Experiment No. 1

Introduction to Network Simulator – Packet Tracer and establish a peer to peer Network.

Objectives

1. Introduction to Packet Tracer Interface
2. To learn how to use different components and build a simple network

Theory

Cisco Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Cisco Packet Tracer (CPT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode.

Steps to Install Cisco Packet Tracer

To obtain and install Cisco Packet Tracer (https://skillsforall.com/resources/lab-downloads), follow these simple steps:

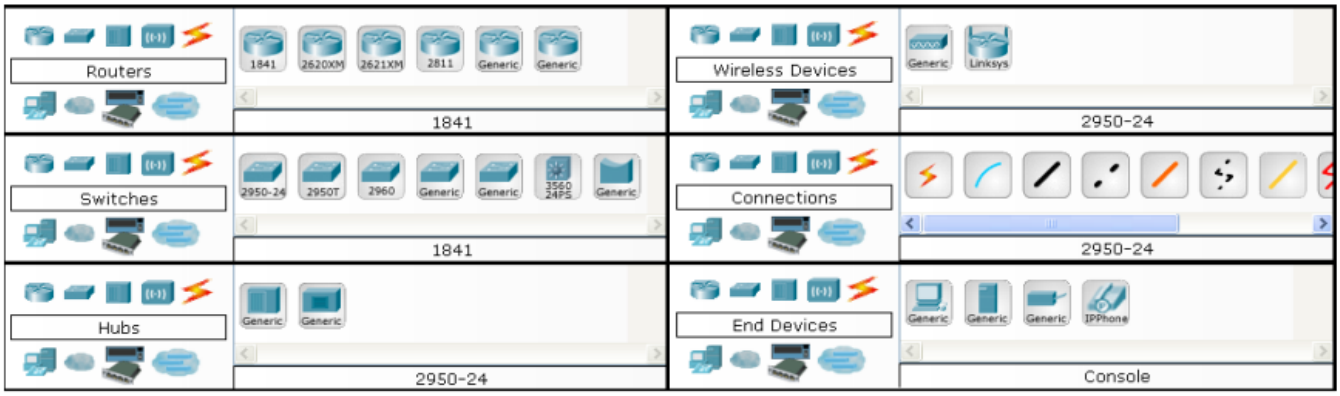
Step 1. Download the version of Packet Tracer you require.

Packet Tracer 8.2.1 MacOS 64bit
Packet Tracer 8.2.1 Ubuntu 64bit
Packet Tracer 8.2.1 Windows 64bit

Step 2. Launch the Packet Tracer install program.
Step 3. Launch Cisco Packet Tracer by selecting the appropriate icon.
Step 4. When prompted, click on Skills For All green button to authenticate.
Step 5. Cisco Packet Tracer will launch and you are ready to explore its features.

Packet Tracer Interface and how to create a topology

Step 1: Start Packet Tracer and Enter into Simulation Mode
Step 2: Choose Devices and Connections



Step 3: Building the Topology – Adding Hosts in following way:

- Single click on End Devices.
- Single click on Generic host.
- Move the cursor into topology area. You will notice it turns into a plus "+" sign. Single click in the topology area and it copies the device.

Step 4: Building Connections amongst devices – Connecting the Hosts PCs to other end devices or network components

- Click once on Copper Straight-through cable when connecting different device types
- Click once on Copper Cross-over cable when connecting with devices with similar types

Step 5: Configuring IP Addresses and Subnet Masks on Hosts

- Click once on PC0.
- Choose the Config tab.
- Click on FastEthernet.
- Enter IP address and Subnet Mask..

Exercises

1. Design a peer to peer network by establishing a connection between two PCs
2. Assign IP address to them as mentioned

Host	IP Address	Subnet Mask
PC0	192.68.1.10	255.255.255.0
PC1	192.68.1.11	255.255.255.0

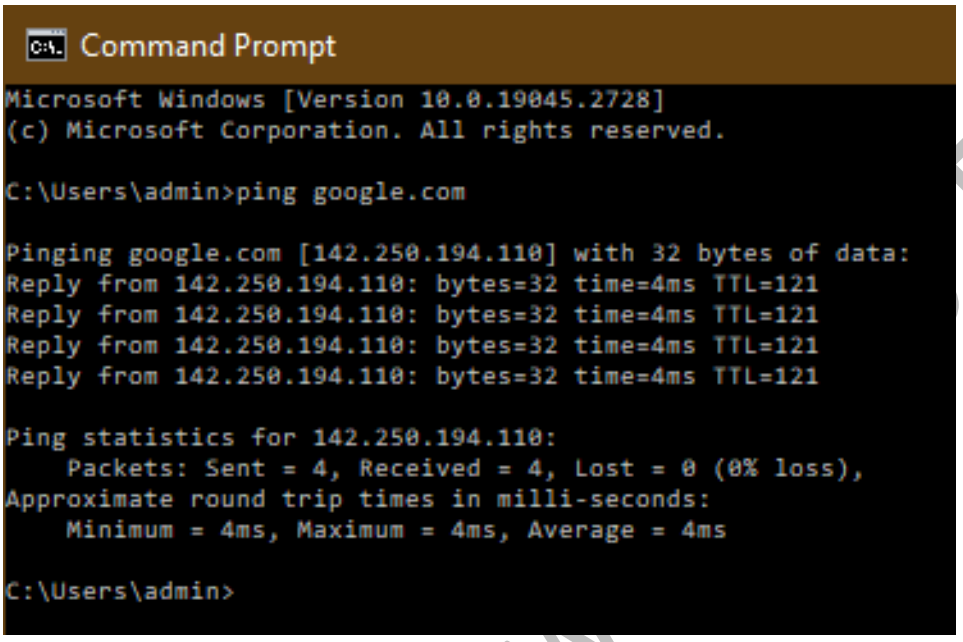
3. Observe the flow of data from host to host by creating network traffic.
4. Use commands such as ipconfig, inconfig /all, ping to check their functions and outputs on CPT- command prompt.

Experiment No. 2

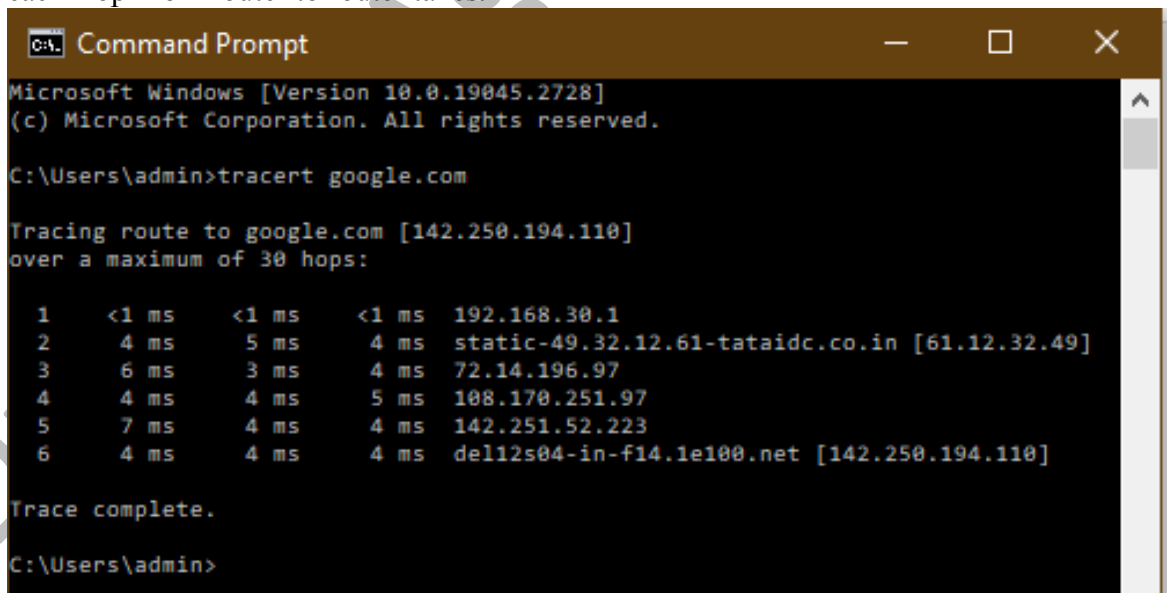
Running and using Services/commands related to networking

Commands:

1. **Ping -** The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer.



2. **Traceroute -** Traceroute is a command which shows the path a packet of information taken from one computer to another. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell how long each 'hop' from router to router takes.



3. **PathPing -** The PathPing tool is a route tracing tool that combines features of Ping and Tracert with additional information that neither of those tools provides. PathPing sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop.

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>pathping google.com

Tracing route to google.com [142.250.194.110]
over a maximum of 30 hops:
  0  win8 [192.168.30.177]
  1  192.168.30.1
  2  static-49.32.12.61-tataidc.co.in [61.12.32.49]
  3  72.14.196.97
  4  108.170.251.97
  5  142.251.52.223
  6  del12s04-in-f14.1e100.net [142.250.194.110]

Computing statistics for 150 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           win8 [192.168.30.177]
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.30.1
                                0/ 100 =  0%   |
  2    4ms     0/ 100 =  0%     0/ 100 =  0%  static-49.32.12.61-tataidc.co.in [61.12.32.49]
                                0/ 100 =  0%   |
  3    7ms     0/ 100 =  0%     0/ 100 =  0%  72.14.196.97
                                0/ 100 =  0%   |
  4    5ms     0/ 100 =  0%     0/ 100 =  0%  108.170.251.97
                                0/ 100 =  0%   |
  5   ---     100/ 100 =100%   100/ 100 =100%  142.251.52.223
                                0/ 100 =  0%   |
  6    5ms     0/ 100 =  0%     0/ 100 =  0%  del12s04-in-f14.1e100.net [142.250.194.110]

Trace complete.

