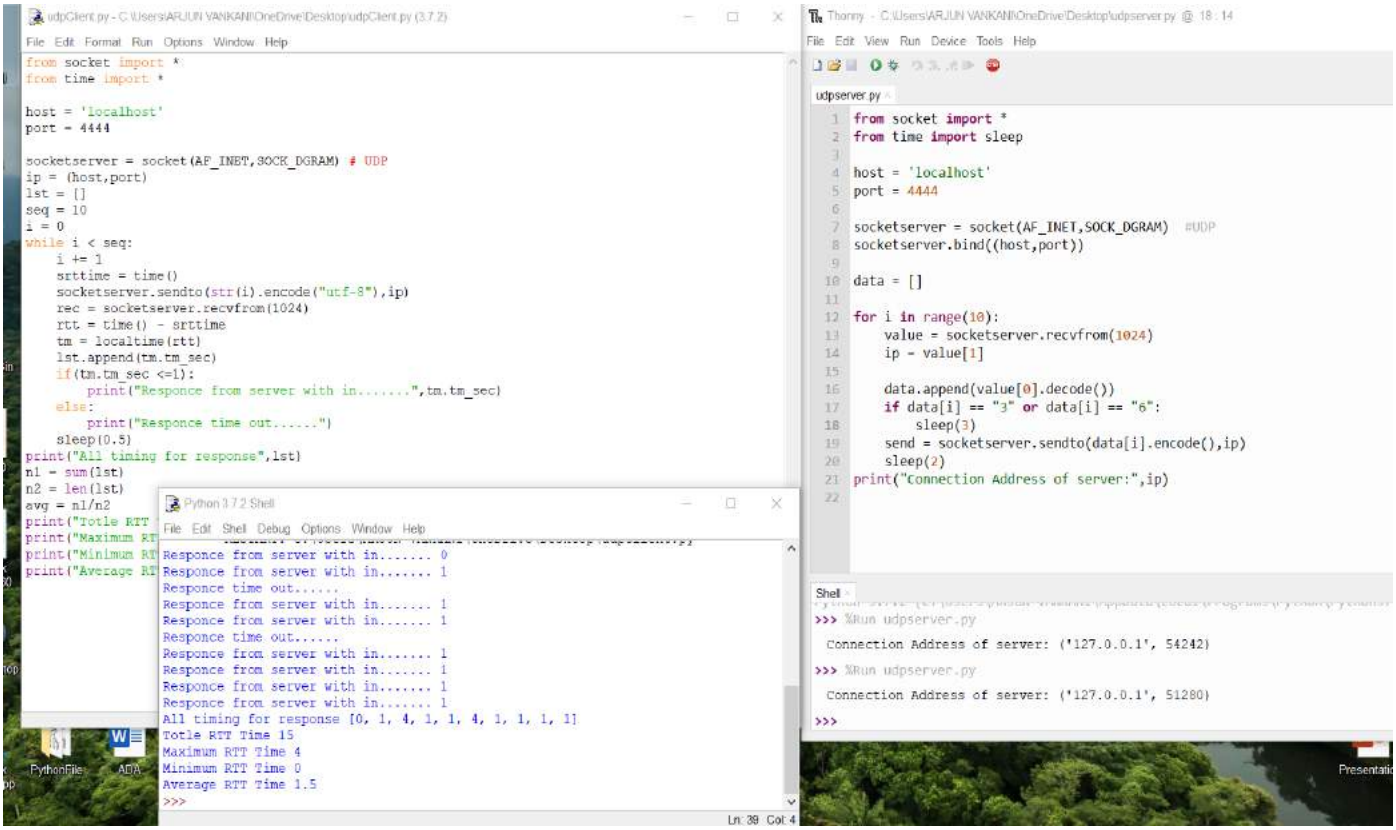
All timing for response [0, 1, 4, 1, 1, 4, 1, 1, 1, 1]

Total RTT Time 15

Maximum RTT Time 4

Minimum RTT Time 0

Average RTT Time 1.5



2.TCP Chatbot

An airline company wants you to implement a chatbot that helps them automate the process of new ticket booking, cancellation of previous bookings and status inquiry for the current booking.

A) Once a client connects with the server, the server chatbot will ask user to enter one of the three possible choices (1, 2or 3).

B) If the client enters 1, it means client wants to book a new ticket. The chatbot will

2 one by one ask three information for booking i.e. Name, Source and Destination. It then generates a random booking ID and stores these details with the booking ID in its database. It also displays the booking confirmation to the user and gives him his booking ID.

C) If the user enters 2, it means that

the user wants to delete the booking made by him. Server chatbot asks for the booking ID from the client and once it receives the booking ID, it checks in the database for the booking information.

If found, it will delete the information and confirmation will be provided to the user.

D) If the user enters 3, it means that the user wants to look into his booking details. In this case, the server chatbot will ask for the booking ID and will send the booking details back to the client if found from the database which then will be printed on the client screen.

E) Chatbot will ask the user to enter the Proper choice if the user enters anything other than the predefined choices (1,2,3).

- **TCP SERVER:**

```
from socket import *
from json import *
from random import randint

host = 'localhost'
port = 4444

serversocket = socket(AF_INET,SOCK_STREAM,0)  #tcp
serversocket.bind((host,port))

serversocket.listen(2)

con,adr = serversocket.accept()
print("Connection From:\t",adr)
Gid = {}   # gerate id
while True:
   ch = con.recv(1024).decode()
   if int(ch) == 1:
      while True:
         val = con.recv(1024).decode()
         data = loads(val)

         strid = randint(1111,9999)
         Bid = "BOOK_ID" + str(strid)  #Booking Id
         Gid[Bid] = {}
         Gid[Bid].update({"Name":data[0]})
         Gid[Bid].update({"Pick up":data[1]})
         Gid[Bid].update({"Drop ":data[2]})
```

```
            keys = []
            for i in Gid.keys():
                keys.append(i)
            con.send(Bid.encode("utf-8"))
            brdata = con.recv(1024).decode()
            if(brdata == "yes"):
                True
            else:
                break
        if(int(ch)==2):
            keys = []
            for i in Gid.keys():
                keys.append(i)
            print(keys)
            while True:
                recdatacan = con.recv(1024).decode()
                if recdatacan in keys:
                    del Gid[recdatacan]
                    str = "0"
                    con.send(str.encode("utf-8"))
                    break
                else:
                    str = "1"
                    con.send(str.encode("utf-8"))
            #display data
        if(int(ch)==3):
            keys = []
            for i in Gid.keys():
                keys.append(i)
            while True:
                recdata = con.recv(1024).decode()
                if recdata in keys:
                    templst = []
                    for i in Gid[recdata].values():
                        templst.append(i)
                    st = dumps(templst)
                    con.send(st.encode("utf-8"))
                    break
                else:
                    str = "0"
                    con.send(str.encode("utf-8"))
        if(int(ch) == 0):
            break
```

OUTPUT:

```
Connection From:        ('127.0.0.1', 3527)
['BOOK_ID2086', 'BOOK_ID8602']
```

TCP CLIENT

```
from socket import *
from json import *

host = 'localhost'
port = 4444

socketclient = socket(AF_INET,SOCK_STREAM,0)  #Tcp
socketclient.connect((host,port))

F = 1
while F == 1:
   print("Welcome to our Airline Service 24*7 \n")
   ans = int(input("\t 1) For Booking Your Ticket: \n\t 2) Process to cancle ticket\n\t
3)History & Cheking Conformation ticket: \n \t 0.Exit\n\t Enter Your choices :\t "))
   socketclient.send(str(ans).encode("utf-8"))
   if(ans == 1):
      while True:
         lst = []
         lst.append(input("Enter Your Name:"))
         lst.append(input("Enter Your Pick up:"))
         lst.append(input("Enter Your Drop:"))

         senddata = dumps(lst)

         socketclient.send(senddata.encode("utf-8"))
         id=socketclient.recv(1024).decode()

         print("Your Booking is Conform And Booking Id Is:",id)
         agindata = input("Do you want to book another Ticket ?\n \t  [yes/no]:")
         socketclient.send(agindata.encode("utf-8"))
         if(agindata == "yes"):
            True
         else:
            break
   if(ans == 2):
      while True:
         getid = input("Enter Your Booking Id:")
         socketclient.send(getid.encode("utf-8"))
         recdata = socketclient.recv(1024).decode()
         if (recdata != "1"):
            print("Your ticket cancle")
            break
         else:
            print("Maybe you type wrong Id or You don't book ticket right now!!")
            break
   if(ans == 3):
```

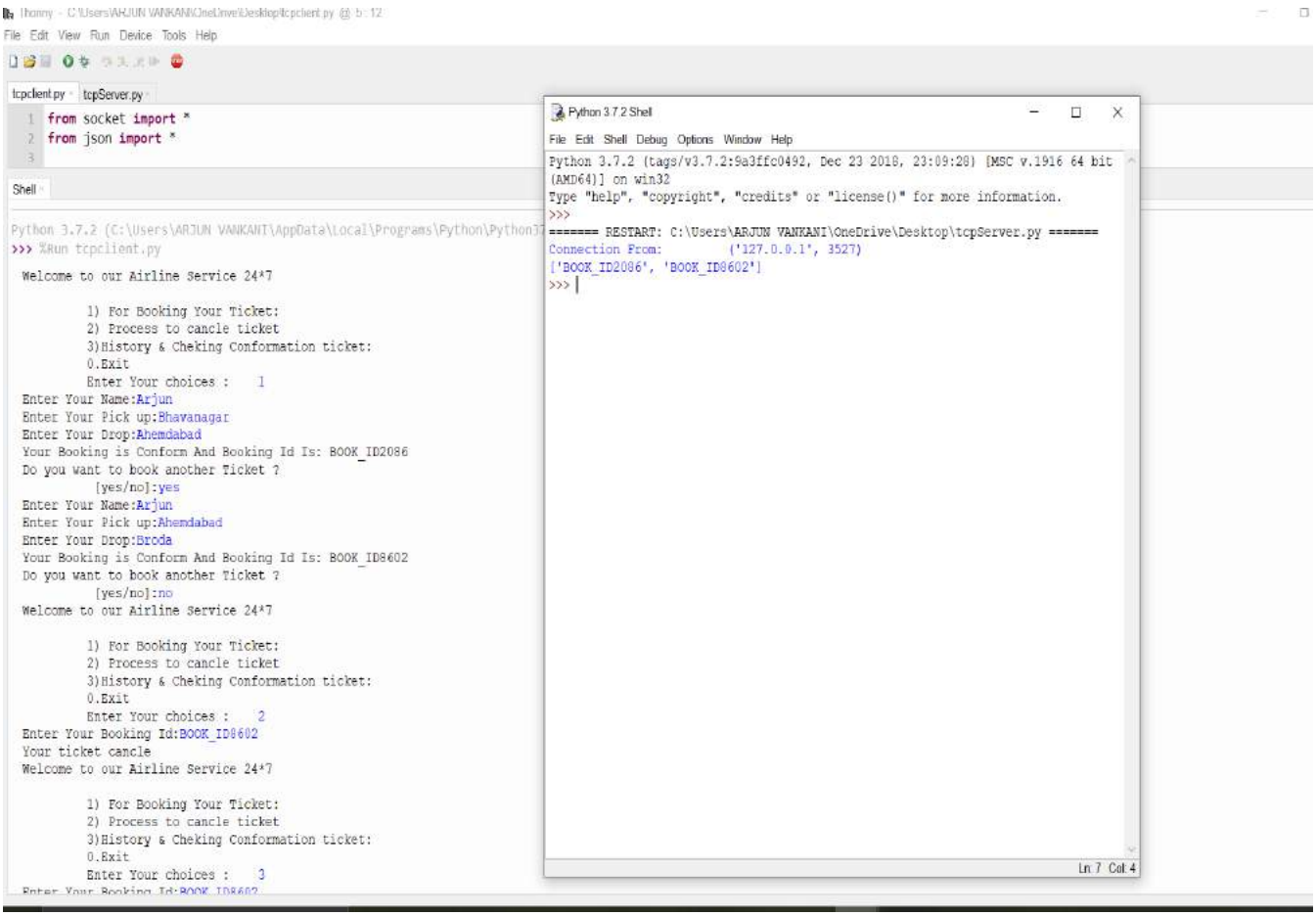
```
    while True:
        getid = input("Enter Your Booking Id:")
        socketclient.send(getid.encode("utf-8"))
        recdata=socketclient.recv(1024).decode()
        if(recdata != "0"):
            ans = loads(recdata)
            print("Booking Conform:")
            print("Your Booking id is:",getid)
            print("Your Name is:",ans[0])
            print("Your Source address:", ans[1])
            print("Your Destination address:", ans[2])
            break
        else:
            print("Maybe you type wrong Id or You don't book ticket right now!!")
if(ans == 0):
    F = 0
```

OUTPUT:

```
        Welcome to our Airline Service 24*7

         1) For Booking Your Ticket:
         2) Process to cancle ticket
         3)History & Cheking Conformation ticket:
         0.Exit
         Enter Your choices :      1
Enter Your Name:Arjun
Enter Your Pick up:Bhavanagar
Enter Your Drop:Ahemdabad
Your Booking is Conform And Booking Id Is: BOOK_ID2086
Do you want to book another Ticket ?
          [yes/no]:yes
Enter Your Name:Arjun
Enter Your Pick up:Ahemdabad
Enter Your Drop:Broda
Your Booking is Conform And Booking Id Is: BOOK_ID8602
Do you want to book another Ticket ?
          [yes/no]:no
Welcome to our Airline Service 24*7

         1) For Booking Your Ticket:
         2) Process to cancle ticket
         3)History & Cheking Conformation ticket:
         0.Exit
         Enter Your choices :      2
Enter Your Booking Id:BOOK_ID8602
Your ticket cancle
Welcome to our Airline Service 24*7
```

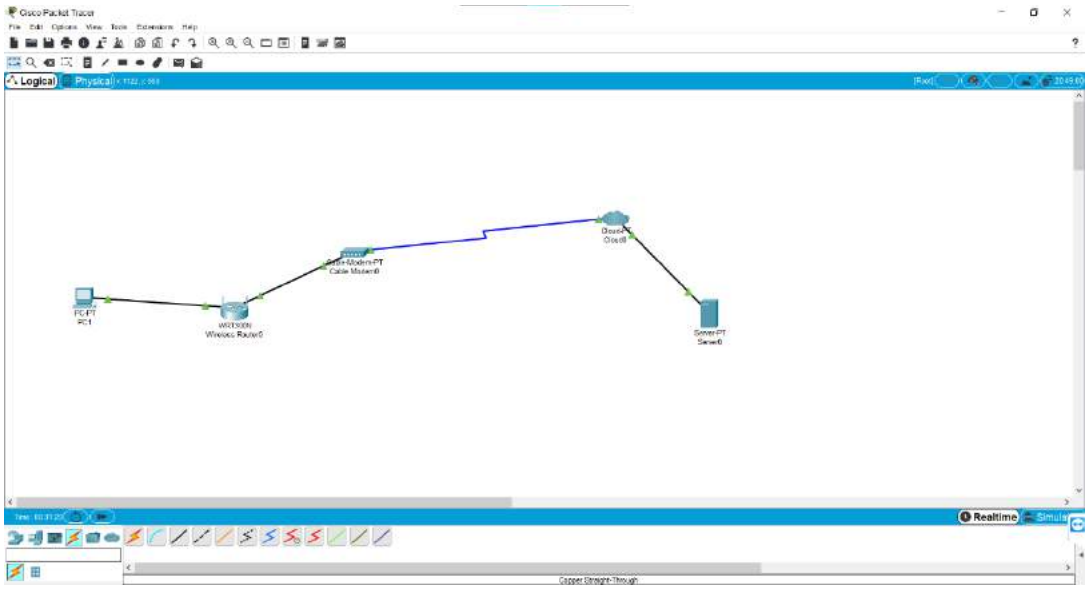
1) For Booking Your Ticket:
2) Process to cancle ticket
3)History & Cheking Conformation ticket:
0.Exit
Enter Your choices : 3
Enter Your Booking Id:BOOK_ID8602
Maybe you type wrong Id or You don't book ticket right now!!
Enter Your Booking Id:BOOK_ID2086
Booking Conform:
Your Booking id is: BOOK_ID2086
Your Name is: Arjun
Your Source address: Bhavanagar
Your Destination address: Ahemdabad
Welcome to our Airline Service 24*7

1) For Booking Your Ticket:
2) Process to cancle ticket
3)History & Cheking Conformation ticket:
0.Exit
Enter Your choices: 0

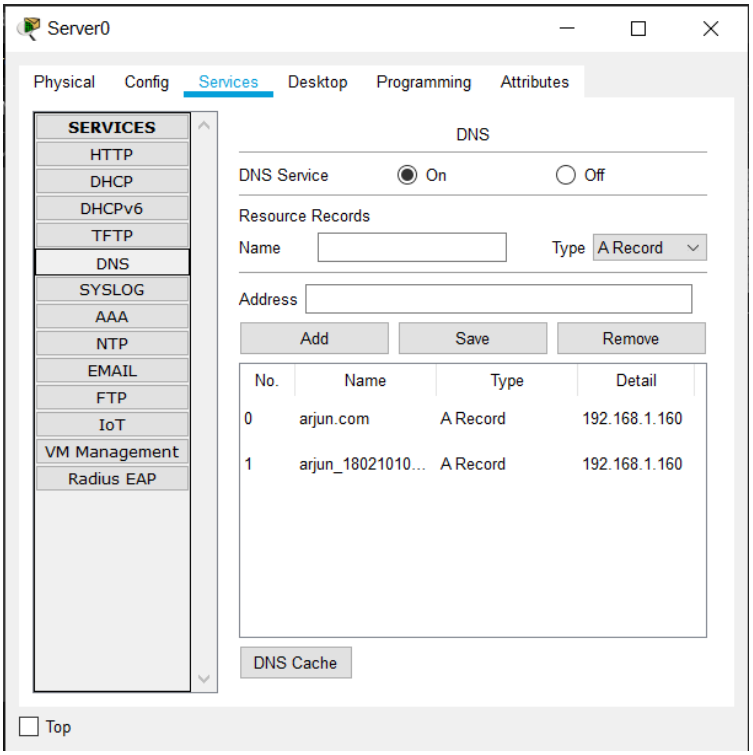


COMPUTER NETWORK (LAB-5)

1) Create a network topology in packet tracer as below.

