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.

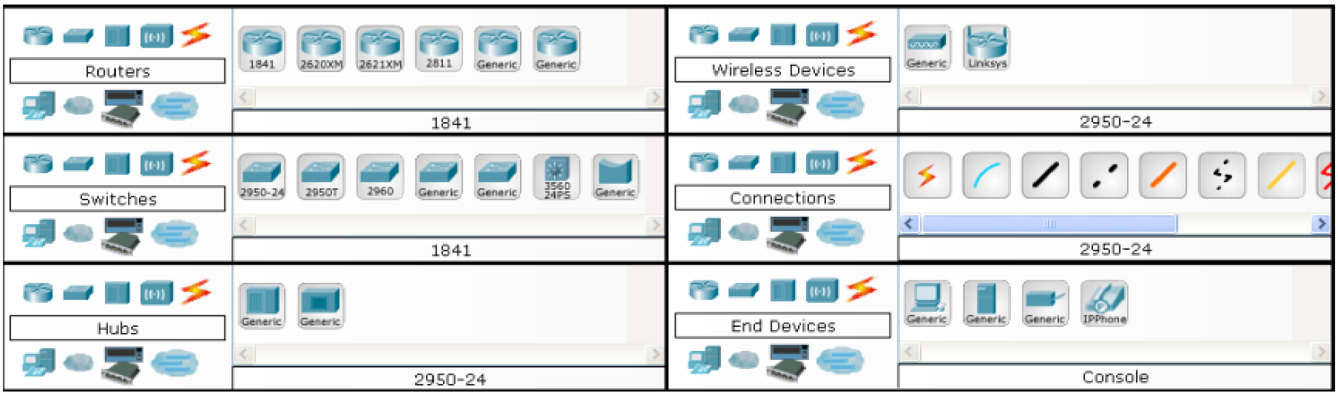
Step 4. When prompted, click on Skills For All green button to authenticate.

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

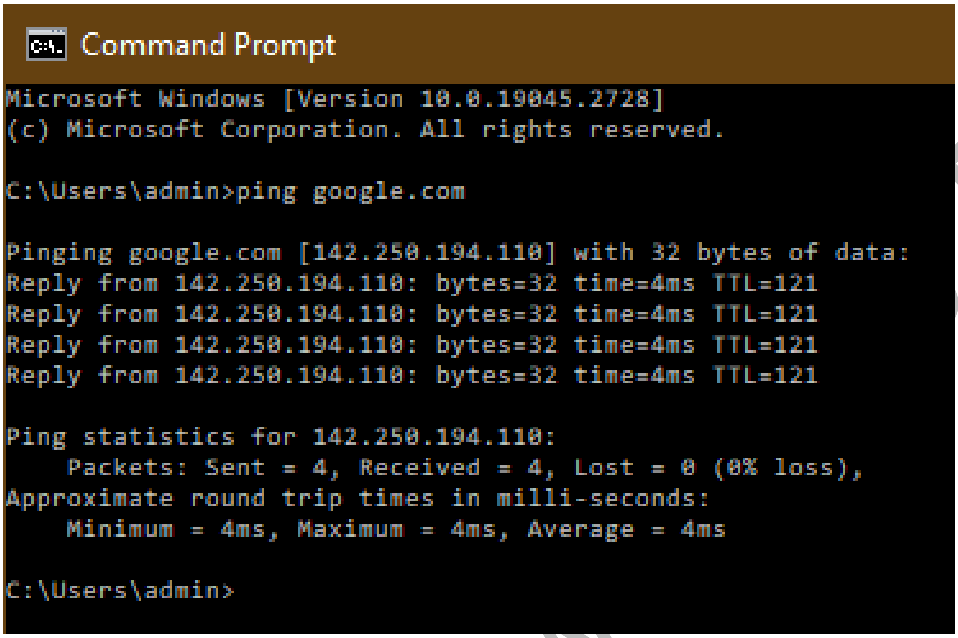
Host	IP Address	Subnet Mask
PC0	192.68.1.10	255.255.255.0
PC1	192.68.1.11	255.255.255.0

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

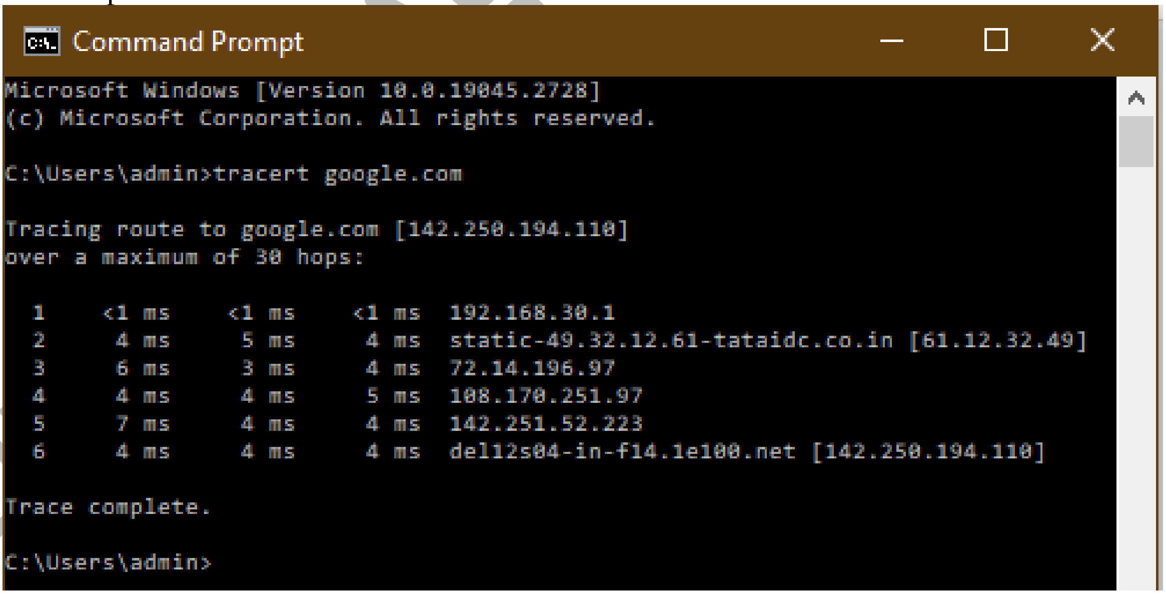
Commands:

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.



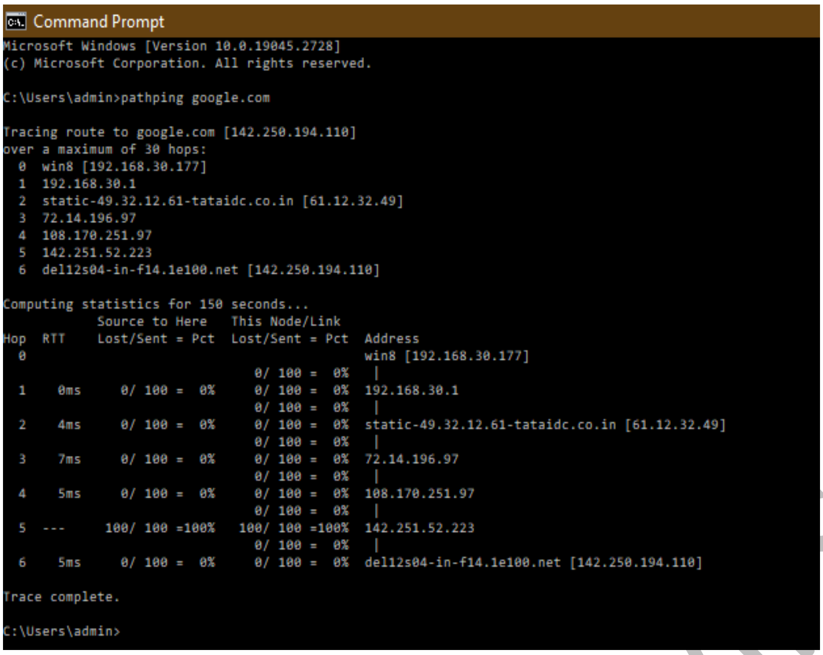
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping google.com

Pinging google.com [142.250.194.110] with 32 bytes of data:
Reply from 142.250.194.110: bytes=32 time=4ms TTL=121
Reply from 142.250.194.110: bytes=32 time=4ms TTL=121
Reply from 142.250.194.110: bytes=32 time=4ms TTL=121
Reply from 142.250.194.110: bytes=32 time=4ms TTL=121

Ping statistics for 142.250.194.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\admin>
```

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.



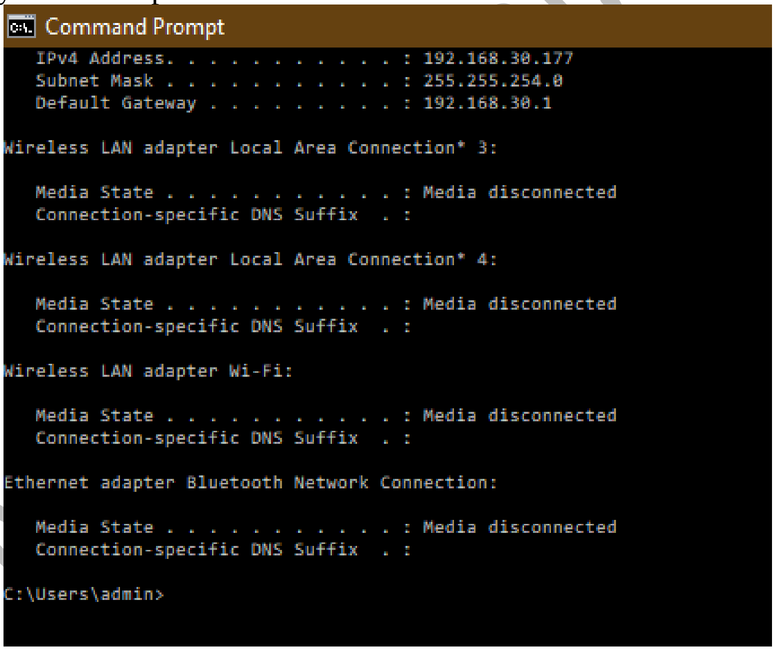
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>tracert google.com

Tracing route to google.com [142.250.194.110]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.30.1
  2     4 ms     5 ms     4 ms  static-49.32.12.61-tataidc.co.in [61.12.32.49]
  3     6 ms     3 ms     4 ms  72.14.196.97
  4     4 ms     4 ms     5 ms  108.170.251.97
  5     7 ms     4 ms     4 ms  142.251.52.223
  6     4 ms     4 ms     4 ms  del12s04-in-f14.1e100.net [142.250.194.110]

Trace complete.

C:\Users\admin>
```

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.



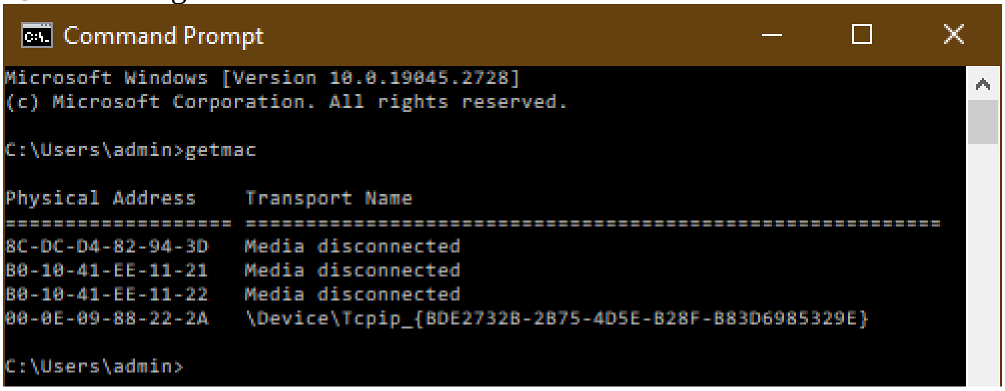
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

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.