C:\Users\admin>
```

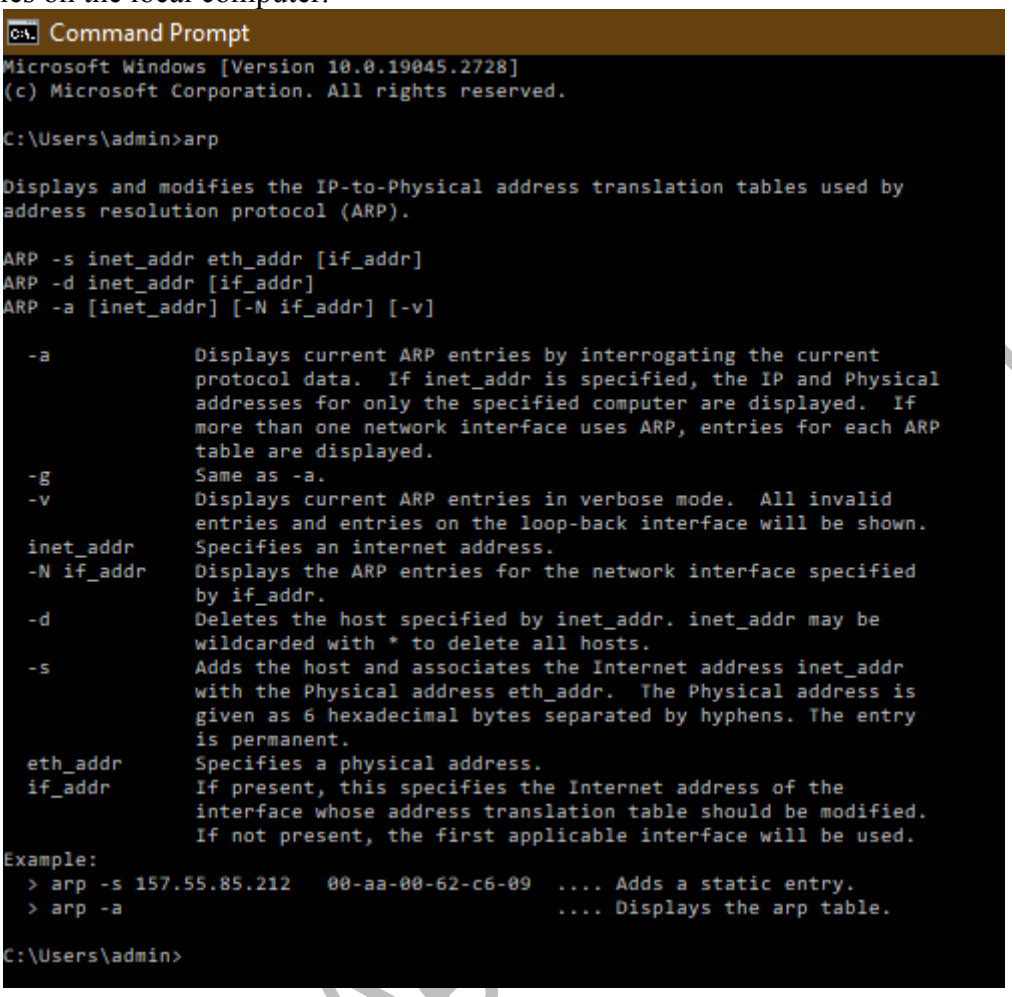
4. **Ipconfig -** Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

```
Command Prompt
   IPv4 Address. . . . . . . . . . . : 192.168.30.177
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 192.168.30.1

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  . :

Wireless LAN adapter Wi-Fi:

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

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\admin>
```

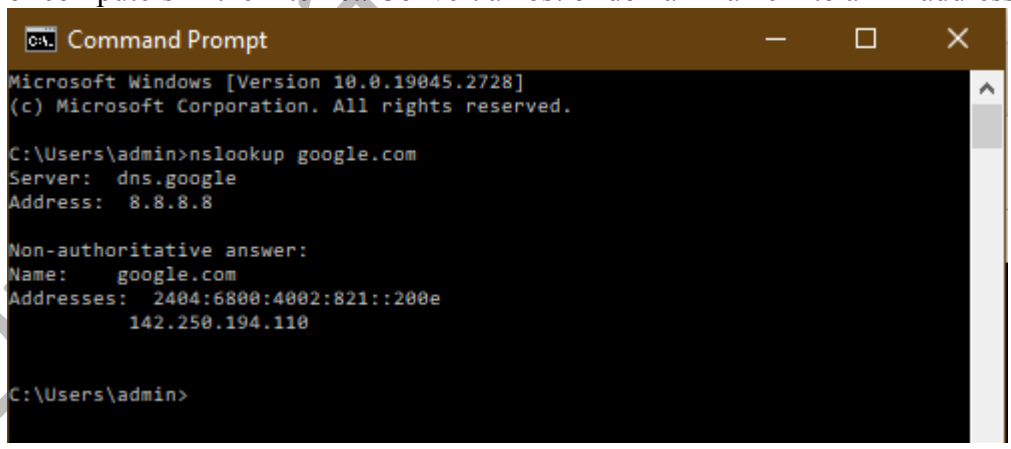
5. **Getmac –** Used to get the mac addresses

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>getmac

Physical Address    Transport Name
=================== ============================================================
8C-DC-D4-82-94-3D   Media disconnected
B0-10-41-EE-11-21   Media disconnected
B0-10-41-EE-11-22   Media disconnected
00-0E-09-88-22-2A   \Device\Tcpip_{BDE2732B-2B75-4D5E-B28F-B83D6985329E}

C:\Users\admin>
```

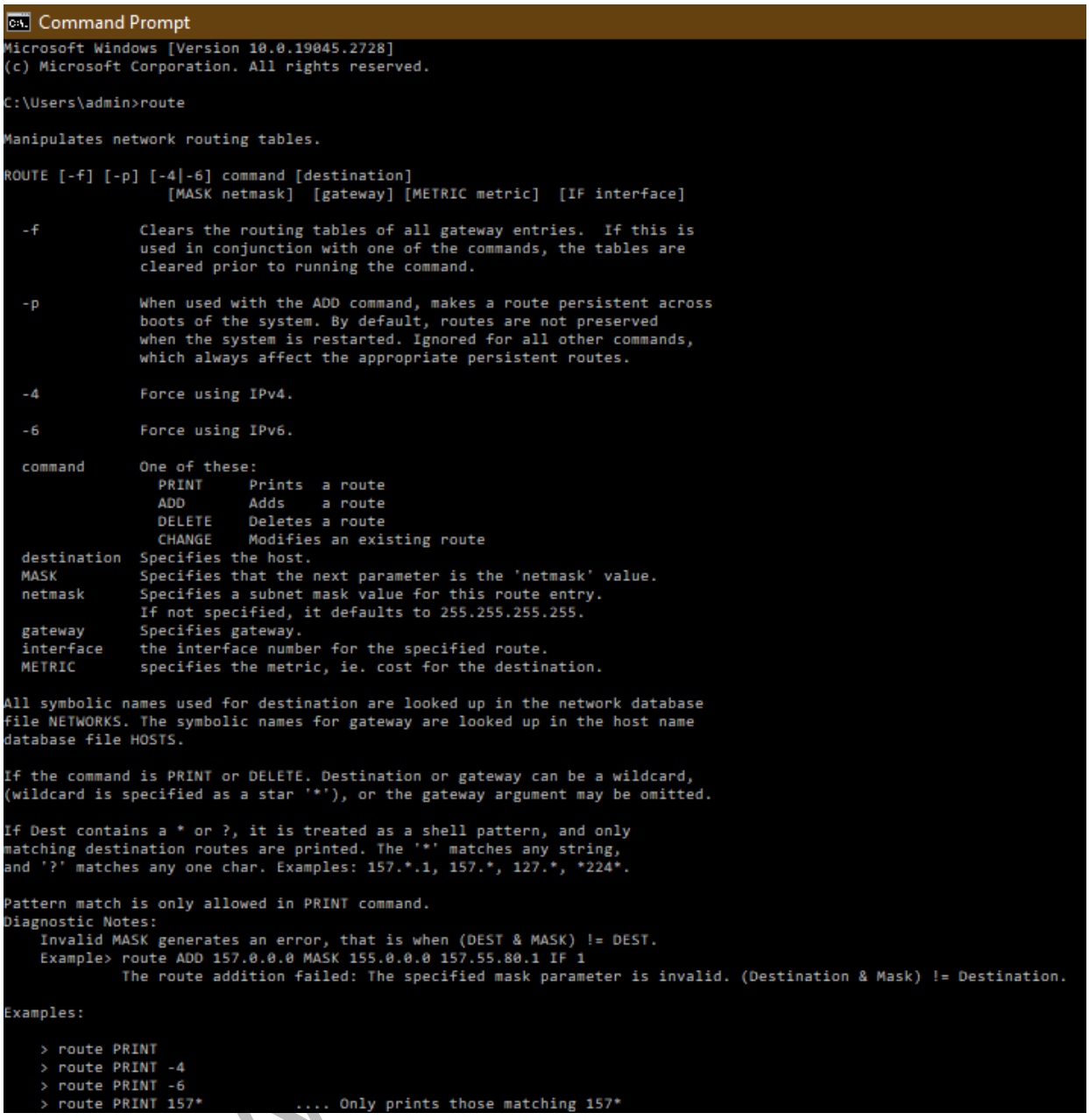
6. **ARP -** ARP stands for Address Resolution Protocol. Network nodes use this protocol to match IP addresses to MAC addresses. arp is used to view and modify the ARP table entries on the local computer.



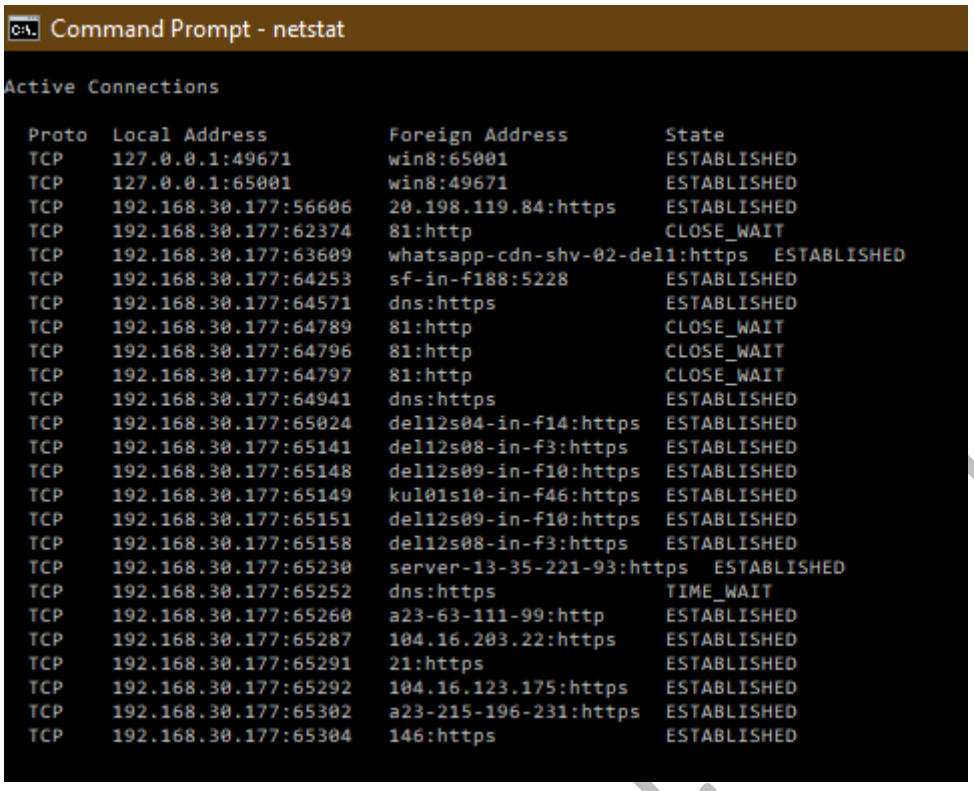
7. **Nslookup -** Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.