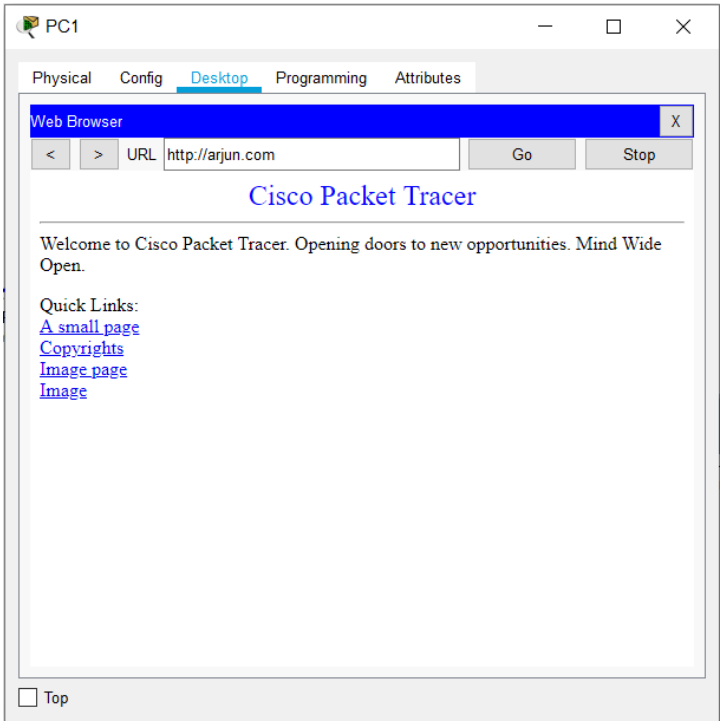


A) Configure the web server as DNS server that resolves the URL with its IP address

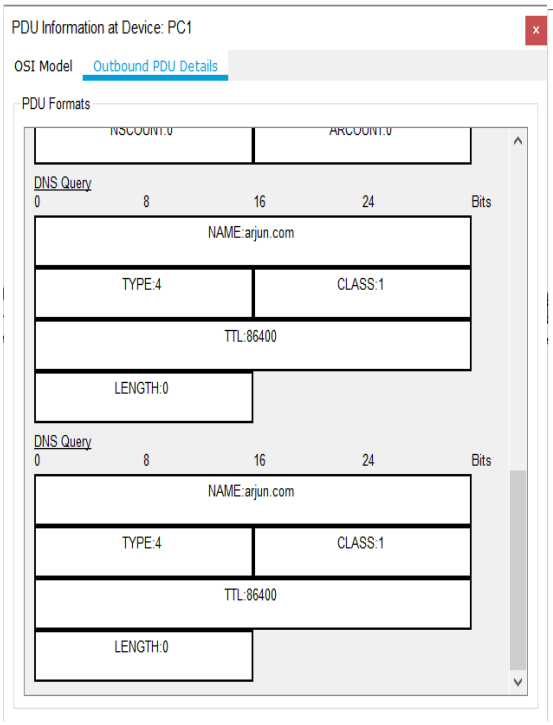


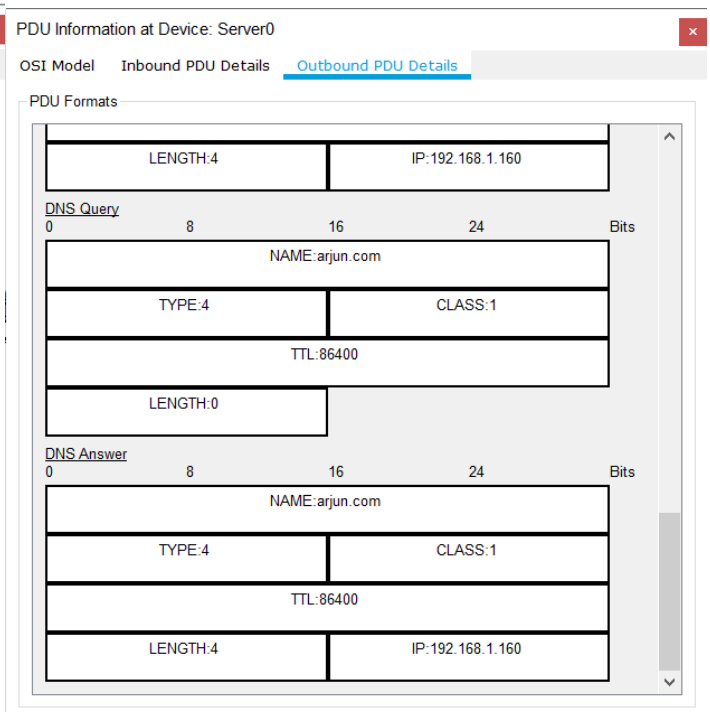
B) Provide the mapping of two URLs (yourName.com and yourName-yourEnrolmentNo.com)with the static IP address of web server in the DNS service tabs o that if client writes any of these two URL in his browser, he/she should be able to open and access the web resources at the server

C) Using simulation mode in packet tracer, observe the network traffic when client opens the website by writing URL in the web browser.

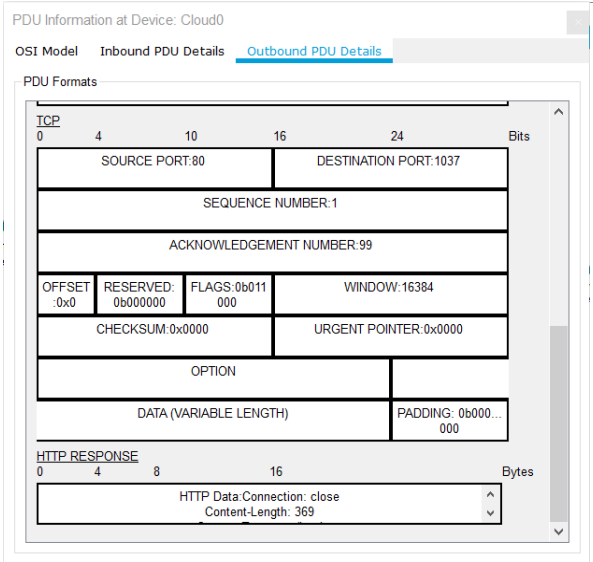


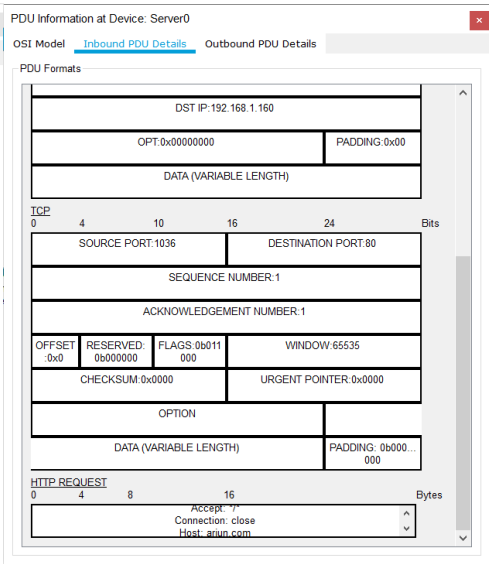
D) capture the DNS query and response message that is used to resolve the host name into IP address





E) Capture the HTTP request and response messages that are passed between client and server when client request the webpage from server





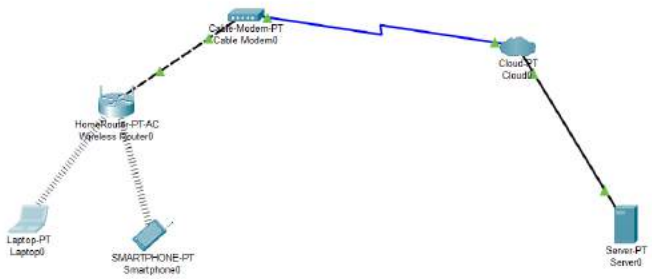
Thank you!!

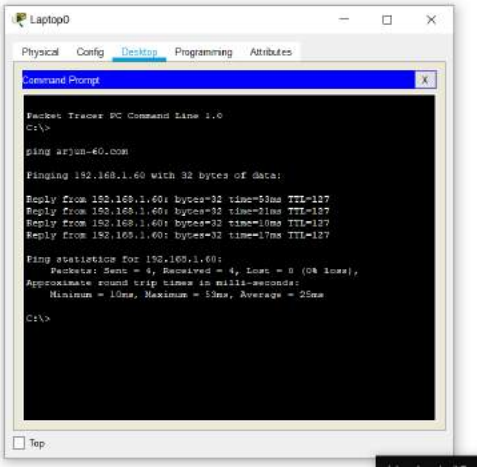
Computer Network LAB Session-7

Implement DNS and FTP Server1

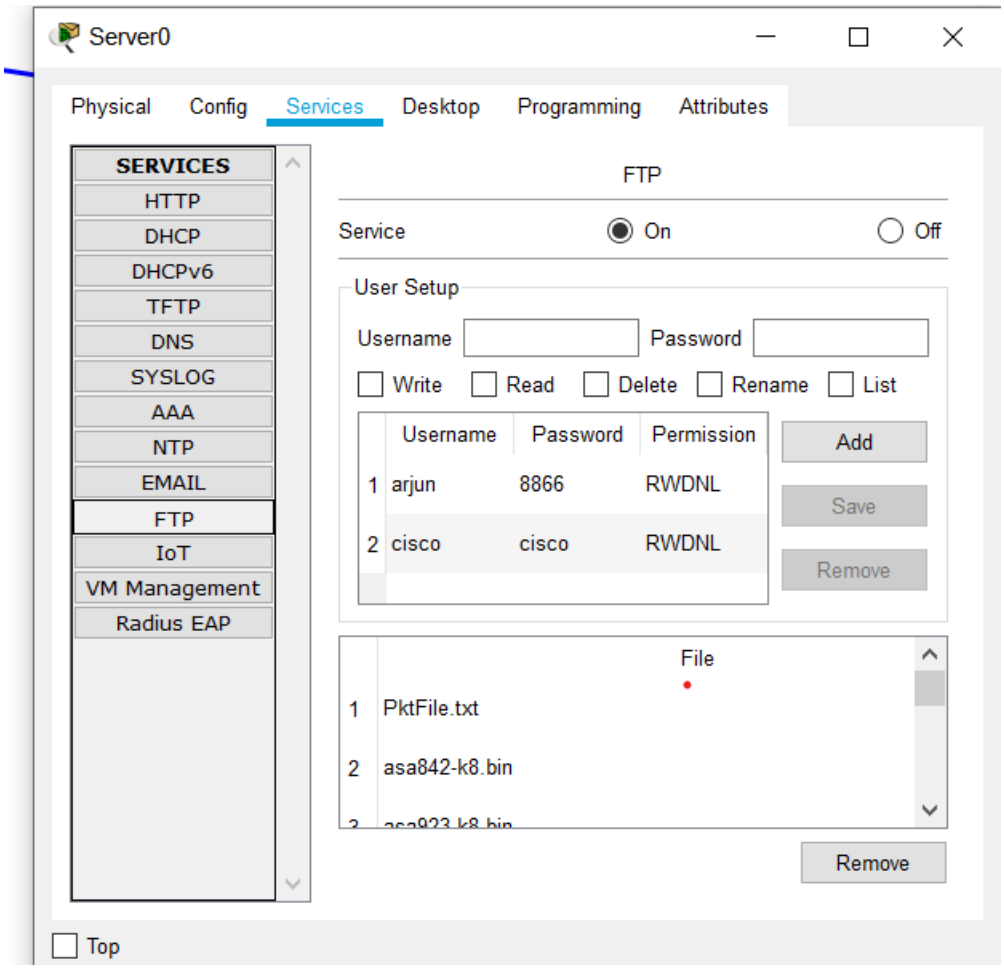
Create network topology in CISCO packet tracer as shown below.

A) Set the URL for the server as yourname-last_two_digits_of_enrl_no.com

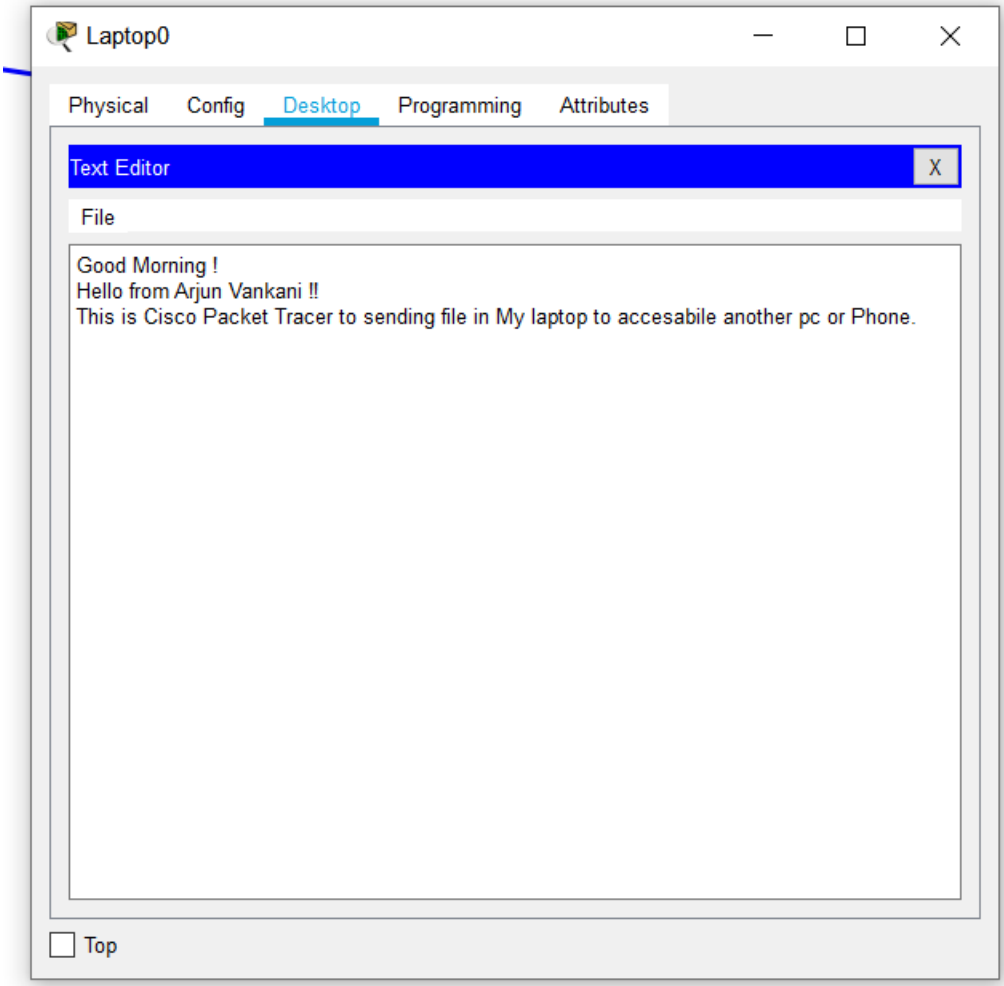




B) Configure the server as FTP server.



C)Create a text file in the laptop. Write your name and enrollment number in the file. Save the file as yourname.txt



D)Login to the FTP server from the laptop using command prompt and upload the text file using ftp commands.

Use “Ftp Url ” for login to FTP server and “put file name ” to upload the file on the FTP server. (Do not login by directly giving IP address of server in the ftp

command even though it is possible). Capture the request and response when you connect to the server using ftp commands.

Laptop0

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ftp arjun-60.com
Trying to connect...arjun-60.com
Connected to arjun-60.com
220- Welcome to PT Ftp server
Username:arjun
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from arjun-60.com:
0    : asa842-k8.bin                                    5571584
1    : asa923-k8.bin                                    30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin           33591768
3    : c1841-ipbase-mz.123-14.T7.bin                    13832032
4    : c1841-ipbasek9-mz.124-12.bin                     16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin           33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin           33591768
7    : c2600-i-mz.122-28.bin                            5571584
8    : c2600-ipbasek9-mz.124-8.bin                      13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin         50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin          33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin                  5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                    15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin           33591768
14   : c2950-i6q412-mz.121-22.EA4.bin                   3058048
15   : c2950-i6q412-mz.121-22.EA8.bin                   3117390
16   : c2960-lanbase-mz.122-25.FX.bin                   4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin                 4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin                 4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin          8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin           10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin             33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin            83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin           505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG              159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG              184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin         160968869
27   : ir800-universalk9-mz.SPA.155-3.M                 61750062
28   : ir800-universalk9-mz.SPA.156-3.M                 63753767
29   : ir800_yocto-1.7.2.tar                            2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar               6912000
31   : pt1000-i-mz.122-28.bin                           5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin                  3117390
ftp>put PktFile.txt

Writing file PktFile.txt to arjun-60.com:
File transfer in progress...

[Transfer complete - 134 bytes]

134 bytes copied in 0.034 secs (3941 bytes/sec)
ftp>
```

E) Login to FTP server from smartphone using command prompt and download the text file from the server(use “get filename” to download the file from

the FTP server).Capture the necessary screenshots while executing the task.

Smartphone0

Physical Config Desktop Programming Attributes

Command Prompt

```
Trying to connect...arjun-60.com
Connected to arjun-60.com
220- Welcome to PT Ftp server
Username:arjun
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from arjun-60.com:
0    : PktFile.txt                                    134
1    : asa842-k8.bin                                  5571584
2    : asa923-k8.bin                                  30468096
3    : c1841-advipservicesk9-mz.124-15.T1.bin         33591768
4    : c1841-ipbase-mz.123-14.T7.bin                  13832032
5    : c1841-ipbasek9-mz.124-12.bin                   16599160
6    : c1900-universalk9-mz.SPA.155-3.M4a.bin         33591768
7    : c2600-advipservicesk9-mz.124-15.T1.bin         33591768
8    : c2600-i-mz.122-28.bin                          5571584
9    : c2600-ipbasek9-mz.124-8.bin                    13169700
10   : c2800nm-advipservicesk9-mz.124-15.T1.bin       50938004
11   : c2800nm-advipservicesk9-mz.151-4.M4.bin        33591768
12   : c2800nm-ipbase-mz.123-14.T7.bin                5571584
13   : c2800nm-ipbasek9-mz.124-8.bin                  15522644
14   : c2900-universalk9-mz.SPA.155-3.M4a.bin         33591768
15   : c2950-i6q4l2-mz.121-22.EA4.bin                 3058048
16   : c2950-i6q4l2-mz.121-22.EA8.bin                 3117390
17   : c2960-lanbase-mz.122-25.FX.bin                 4414921
18   : c2960-lanbase-mz.122-25.SEE1.bin               4670455
19   : c2960-lanbasek9-mz.150-2.SE4.bin               4670455
20   : c3560-advipservicesk9-mz.122-37.SE1.bin        8662192
21   : c3560-advipservicesk9-mz.122-46.SE.bin         10713279
22   : c800-universalk9-mz.SPA.152-4.M4.bin           33591768
23   : c800-universalk9-mz.SPA.154-3.M6a.bin          83029236
24   : cat3k_caa-universalk9.16.03.02.SPA.bin         505532849
25   : cgr1000-universalk9-mz.SPA.154-2.CG            159487552
26   : cgr1000-universalk9-mz.SPA.156-3.CG            184530138
27   : ir800-universalk9-bundle.SPA.156-3.M.bin       160968869
28   : ir800-universalk9-mz.SPA.155-3.M               61750062
29   : ir800-universalk9-mz.SPA.156-3.M               63753767
30   : ir800_yocto-1.7.2.tar                          2877440
31   : ir800_yocto-1.7.2_python-2.7.3.tar             6912000
32   : pt1000-i-mz.122-28.bin                         5571584
33   : pt3000-i6q4l2-mz.121-22.EA4.bin                3117390
ftp>get PktFile.txt

Reading file PktFile.txt from arjun-60.com:
File transfer in progress...