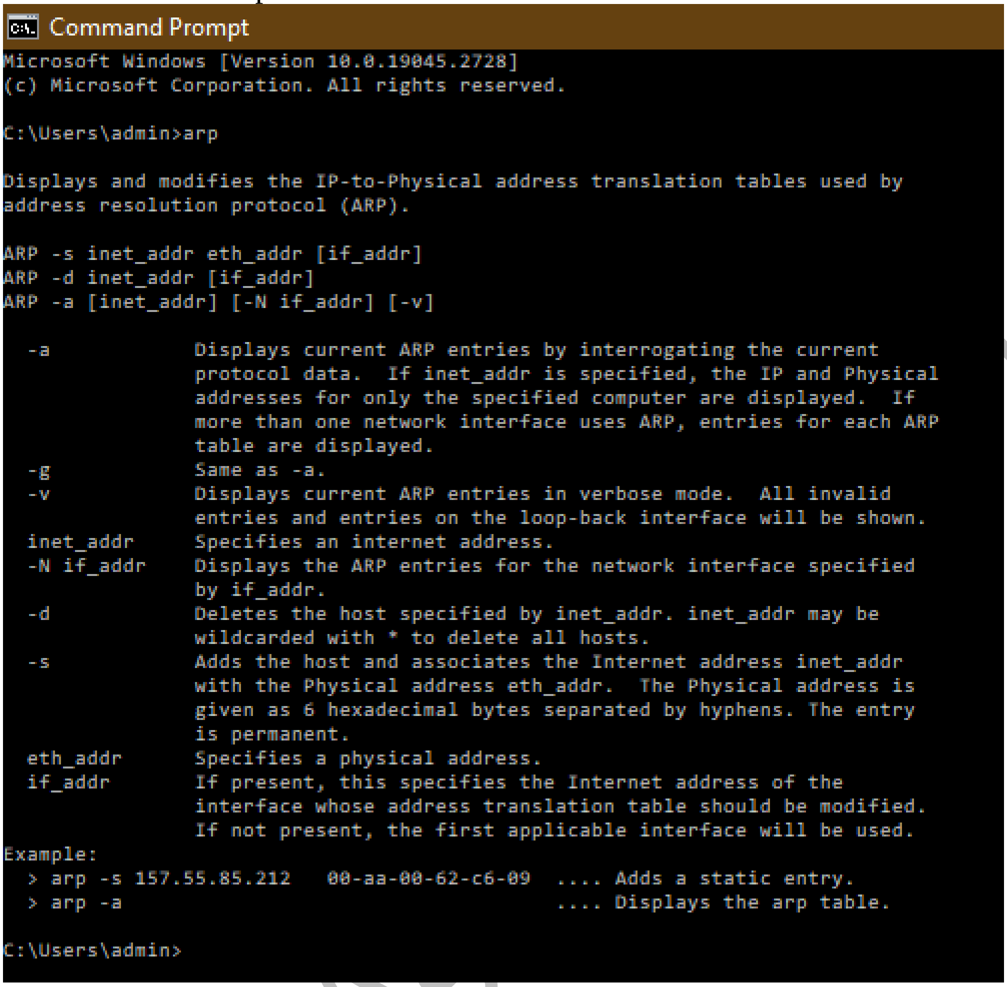
```
   IPv4 Address. . . . . . . . . . . : 192.168.30.177
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 192.168.30.1

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



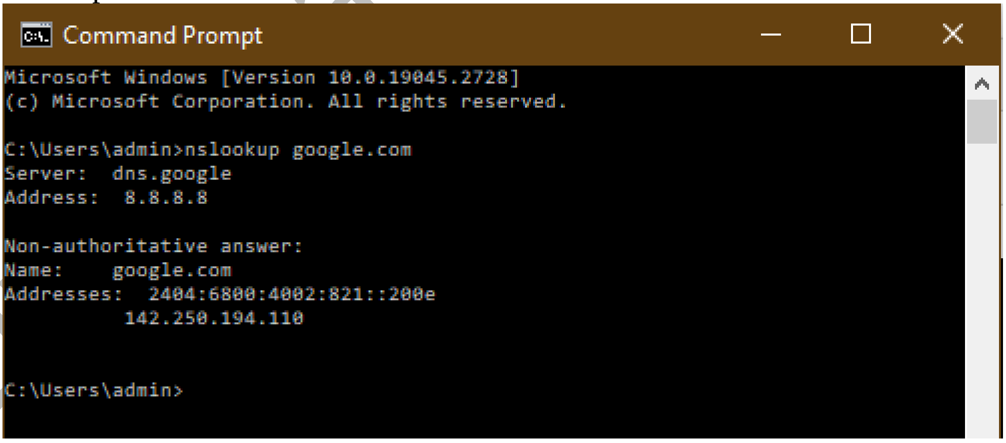
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

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.



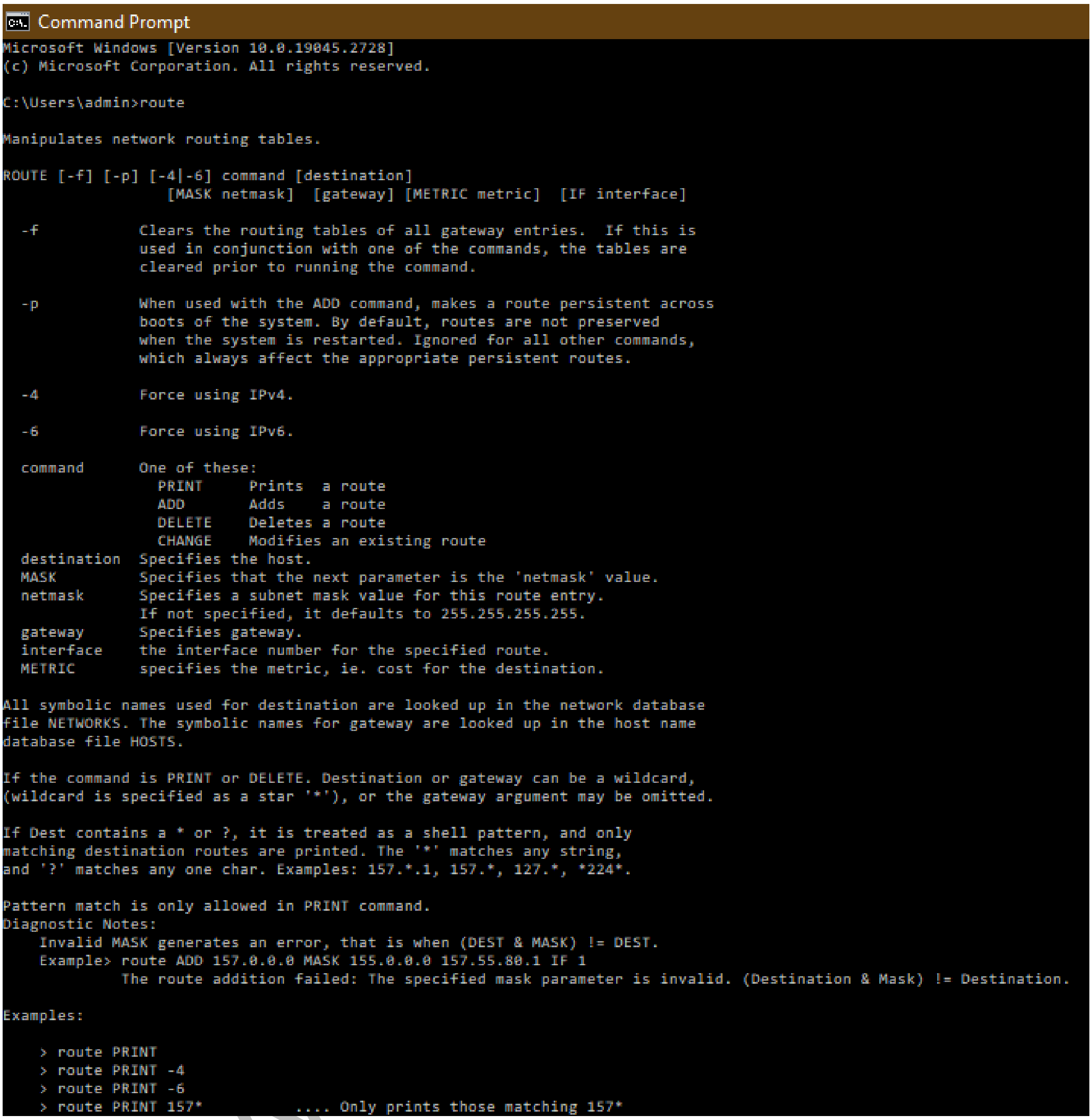
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>arp

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

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

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

C:\Users\admin>
```

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.



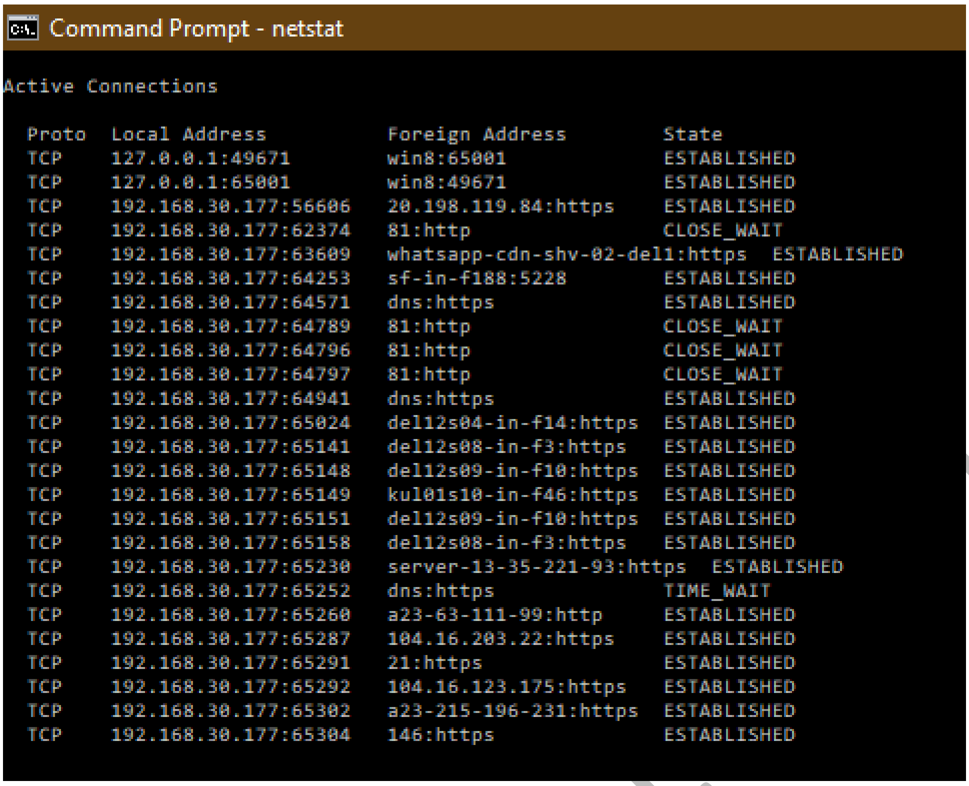
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>nslookup google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:821::200e
          142.250.194.110


C:\Users\admin>
```

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



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

C:\Users\admin>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

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

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

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

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

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*
```