8. **Route -** To view the routing table



9. Netstat - The netstat command is used to show detailed network status



Command Prompt - netstat

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        win8:65001             ESTABLISHED
  TCP    127.0.0.1:65001        win8:49671             ESTABLISHED
  TCP    192.168.30.177:56606   20.198.119.84:https    ESTABLISHED
  TCP    192.168.30.177:62374   81:http                CLOSE_WAIT
  TCP    192.168.30.177:63609   whatsapp-cdn-shv-02-del1:https  ESTABLISHED
  TCP    192.168.30.177:64253   sf-in-f188:5228        ESTABLISHED
  TCP    192.168.30.177:64571   dns:https              ESTABLISHED
  TCP    192.168.30.177:64789   81:http                CLOSE_WAIT
  TCP    192.168.30.177:64796   81:http                CLOSE_WAIT
  TCP    192.168.30.177:64797   81:http                CLOSE_WAIT
  TCP    192.168.30.177:64941   dns:https              ESTABLISHED
  TCP    192.168.30.177:65024   del12s04-in-f14:https  ESTABLISHED
  TCP    192.168.30.177:65141   del12s08-in-f3:https   ESTABLISHED
  TCP    192.168.30.177:65148   del12s09-in-f10:https  ESTABLISHED
  TCP    192.168.30.177:65149   kul01s10-in-f46:https  ESTABLISHED
  TCP    192.168.30.177:65151   del12s09-in-f10:https  ESTABLISHED
  TCP    192.168.30.177:65158   del12s08-in-f3:https   ESTABLISHED
  TCP    192.168.30.177:65230   server-13-35-221-93:https  ESTABLISHED
  TCP    192.168.30.177:65252   dns:https              TIME_WAIT
  TCP    192.168.30.177:65260   a23-63-111-99:http     ESTABLISHED
  TCP    192.168.30.177:65287   104.16.203.22:https    ESTABLISHED
  TCP    192.168.30.177:65291   21:https               ESTABLISHED
  TCP    192.168.30.177:65292   104.16.123.175:https   ESTABLISHED
  TCP    192.168.30.177:65302   a23-215-196-231:https  ESTABLISHED
  TCP    192.168.30.177:65304   146:https              ESTABLISHED
```

Experiment No. 3

Create LAN network using Hub, Switch. Establish InterLAN communication using Router

Objective:
To Install and configure Network Devices HUB, Switch and Routers PCs are interfaced using connectivity devices.

Theory:

1. **Repeater:** Functioning at Physical Layer.A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater has two ports, so cannot be used to connect for more than two devices.
2. **Hub:** An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.
3. **Switch:** A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.
4. **Bridge:** A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1 D standards. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.
5. **Router:** A router is an electronic device that interconnects two or more computer networks, and electively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.
6. **Gate Way:** In a communications network, a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Procedure:

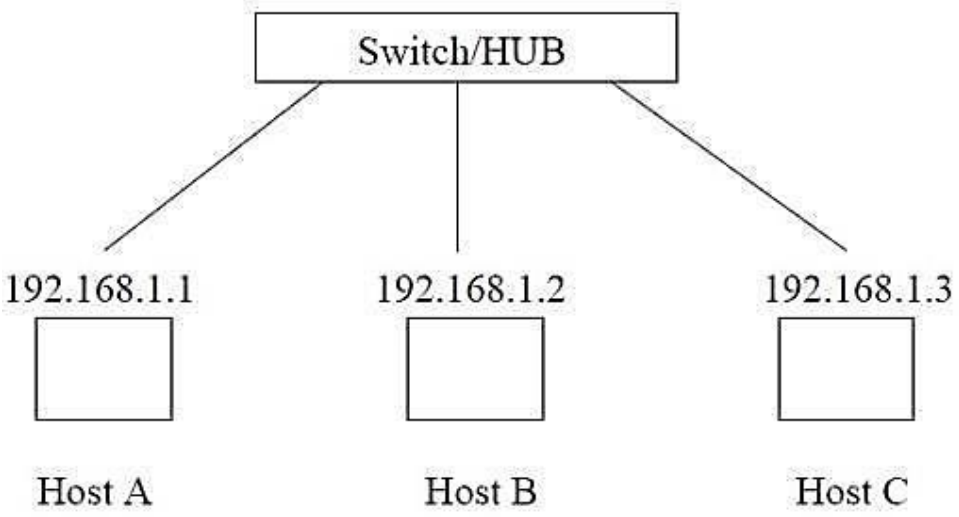
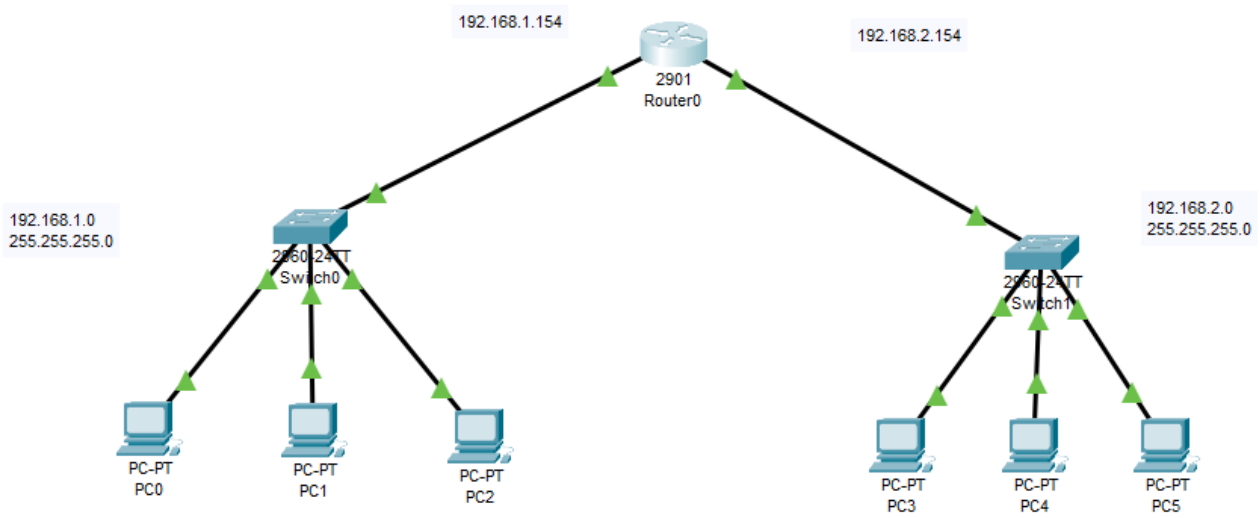


Figure 1: Establishing a LAN



Result:

Thus install and configure Network Devices PCs are interfaced using connectivity devices – Hub, routerand switch have been done successfully.

Experiment No. 4

Objective: Create Ring, Bus, Star and Mesh topology using cisco packet Tracer.

Objectives

1. To learn to implement different network topologies in CPT
2. To analyse their working and applications

Implementation of Ring Topology