[Transfer complete - 134 bytes]

134 bytes copied in 0.035 secs (3828 bytes/sec)
ftp>quit
```

Smartphone0

Physical Config Desktop Programming Attributes

Text Editor

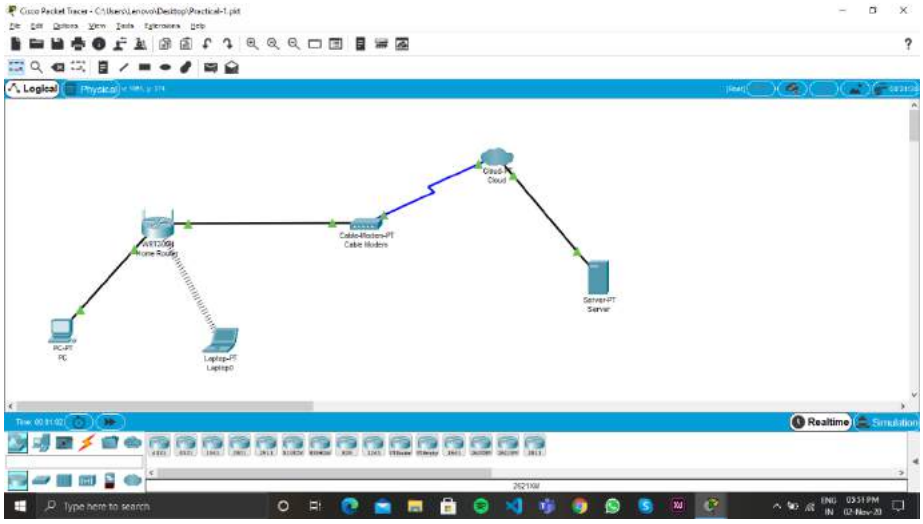
File

Good Morning !
Hello from Arjun Vankani !!
This is Cisco Packet Tracer to sending file in My laptop to accesabile another pc or Phone.

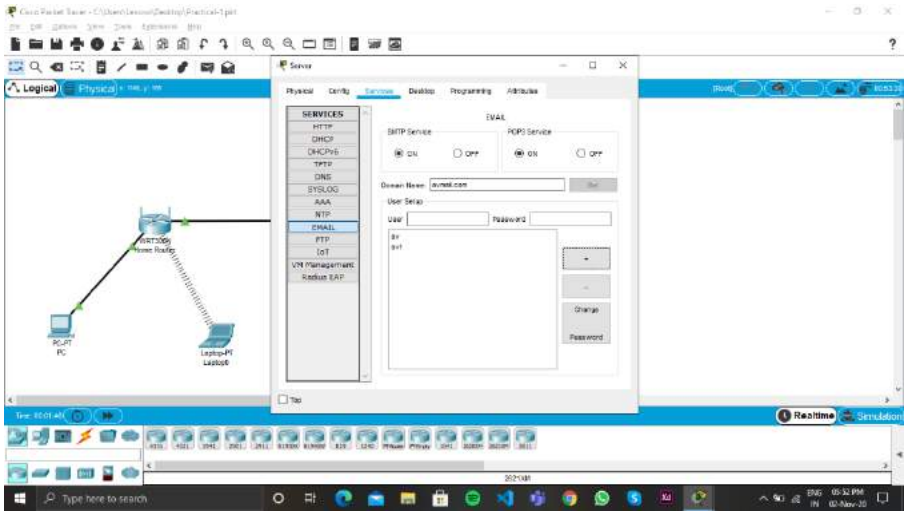
Computer Network Lab session 14

Q-1) Use the network topology used in DNS configuration (add one more end device) and perform SMTP configuration on the server. After configuration, both the device should be able to send and receive email to each other.

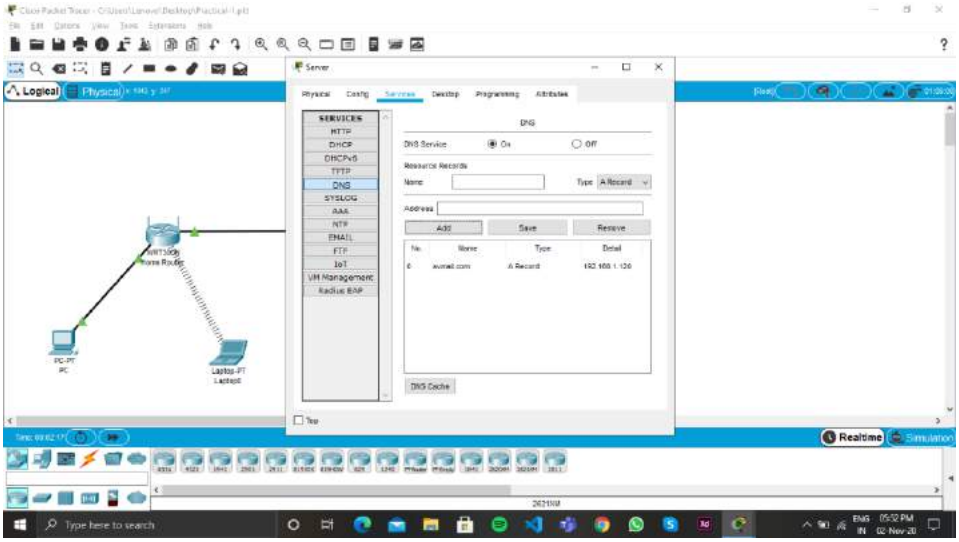
- **Topology**



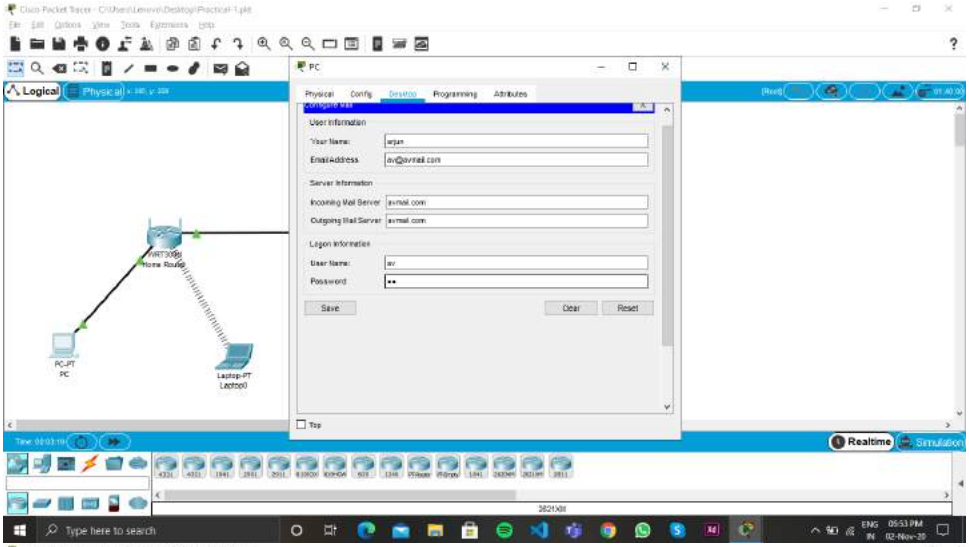
- **Configure SMTP service on server.**

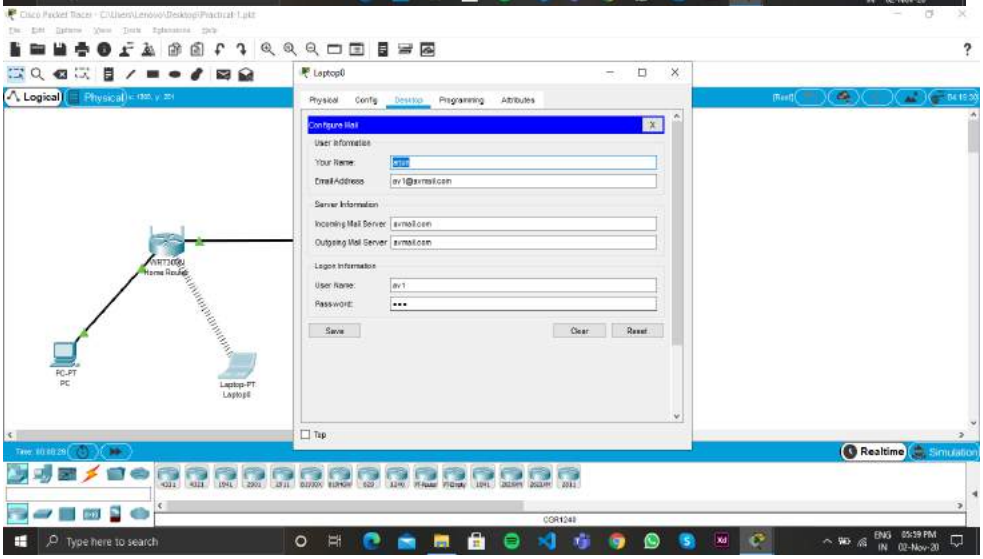


- **Add “avmail.com” in DNS record.**

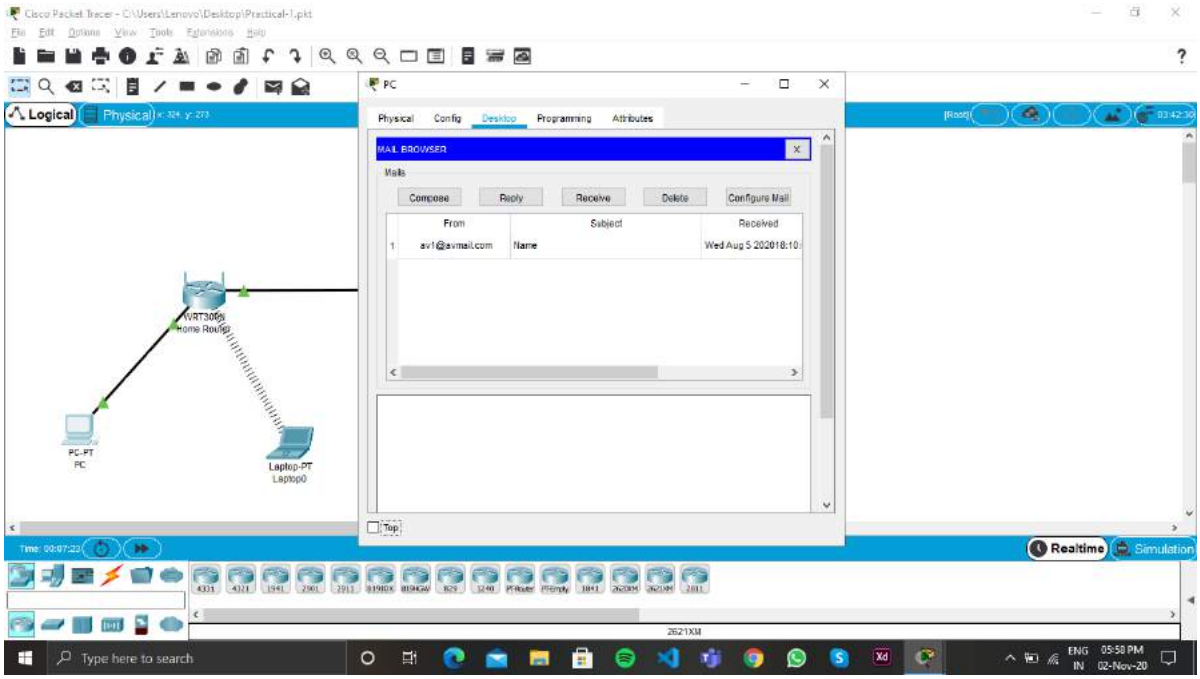


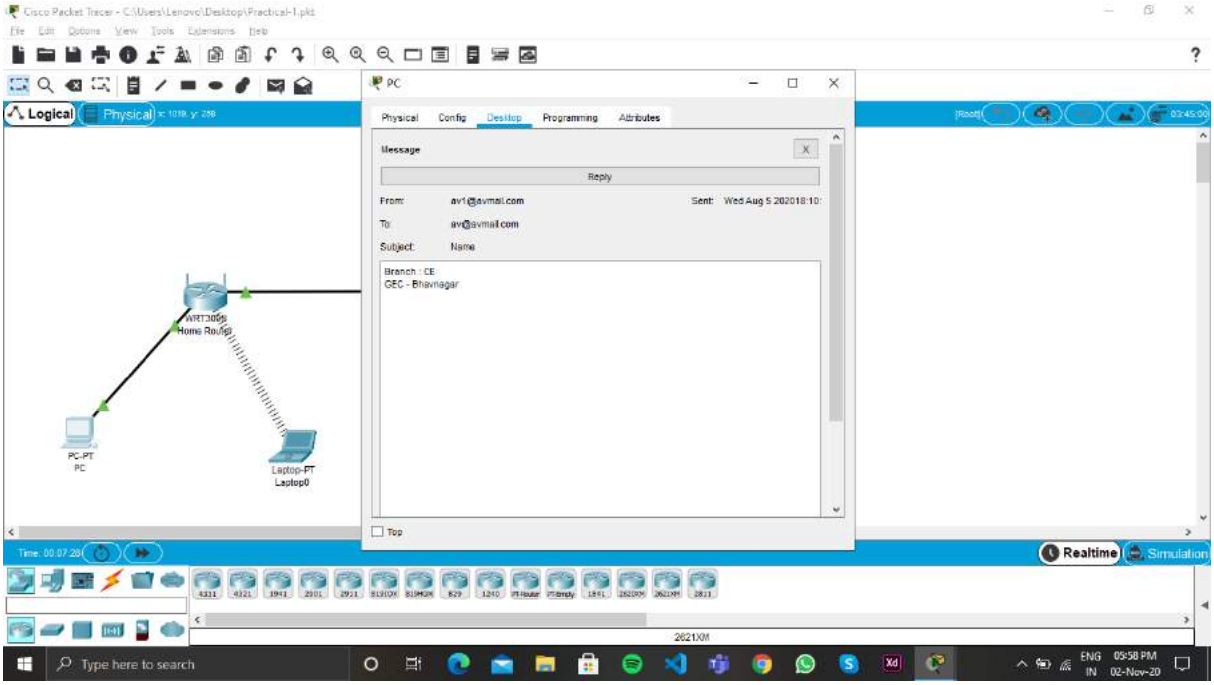
- **Create email and login**



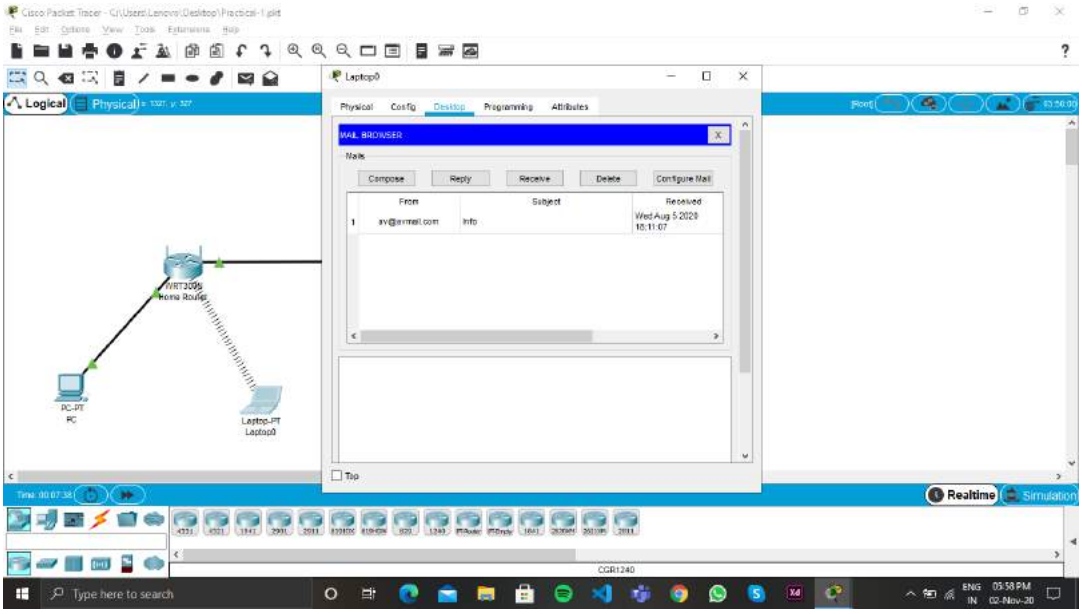


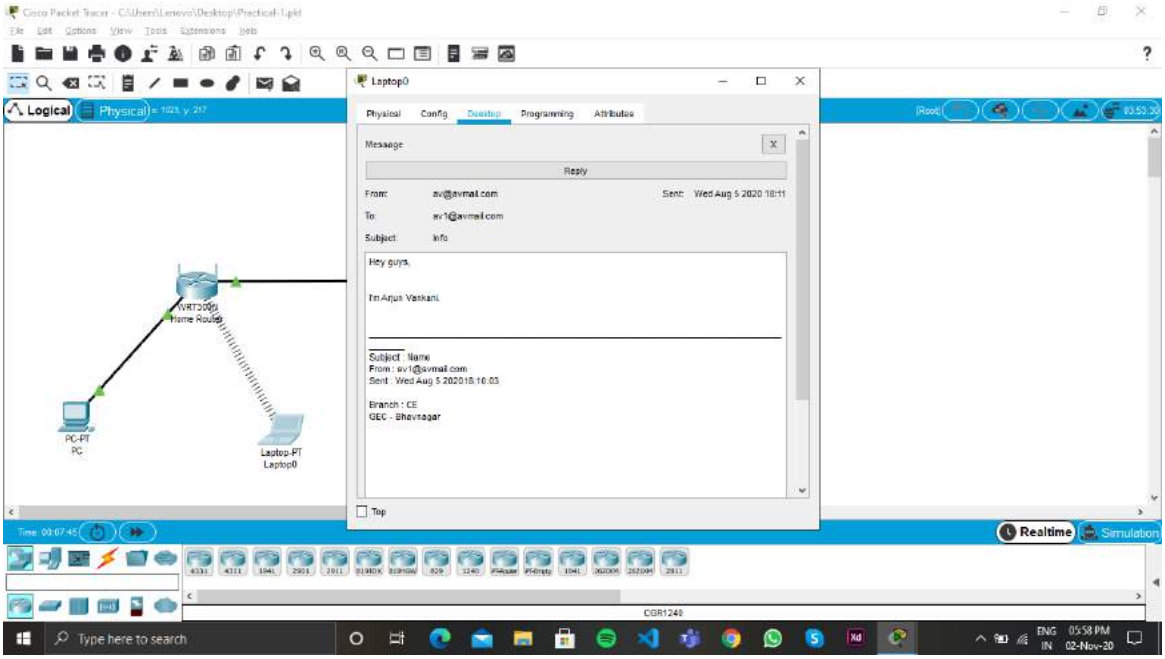
➢ Send emails:


Cisco Packet Tracer - C:\Users\Lenovo\Desktop\Practical-1.pkt
Logical
Physical
PC
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
av1@avmail.com
Name
Wed Aug 5 202018:10
WRT300N
Home Router
PC-PT
PC
Laptop-PT
Laptop0
Top
Realtime
Simulation
Type here to search
ENG
IN
05:58 PM
02-Nov-20


Cisco Packet Tracer - C:\Users\Lenovo\Desktop\Practical-1.pkt
Logical
Physical
PC
Physical
Config
Desktop
Programming
Attributes
Message
Reply
From:
av1@avmail.com
Sent:
Wed Aug 5 202018:10
To:
av@avmail.com
Subject:
Name
Branch : CE
GEC - Bhavnagar
WRT300N
Home Router
PC-PT
PC
Laptop-PT
Laptop0
Top
Realtime
Simulation
Type here to search
ENG
IN
05:58 PM
02-Nov-20

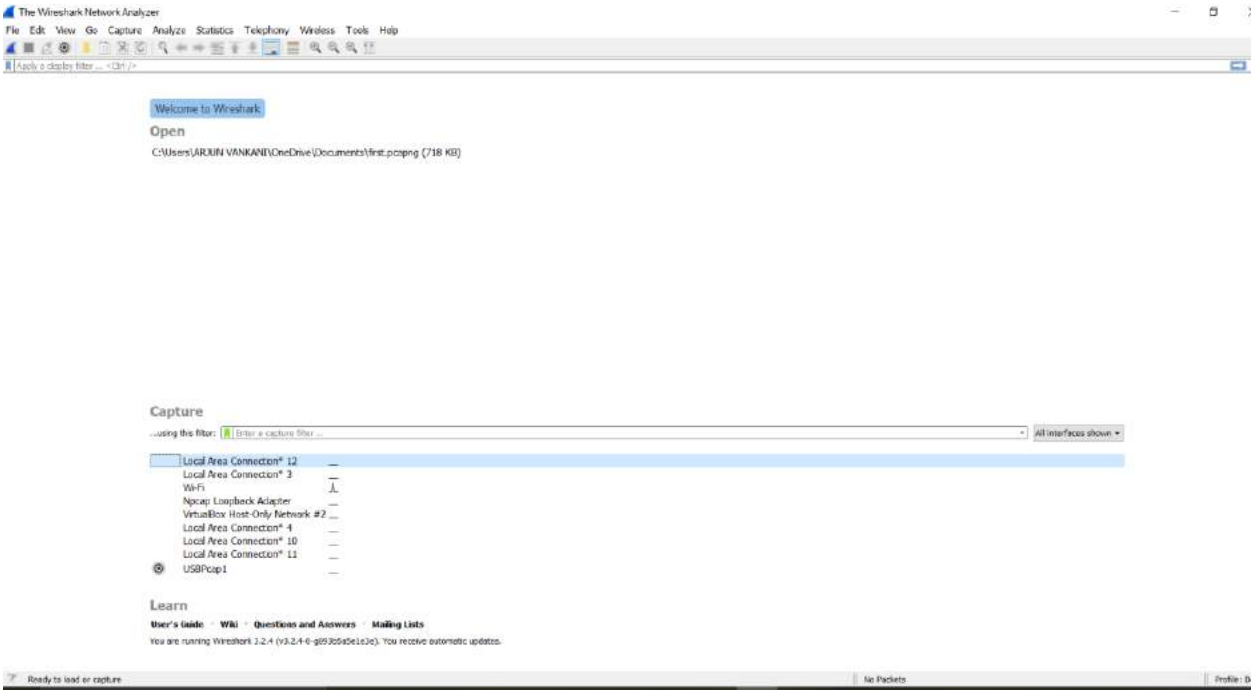
➢ Receiving mail



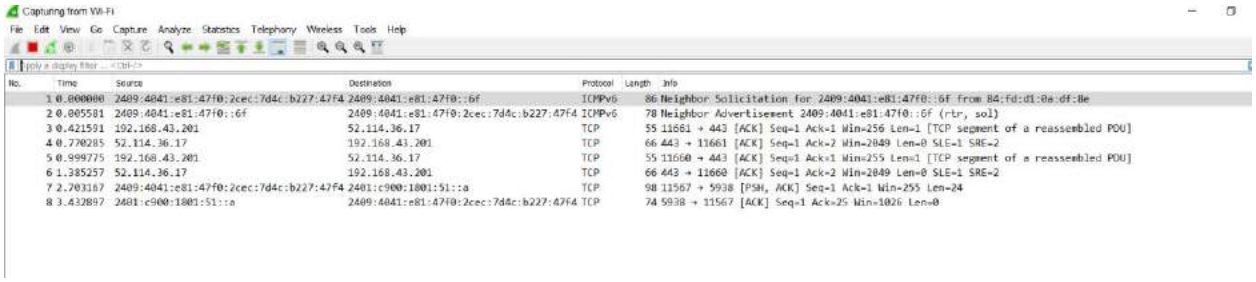


Computer Network LAB (Session -8)

- Packet capture and header analysis by Wireshark
- **Download and install Wireshark(https://www.wireshark.org/).**
- First, we have to download Wireshark is the world's foremost and widely-used network protocol analyzer.
- And mostly it used for Ip tracing as well as all know about all layer's handshaking and data transfer protocol.

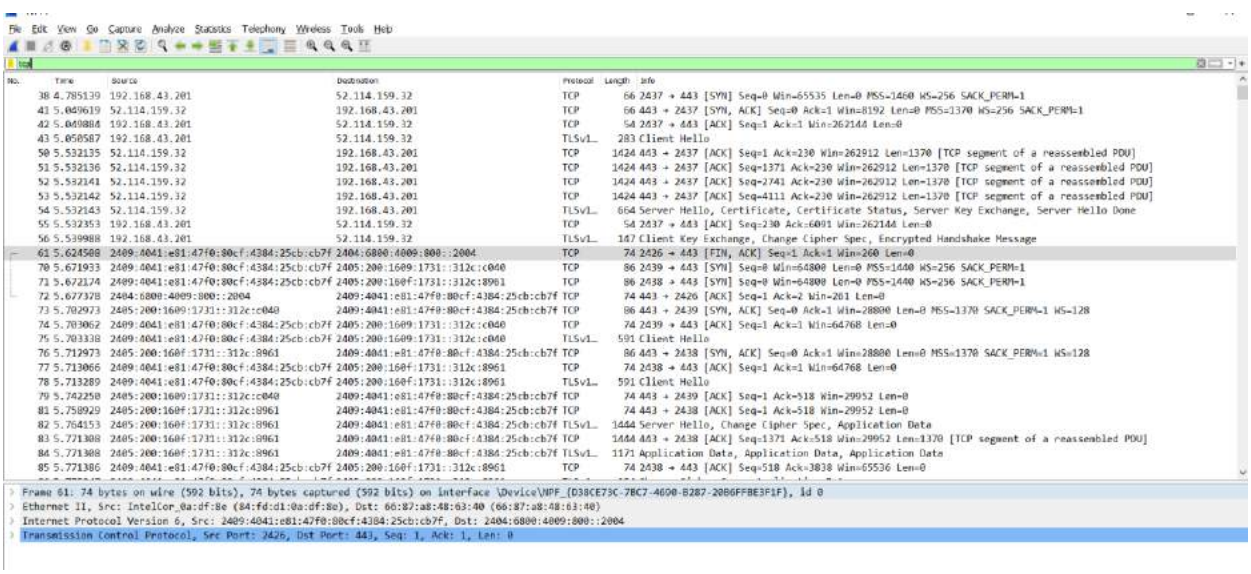


- This is Wireshark, if we want to analysis protocol then clicks on Wi-Fi connection and Start capture.
- After Start kernel that was shown below



Q-A) Access a website and capture the protocol message being exchanged between your web browser and the web server.

- Frist, we requesting for URL to send data that why opening browser and search for website.



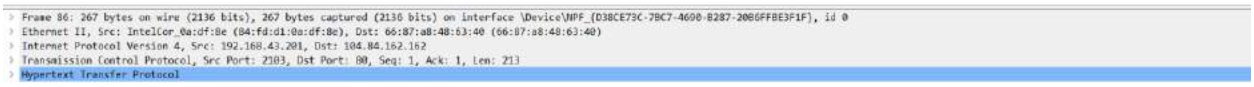
- TCP means transmission control protocol.

- This is Ipv4 and data bytes are (600bits) where UDP source port 58453 and destination port 53 length 41.

- For message and query requesting for seq num and ack is shown above figure for Client say Hello
- Seq =1, ack =230, Len =1370
  Seq = 1371, ack=230, Len=1370
  And after Server say Hello
  Seq = 230, Ack=6091, Len =0
  Now Encrypted handshaking for message.

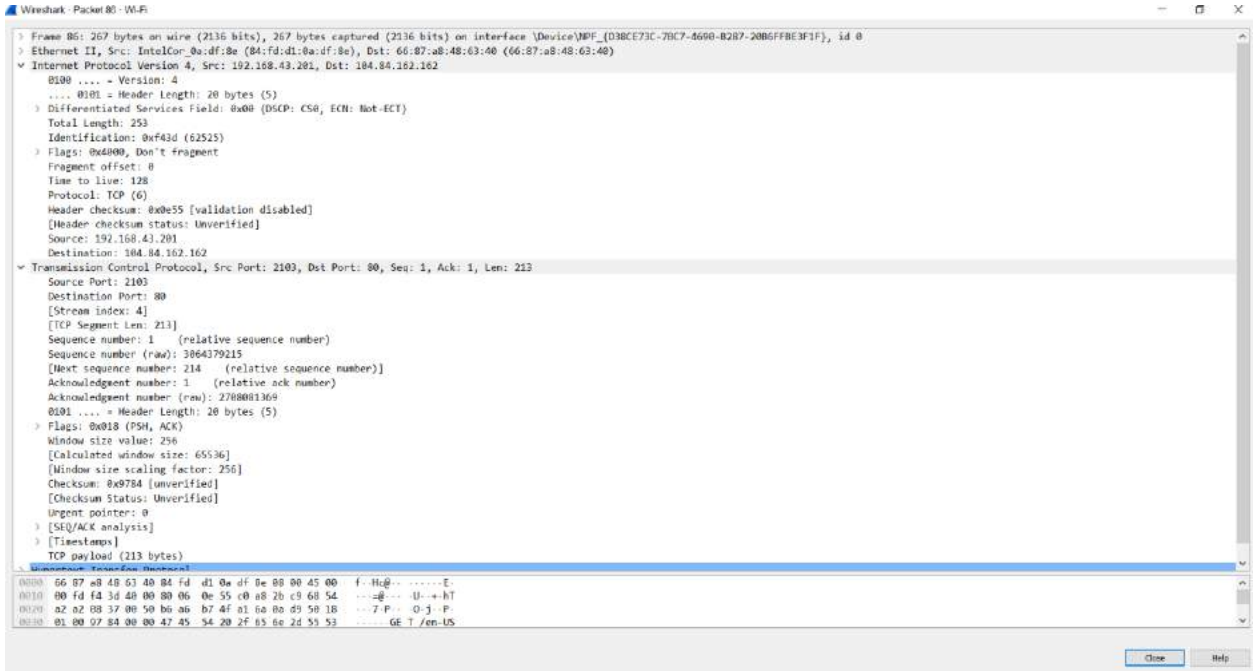
Q-B) Explore different aspect of HTTP protocol, GET/reply interaction, HTTP message format, persistent and non-persistent HTTP connections.

- Http stands for Hypertext transfer protocol.
- Where we start website and it req for HTTP ok response. After that cache will shown our web data if we are going to second time on this website.



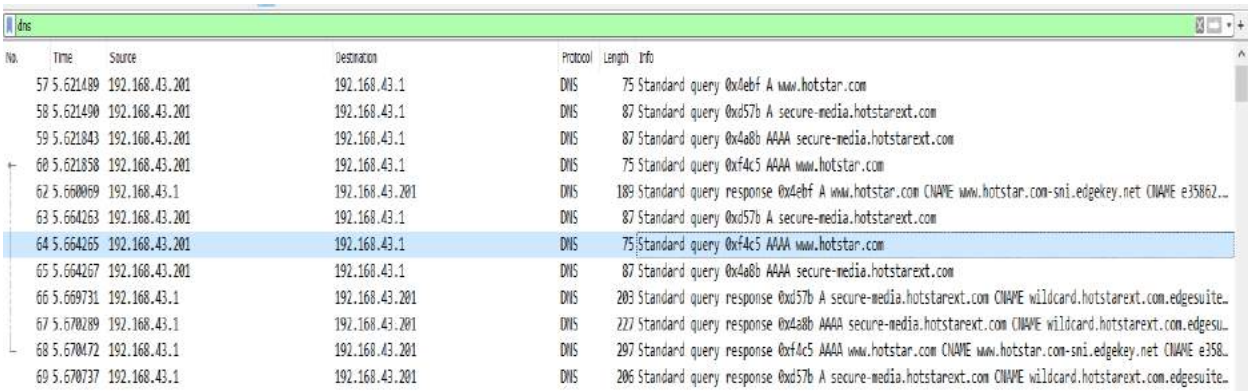
- Here, Fig shows source ip 192.168.43.201 when we req to load data at that time GET method is used and data Length 267.

After second server is source when it gives OK response to us that is why both source and destination changed.



- Data length is 2136 bits and IPv4 with source-ip 192.168.43.201 and destination-ip 104.84.162.162 for Hotstar-ip, with source-port: 2103 and des-port :80 For HTTP. 1.1 version represent connection close and Persistent connection.
- In HTTP/1.0 the connection is non-persistent by default unless you add the Connection: keep-alive.
- In HTTP/1.1 the connection is persistent by default unless you add the Connection: close

Q-C) Explore the process of resolving a DNS query, recursive/iterative communication between different DNS servers and DNS response from different DNS servers.

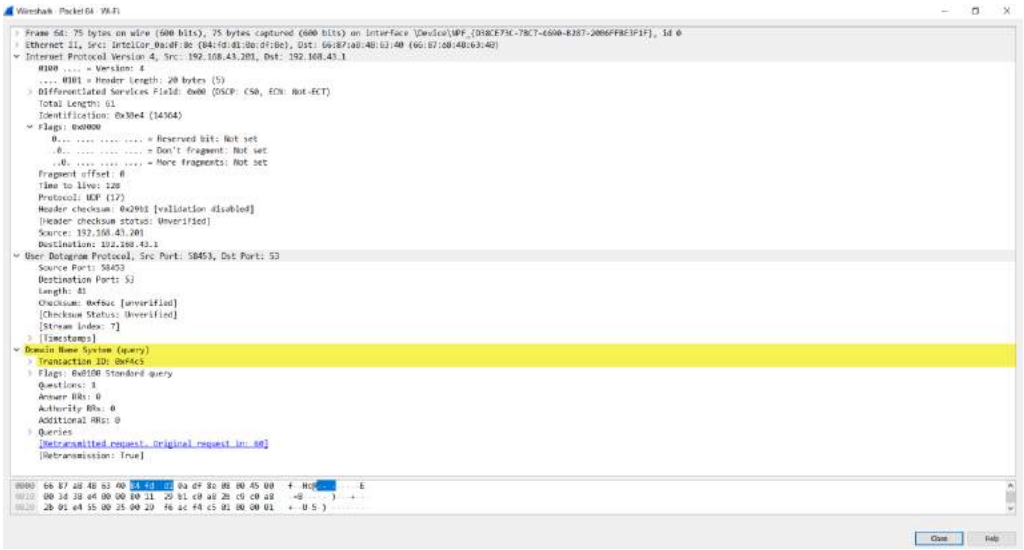


dns

No.	Time	Source	Destination	Protocol	Length	Info
57	5.621489	192.168.43.201	192.168.43.1	DNS	75	Standard query 0x4ebf A www.hotstar.com