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



```
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:

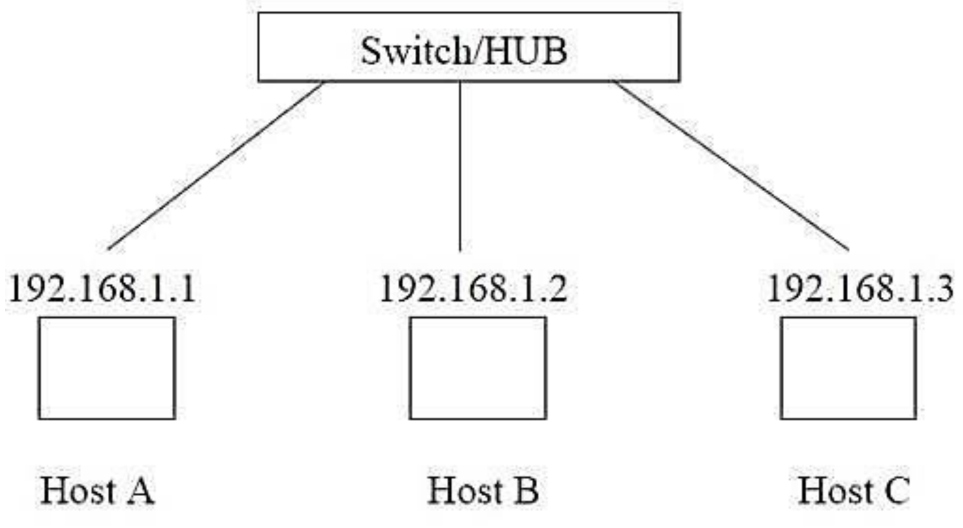
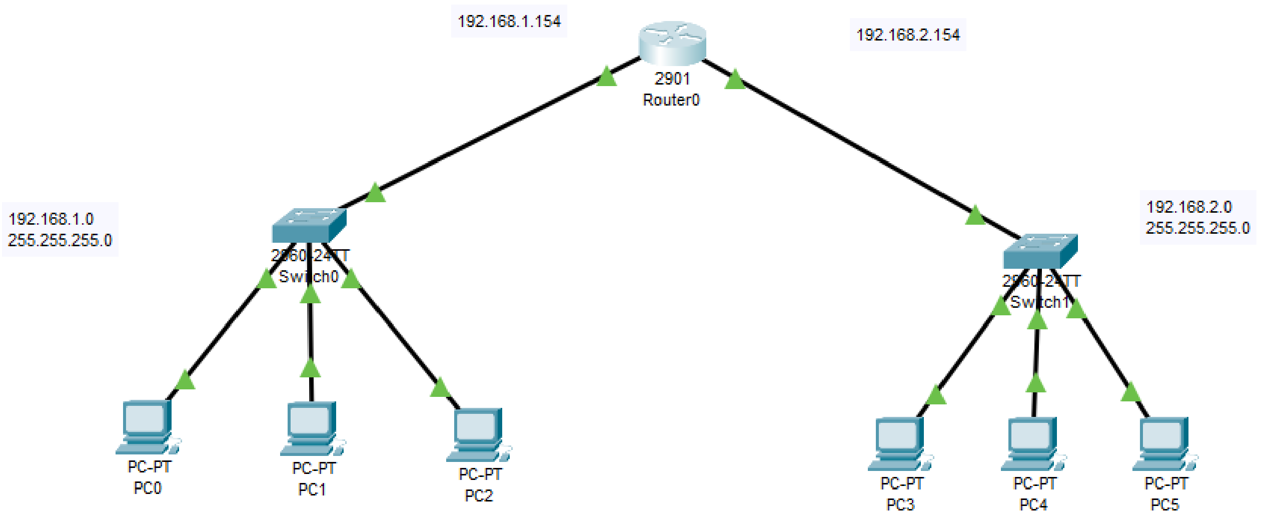


Figure 1: Establishing a LAN



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 :

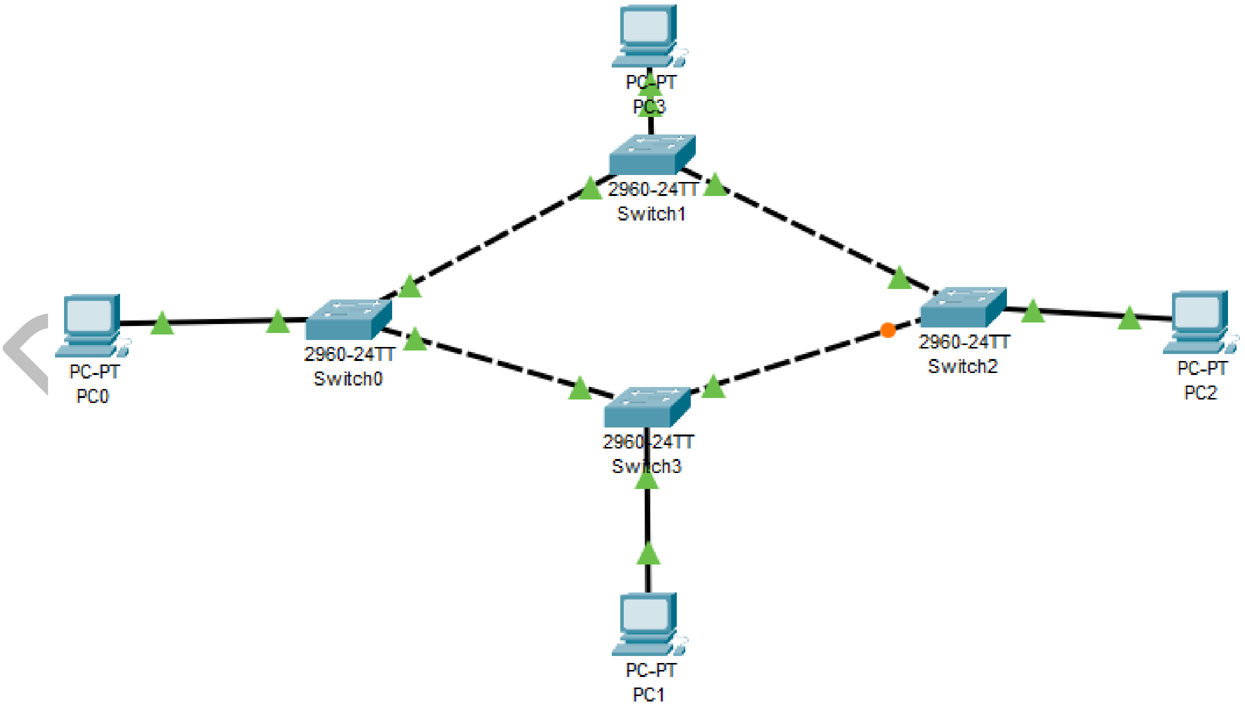
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

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

IP Addressing Table

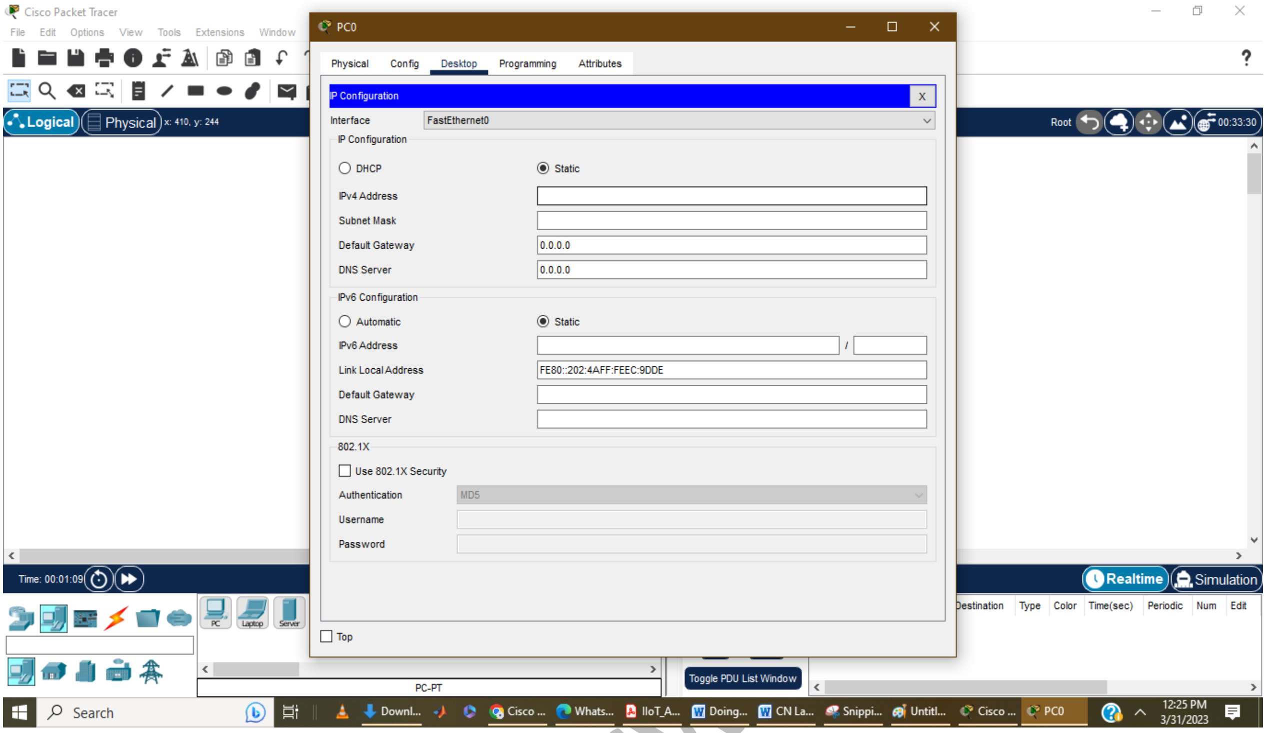
S.NO	Device	IPv4 Address	Subnet Mask
1.	**PC0**	192.168.0.1	255.255.255.0
2.	**PC1**	192.168.0.2	255.255.255.0
3.	**PC2**	192.168.0.3	255.255.255.0
4.	**PC3**	192.168.0.4	255.255.255.0

- 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.



PC0 — Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:4AFF:FEEC:9DDE

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

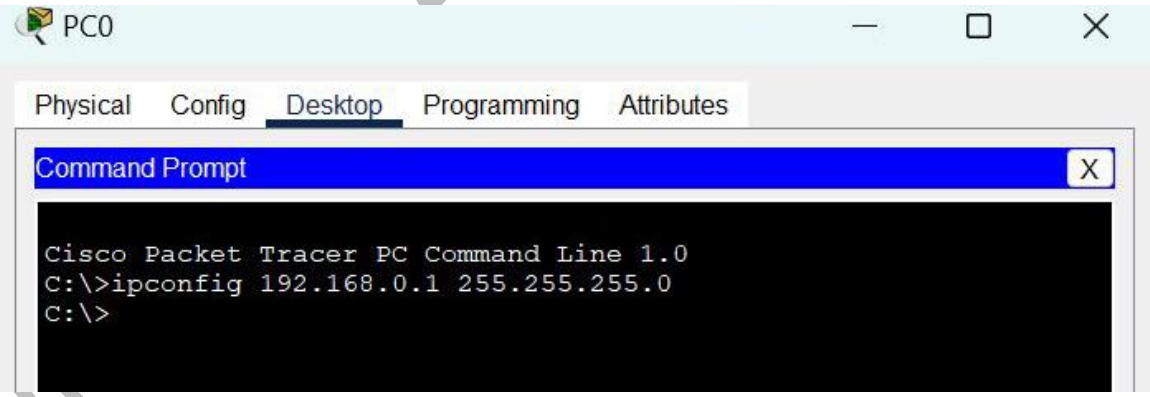
Username:

Password:

□ Top

- 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

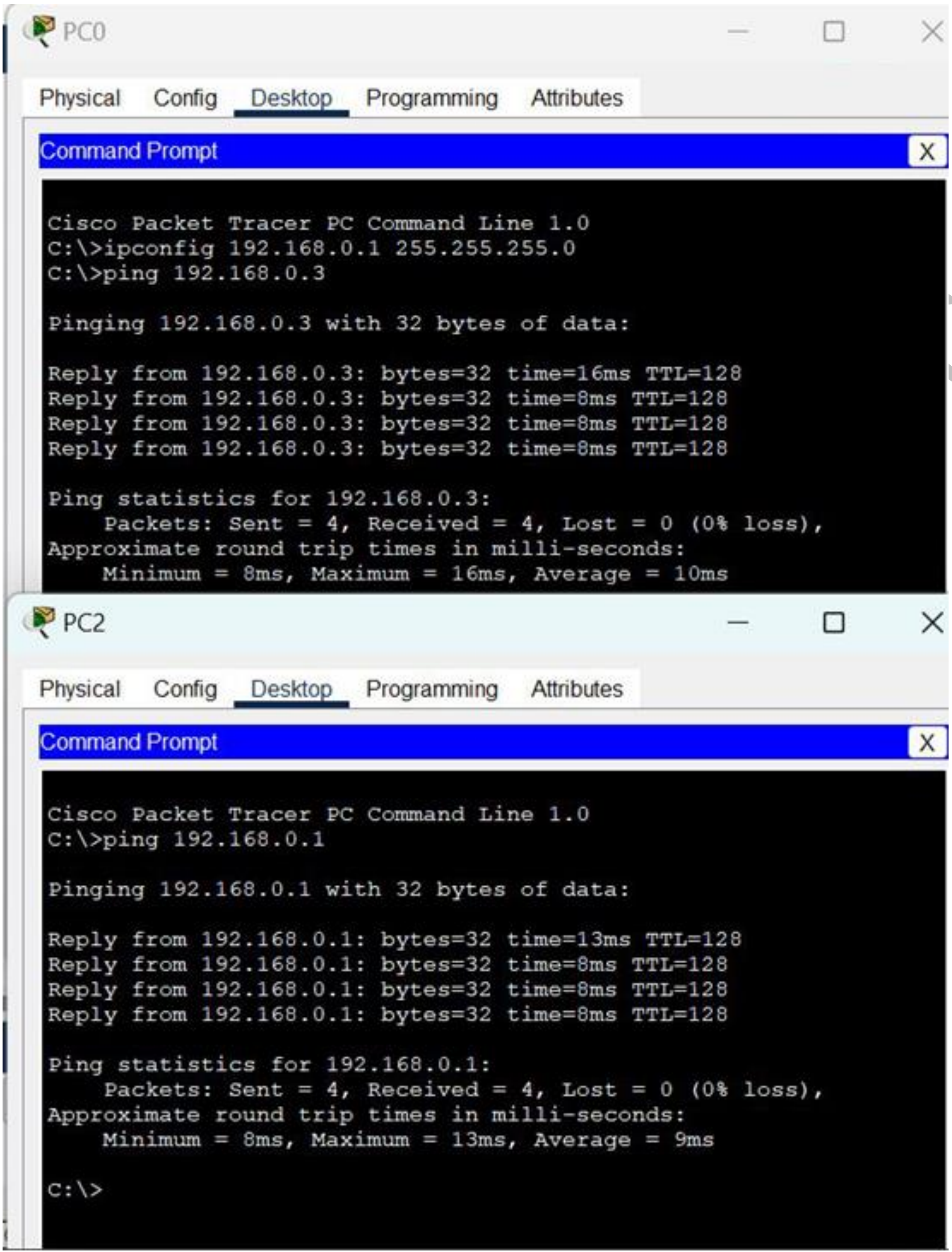


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.0.1 255.255.255.0
C:\>
```

- 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.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.0.1 255.255.255.0
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=16ms TTL=128
Reply from 192.168.0.3: bytes=32 time=8ms TTL=128
Reply from 192.168.0.3: bytes=32 time=8ms TTL=128
Reply from 192.168.0.3: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 16ms, Average = 10ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=13ms TTL=128
Reply from 192.168.0.1: bytes=32 time=8ms TTL=128
Reply from 192.168.0.1: bytes=32 time=8ms TTL=128
Reply from 192.168.0.1: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 13ms, Average = 9ms