Ring topology is a kind of arrangement of the network in which every device is linked with two other devices. This makes a circular ring of interconnected devices which gives it its name. Data is usually transmitted in one direction along the ring, known as a unidirectional ring. The data is delivered from one device to the next until it reaches the decided destination. In a bidirectional ring, data can travel in either direction.

Steps to Configure and Setup Ring Topology in Cisco Packet Tracer :

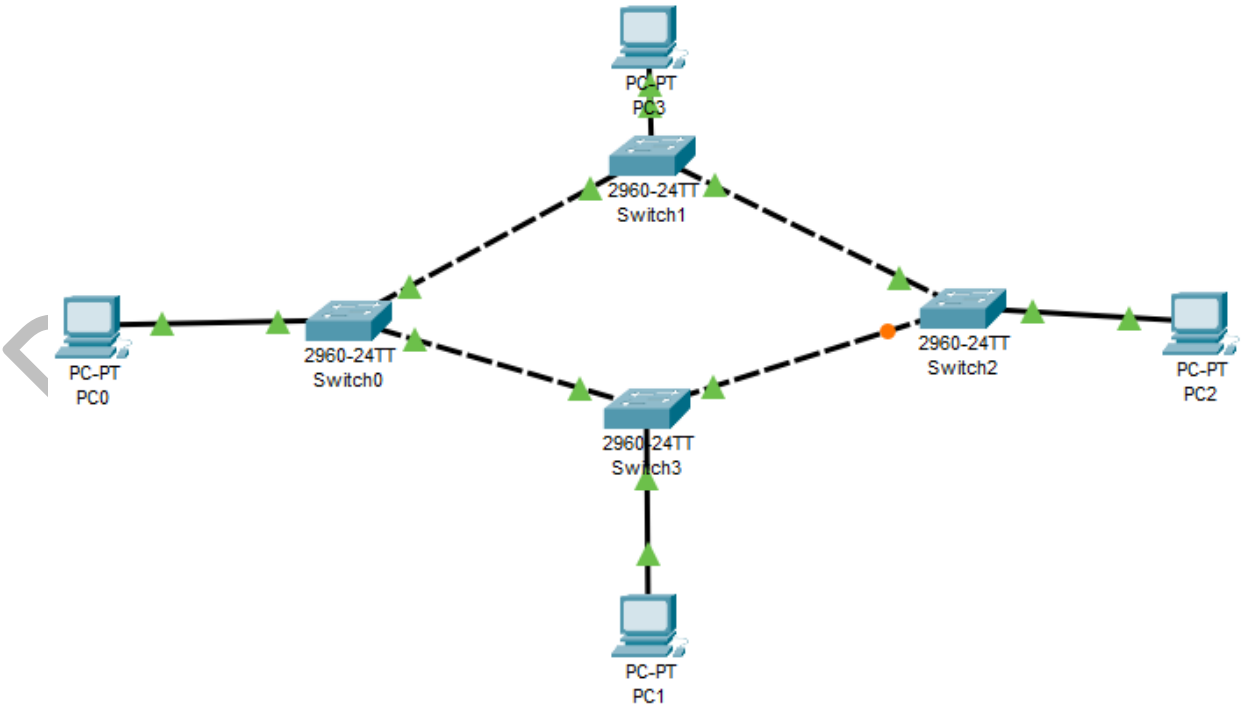
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S. No	Device	Model Name
1.	PC	PC
2.	Switch	PT-Switch

IP Addressing Table

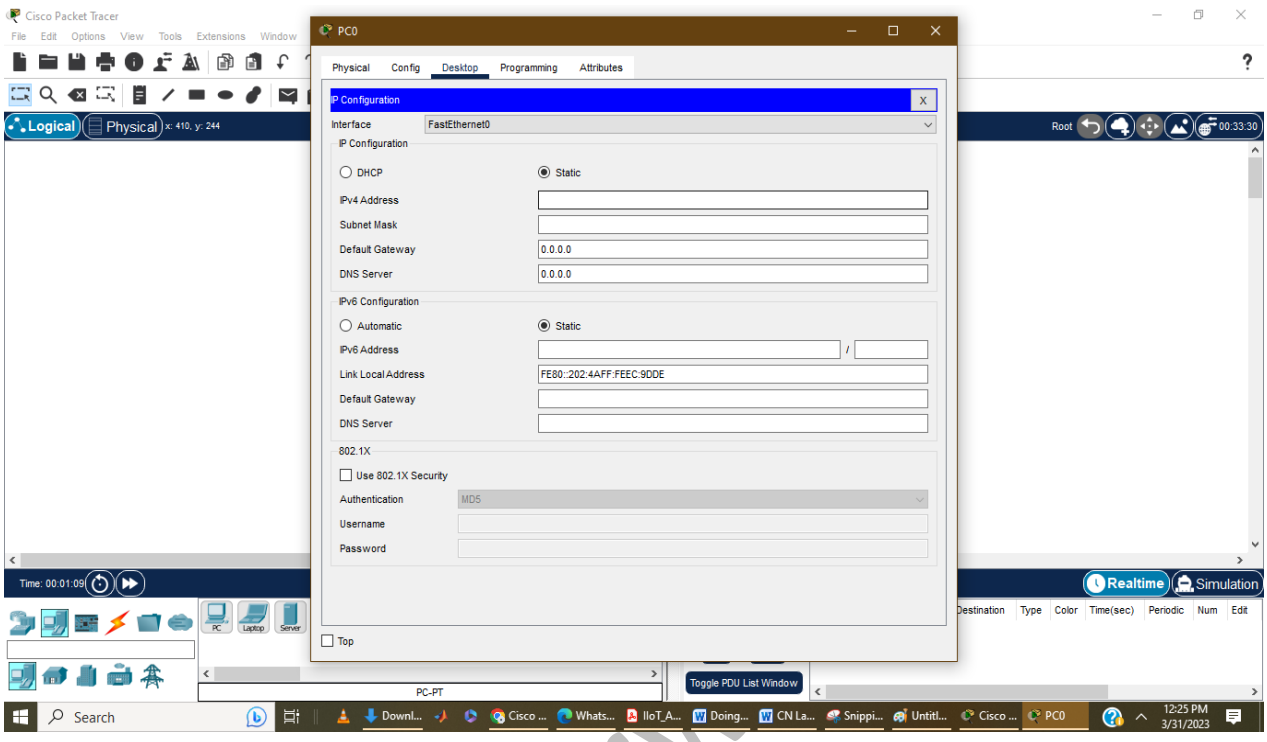
S.NO	Device	IPv4 Address	Subnet Mask
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.0.2	255.255.255.0
3.	PC2	192.168.0.3	255.255.255.0
4.	PC3	192.168.0.4	255.255.255.0

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



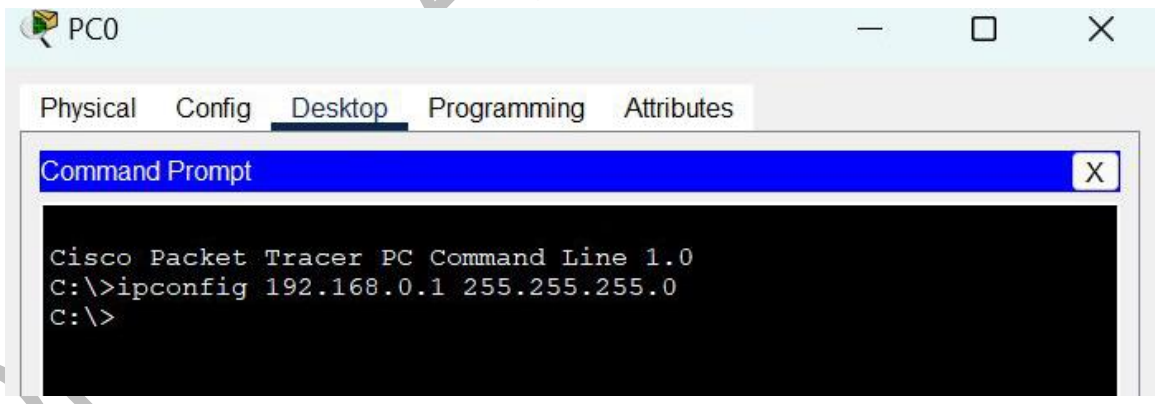
Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.



- Assigning IP address using the ipconfig command, or we can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

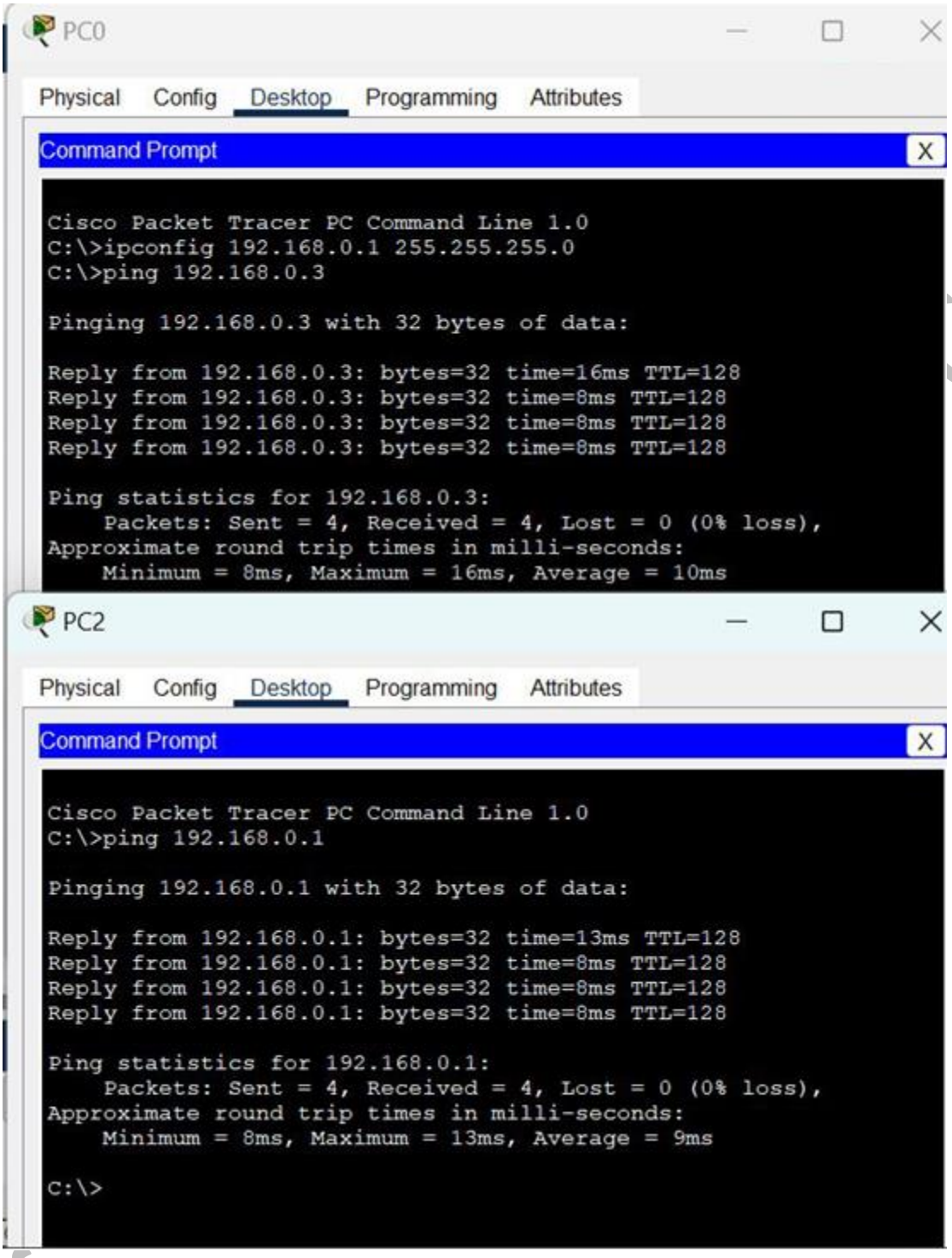
Example: ipconfig 192.168.0.1 255.255.255.0



- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: Verify the connection by pinging the IP address of any host in PC0.

- Use the ping command to verify the connection.
- As we can see we are getting replies from a targeted node on both PCs.
- Hence the connection is verified.



Simulation Result:

- Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another targeted from PC1 to PC3.

Implementation of Bus Topology

A bus topology is a network in which nodes are directly linked with a common half-duplex link. A host on a bus topology is called a station. In a bus network, every station will accept all network packets, and these packets generated by each station have equal information priority. A bus network includes a single network segment and collision domain.

Steps to Configure and Setup Bus Topology in Cisco Packet Tracer:

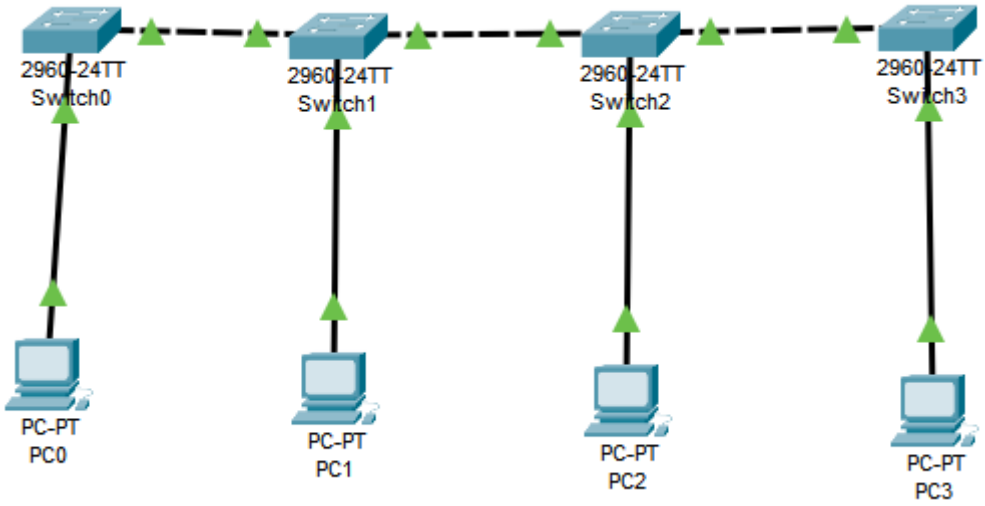
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S. No	Device	Model Name
1.	PC	PC
2.	Switch	PT-Switch

IP Addressing Table

S.NO	Device	IPv4 Address	Subnet Mask
1.	**PC0**	192.168.0.1	255.255.255.0
2.	**PC1**	192.168.0.2	255.255.255.0
3.	**PC2**	192.168.0.3	255.255.255.0
4.	**PC3**	192.168.0.4	255.255.255.0

- Then, create a network topology as shown below image:
- Use an Automatic connecting cable to connect the devices with others.



Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.
- Assigning an IP address using the ipconfig command, or we can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

Example: ipconfig 192.168.0.1 255.255.255.0

- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: Verify the connection by pinging the IP address of any host in PC0.

- Use the ping command to verify the connection.
- As we can see we are getting replies from a targeted node on both PCs.
- Hence the connection is verified.

Simulation Result:

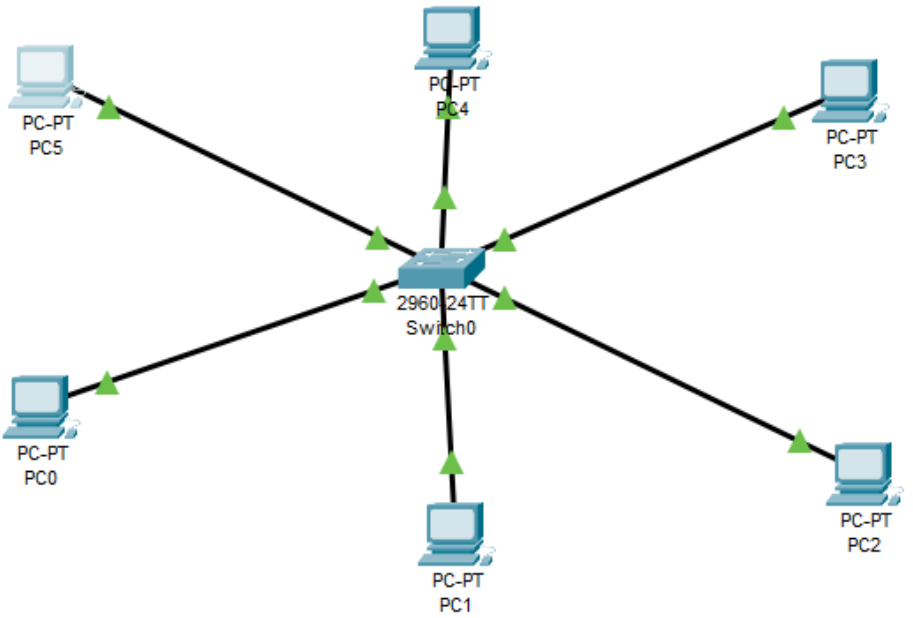
- Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another targeted from PC1 to PC3.

Implementing Star Topology