58	5.621490	192.168.43.201	192.168.43.1	DNS	87	Standard query 0xd57b A secure-media.hotstarext.com
59	5.621843	192.168.43.201	192.168.43.1	DNS	87	Standard query 0x4a8b AAAA secure-media.hotstarext.com
60	5.621858	192.168.43.201	192.168.43.1	DNS	75	Standard query 0xf4c5 AAAA www.hotstar.com
62	5.660069	192.168.43.1	192.168.43.201	DNS	189	Standard query response 0x4ebf A www.hotstar.com CNAME www.hotstar.com-sni.edgekey.net CNAME e35862...
63	5.664263	192.168.43.201	192.168.43.1	DNS	87	Standard query 0xd57b A secure-media.hotstarext.com
64	5.664265	192.168.43.201	192.168.43.1	DNS	75	Standard query 0xf4c5 AAAA www.hotstar.com
65	5.664267	192.168.43.201	192.168.43.1	DNS	87	Standard query 0x4a8b AAAA secure-media.hotstarext.com
66	5.669731	192.168.43.1	192.168.43.201	DNS	203	Standard query response 0xd57b A secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesuite...
67	5.670289	192.168.43.1	192.168.43.201	DNS	227	Standard query response 0x4a8b AAAA secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesu...
68	5.670472	192.168.43.1	192.168.43.201	DNS	297	Standard query response 0xf4c5 AAAA www.hotstar.com CNAME www.hotstar.com-sni.edgekey.net CNAME e358...
69	5.670737	192.168.43.1	192.168.43.201	DNS	206	Standard query response 0xd57b A secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesuite...

- DNS is Domain name server.

- Now we are opening Google browser and https://www.hotstar.com/ search this URL for capturing query and response.
- DNS req is going through many sources and also destination is more than one. Shown above figure
- DNS server firstly req query to server and waiting for its response or ack.
- Here, Source ip is 192.168.43.1 Which is our laptop ip address and Destination ip is 192.168.43.201



- Ipv4 with source and destination share UDP source-port: 58453 and destination-port: 53 where length 41 (600bits) sending. And All flag shown above as Question: 1, Answer: 0, Authority: 0, Additional:0, as well as Queries requesting for answer

- OSI Model shown below work with Wireshark.

1) Application layer as HTTP format

- Which is shown above Hypertext transfer protocol. The HTTP is our Application layer, with its own headers. HTTP is an application protocol for distributed, collaborative, hypermedia information systems.

2) Transport layer as TCP/UDP

- TCP is connection oriented and a connection between client and server is established before data can be sent. UDP uses a simple connectionless communication model with a minimum of protocol mechanisms.

3) Network Layer

- It includes the process of ICMP protocols, ICMP stands for Internet control message protocol.

4) Data link layer

- The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. ARP stands for address resolution protocol works with data link layer.

Computer Network (Lab session -11)

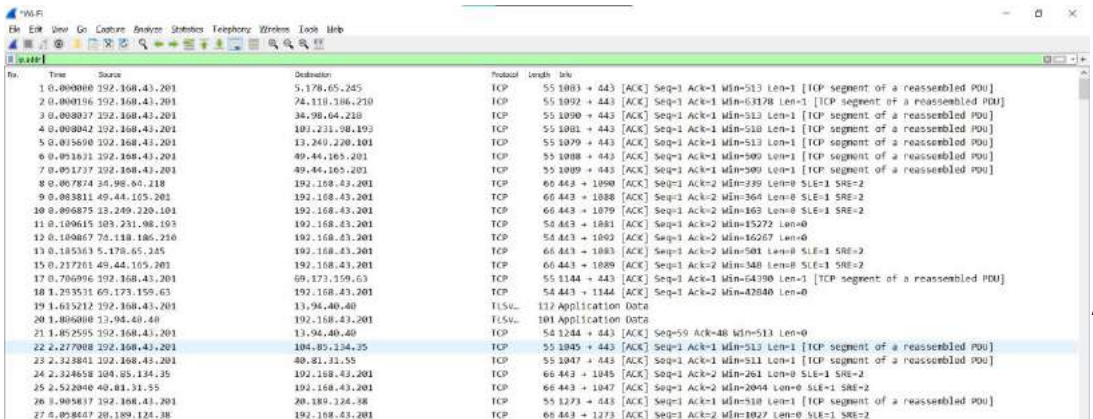
Wireshark with IP & ICMP protocol

Q-1) Wireshark Software

A -> Capture analyze IP protocol message being exchanged.

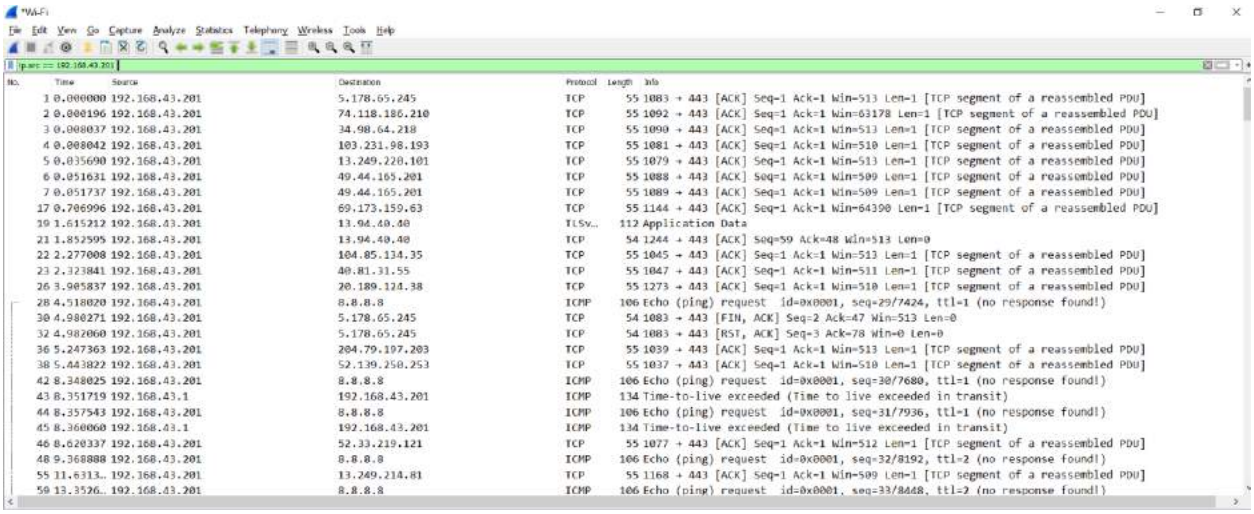
B -> Capture analyze ICMP message being exchanged.

- Wireshark is the world's foremost and widely-used network protocol analyzer. We also perform practical on TCP, UDP protocol, DNS services and HTTP response.
- Now working with IP protocol, that give us the full information about IP address. Like Source address, destination address and IPV6 address.
- IPv4 is a **32-bit address** in which each group represents 8 bits ranging from 0 to 255.
- IPv6 is a 128-bit address. Ip.addr gives the all the address where no condition.

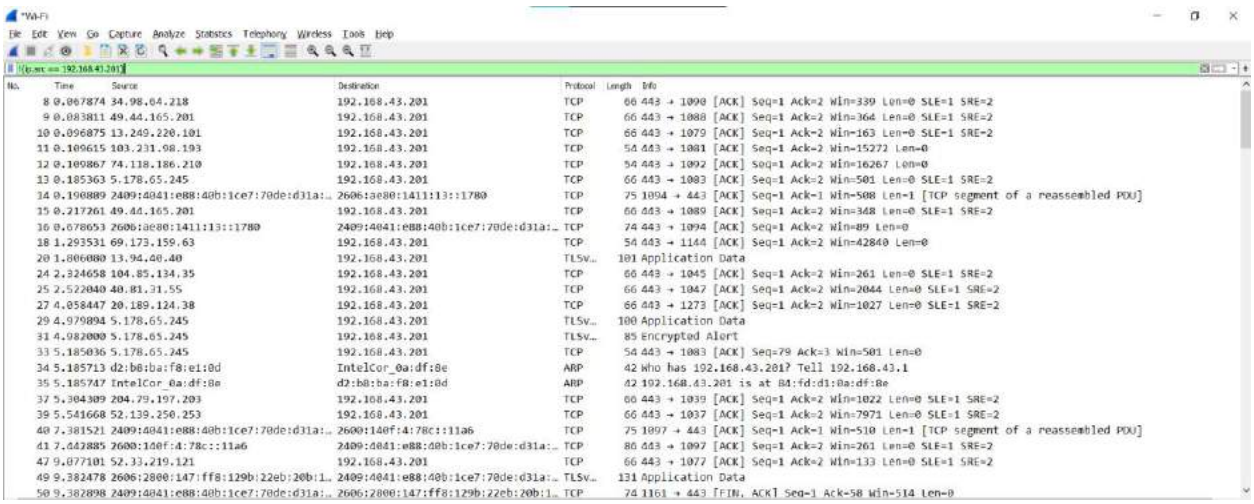


ARJUN

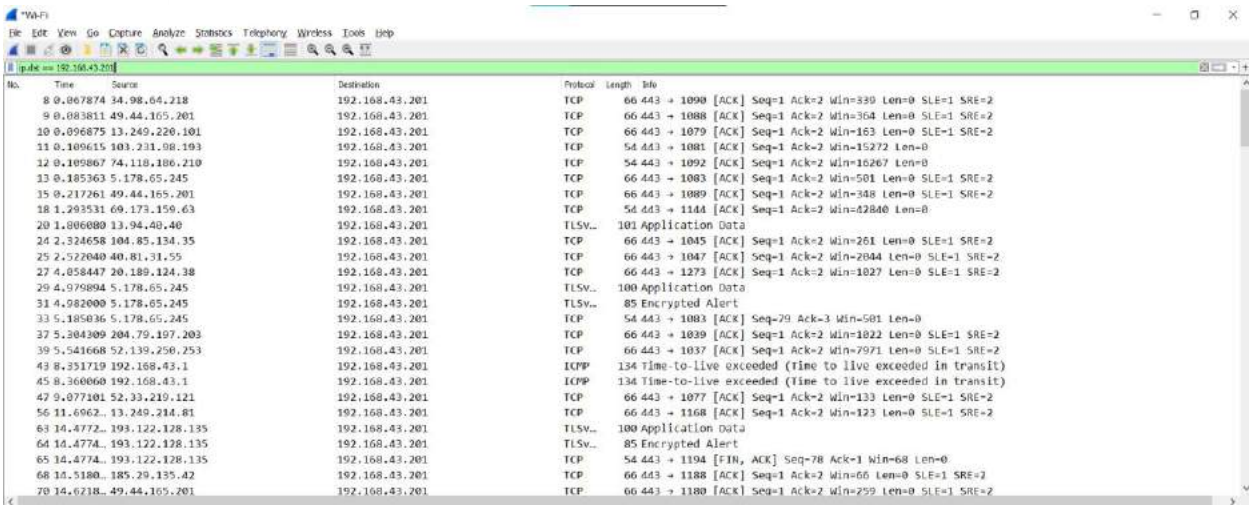
- Ip.src == 192.168.43.201 gives the source IP address where source is only on 192.168.43.201



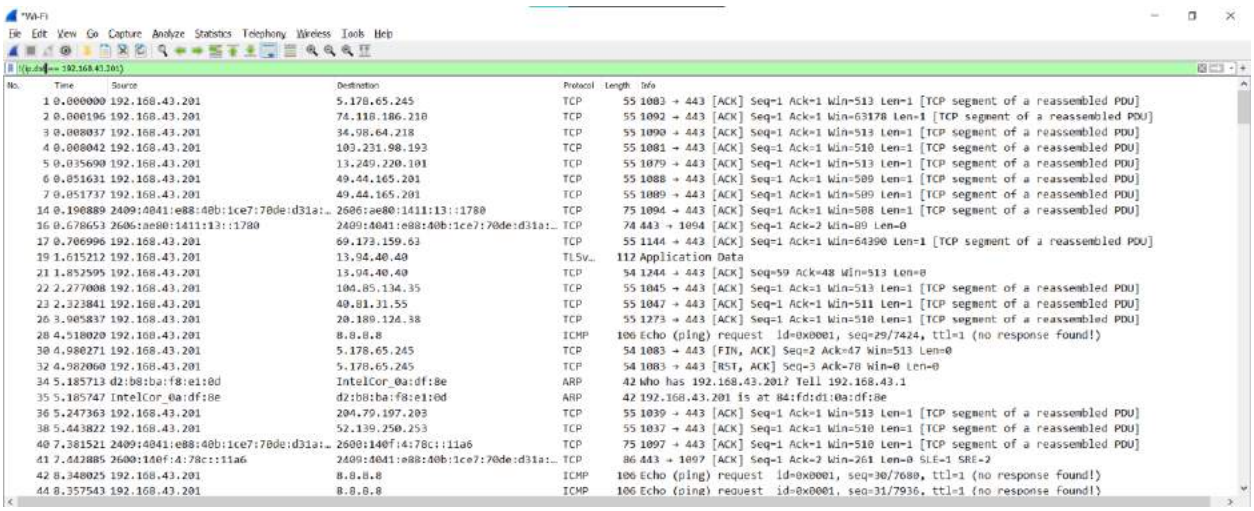
- ! (Ip.src == 192.168.43.201) gives the source IP address where source is not 192.168.43.201



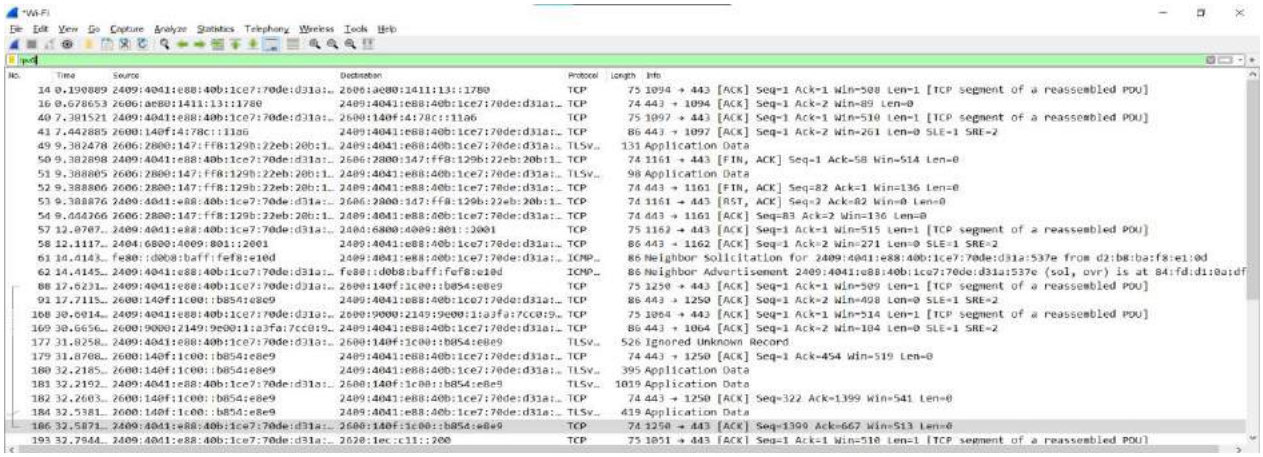
- Ip.dst == 192.168.43.201 gives the destination IP address where destination is only on 192.168.43.201



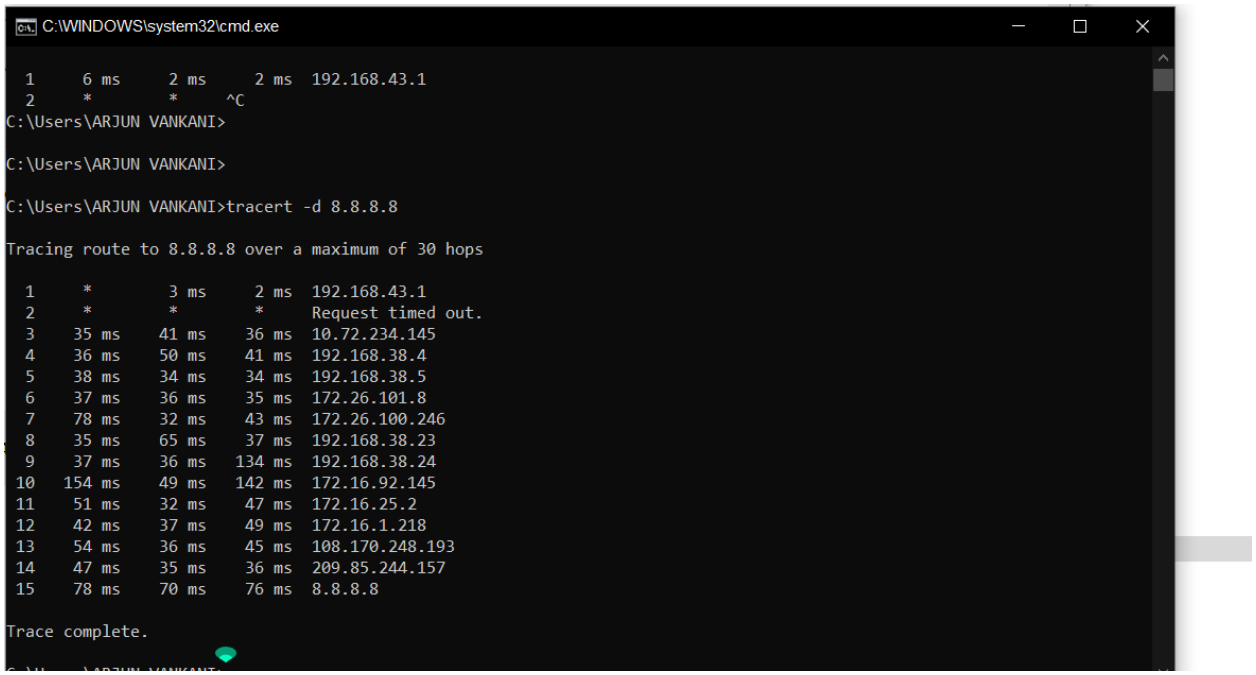
- !(Ip.dst == 192.168.43.201) gives the destination IP address where destination is not 192.168.43.201



- Ipv6 gives all IP address

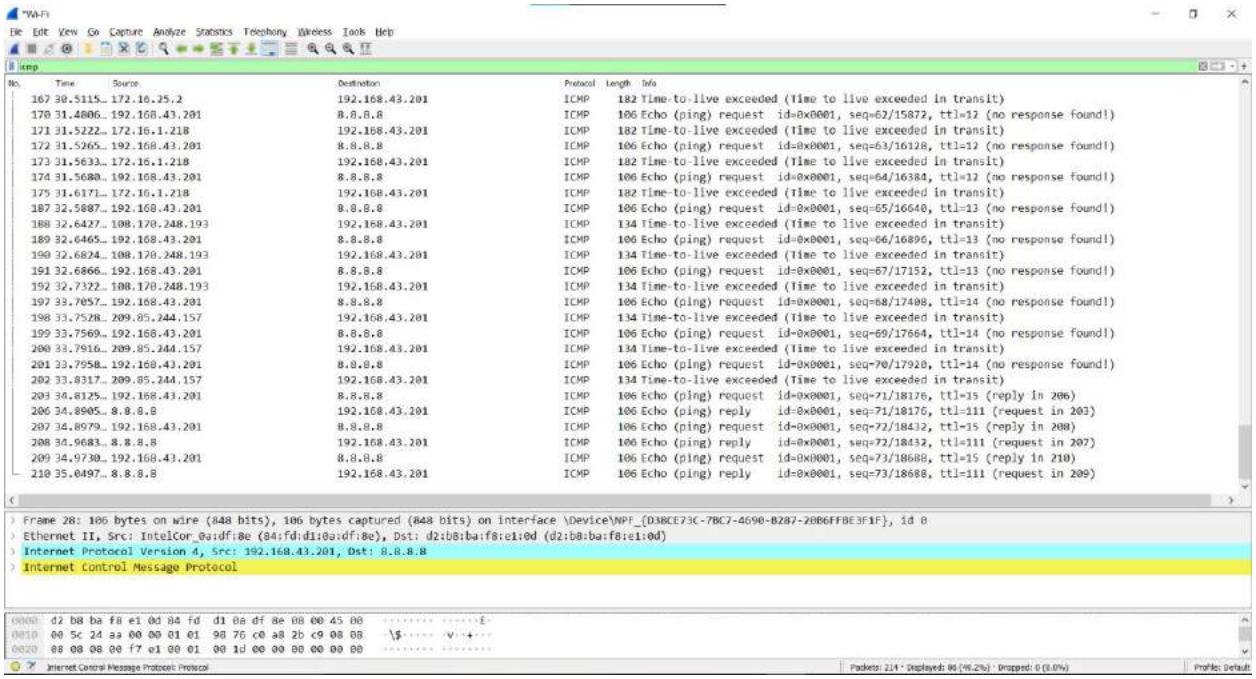


- ICMP protocol is Internet Control Message Protocol.
- Where we first run the command tracert-d 8.8.8.8 for google DNS public services.

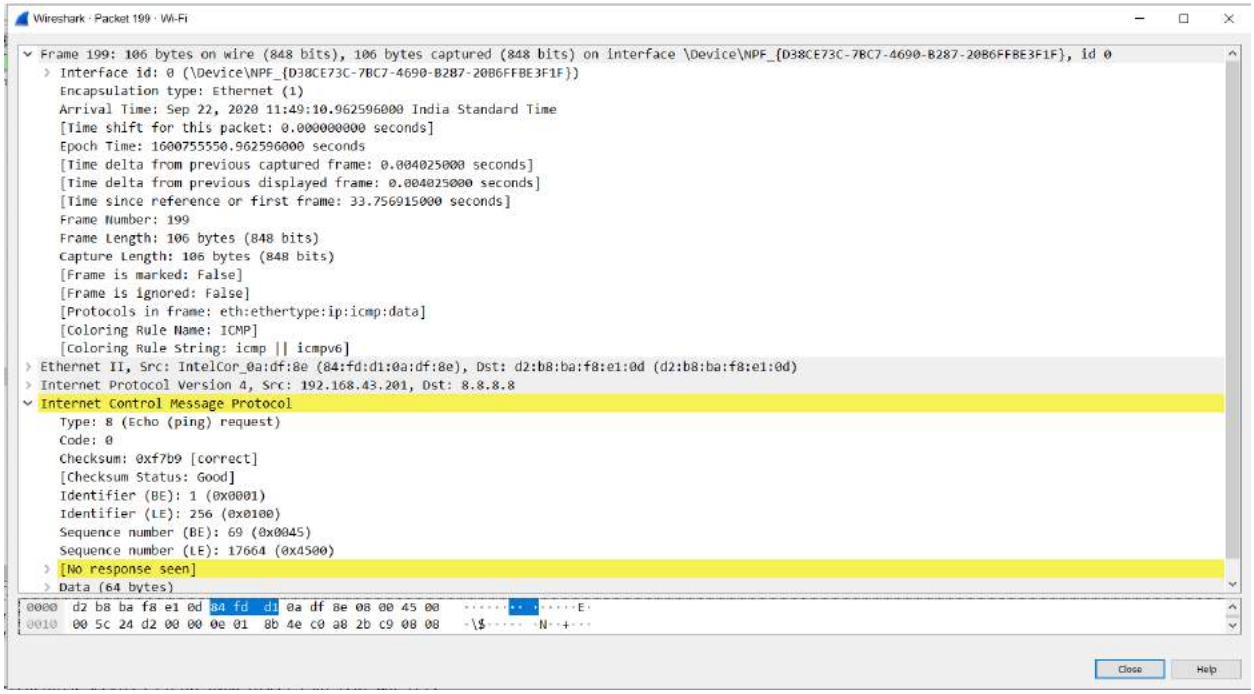