C:\>
```

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:

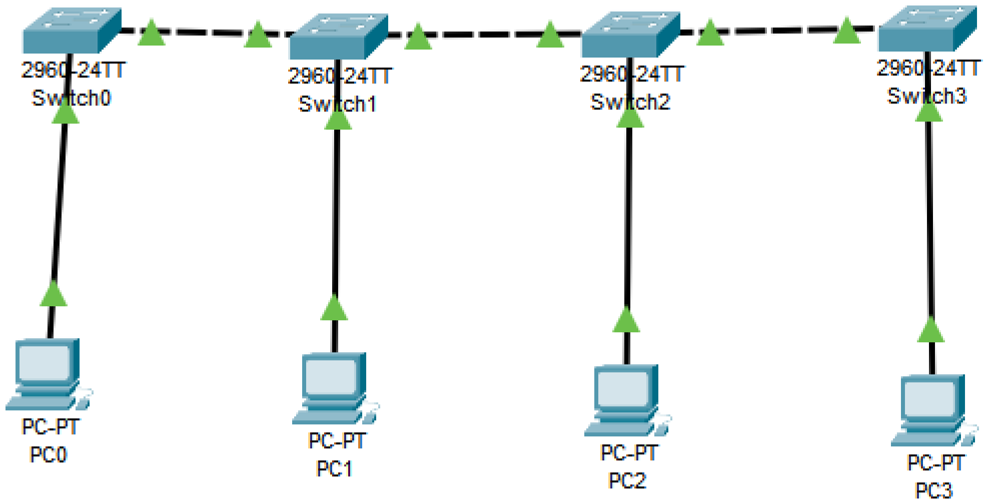
Step 1: First, open the cisco packet tracer desktop and select the devices given below:

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.

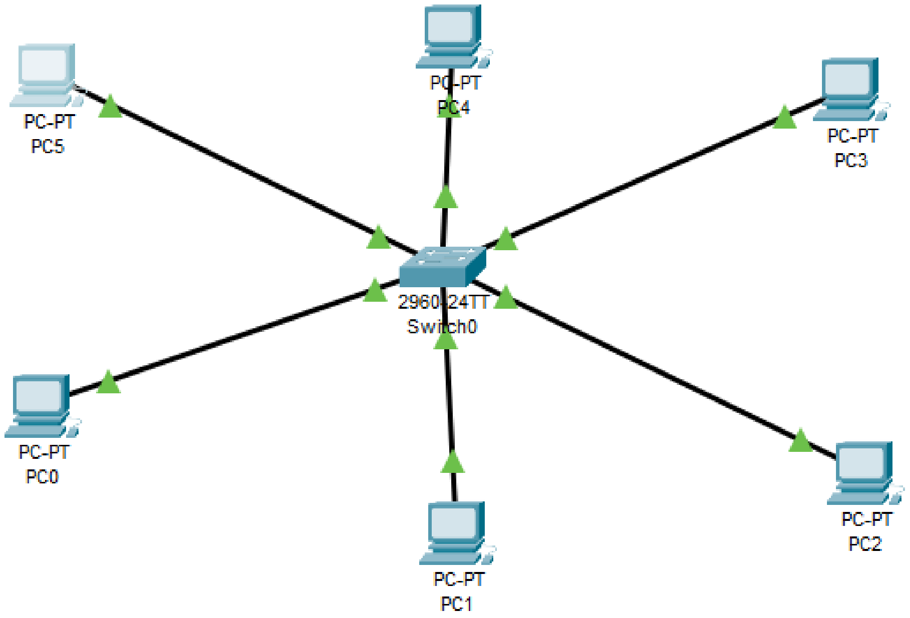
Simulation Result:

- 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

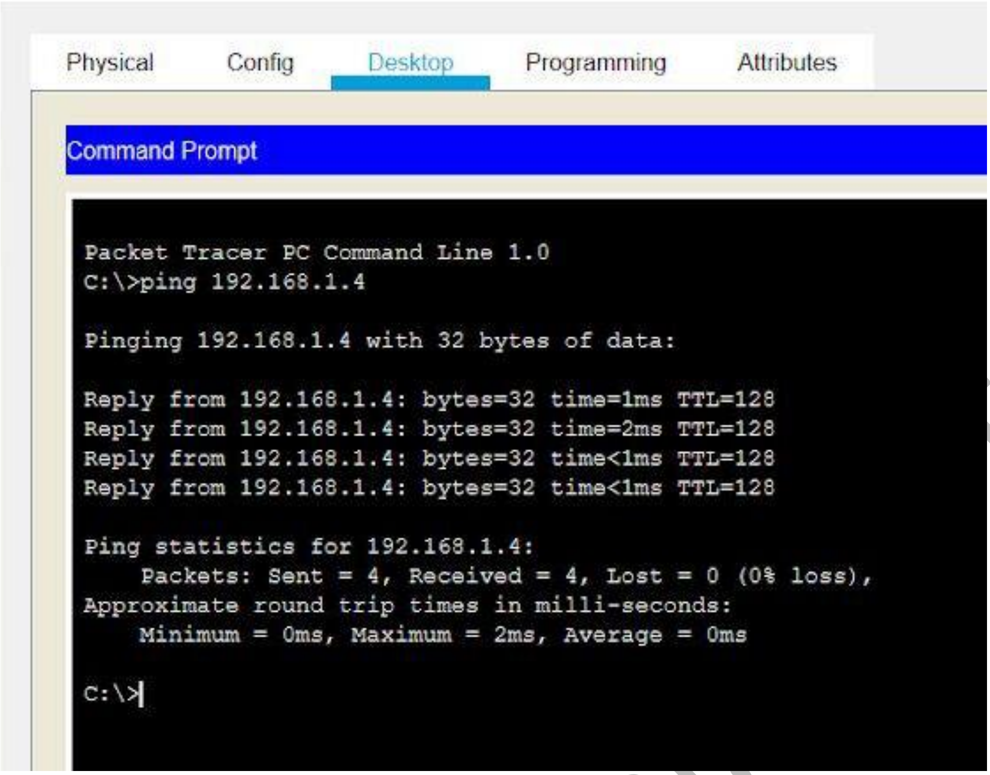
To do ping one terminal of one device and run the following command:

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.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=2ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

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:

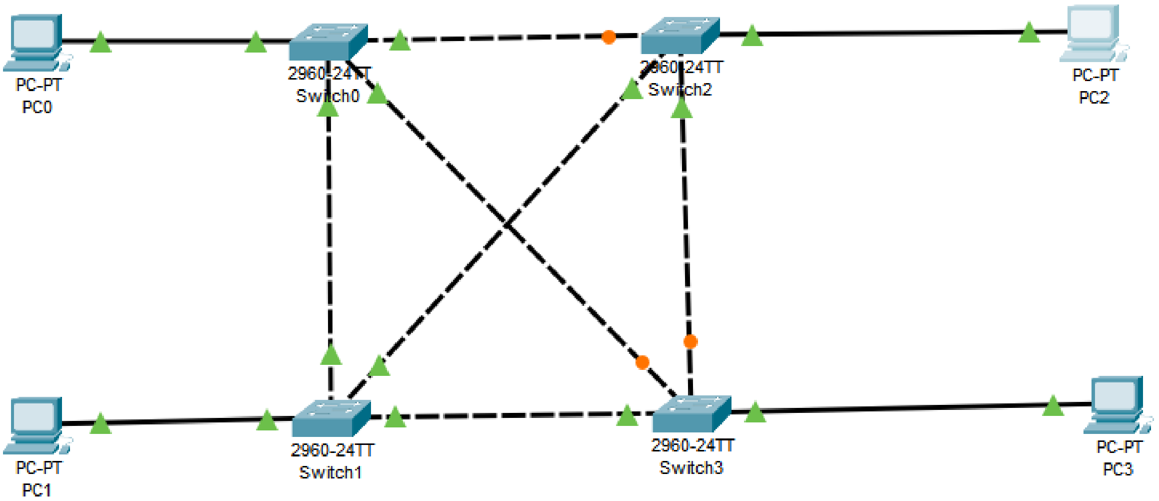
Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

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 No. 5

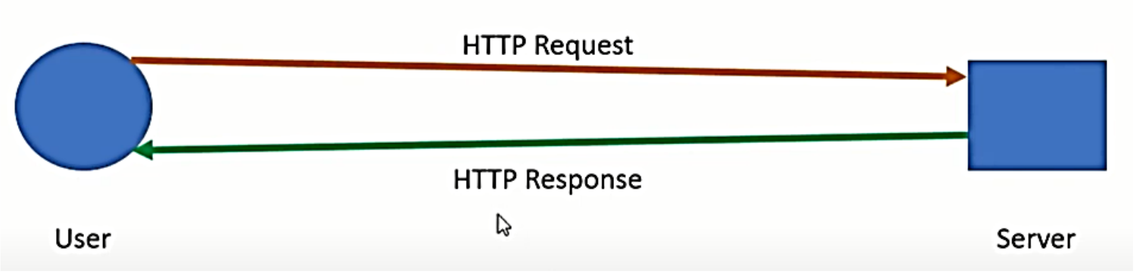
Explore various aspects of HTTP Protocols.

Objectives

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

Theory

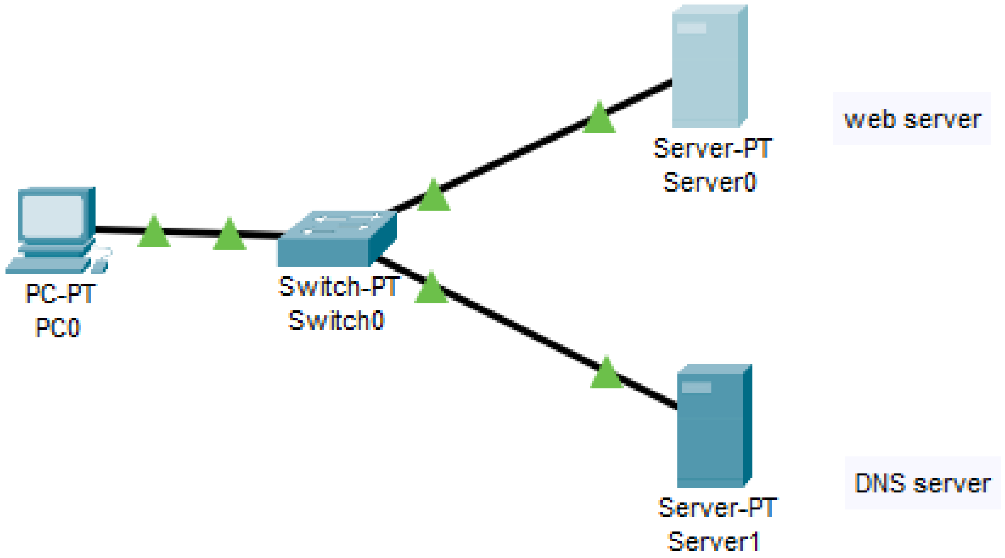
Hypertext is text that links to other information by clicking on a link in a hypertext document, a user can quickly jump to different content through hypertext. It is associated with web pages and this technology has been around since 1960s. Today, the web is where hypertext reigns, where nearly every page includes links to other pages and both text and images can be used as links to more content. HTTP protocol stands for Hyper Text Transfer Protocol. Work of DNS server is to map domain name to its corresponding IP address.



Steps to Configure Web Server / HTTP in CPT

Step 1. Open Cisco Packet Tracer

Step 2. Make a topology as shown in picture by selecting 1 PC/Laptop, 1 PT switch and 2 servers. (Label one server as web server and another as DNS server)



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	IP Address	Subnet Mask	DNS server
PC0	192.168.1.1	255.255.255.0	192.168.1.3
Web Server	192.168.1.2	255.255.255.0	192.168.1.3
DNS server	192.168.1.3	255.255.255.0	192.168.1.3

Step 5.Double click on web server (Server 0) and select services tab. Go to HTTP option. Open index.html.

Step 6. In index.html file, edit the pre-written code to code shown below.

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to Computer Networks Lab to learn about various aspects of HTTP
protocol in Cisco Packet Tracer.
<h2> by Dr. Divya Agarwal<h2>
</html>
```

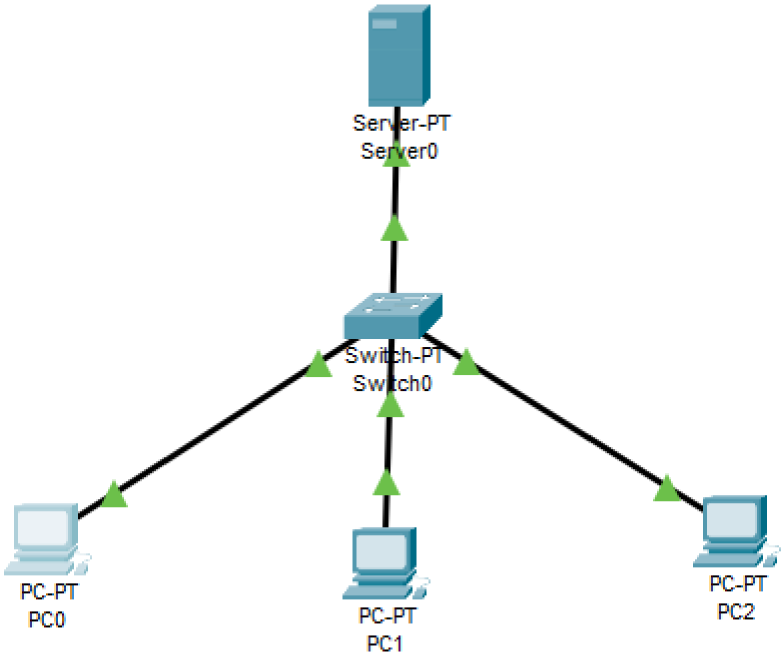
Step 7. Click on Save and in dialog box press yes.

Step 8. Double click on DNS server. Under services tab, select DNS option. Turn on the radio button next to DNS option. In the DNS tab mention name **(Your name)** of the website that you created in web server and in the address option mention web server IP address (refer table). Click on save

Step 9. Double click on PC/Laptop. Go to services tab and select web browser option. In the url field write the name of website created or IP address of web server. Click ok

Exercises to do

Task 1. Open Cisco Packet Tracer, Make a topology as shown in picture by selecting 3 PC/Laptop, 1 PT switch and 1 servers. (Label server as web server). Assign IP address as given



Host	IP Address	Subnet Mask	DNS server
PC0	192.168.1.1	255.255.255.0	192.168.1.5
PC1	192.168.1.2	255.255.255.0	192.168.1.5
PC2	192.168.1.3	255.255.255.0	192.168.1.5
Web Server	192.168.1.4	255.255.255.0	192.168.1.5

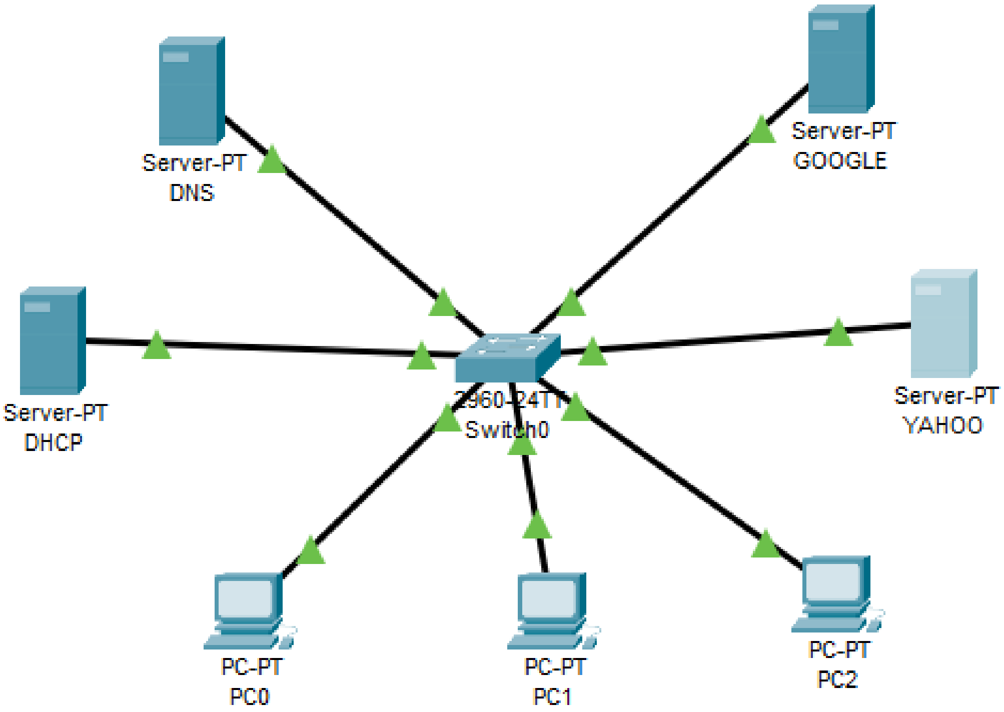
In index.html file, edit the pre-written code to code shown below.