A star topology for a Local Area Network (LAN) is one in which each node is connected to a central connection point, such as a hub or switch. Whenever a node tries to connect with another node then the transmission of the message must be happening with the help of the central node. The best part of star topology is the addition and removal of the node in the network but too many nodes can cause suffering to the network.

Steps Implementing Star Topology using Cisco Packet Tracer:

Step 1: We have taken a switch and linked it to six end devices.



Step 2: Link every device with the switch.
Step 3: Provide the IP address to each device.
Step 4: Transfer message from one device to another and check the Table for Validation.
Now to check whether the connections are correct or not try to ping any device.

IP Addressing Table

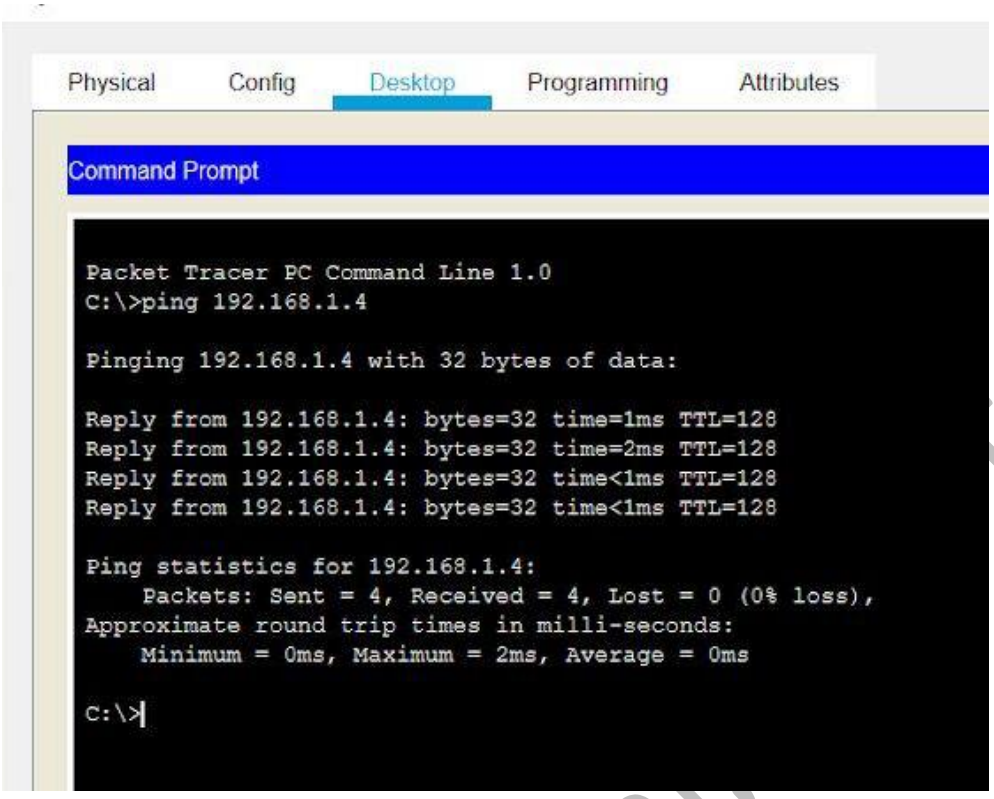
S.NO	Device	IPv4 Address	Subnet Mask
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.0.2	255.255.255.0
3.	PC2	192.168.0.3	255.255.255.0
4.	PC3	192.168.0.4	255.255.255.0
5.	PC4	192.168.0.5	255.255.255.0
6.	PC5	192.168.0.6	255.255.255.0

To do ping one terminal of one device and run the following command:

Command:
"ping ip_address_of _any_device"

Example:
ping 192.168.1.4

Note: If the connections are correct then you will receive the response.



Simulation Result:

- Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another targeted from PC1 to PC3.

Implementation of Mesh Topology

In the mesh topology of networking, each and every device sends its own signal to the other devices that are present in the arrangement of the network.

Steps to Configure and Setup Ring Topology in Cisco Packet Tracer:

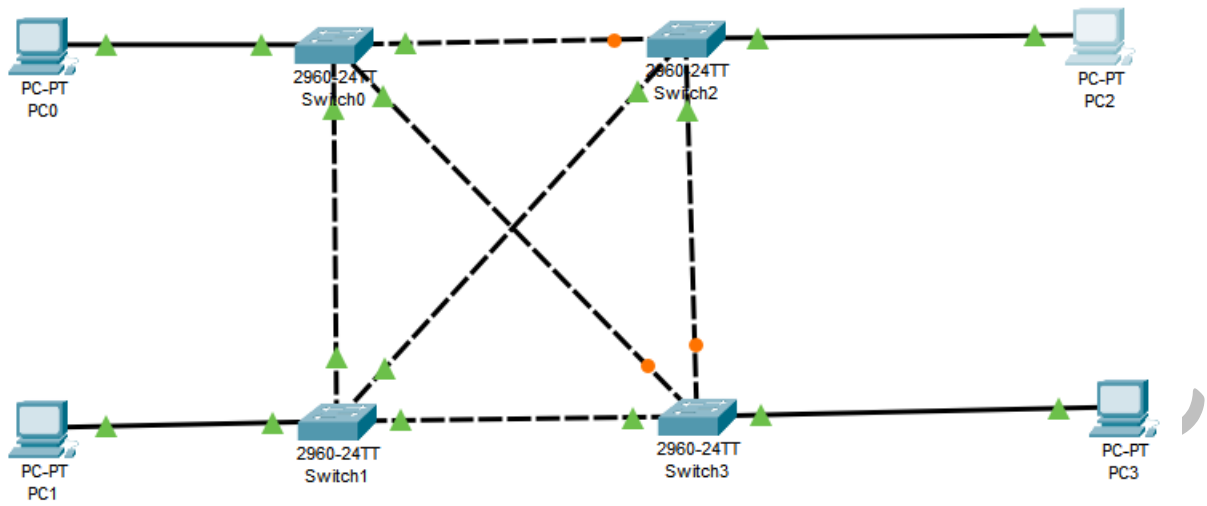
Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

S. No	Device	Model Name
1.	PC	PC
2.	Switch	PT-Switch

IP Addressing Table

S.NO	Device	IPv4 Address	Subnet Mask
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.0.2	255.255.255.0
3.	PC2	192.168.0.3	255.255.255.0
4.	PC3	192.168.0.4	255.255.255.0

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.
- Assigning IP address using the ipconfig command.
- Also, we can also assign an IP address with the help of a command.
- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

Example: ipconfig 192.168.0.1 255.255.255.0

- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: Verify the connection by pinging the IP address of any host in PC0.

- Use the ping command to verify the connection.
- We will check if we are getting any replies or not.
- Here we get replies from a targeted node on both PCs.
- Hence the connection is verified.

Simulation Result:

- Check a simulation of the experiment by sending two PDU packets one targeted from PC0 to PC2 and another targeted from PC1 to PC3.

Experiment - 5

Explore various aspects of HTTP protocols.

Objective :

1. **Introduction to HTTP protocol**
2. **To learn how to use different components and build a simple network.**

Steps to configure web server/HTTP in CPT

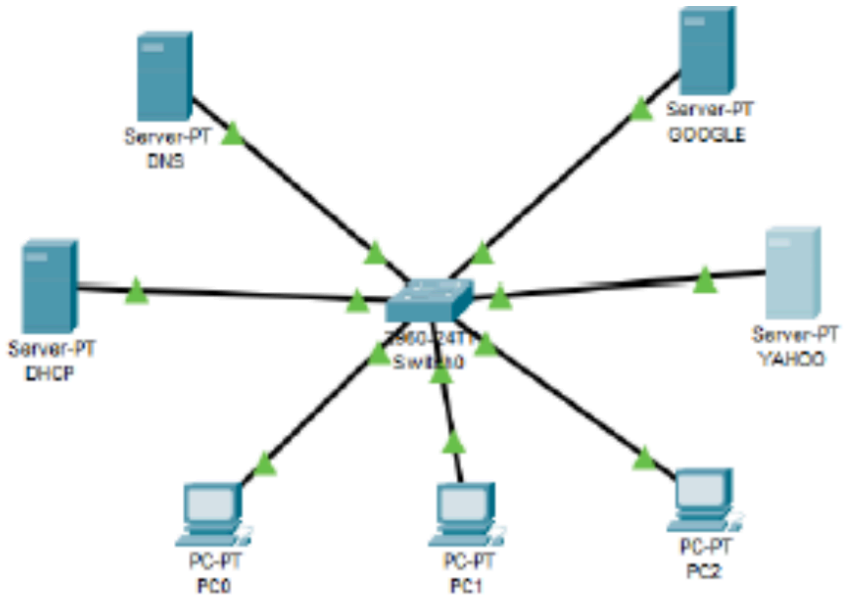
1. Open cisco packet tracer
2. Make a topology using 1PC/laptop , 1 PT switch and 2 servers (label one as web server and one as DNS server)
3. Connect all the device using copper straight through cable connecting using fast ethernet port.
4. Assign ip address to all devices.
5. Double click on web server and select services tab. Go to HTTP option. Open index.html
6. In index.html file, edit pre-written code to code given below :