```
C:\WINDOWS\system32\cmd.exe

  1     6 ms     2 ms     2 ms  192.168.43.1
  2     *        *     ^C
C:\Users\ARJUN VANKANI>

C:\Users\ARJUN VANKANI>

C:\Users\ARJUN VANKANI>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     *        3 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    35 ms    41 ms    36 ms  10.72.234.145
  4    36 ms    50 ms    41 ms  192.168.38.4
  5    38 ms    34 ms    34 ms  192.168.38.5
  6    37 ms    36 ms    35 ms  172.26.101.8
  7    78 ms    32 ms    43 ms  172.26.100.246
  8    35 ms    65 ms    37 ms  192.168.38.23
  9    37 ms    36 ms   134 ms  192.168.38.24
 10   154 ms    49 ms   142 ms  172.16.92.145
 11    51 ms    32 ms    47 ms  172.16.25.2
 12    42 ms    37 ms    49 ms  172.16.1.218
 13    54 ms    36 ms    45 ms  108.170.248.193
 14    47 ms    35 ms    36 ms  209.85.244.157
 15    78 ms    70 ms    76 ms  8.8.8.8

Trace complete.
```

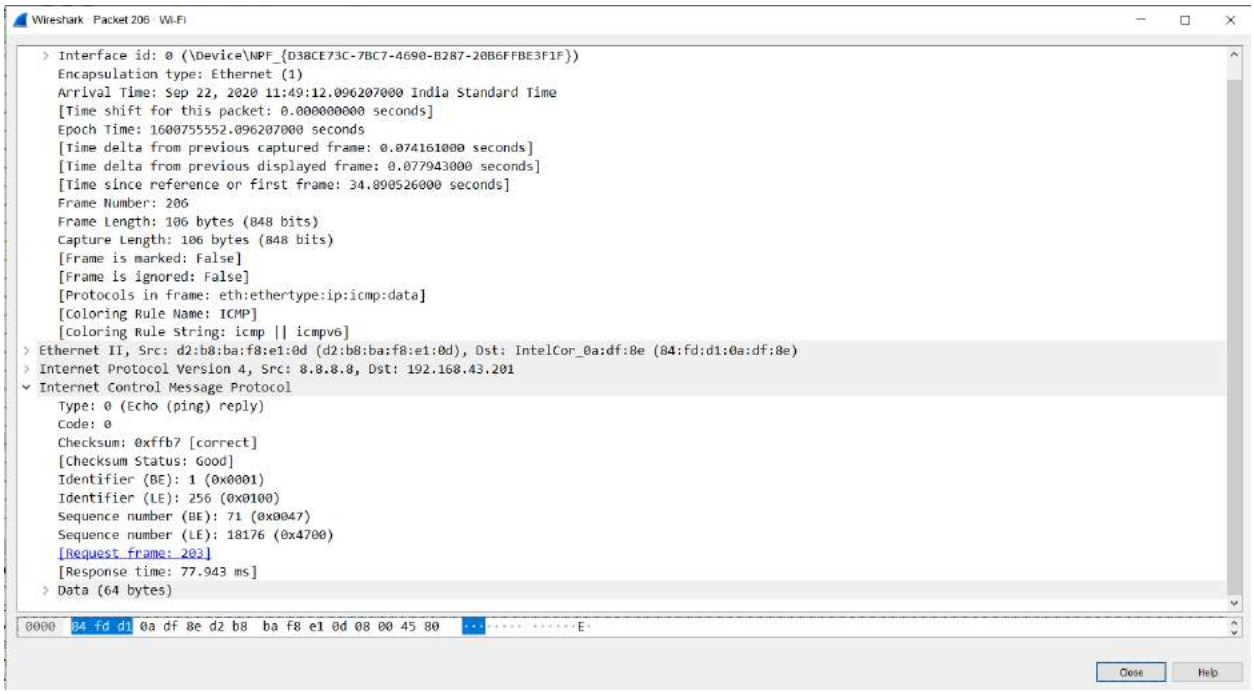
- At the time we analysis the Wireshark software ICMP protocol.



This is for message request to DNS



This is for message reply to DNS



Q-2) **Use Wireshark to analyze the network traffic of TCP and UDP Protocol.**

❖ UDP:

- We first analyze on UDP protocol in Transport layer, we know that the DNS uses the UDP protocol then we capture UDP from a DNS request of www.google.com.
- Here this DNS request is sent from google server port 53 to our system port 64029, that specified in UDP segment.