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer Task 1</font></center>
<hr>Learning about various aspects of HTTP protocol in Cisco Packet Tracer.
<h2> by (your name)<h2>
```

</html>

Now call web server ip address, helloworld.html, image.html, copyrights.html from each PC and paste its screenshots

Task 2. Open Cisco Packet Tracer, Make a topology as shown in picture by selecting 3 PC/Laptop, 1 2960 switch and 4 servers. (Label all servers as mentioned).



- 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>
  <center><font size='+2' color='blue'>Welcome to google.com </font></center>
  <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:

```
<html>
<center><font size='+2' color='blue'>Welcome to yahoo.com </font></center>
<hr>Computer Networks Lab task 2.
</html>
```

- **Now call www.google.com, www.yahoo.com from each PC using web browser service option and paste its screenshots**

Experiment No. 6
Analyzing various parameters for TCP protocol in action

Objectives

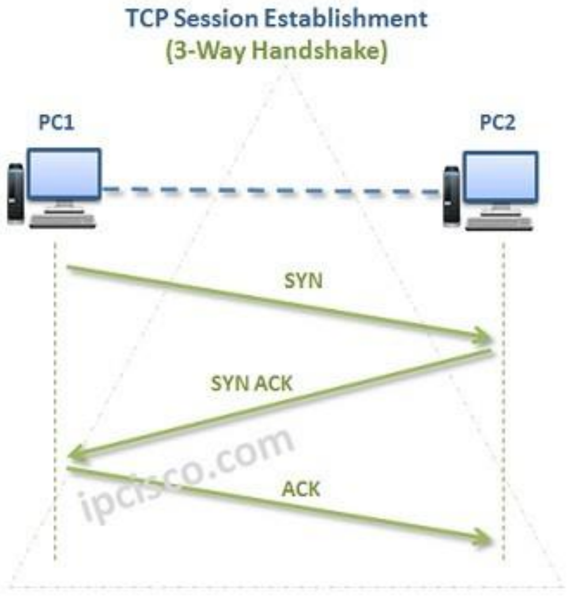
- To generate Network Traffic in Simulation Mode
- This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail.
- Examine the Functionality of the TCP and UDP Protocols in a network setup and its demonstration through Cisco Packet Tracer Tool

Theory

Simulation mode provides the ability to view the functionality of the different protocols. As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC. This activity provides an opportunity to explore the functionality of the TCP and UDP protocols, multiplexing and the function of port numbers in determining which local application requested the data or is sending the data.

Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets. TCP is a Connection Oriented Transport Protocol. A TCP session must be established to use TCP. This TCP Session is established with a Three-way Handshake mechanism. And it can be terminated with Four-way Handshake mechanism.

Three-way Handshake mechanism consists of three messages as its name implies. These messages are: SYN, SYN-ACK, ACK. In these segments, related TCP Header Flags are set to 1 i.e., if it is a SYN message, SYN bit is set to 1; if it is a SYN-ACK message, SYN and ACK bits are set to 1; or if it is an ACK message, ACK bit is set to 1.



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 No. 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

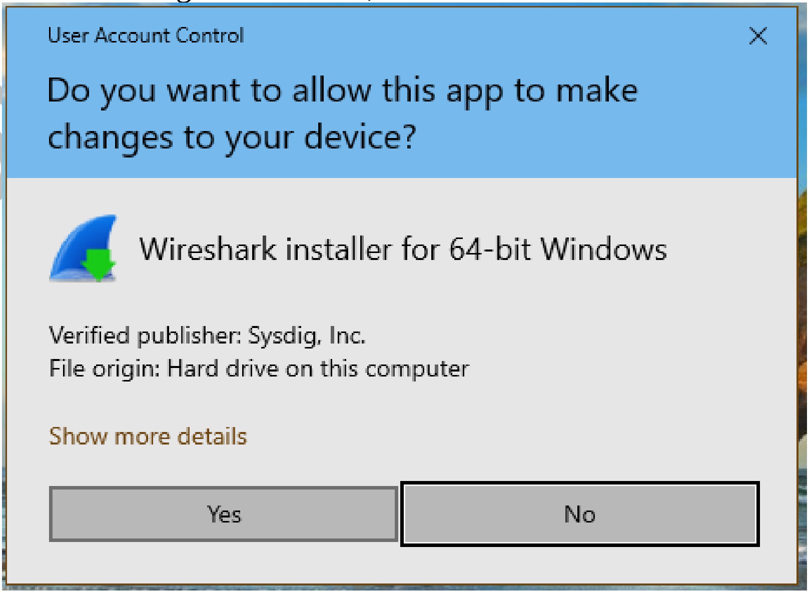
Wireshark offers several benefits that make it appealing for everyday use. It is aimed at both single-user and expert packet analyst, and offers a variety of features to entice each.

- **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.

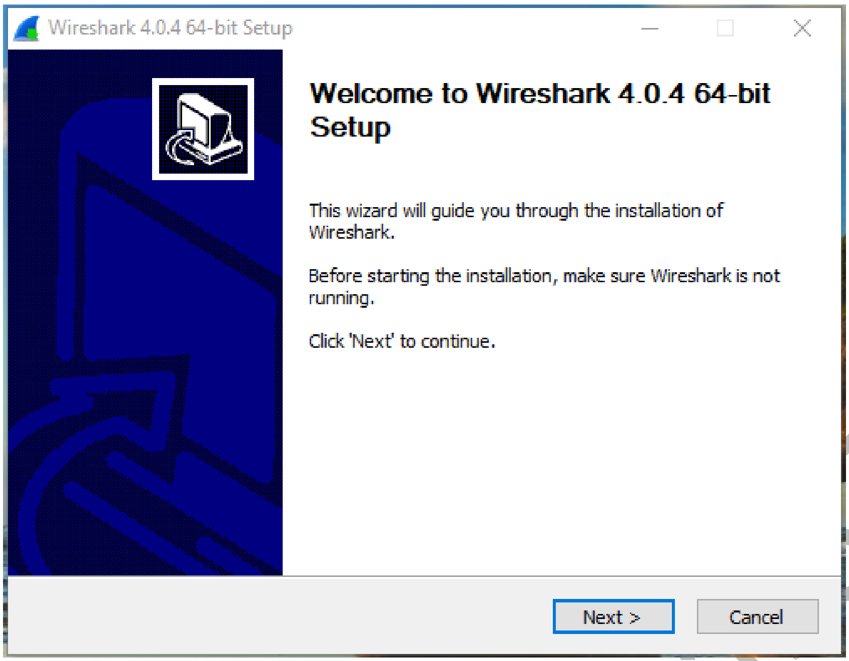


User Account Control

Do you want to allow this app to make changes to your device?

Wireshark installer for 64-bit Windows

Verified publisher: Sysdig, Inc.
File origin: Hard drive on this computer



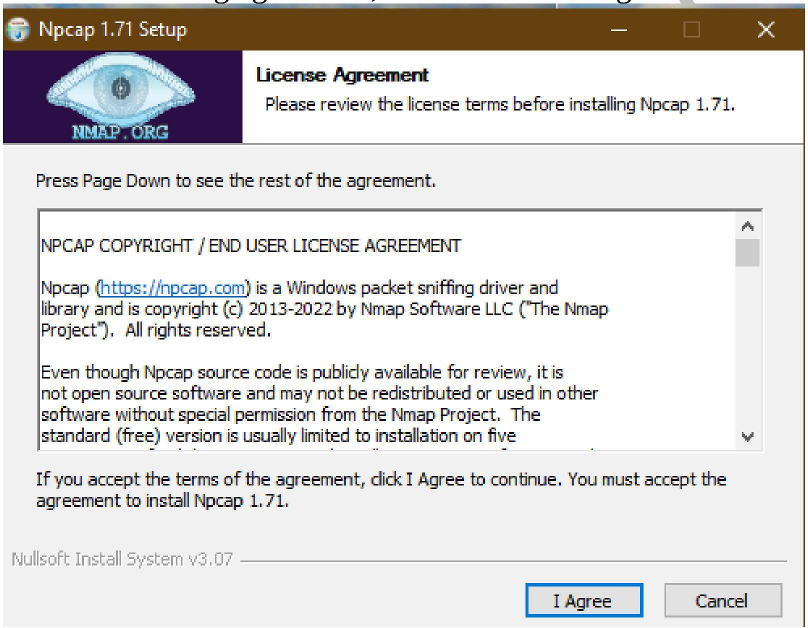