```
<html>
<cente><font size="+2" cooler ="blue">cisco packet tracer</font></centre>
<hr>Welcome to CN lab.
<h2>By Ms. Khushboo Vijayran</h2>
</html>
```

7. Click on save and in dialog box press yes.
8. Double click on DNS server. Under services tab, select DNS. Turn on the radio button next to DNS option. In the DNS tan mention name of the website that you creates in the web server and in the address option mention web server IP address.click on save.
9. Double click on PC/Laptop. Go to services tab and select web browser option. In URL field write the name of the website creates or IP address of the web server. Click OK.

Exercises :

1. **Open Cisco packet tracer, make a topology by selecting 3 PC/Laptop, 1 PT switch and 1 server. (Label as web server).**
2. **Open Cisco packet tracer , make a topology as shown :**



- Assign IP address as given

Host	IP Address	Subnet Mask	DNS server
Google	192.168.1.1	255.255.255.0	192.168.1.4
Yahoo	192.168.1.2	255.255.255.0	192.168.1.4
DHCP	192.168.1.3	255.255.255.0	192.168.1.4
DNS	192.168.1.4	255.255.255.0	192.168.1.4

- Set DNS for DHCP: For it, go to services tab and configure DHCP by enabling DNS IP address and disabling all other services/options. In DHCP service option, turn on DHCP and set DNS server IP address to be **192.168.1.4**. and start IP address to be 192.168.1.10
- Set IP address of PCs by turning on DHCP option instead of static.
- Configure DNS server. Double click on DNS server, go to services tab and disable all services options except DNS in order to avoid error due to multiple servers. In the DNS option, turn on DNS service. In the name option type
    1. www.google.com and address to be: 192.168.1.1 and click on add
    2. www.yahoo.com and address to be: 192.168.1.2 and click on add
- Double click on Google server. Go to services tab and select HTML option. In the HTML option, edit index.html file to be:
  <html>
  Welcome to google.com
  <hr>Computer Networks Lab task 2.
  </html>
  Click on Save
- Double click on Yahoo server. Go to services tab and select HTML option. In the HTML option, edit index.html file to be:

Experiment No. 6

Analyzing various parameters for TCP protocol in action

Objectives

- To generate Network Traffic in Simulation Mode
- This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail.
- Examine the Functionality of the TCP and UDP Protocols in a network setup and its demonstration through Cisco Packet Tracer Tool

---

Steps to Configure TCP and UDP protocol simulation in Cisco Packet Tracer

Step 1. Open Cisco Packet Tracer

Step 2. Make a topology as shown in picture by selecting 4 PC/Laptop, 1 2960 switch and 1 server. (Label server as multi-server and PCs as Web Client, Email Client, FTP Client and DNS Client)

Step 3. Connect all the devices using copper straight through cable, connecting all using Fast Ethernet port.

Step 4. Assign IP address to all devices.

Host	Label	IP Address	Subnet Mask	DNS Server
PC0	Web Client	192.168.11.1	255.255.255.0	192.168.11.5
PC1	Email Client	192.168.11.2	255.255.255.0	192.168.11.5
PC2	DNS Client	192.168.11.3	255.255.255.0	192.168.11.5
PC3	FTP Client	192.168.11.4	255.255.255.0	192.168.11.5
Server	Multi-Server	192.168.11.5	255.255.255.0	192.168.11.5

Step 5. Double click on Multi-Server, from the pop-up window, select services tab,

- Under services select DNS service.
- Turn on DNS service.
- Within DNS, name record to be www.google.com; address – **192.168.11.5**.
- Click on Add record

Step 6. Double click on Multi-Server, from the pop-up window, select services tab,

- Under services select HTTP service
- Turn on HTTP and HTTPs options **ON**
- Select index.html and click on edit option
- Type the following text

  <html>
  Welcome to Computer Networks Lab. Experiment no 6
  We are Learning about Simulation of TCP and UDP Protocols
  <html>
- Click on Save, click on yes

Step 7. Double click on DNS Client,

- Within the Desktop Tab select Command Prompt Option.
- Type nslookup www.google.com (SCREENSHOT)
- This statement lets you know whether DNS client can connect to server or not and resolve the IP address issues.
- Within the Desktop Tab select Web browser Option.
- In the url type www.google.com (SCREENSHOT)

Step 8.Double click on Web Client,

- Within the Desktop Tab select Email Option.
- In the configure mail dialog box write:
- Name: **Your Name (Divya)**
- Email address: **divya@gmail.com**
- Incoming Mail Server: **192.168.11.5**
- Outgoing Mail Server: **192.168.11.5**
- User Name: **divya**
- Password: **Cisco_aiml**
- **Click on Save** (SCREENSHOT)

Step 9.Double click on Email Client,

- Within the Desktop Tab select Email Option.
- In the configure mail dialog box write:
- Name: **Your Surname (Agarwal)**
- Email address: **agarwal@gmail.com**
- Incoming Mail Server: **192.168.11.5**
- Outgoing Mail Server: **192.168.11.5**
- User Name: **agarwal**
- Password: **Cisco_aiml**
- **Click on Save** (SCREENSHOT)

Step 10.Double click on Multi-Server

- Within the Services tab, select Email Option.
- Switch on SMTP and POP3 service
- Type domain name: **gmail.com**
- Under User Setup: **Name: divya; Password: Cisco_aiml**
- Click on Add
- Under User Setup: **Name: agarwal; Password: Cisco aiml**
- Click on Add (SCREENSHOT)

Step 11.Double click on Web Client

- Within the Desktop tab, select Email Option.
- Send a mail by composing a mail.
- In the **To** section write: agarwal@gmail.com
- Subject: Hi
- Mail Box: Hello
- Click on Send Mail (SCREENSHOT)

Step 12.Double click on EMail Client

- Within the Desktop tab, select Email Option.
- In the Pop-up window, Select Receive Option
- SCREENSHOT

Step 13.Double click on Email Client

- Within the Desktop tab, select Email Option.
- Send a mail by composing a mail.
- In the **To** section write: divya@gmail.com
- Subject: Hi
- Mail Box: I received the mail
- Click on Send Mail (SCREENSHOT)

Step 14.Double click on Web Client

- Within the Desktop tab, select Email Option.
- In the Pop-up window, Select Receive Option
- SCREENSHOT

Step 15.Double click on Multi-Server, from the pop-up window, select services tab,

- Under services select FTP service.
- Set Username and Password as **admin**.
- Enable all options: write, read, delete, rename and list
- Click on Add record, (SCREENSHOT)

Step 16.Double click on FTP Client,