```
User Datagram Protocol, Src Port: 53, Dst Port: 64029
    Source Port: 53
    Destination Port: 64029
    Length: 268
    Checksum: 0x1d41 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  > [Timestamps]
Domain Name System (response)
    Transaction ID: 0xf442
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 14
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 12]
    [Time: 0.064875000 seconds]
```

❖ TCP:

Now on going to analyse TCP protocol where we detect synchronize flag

tcp

No.	Time	Source	Destination	Protocol	Length	Info
14	1.002864	192.168.43.184	172.217.27.196	TCP	66	3615 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	1.004980	192.168.43.184	172.217.27.196	TCP	66	3616 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	1.066440	192.168.43.184	172.217.160.170	TCP	66	3617 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	1.074088	192.168.43.184	172.217.160.205	TCP	66	3618 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
25	1.084626	172.217.27.196	192.168.43.184	TCP	66	80 → 3615 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 WS=256
26	1.084689	192.168.43.184	172.217.27.196	TCP	54	3615 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
27	1.085195	192.168.43.184	172.217.27.196	HTTP	847	GET / HTTP/1.1
30	1.090807	192.168.43.184	172.217.166.162	TCP	66	3619 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
33	1.108063	172.217.27.196	192.168.43.184	TCP	66	443 → 3616 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 WS=256
34	1.108126	192.168.43.184	172.217.27.196	TCP	54	3616 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
35	1.108479	192.168.43.184	172.217.27.196	TLSv1.3	571	Client Hello
38	1.143265	172.217.160.170	192.168.43.184	TCP	66	443 → 3617 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 WS=256
39	1.143336	192.168.43.184	172.217.160.170	TCP	54	3617 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
40	1.143730	192.168.43.184	172.217.160.170	TLSv1.3	571	Client Hello
48	1.171091	172.217.27.196	192.168.43.184	TCP	54	80 → 3615 [ACK] Seq=1 Ack=794 Win=67328 Len=0
50	1.172669	172.217.160.205	192.168.43.184	TCP	66	443 → 3618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 WS=256
51	1.172729	192.168.43.184	172.217.160.205	TCP	54	3618 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52	1.172951	192.168.43.184	172.217.160.205	TLSv1.3	571	Client Hello
54	1.180651	172.217.166.162	192.168.43.184	TCP	66	443 → 3619 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 WS=256
55	1.180733	192.168.43.184	172.217.166.162	TCP	54	3619 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
56	1.181305	192.168.43.184	172.217.166.162	TLSv1.3	571	Client Hello
58	1.194560	172.217.27.196	192.168.43.184	TCP	54	443 → 3616 [ACK] Seq=1 Ack=518 Win=66816 Len=0
77	1.216663	172.217.160.170	192.168.43.184	TCP	54	443 → 3617 [ACK] Seq=1 Ack=518 Win=66816 Len=0
84	1.228919	172.217.160.205	192.168.43.184	TCP	54	443 → 3618 [ACK] Seq=1 Ack=518 Win=66816 Len=0
85	1.230727	172.217.166.162	192.168.43.184	TCP	54	443 → 3619 [ACK] Seq=1 Ack=518 Win=66816 Len=0
95	1.254016	172.217.27.196	192.168.43.184	HTTP	1004	HTTP/1.1 302 Found (text/html)
96	1.255859	172.217.27.196	192.168.43.184	TLSv1.3	1424	Server Hello, Change Cipher Spec
97	1.256101	172.217.27.196	192.168.43.184	TLSv1.3	1317	Application Data
98	1.256146	192.168.43.184	172.217.27.196	TCP	54	3616 → 443 [ACK] Seq=518 Ack=2634 Win=65536 Len=0
100	1.265621	192.168.43.184	172.217.27.196	TLSv1.3	118	Change Cipher Spec, Application Data

A) Frist sent a segment with SYN to google.com that is located in 16th line in figure.

```
> Internet Protocol Version 4, Src: 192.168.43.184, Dst: 172.217.27.196
v Transmission Control Protocol, Src Port: 3616, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 3616
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2608526033
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··********S·]
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x20fa [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (
```

B) 2nd server response with SYN and ACK that located on 33rd line in figure.

```
Transmission Control Protocol, Src Port: 443, Dst Port: 3616, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 3616
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 1779241725
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 2608526034
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·******A··S·]
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x9f29 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK
```

C) 3rd last ACK can send by user that located on 58th line in figure.