Welcome to Wireshark 4.0.4 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

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



License Agreement

Please review the license terms before installing Npcap 1.71.

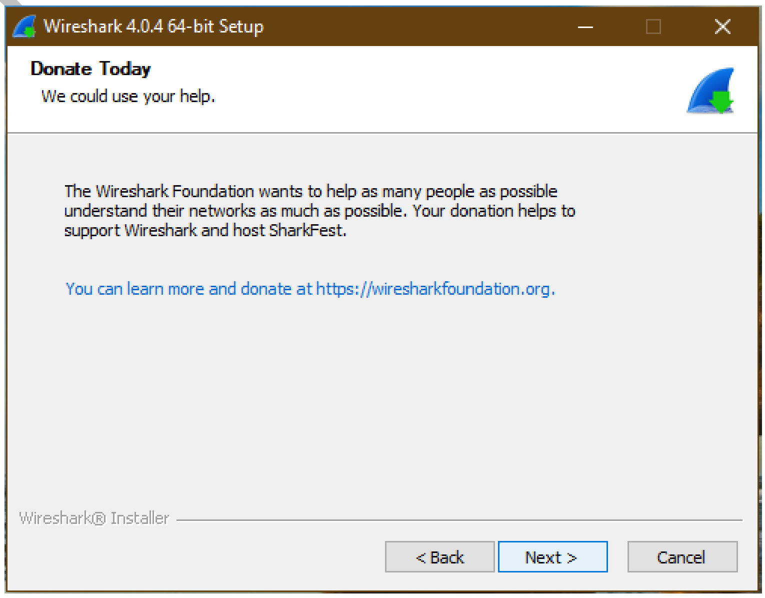
Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.71.



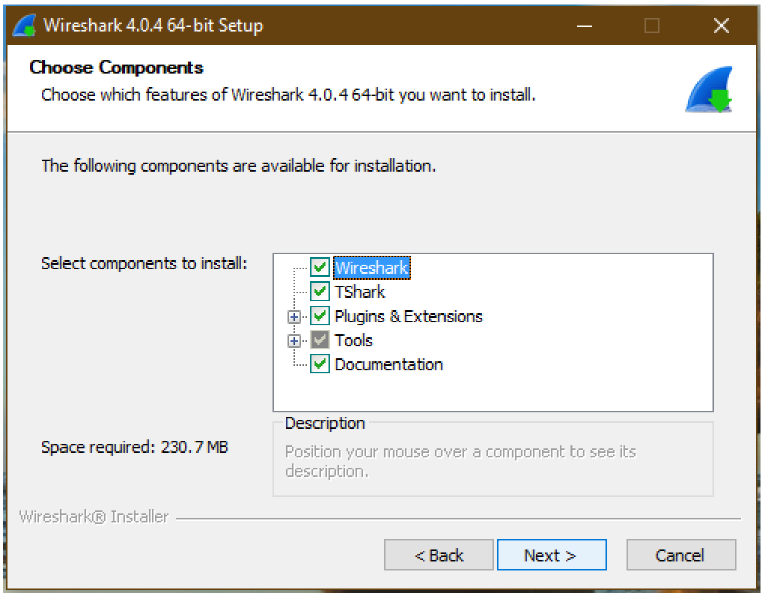
Donate Today

We could use your help.

The Wireshark Foundation wants to help as many people as possible understand their networks as much as possible. Your donation helps to support Wireshark and host SharkFest.

You can learn more and donate at https://wiresharkfoundation.org.

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



Wireshark 4.0.4 64-bit Setup

Choose Components

Choose which features of Wireshark 4.0.4 64-bit you want to install.

The following components are available for installation.

Select components to install:

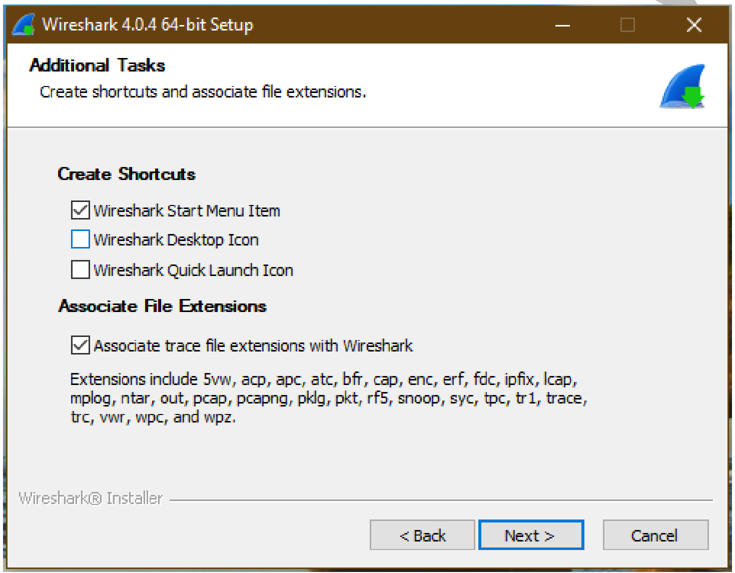
- ☑ Wireshark
- ☑ TShark
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ Documentation

Description

Position your mouse over a component to see its description.

Space required: 230.7 MB

4. Click Next in Additional Tasks window.



Wireshark 4.0.4 64-bit Setup

Additional Tasks

Create shortcuts and associate file extensions.

Create Shortcuts

☑ Wireshark Start Menu Item

□ Wireshark Desktop Icon

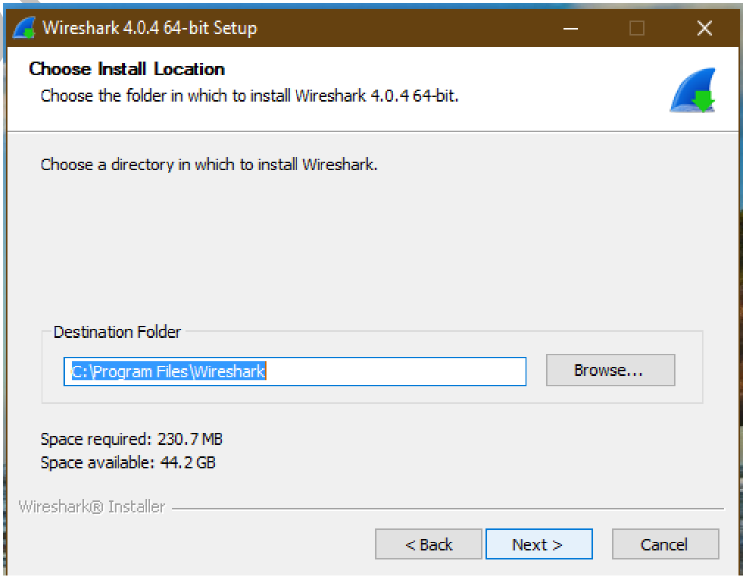
□ Wireshark Quick Launch Icon

Associate File Extensions

☑ Associate trace file extensions with Wireshark

Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.

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



Wireshark 4.0.4 64-bit Setup

Choose Install Location

Choose the folder in which to install Wireshark 4.0.4 64-bit.

Choose a directory in which to install Wireshark.

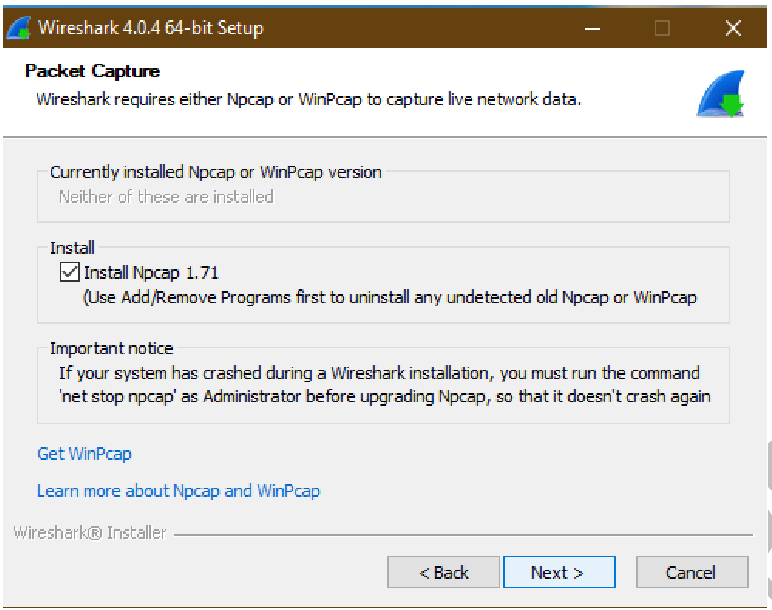
Destination Folder

C:\Program Files\Wireshark

Space required: 230.7 MB

Space available: 44.2 GB

6. Make sure Install WinPcap box is checked, as shown in Figures, and then click Install.


Wireshark 4.0.4 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap or WinPcap version

Neither of these are installed

Install

☑ Install Npcap 1.71

(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap

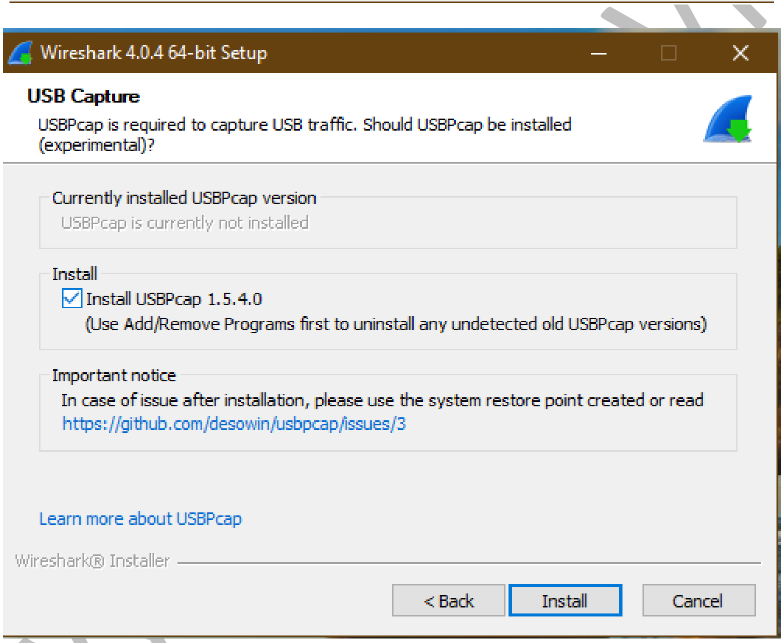
Important notice

If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again

Get WinPcap

Learn more about Npcap and WinPcap

Wireshark® Installer


Wireshark 4.0.4 64-bit Setup

USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version

USBPcap is currently not installed

Install

☑ Install USBPcap 1.5.4.0

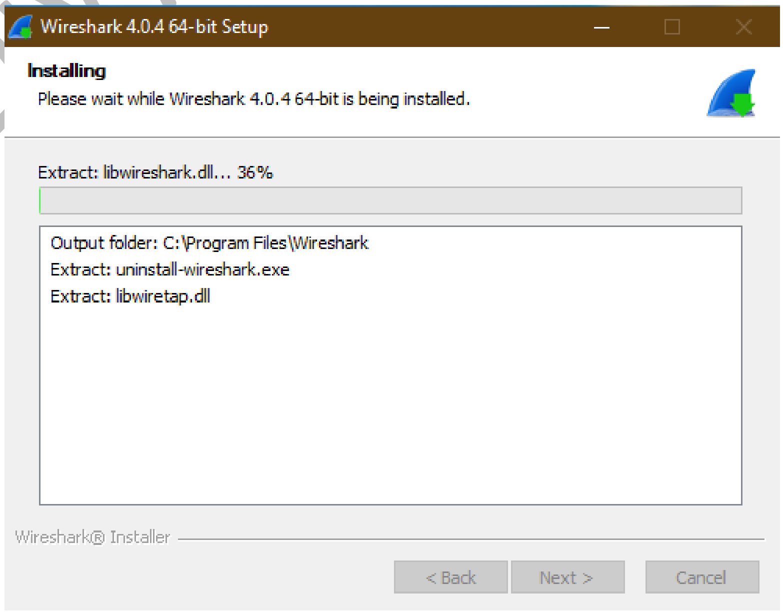
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

Important notice

In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

Learn more about USBPcap

Wireshark® Installer


Wireshark 4.0.4 64-bit Setup

Installing

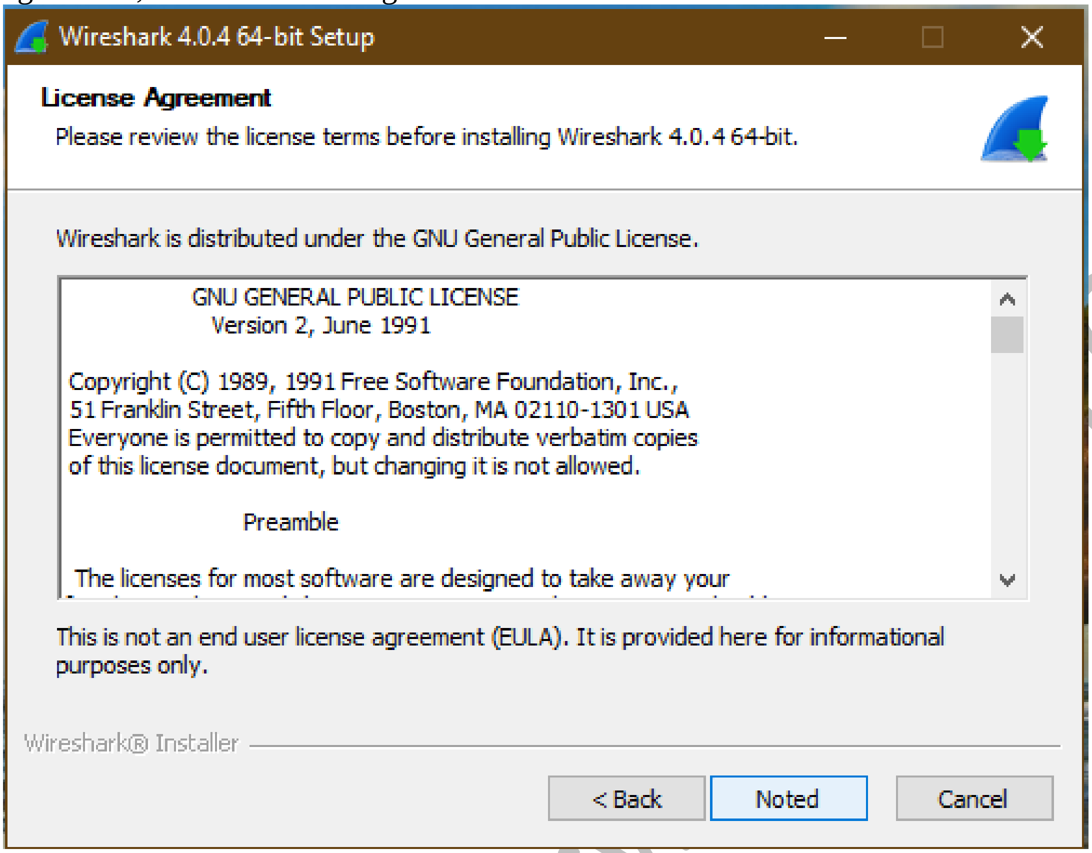
Please wait while Wireshark 4.0.4 64-bit is being installed.

Extract: libwireshark.dll... 36%