- Within the Desktop Tab select Command Prompt Option.
- Type ftp www.google.com (SCREENSHOT)
- Username: **admin**.
- Password: **admin**.
- Close the command prompt window
- Open Texteditor services
- Type any message and save it as **test.txt**
- Now open command prompt again
- Type: put test.txt (SCREENSHOT)
- Type: dir (directory option to check whether test.txt is put up in server or not)
- (SCREENSHOT)

Step 17.Double click on DNS Client,

- Within the Desktop Tab select Command Prompt Option.
- Type ftp www.google.com (SCREENSHOT)
- Username: **admin**.
- Password: **admin**.
- Type: get test.txt (SCREENSHOT)
- Type: dir (directory option to check whether test.txt is put up in server or not)
- (SCREENSHOT)

Experiment - 7

AIM: Introduction to basic networking tools: Wire shark and Network Miner

Learning Objective: At the end of the session you will be able to

- Use one of the best packet sniffing tools i.e. "Wireshark".
- Use "NetworkMiner" great tool for automatic extraction of files from a packet capture
- Control upon ports, protocols and data packets.
- Start capturing and analyzing packets.

2.1 What is Wireshark?

Wireshark has a very rich history ranging to mid-2006. Wireshark is a network packet analyzer which presents captured packet data in detail. It is a measuring device for examining what's happening inside a network cable. Wireshark is available for free and is open source.

2.2 Benefits of Wireshark

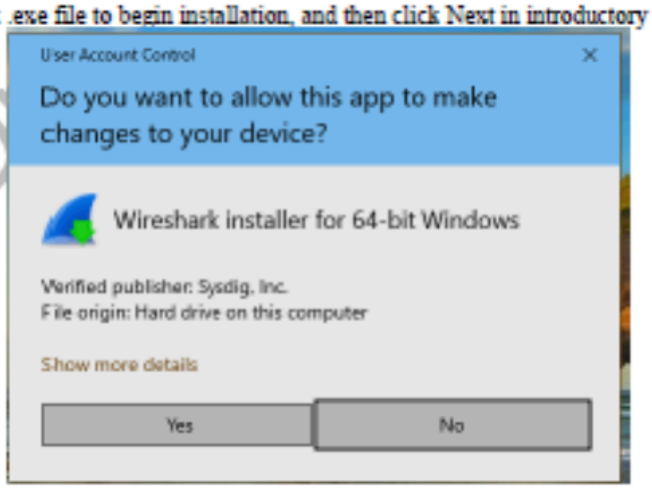
Wireshark offers several benefits that make it appealing for everyday use. It is aimed at both single-user and expert packet analyst, and offers a variety of features to entice each.

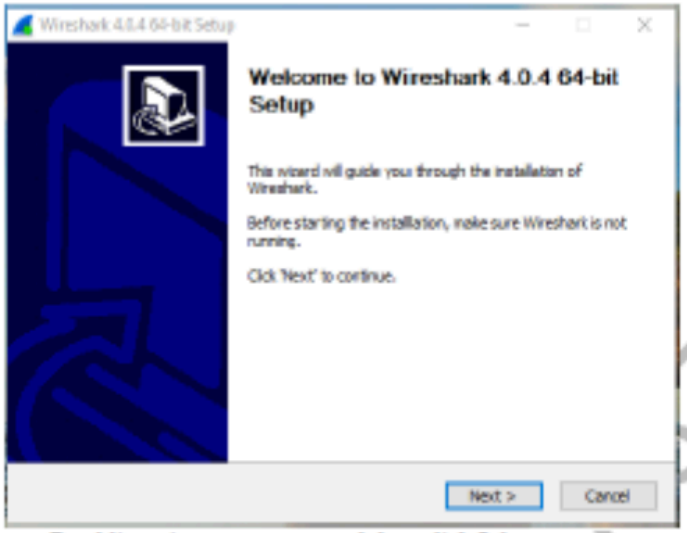
- **Supported protocols:** Wireshark excels in number of protocols (more than 850).
- **User-friendliness:** GUI-based, with very clearly written context menus and a straightforward layout.
- **Cost:** Available for free and is open source.
- **Program support:** Freely distributed software, relies on its user base to provide support.
- **Operating system support:** Supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms.

2.3 Installing Wireshark on Microsoft Windows Systems

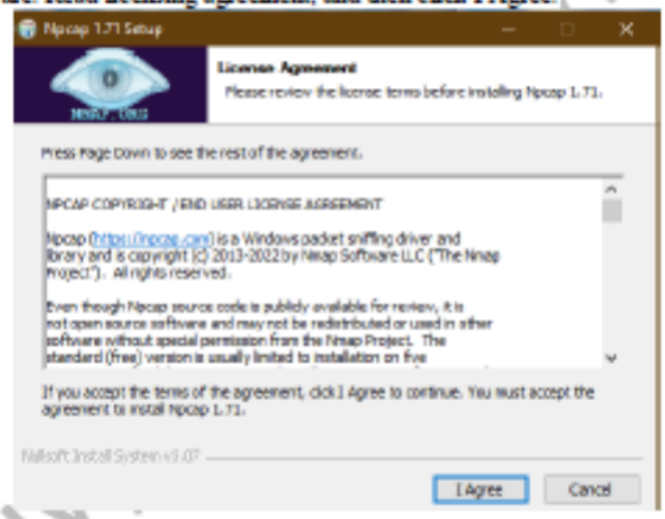
Open Wireshark web page, http://www.wireshark.org/. Navigate to Downloads section (https://www.wireshark.org/download.html) on website and choose a mirror. Once downloaded, follow these steps:

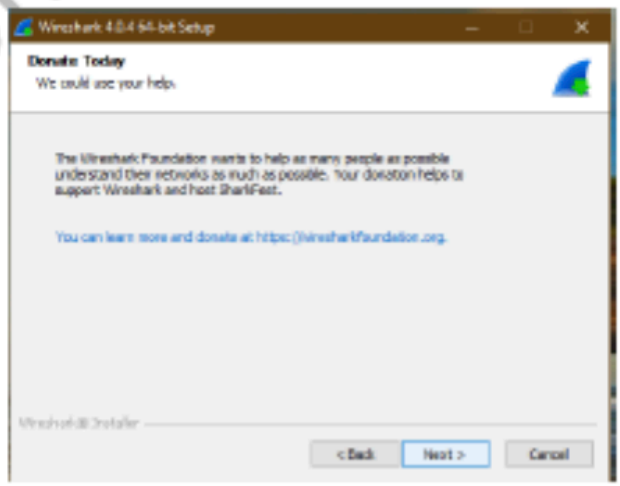
1. Double-click .exe file to begin installation, and then click Next in introductory window.



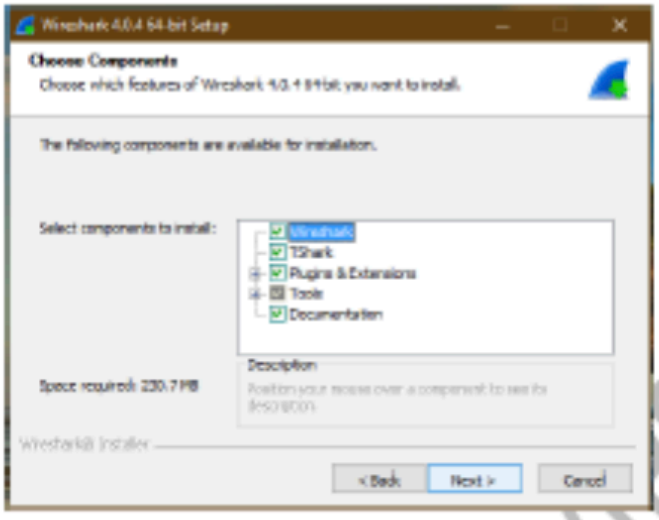


2. Install software. Read licensing agreement, and then click I Agree.

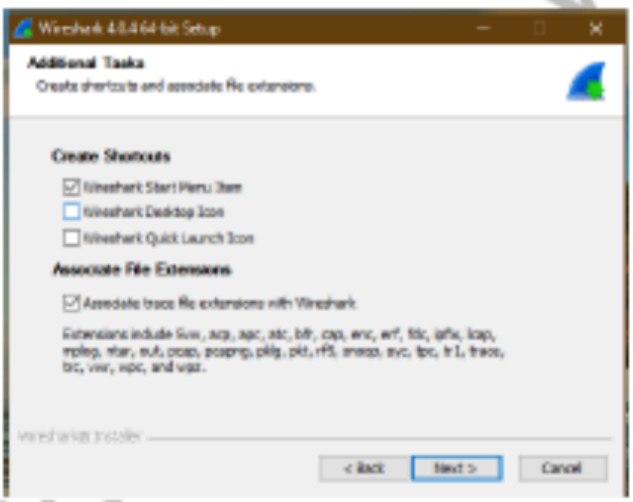




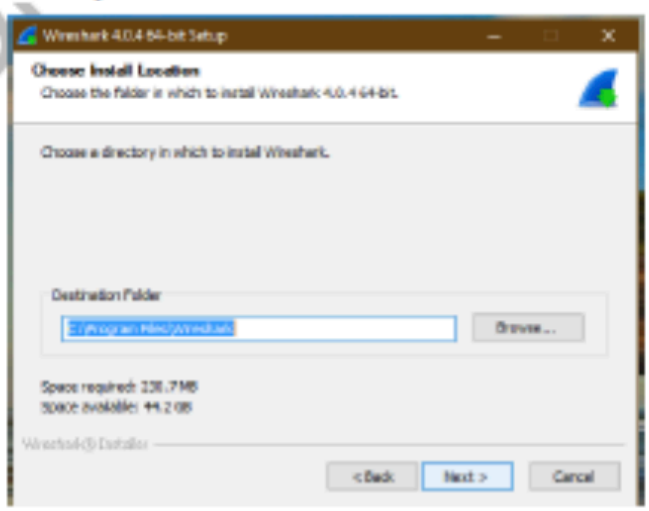
3. Select components of Wireshark to install, as shown below.



4. Click Next in Additional Tasks window.



5. Select location where you wish to install Wireshark, and then click Next.



2.1 What is Network Miner?

Open source network forensics tool that extracts files, images, emails and passwords, from captured network traffic in PCAP files. Can be used to capture live network traffic by sniffing a network interface. Primarily designed to run in Windows, but can also be used in Linux.

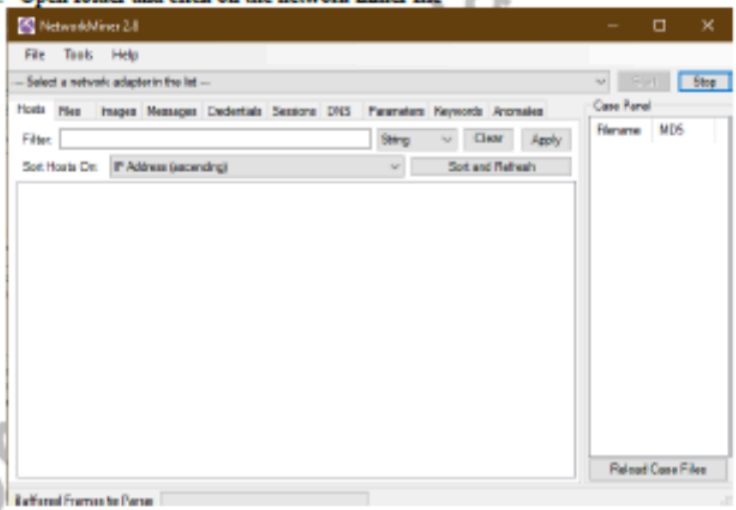
2.2 Benefits of Using Network Miner

Easy-to-use packet capture viewer, easier to use than Wireshark for packet capture analysis as it extracts and sorts found data into categories of hosts (with operating system fingerprinting), files, images, messages, sessions, and more by parsing .**pcapfile**.

- Easy to use, requiring least processing time
- Can extract user credentials (usernames and passwords) for supported protocols and display under "Credentials" tab.
- User can search sniffed or stored data for keywords.
- Allows user to insert arbitrary string or byte-patterns that shall be searched for with keyword search functionality.
- Portable application that doesn't require any installation, which means that USB version, can run directly from USB flash drive.

2.3 Installing Network Miner on Microsoft Windows Systems

1. Download from link: https://www.netresec.com/?download=NetworkMiner
2. Right click on the file and select option extract here
3. Open folder and click on the network miner file



Result:

Thus, basic interface, layout and capabilities of networking tools such as Wire shark and Network Miner was studied and demonstrated through softwares.

Exercise. :

To familiarize with basic network analysis tools, Wireshark and Network Miner, and understand their functionalities in monitoring and analyzing network traffic.

Steps to Perform the Experiment

Part 1: Capturing Packets with Wireshark

1. **Open Wireshark** and select the network interface (Wi-Fi or Ethernet).

2. Click **Start** to begin capturing packets.
3. Open a web browser and visit a website (e.g., www.google.com).
4. Stop the capture after a few seconds.
5. Analyze the captured packets:
    - Use filters (e.g., `http`, `tcp`, `udp`, `dns`) to inspect different protocols.
    - Observe source and destination IP addresses.
    - Check TCP Handshake (SYN, SYN-ACK, ACK).
    - Analyze HTTP requests and responses.
6. Save the captured packets for further analysis.

Part 2: Analyzing Packets with Network Miner

1. Open **Network Miner**.
2. Load the previously captured Wireshark file (`.pcap` file).
3. Analyze extracted data:
    - Identify **hosts** in the network.
    - Check **open ports and services**.
    - Inspect **transferred files and credentials** (if any).
    - Examine DNS queries and responses.
4. Document key findings from the analysis.

Conclusion

This experiment provided hands-on experience with Wireshark and Network Miner. Wireshark is useful for real-time packet capture and deep analysis, while Network Miner is valuable for forensic analysis and extracting meaningful data from captured traffic.

EXPERIMENT - 8

Experiment No. 8
Introduction to Datadog tool for data monitoring in network

Objectives

- To familiarize students with the Datadog tool and its capabilities for monitoring network data.
- To train students on how to use the Datadog tool to monitor network data and analyze data trends.

Theory