```
Internet Protocol Version 4, Src: 192.168.43.184, Dst: 172.217.27.196
Transmission Control Protocol, Src Port: 3616, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 3616
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 2608526034
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1779241726
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·******A····]
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0xdea2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
```

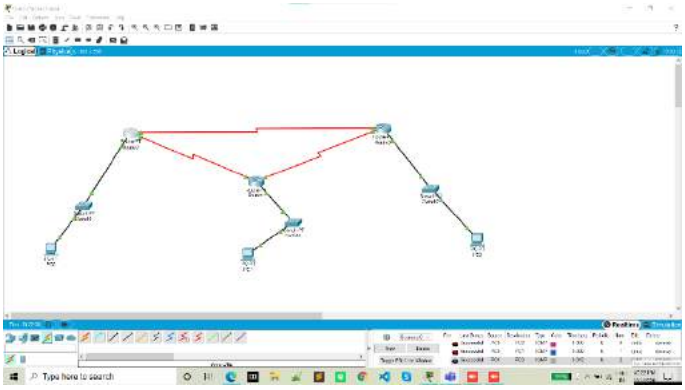
Q-3) Create a simple network topology and configure OSPF routing for data communication. Record necessary steps and screenshots.

Computer Network (Lab session 12)

Q-1) Create below topology.

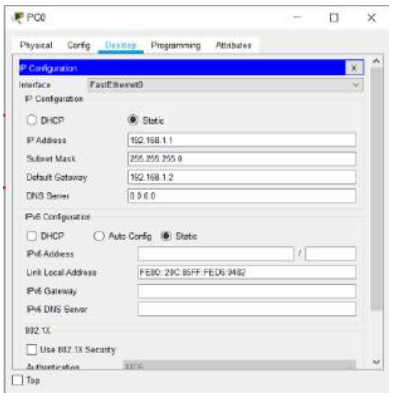
a. Provide proper IP address to each interface as displayed here in the
topology
b. Add a path such that packets from network 192.168.1.0 with destination in network 192.168.2.0 will be routed via interface 192.168.3.2
c. Add a path such that packets from network 192.168.1.0 with destination in network 192.168.4.0 will be routed via interface 192.168.5.2
d. Observe the traffic flow by switching to the simulation mode in packet
tracer
e. Write down the steps you have followed with screenshots of each
step.

- A) -> Create topology

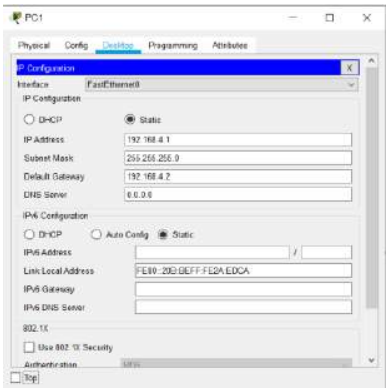


B) Now give every pc connect with switch and those switches connect with router

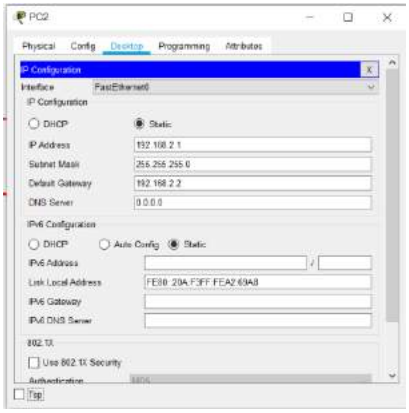
PC-0



PC-1

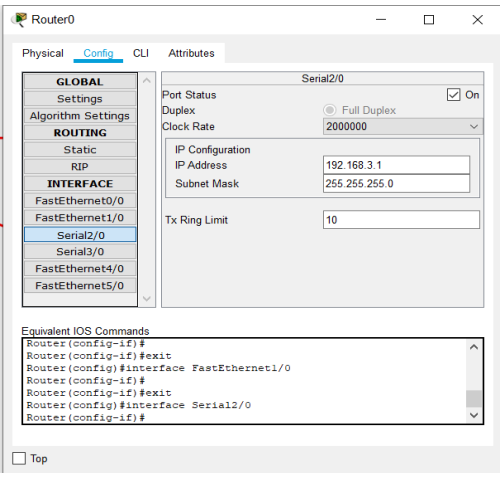


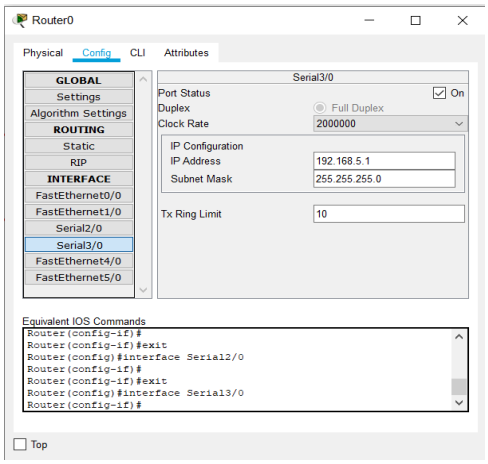
PC-2

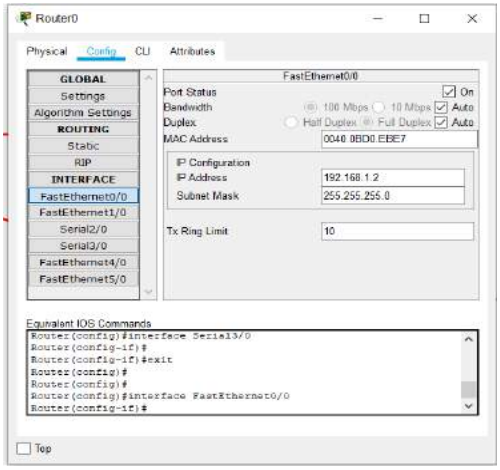


C) Router configure by connection of serial number 2-3 and Fast Ethernet.

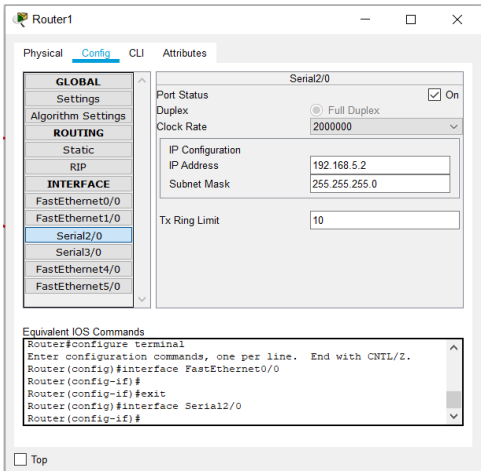
Router-0

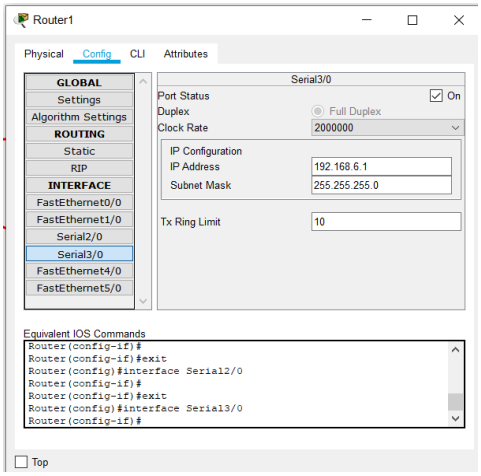


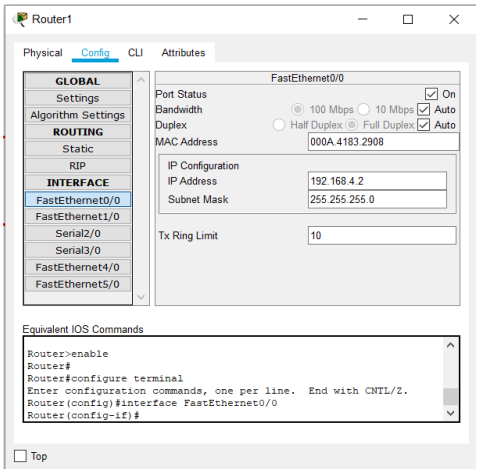




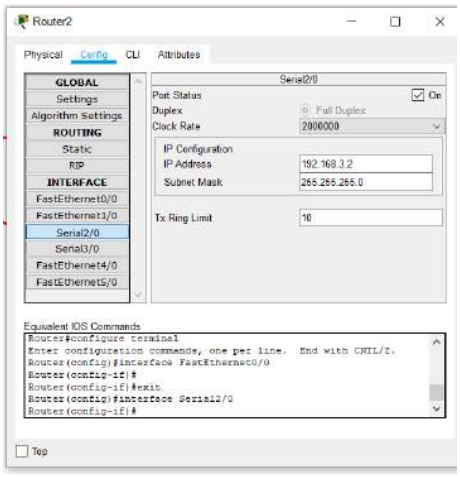
Router-1

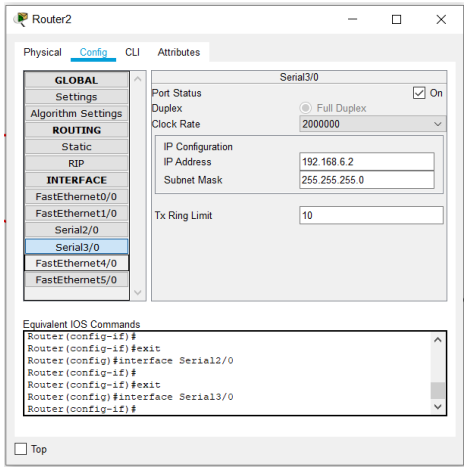


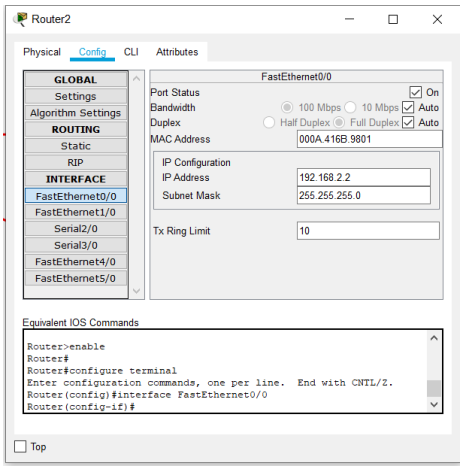




Router-2

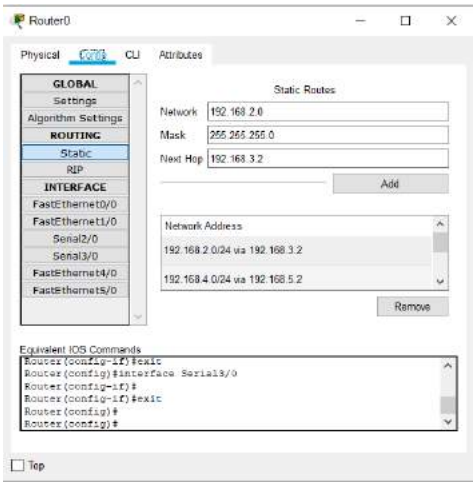


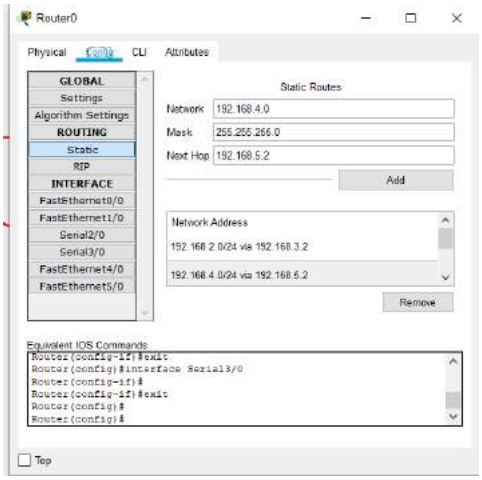




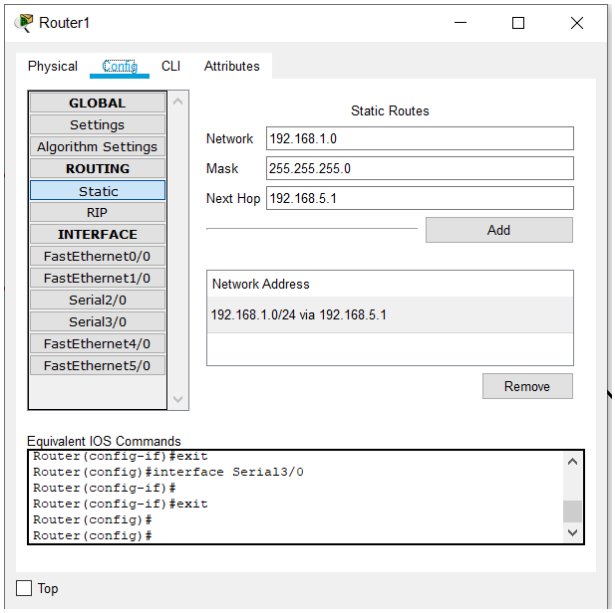
D) After set wired now, we have to give path of data sharing or routing static path

Router-0

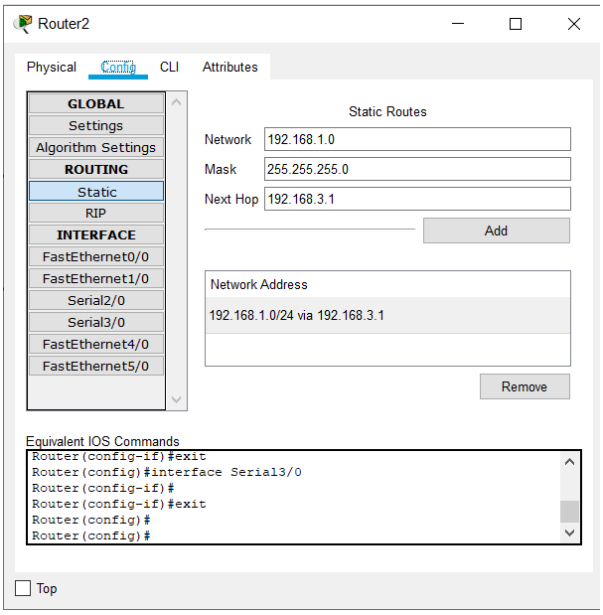




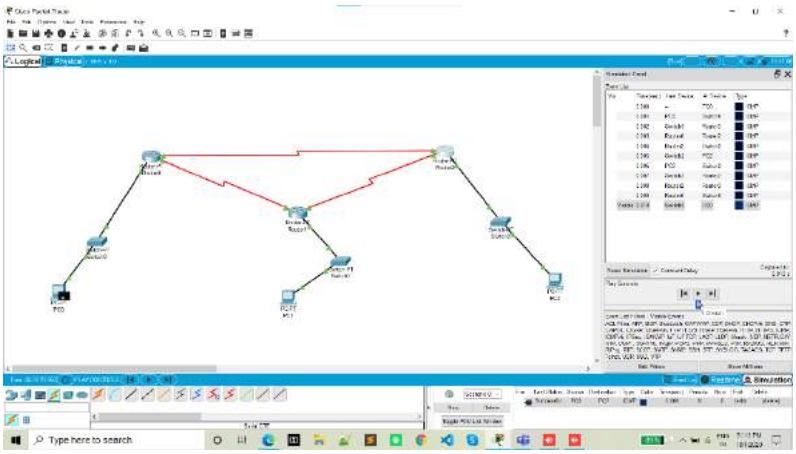
Router-1



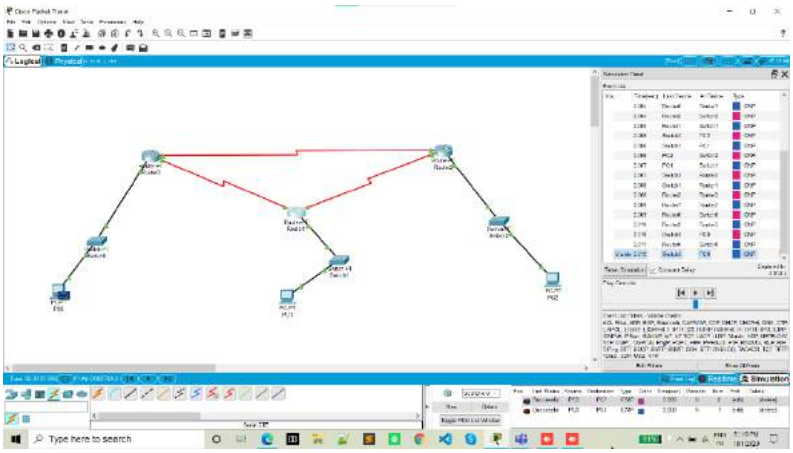
Router-2



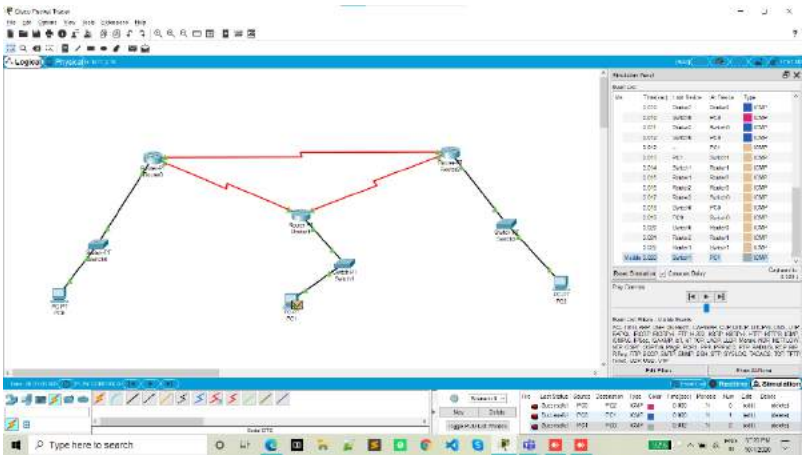
E) At last we perform to send packet on packet 0-1 and 0-2,1-0 , Those three-packet given below: Packet sending from 0-2



Packet sending from 0-1



Packet sending from 1-0

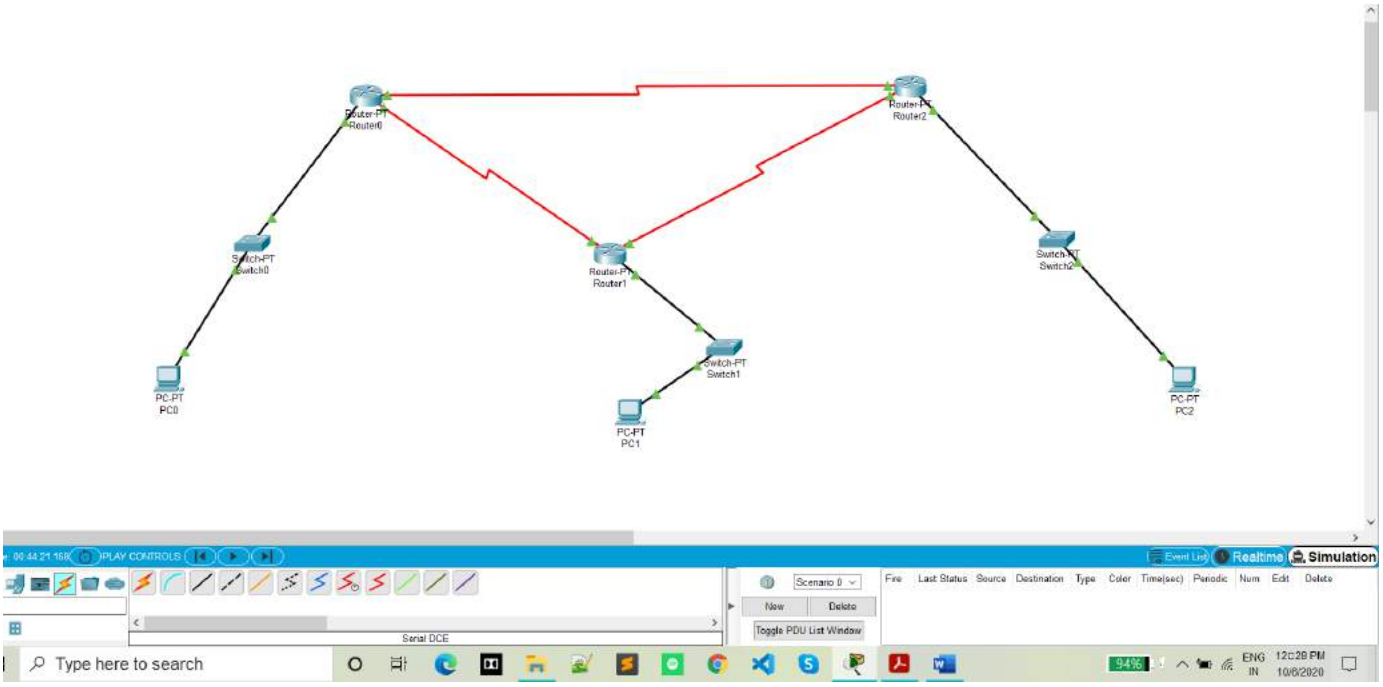


Computer Network (Lab session 13)

Q-1) Create below topology.

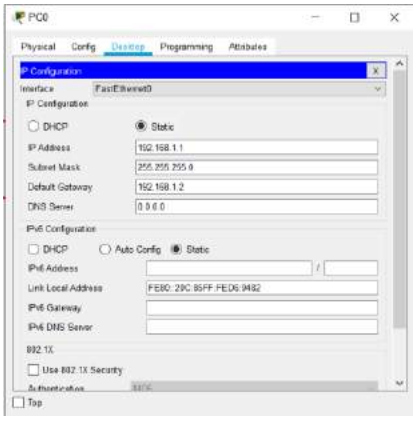
Set as RIP routing algorithm

A) -> Create topology

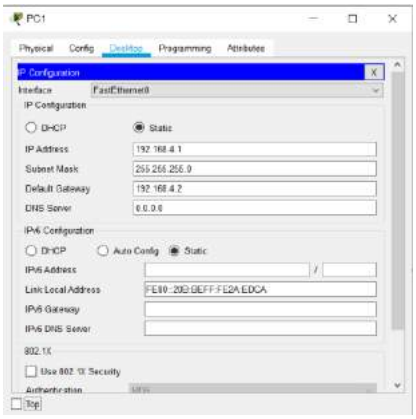


B) Now give every pc connect with switch and those switches connect with router

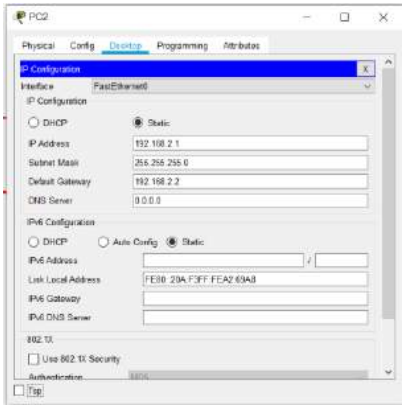
Pc-0



Pc-1

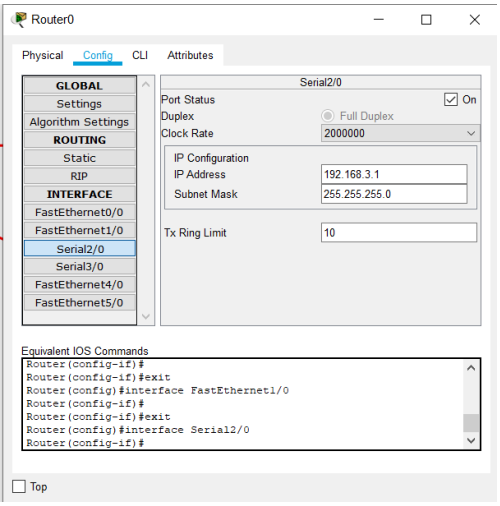


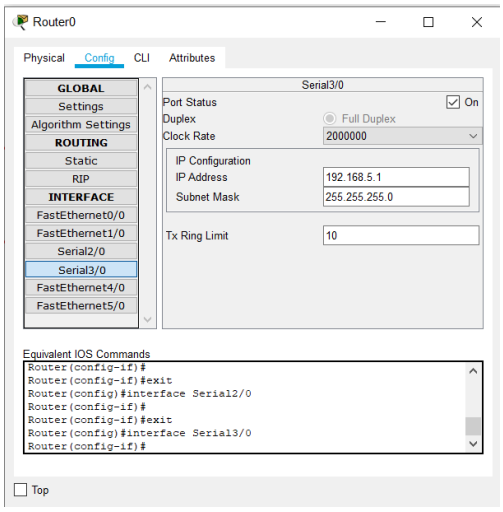
Pc-2

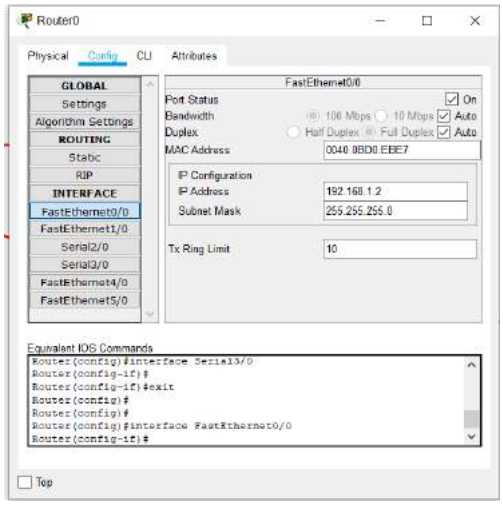


C)Router configure by connection of serial number 2-3 and Fast Ethernet.

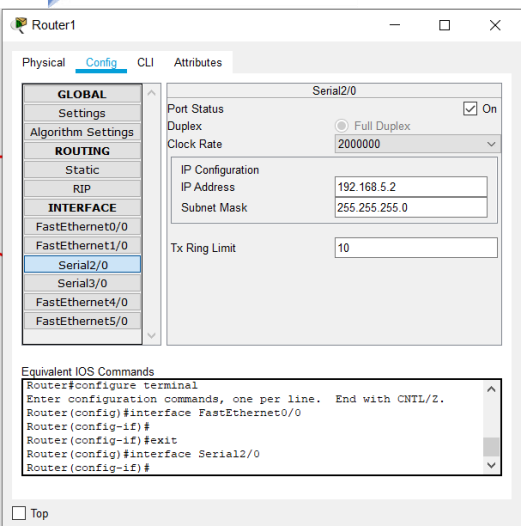
Router-0

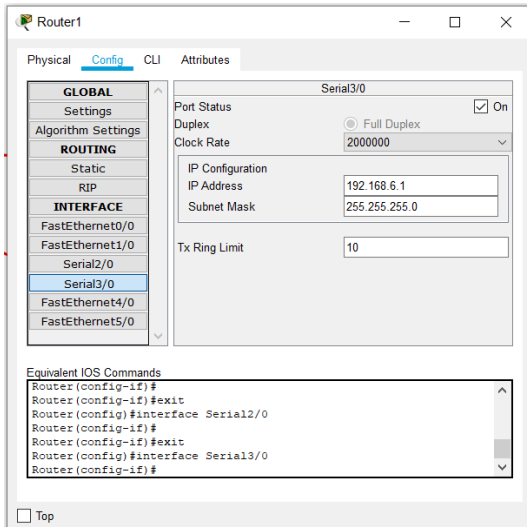


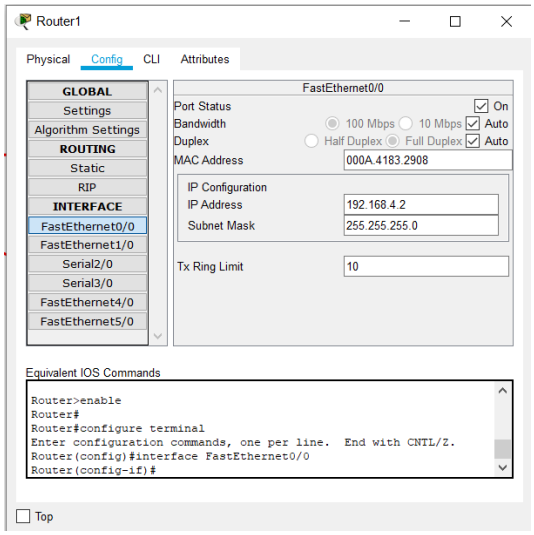




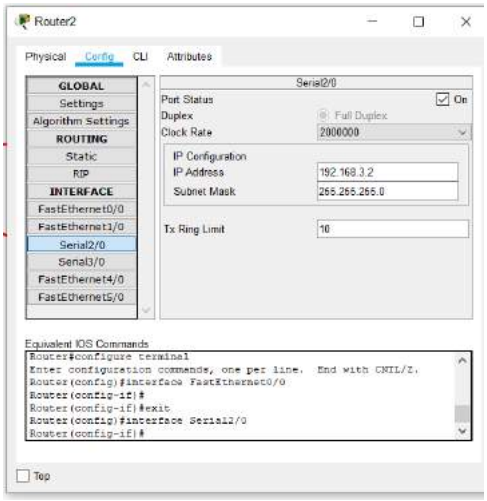
Router-1

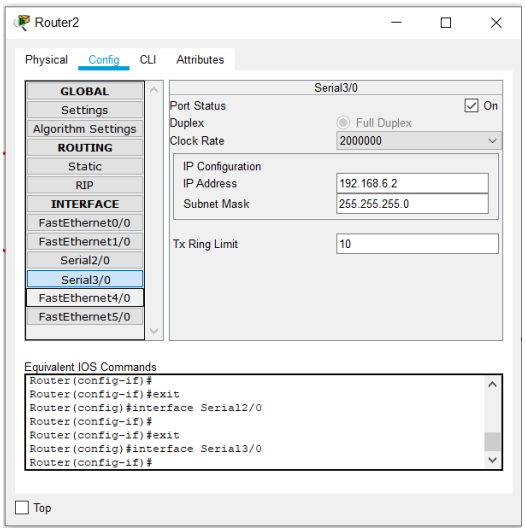


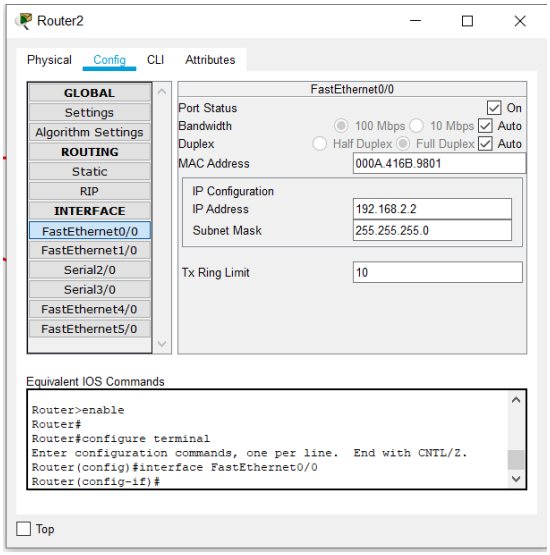




Router-2

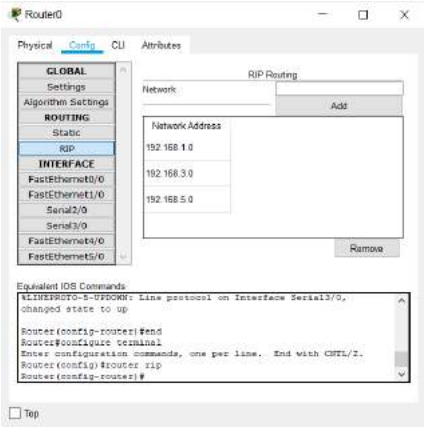




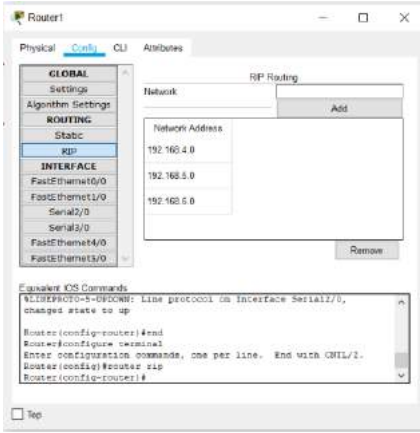


D)Now give all the router to network with RIP

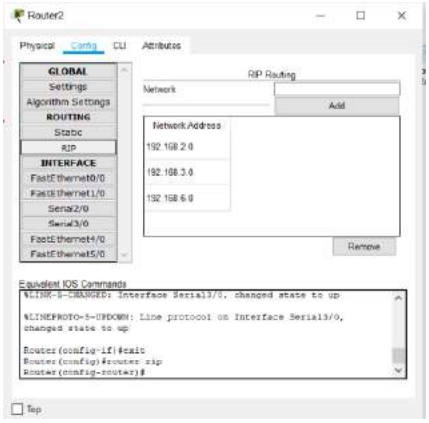
Router-0



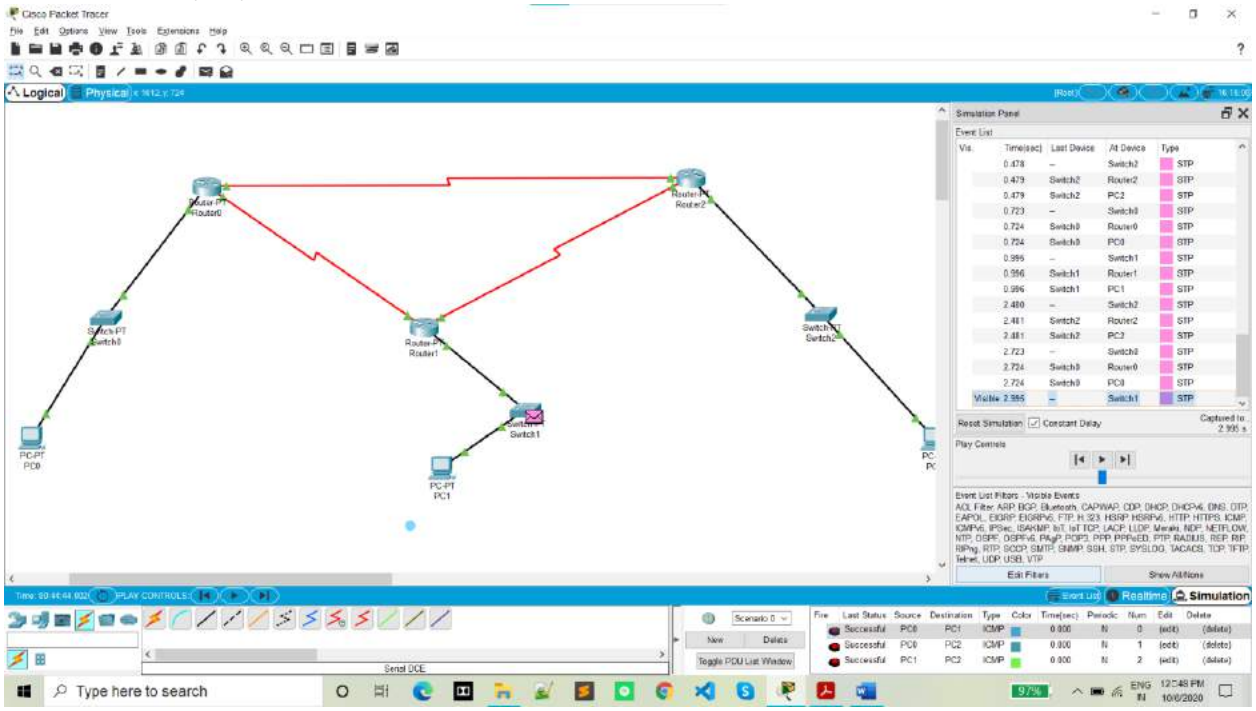
Router-1



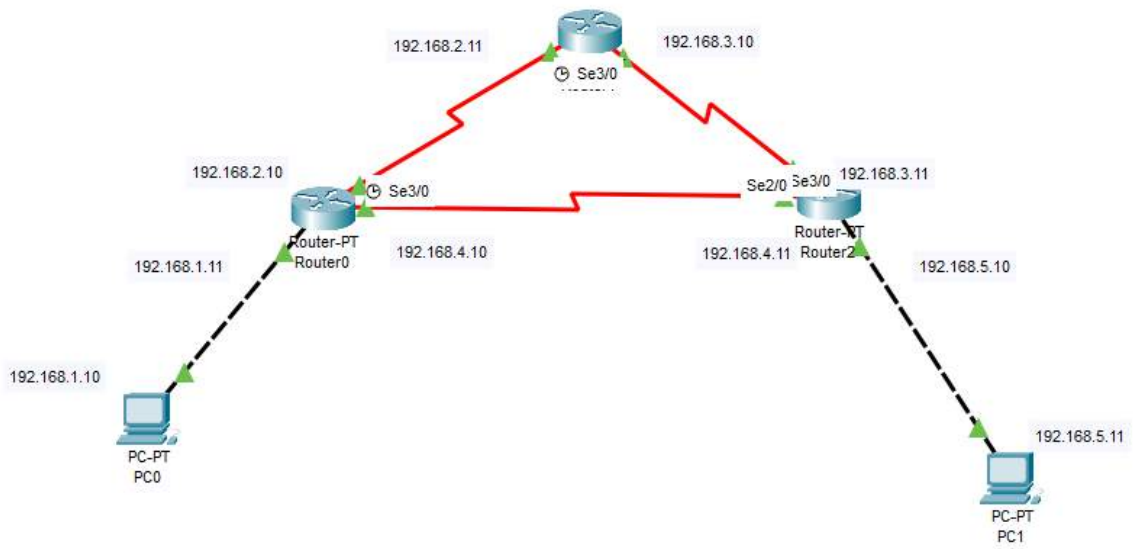
Router-2



E) All the path set packet and its simulation can view below
From Path : 0-1 ,0-2, 1-2

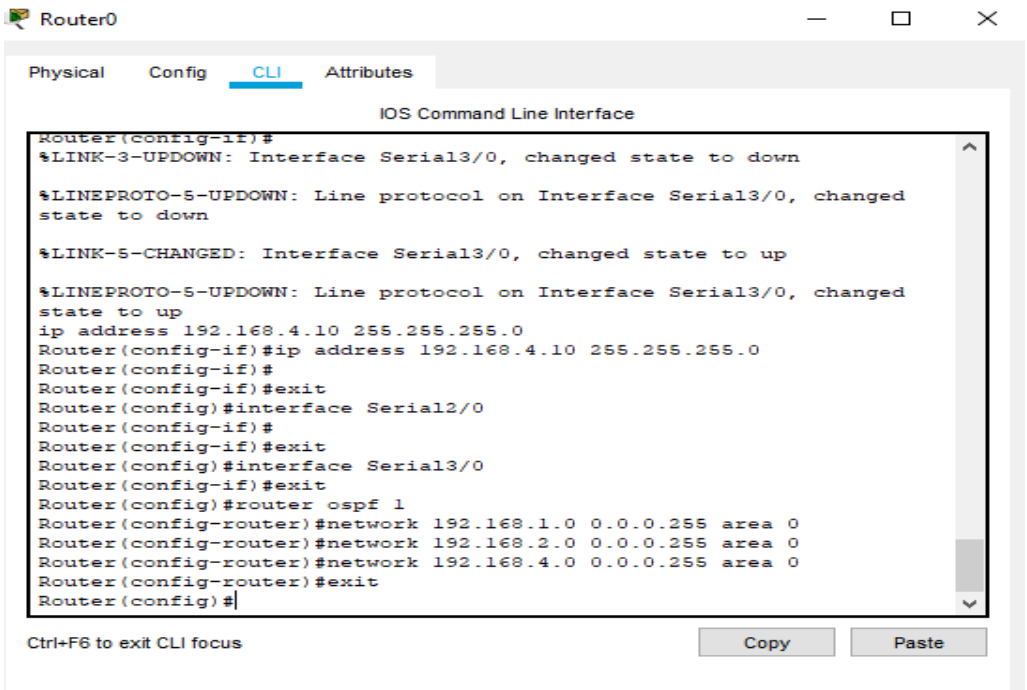


Q-3) Create a simple network topology and configure OSPF routing for data communication. Record necessary steps and screenshots.



OSPF as Open shortest path first

- Frist, configure all routers and pc with IP address and after setup whole network we can configure for OSPF routing on both router.
- OSPF configuration on Router 0 by using below commands.



- Here, Router 0 can connect with network 192.168.1.0, 192.168.2.0 and 192.168.4.0. So, we can define that in OSPF configuration.

- OSPF configuration for Router 1 by using below commands.

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#exit
00:44:08: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.10 on Serial2/0
from LOADING to FULL, Loading Dnetwork 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

- Here, Router 1 can connect with network 192.168.2.0 and 192.168.3.0. So, we can define that in OSPF configuration.

Router2

Physical Config CLI Attributes

IOS Command Line Interface

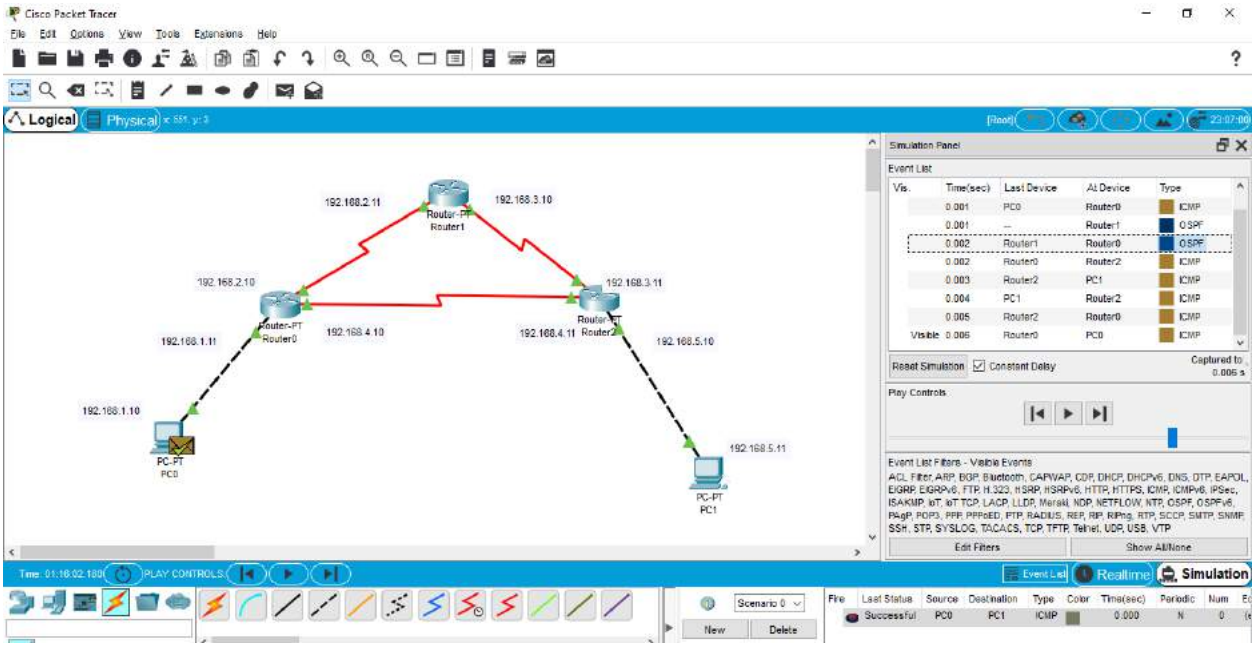
```
% Incomplete command.
Router#configuring terminal
                   ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#
00:50:42: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.10 on Serial2/0
from LOADING to FULL, Loading Done