```
Output folder: C:\Program Files\Wireshark
Extract: uninstall-wireshark.exe
Extract: libwiretap.dll
```

Wireshark® Installer

7. When WinPcap installation starts, click next in introductory window, read licensing agreement, and then click I Agree.



License Agreement

Please review the license terms before installing Wireshark 4.0.4 64-bit.

Wireshark is distributed under the GNU General Public License.

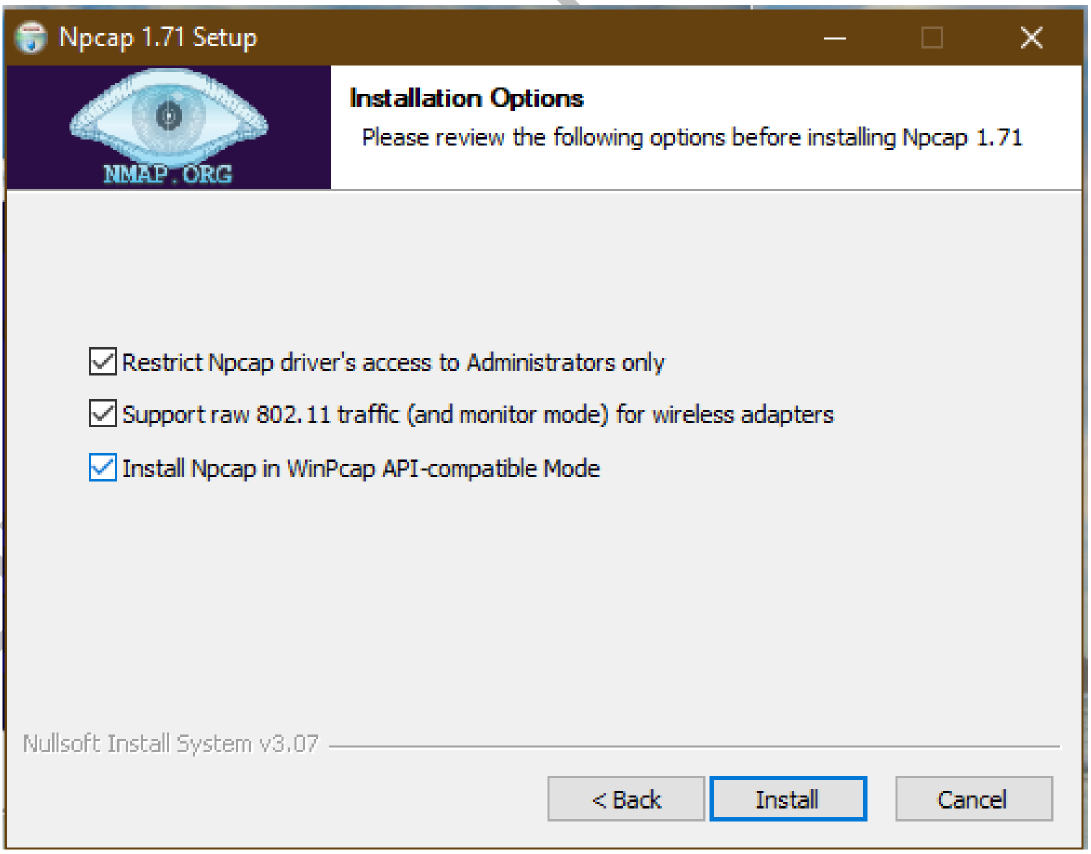
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

This is not an end user license agreement (EULA). It is provided here for informational purposes only.



Installation Options

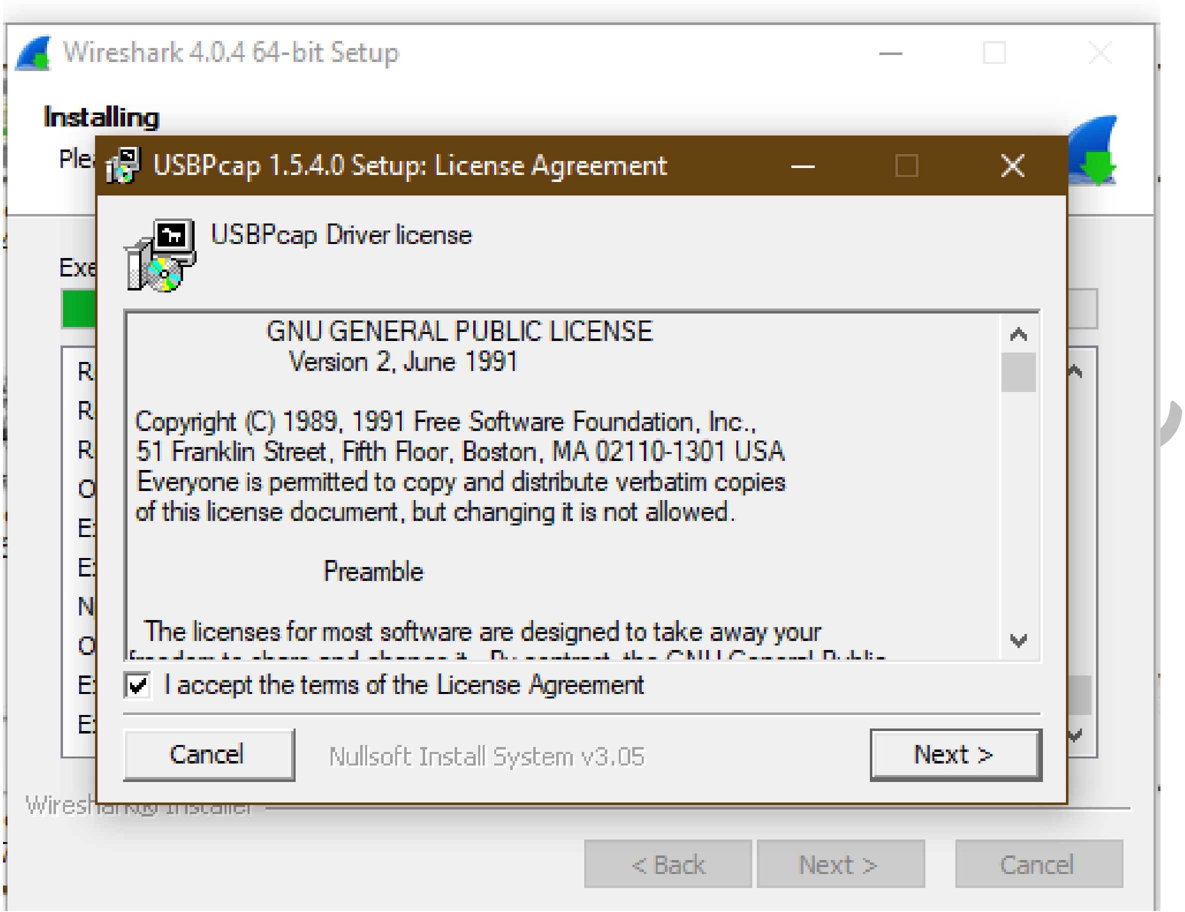
Please review the following options before installing Npcap 1.71

☑ Restrict Npcap driver's access to Administrators only

☑ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☑ Install Npcap in WinPcap API-compatible Mode

8. WinPcap installs on computer/laptop. After installation is complete, click Finish.
9. Wireshark should complete its installation. When it's finished, click Next.


Wireshark 4.0.4 64-bit Setup
Installing
USBPcap 1.5.4.0 Setup: License Agreement
Cancel
Nullsoft Install System v3.05
Next >
< Back
Next >
Cancel

USBPcap Driver license

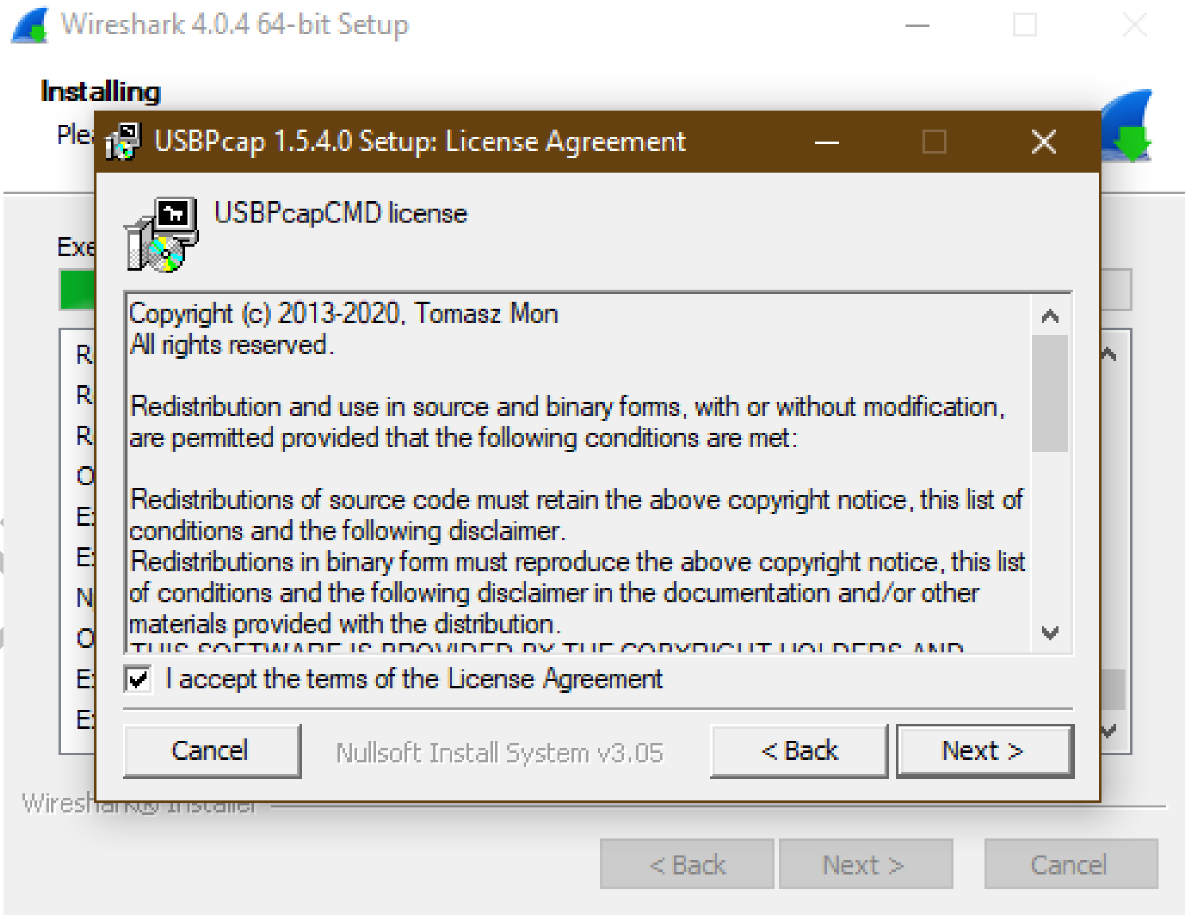
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

☑ I accept the terms of the License Agreement


Wireshark 4.0.4 64-bit Setup
Installing
USBPcap 1.5.4.0 Setup: License Agreement
Cancel
Nullsoft Install System v3.05
< Back
Next >
< Back
Next >
Cancel

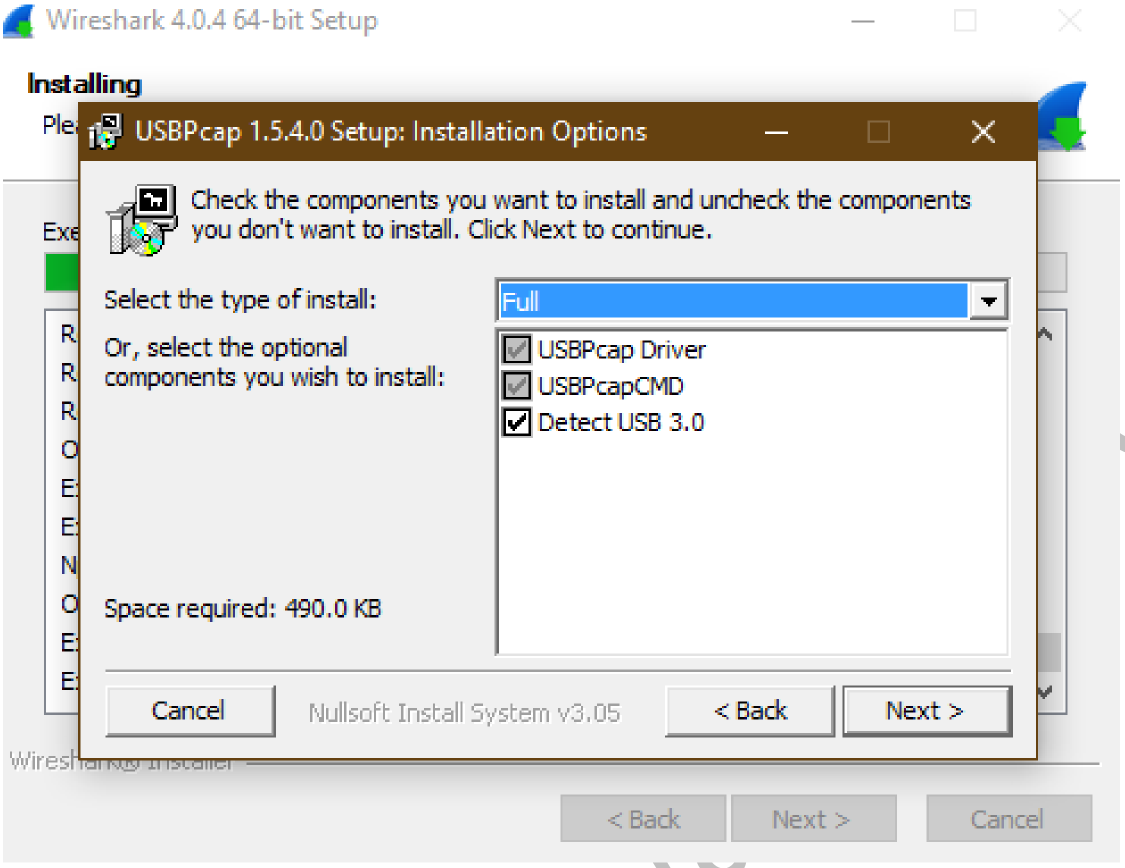
USBPcapCMD license

Copyright (c) 2013-2020, Tomasz Mon
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

☑ I accept the terms of the License Agreement



USBPcap 1.5.4.0 Setup: Installation Options

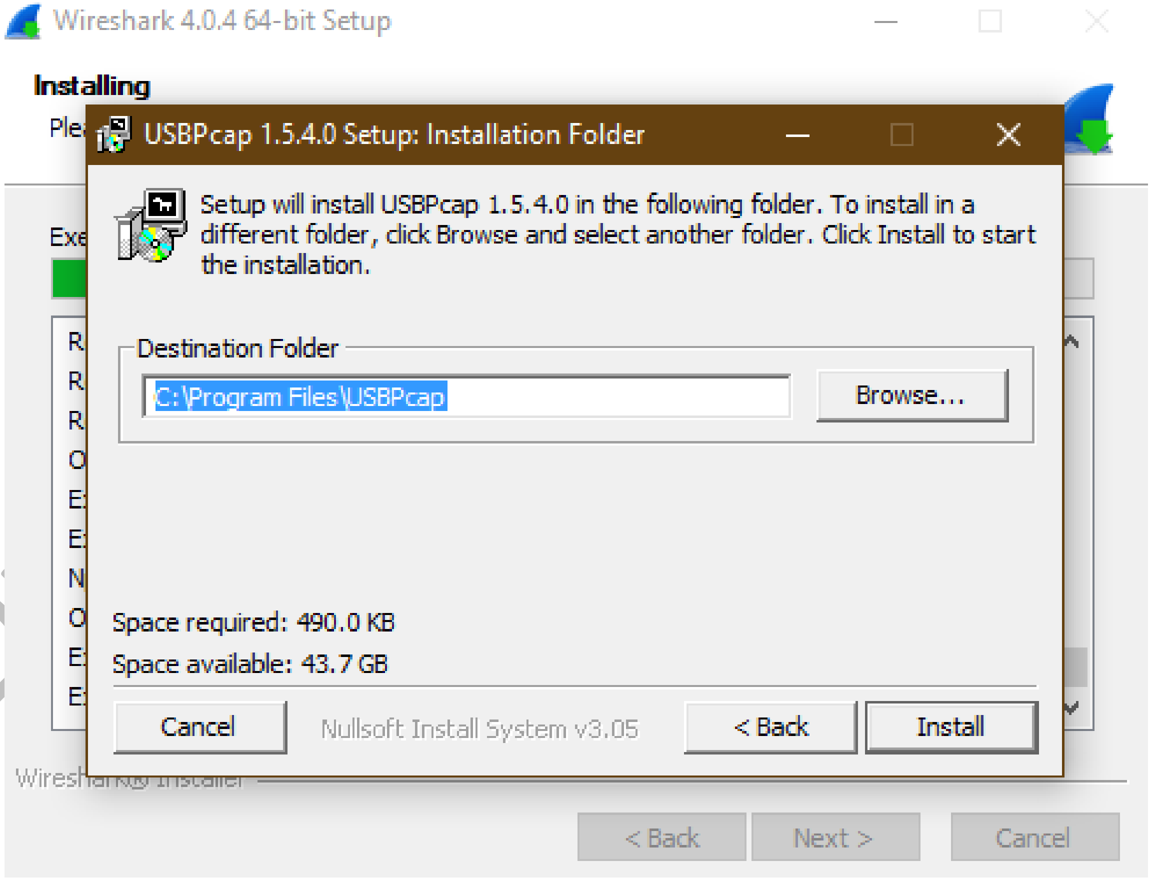
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

- ☑ USBPcap Driver
- ☑ USBPcapCMD
- ☑ Detect USB 3.0

Space required: 490.0 KB



USBPcap 1.5.4.0 Setup: Installation Folder

Setup will install USBPcap 1.5.4.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\USBPcap

Space required: 490.0 KB