- Datadog is a monitoring service for cloud scale applications, providing monitoring of servers databases tools and services through a SaaS-based data analytics platform
- It is used for log management, infrastructure monitoring, and application monitoring.
- It can collect data from servers, databases, containers, and cloud services.
- With Datadog, users can monitor their network in real-time and get alerts when anomalies occur.
- Datadog makes it easy to integrate services such as Slack and PagerDuty for notifications.
- Datadog was built to a cloud infrastructure monitoring service, with a dashboard, alerting and visualizations of metrics
- Datadog was found in 2010 by Oliver Pomel and Alexis Le-Quoc
- Data dog provides functionality in an easy-to-use manner that would be difficult to build and maintain ourselves

- Data dog gathers system metrics, integrates with key software we use, and provides a standard interface to which our applications can send custom metrics
- Has prebuilt integrations to pull data from almost every important service we use
- Generates a consolidated event stream that can be filtered and searched as needed
- Builds dashboards that combine metrics from many different sources to make them more useful. Also provides an powerful interface for interactive exploration of metrics
- Have nice stream processing capabilities for generating alerts, and it can surface them in services like pager duty and slack.

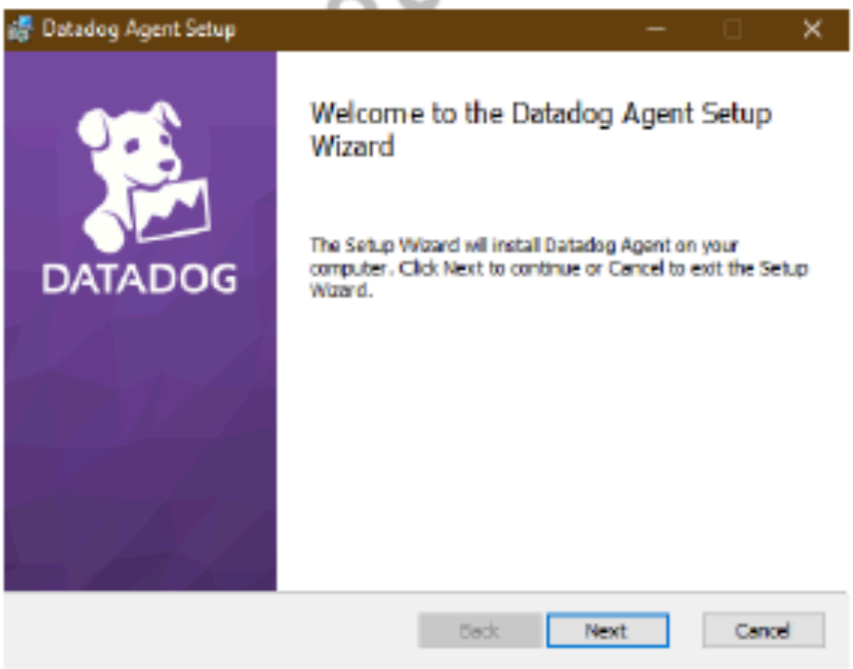
Procedure to download Data Dog Agent

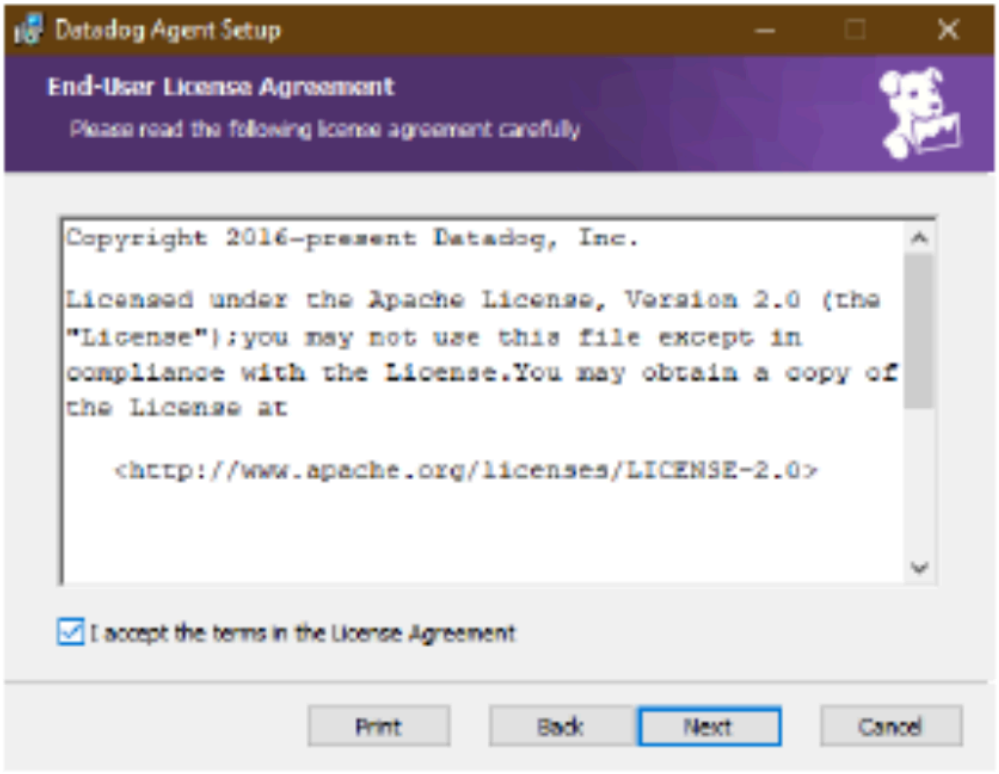
Step 1: Register for Datadog - Monitoring as a Service To register for Datadog, follow the steps given below:

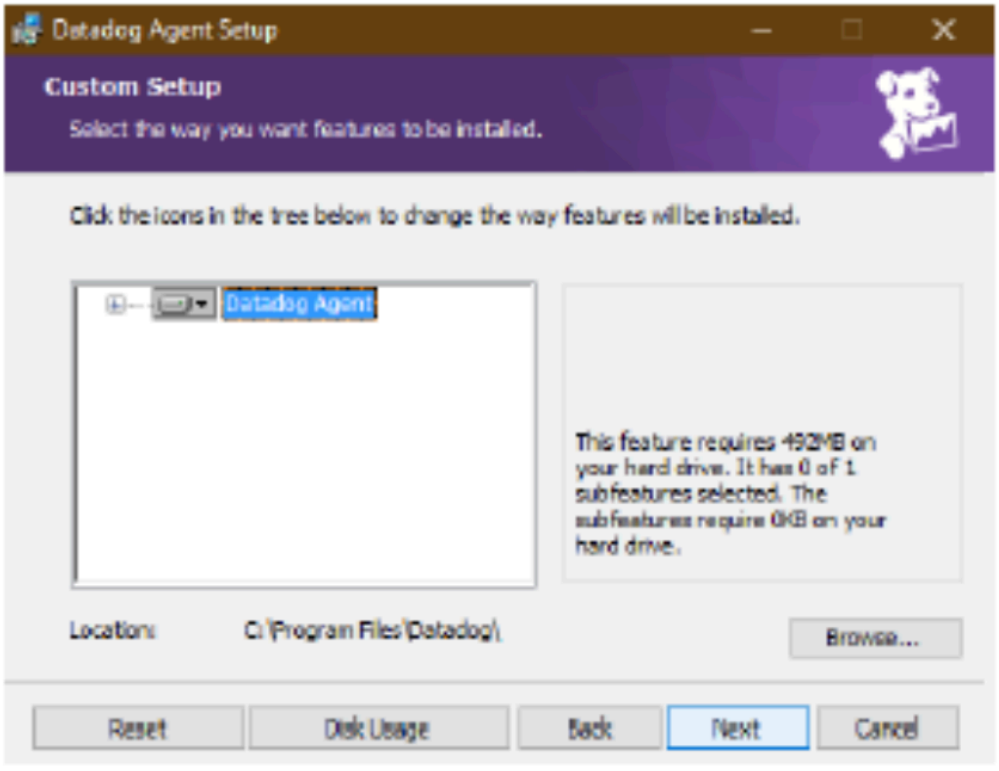
- Go to the Datadog website https://www.datadoghq.com/
- Click on the "start free trial" button on the top right of the website.
- Fill out the form and click on the "Create Account" button.

Step 2: Installation of agents on Windows machines: to install Datadog agents on Windows machines, follow the steps given below:

- Log in to your Datadog account.
- Go to the Agents Download page.
- Download the Datadog Agent installer.
- Run the installer (as Administrator) by opening **datadog-agent-7-latest.amd64.msi**.
- Follow the prompts, accept the license agreement, and enter your Datadog API key: 68e98ae58bf1b1a95dcf609b8e2ce2e3.
- Then enter your Datadog Region: datadoghq.com .
- Follow the on-screen instructions to install the agent on your Windows machine.
- When the install finishes, you are given the option to launch the Datadog Agent Manager.




Datadog Agent Setup
End-User License Agreement
Please read the following license agreement carefully
Copyright 2016-present Datadog, Inc.
Licensed under the Apache License, Version 2.0 (the "License");you may not use this file except in compliance with the License.You may obtain a copy of the License at
<http://www.apache.org/licenses/LICENSE-2.0>
I accept the terms in the License Agreement
Print
Back
Next
Cancel


Datadog Agent Setup
Custom Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
Datadog Agent
This feature requires 492MB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.
Location:
C:\Program Files\Datadog\
Browse...
Reset
Disk Usage
Back
Next
Cancel

Step 4: Monitor your network data with Datadog: To monitor the network data with Datadog, follow the steps given below:

- Log in to your Datadog account.
- Navigate to the Monitoring page.
- Customize the dashboard as per your requirement.
- Add widgets for the services that you want to monitor.
- Configure alerts for anomalies in the network data.

Result:

In this practical, how to set up Datadog and monitor network data using it was studied. It was observed how Datadog helps analyze the data trends and identifies anomalies in real-time. Additionally, Datadog was demonstrated to be effective for monitoring infrastructure and applications in cloud-based environments, utilizing its user-friendly interface and integration capabilities. Given its powerful monitoring and analytics capabilities, Datadog is a valuable tool for network data analysis.

Exercise 1: Setting Up Datadog for Network Monitoring

Objective: Install and configure Datadog to monitor a network.

Steps:

1. **Sign Up & Install**
    - Sign up on Datadog.
    - Install the **Datadog Agent** on your system using the provided instructions.
2. **Enable Network Monitoring**
    - Navigate to **Integrations > Agent** and enable **Network Performance Monitoring (NPM)**.
    - Verify that the agent is running using: **sudo datadog-agent status**

3. Check Network Traffic

- View the **Network Map** under **Network Monitoring** in the Datadog dashboard.
- Identify top talkers (hosts with high network activity).

4. Analyze TCP Connections

- Run: **sudo netstat -an**

Exercise 2: Detecting Anomalous Network Behavior

Objective: Set up alerts for unusual network traffic.

Steps:

1. **Create a Custom Alert**
    - In Datadog, go to **Monitors > New Monitor**.
    - Select **Network Performance** as the type.
    - Set a condition: “Alert me if network traffic exceeds X Mbps for Y minutes.”
2. **Simulate High Traffic**
    - Use **iPerf** to generate network load:

```
iperf3 -s                          # On one machine (server)
iperf3 -c <server-ip> -t 60 -b 100M                    # On another machine (client)
```

Exercise 3: Log Analysis for Network Security

Objective: Analyze logs to detect security threats.

Steps:

1. **Enable Log Collection**
    - Go to **Logs > Configure** and enable log collection.
    - Run:

sudo datadog-agent config set logs_enabled true

sudo systemctl restart datadog-agent

2. Inject a Suspicious Log Entry

- Append this to `/var/log/syslog`: **echo "Unauthorized access attempt detected" >> /var/log/syslog**

3. Query Logs in Datadog

- Use the **Log Explorer** in Datadog to search for `"Unauthorized access"`.

Exercise 4: Monitoring Packet Loss & Latency

Objective: Track packet loss and network latency using Datadog.

Steps:

1. **Enable Ping Monitoring**
    - In Datadog, go to **Synthetic Monitoring** and create a new **Ping Test** to an external server (e.g., Google DNS `8.8.8.8`).
2. **Check for Packet Loss**
    - Run: **ping -c 50** google.com

3. Compare Results in Datadog

- Check if Datadog's network monitoring matches the command-line results.