Router(config-router)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
00:51:05: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.10 on Serial3/0
Router(config-router)#
Router(config-router)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

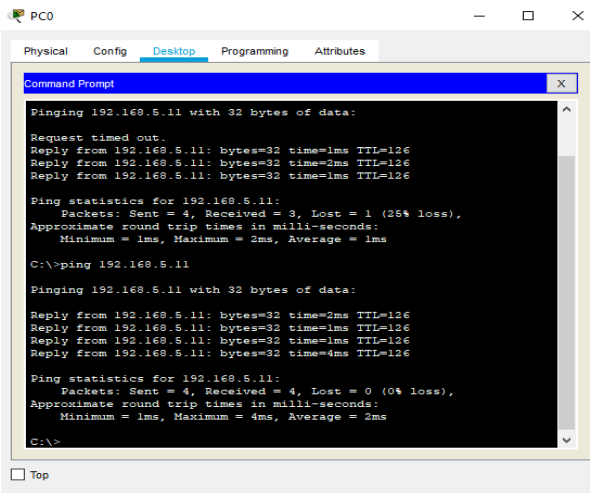
- OSPF configuration for Router 2 by using below common

- Here, Router 0 can connect with network 192.168.3.0, 192.168.4.0 and 192.168.5.0. So, we can define that in OSPF configuration.

- In command “Router OSPF 1” means here 1 is process_id you can assign it to anything.



- Now let’s check if it working or not, for checking we can ping PC0 from PC1.

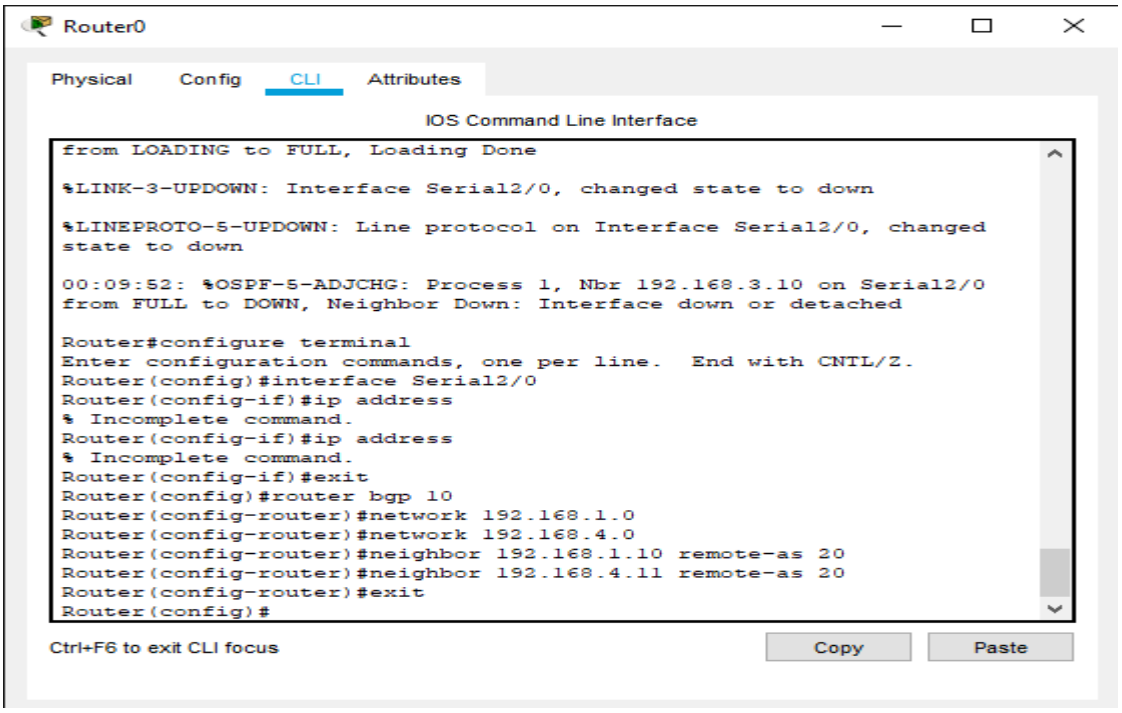


Q-4) Create a simple network topology and configure BGP routing for data communication. Record necessary steps and screenshots.

BGP as Border gateway protocol

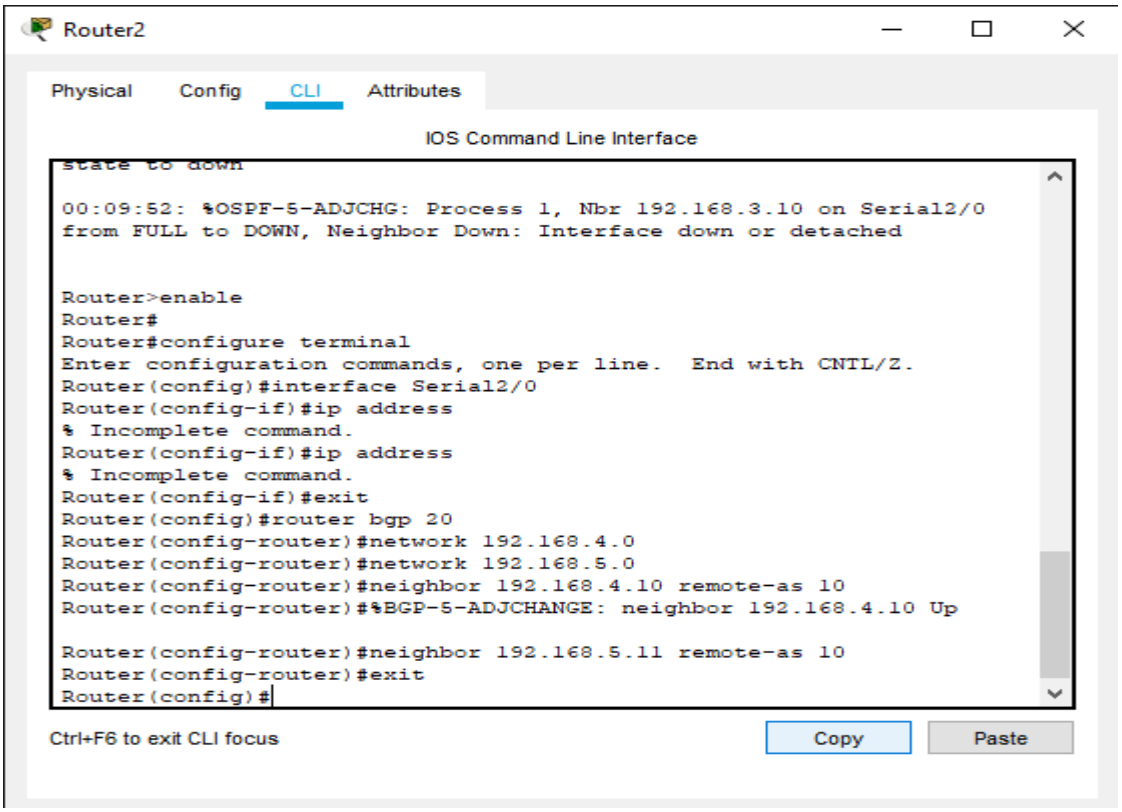
- 1st configure all routers and pc with IP address and after setup whole network we can configure for BGP routing on both router.

- BGP configuration on Router 0 by using below commands.

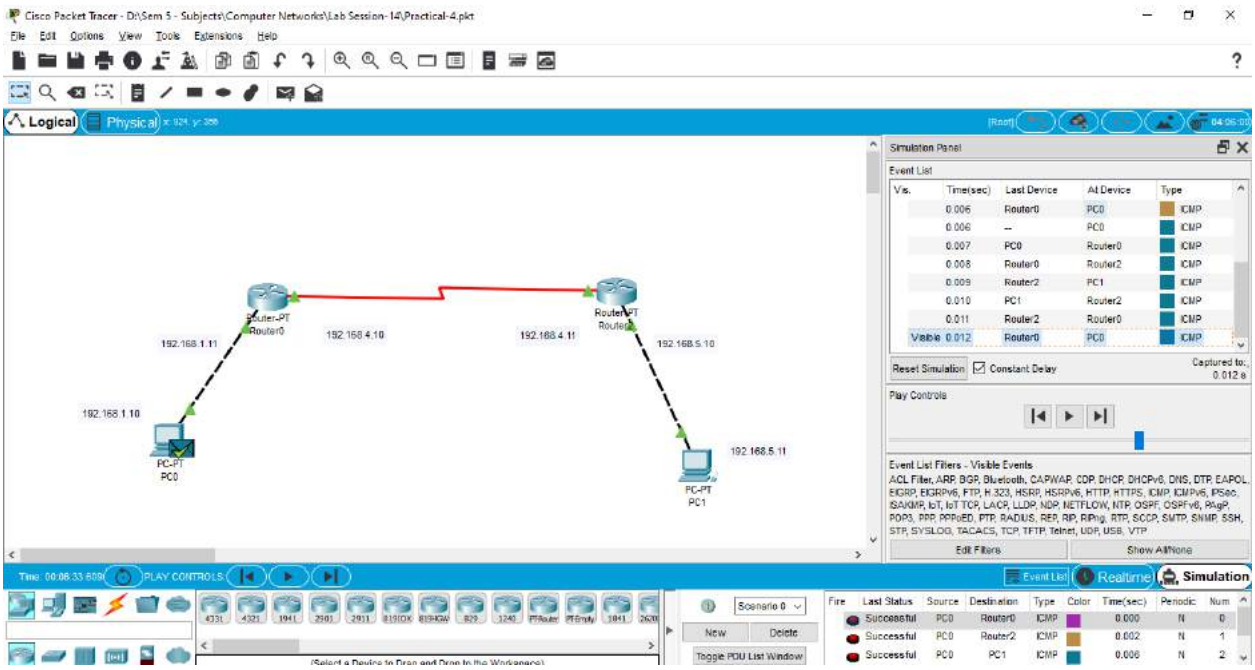
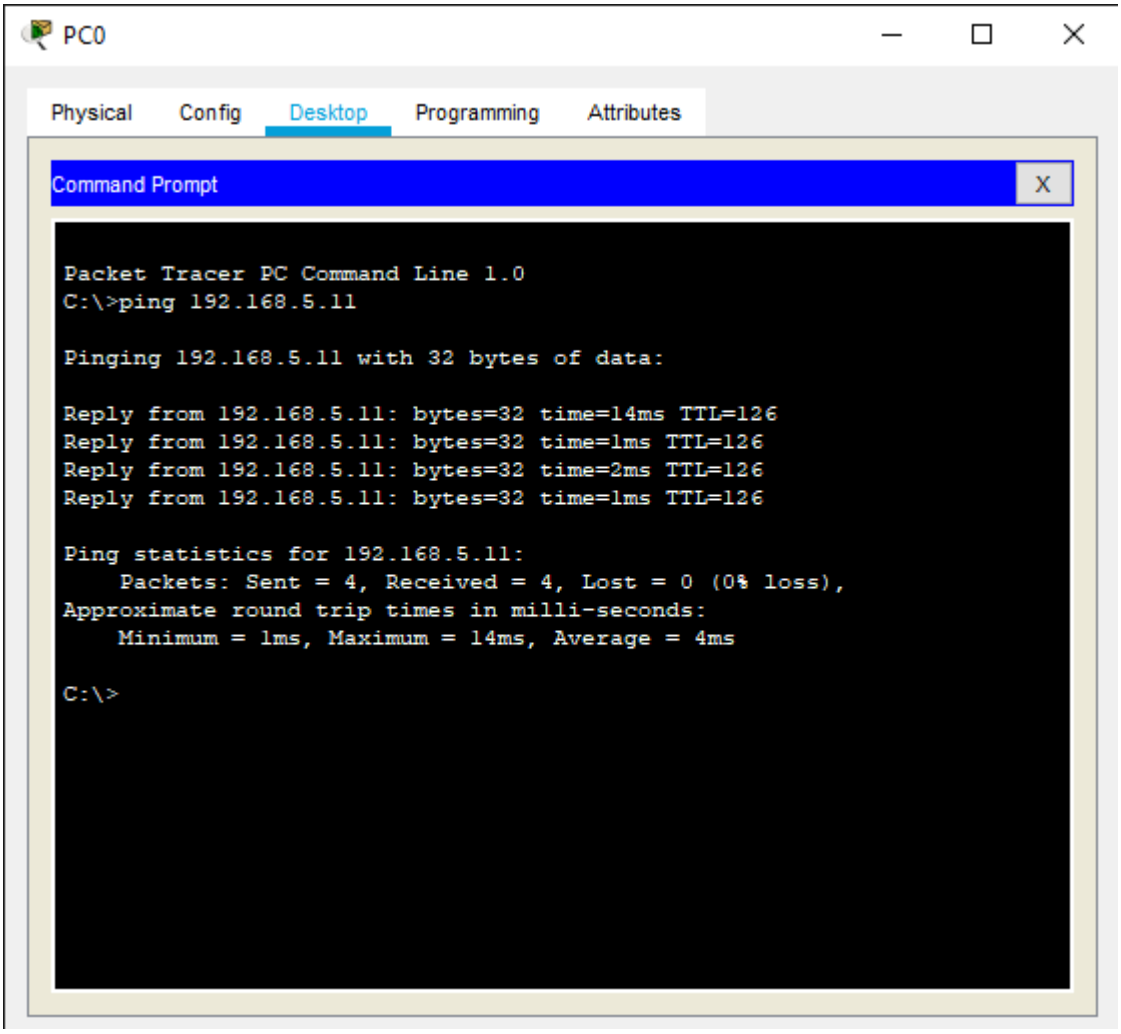


(Here, after BGP 10 is the id of that BGP)

- BGP configuration for Router 2 by using below commands.



- Now let's check if it working or not.



- Check using to send ping request from pc0 to pc1.