Space available: 43.7 GB

10. In installation confirmation window, click Finish.

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.

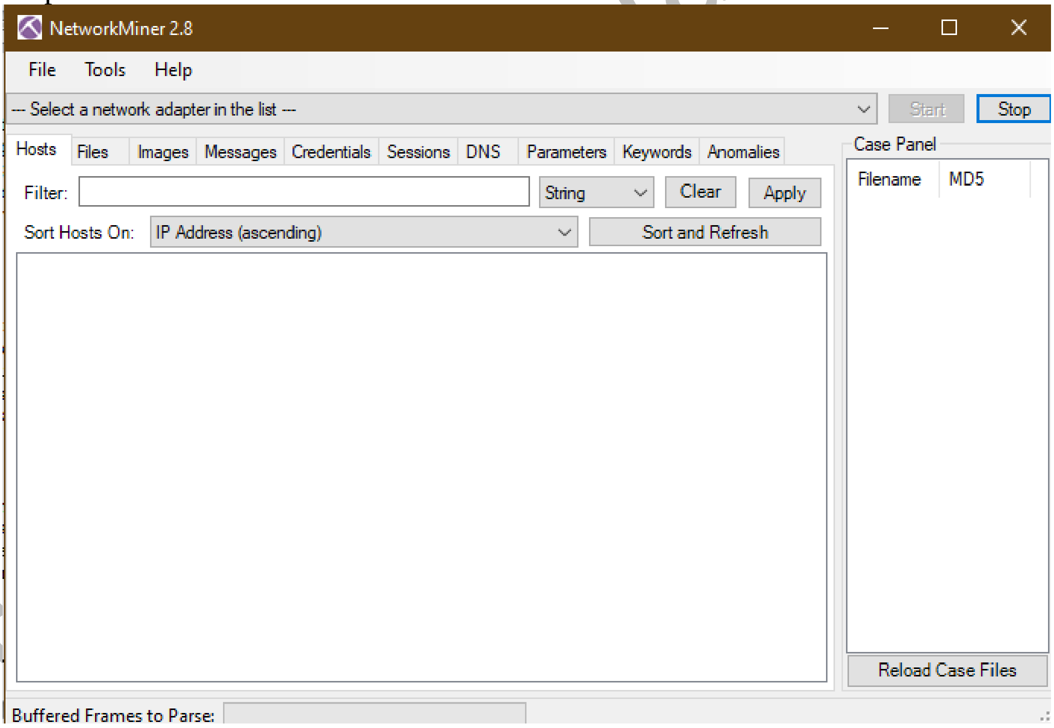
2.2 Benefits of Using Network Miner

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.

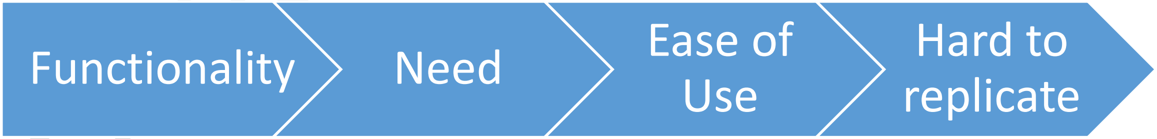
Experiment No. 8
Introduction to Datadog tool for data monitoring in network

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.

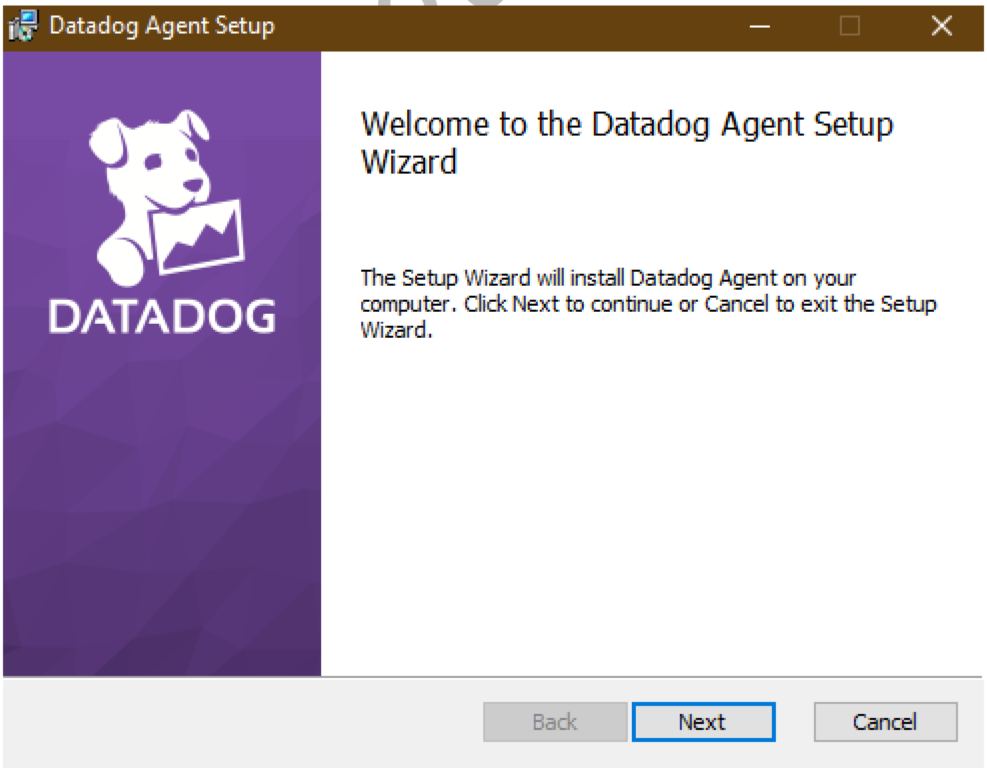
Procedure to download Data Dog Agent

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:

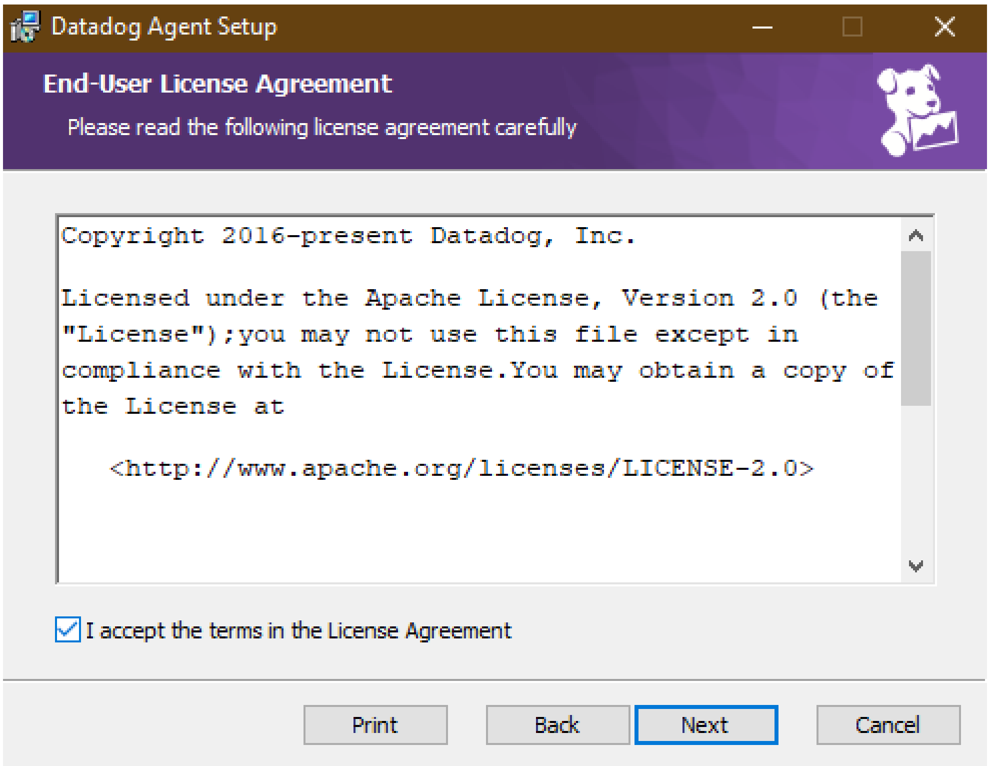
- Log in to your Datadog account.
- Go to the Agents Download page.
- Download the Datadog Agent installer.
- Run the installer (as Administrator) by opening **datadog-agent-7-latest.amd64.msi.**
- Follow the prompts, accept the license agreement, and enter your Datadog API key: 68e98ae58bf1b1a95dcf609b8e2ce2e3.
- 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

Welcome to the Datadog Agent Setup Wizard

The Setup Wizard will install Datadog Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

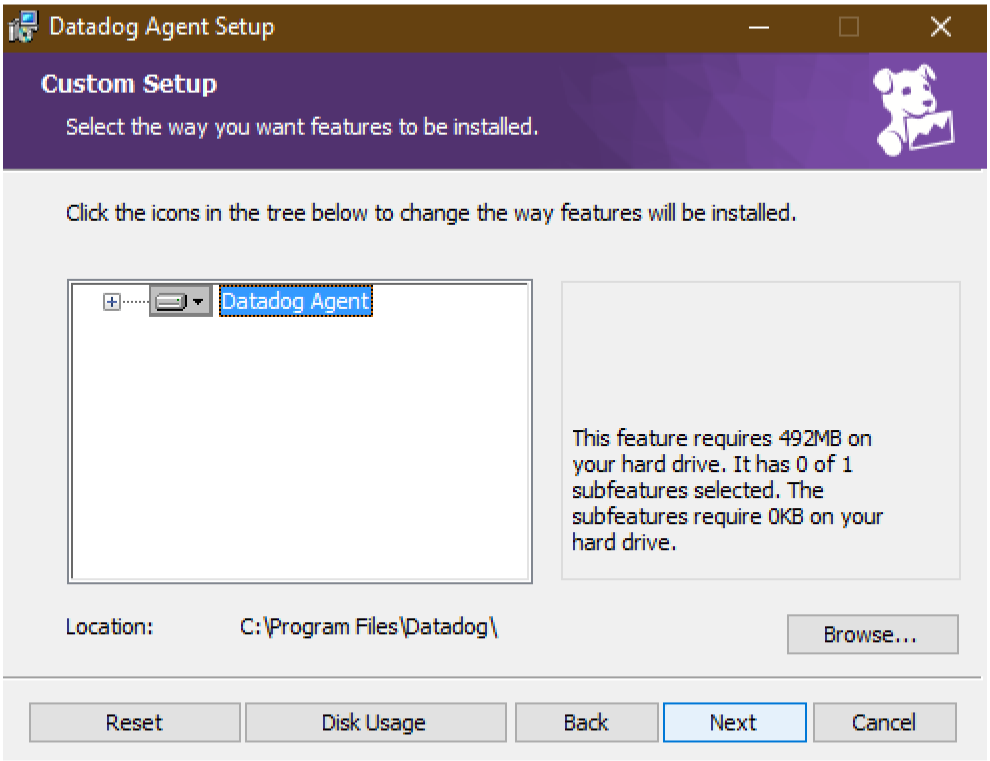


End-User License Agreement

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



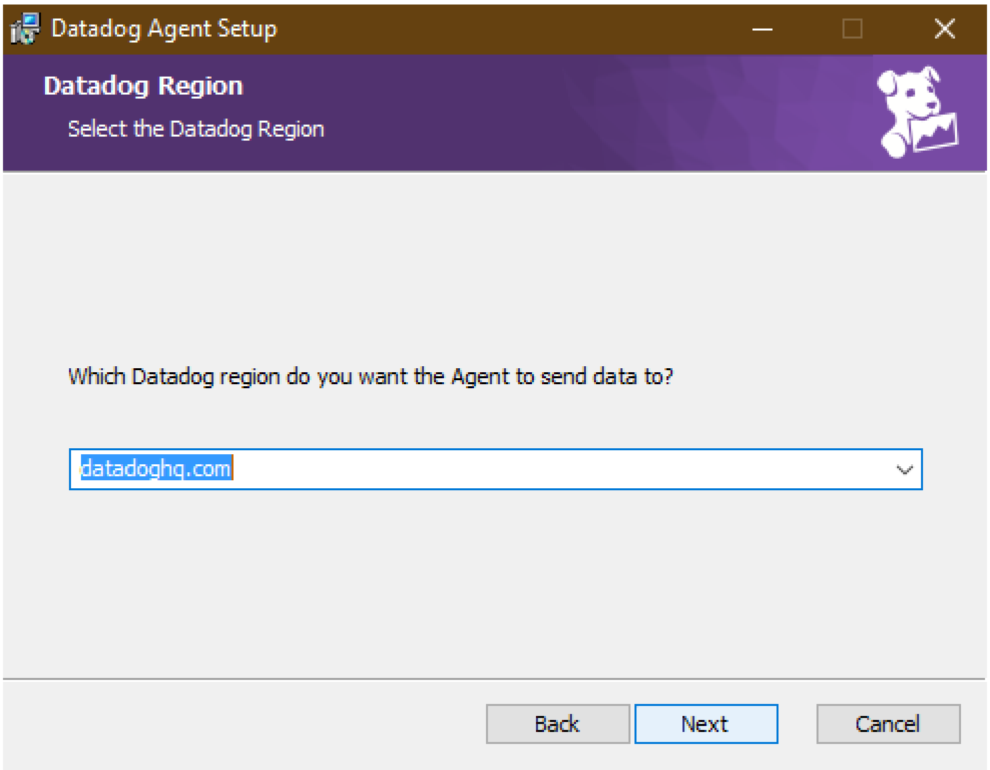
Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

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\



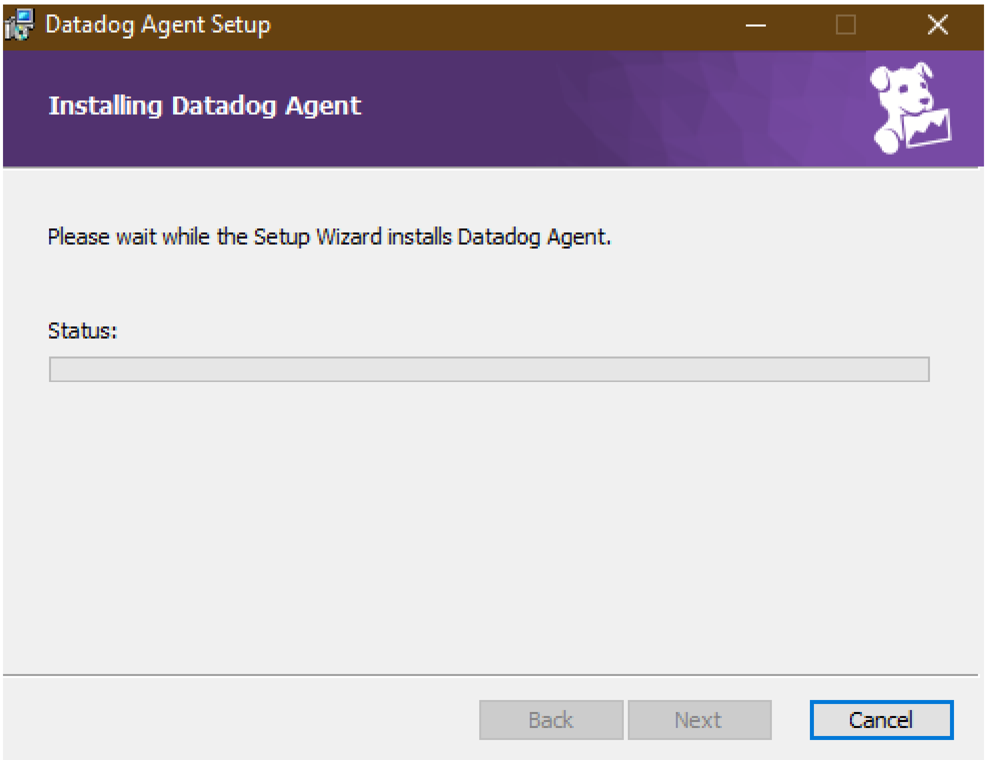
Datadog Agent Setup

Datadog Region

Select the Datadog Region

Which Datadog region do you want the Agent to send data to?

datadoghq.com



Datadog Agent Setup

Installing Datadog Agent

Please wait while the Setup Wizard installs Datadog Agent.

Status:

Step 3: Connect the agents to the Datadog platform: To connect the installed agents to the Datadog platform, follow the steps given below:

- Log in to your Datadog account.
- Navigate to the Integrations page.
- Select the corresponding Windows service that you want to monitor

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.

Experiment No. 9

Configure a network using distance vector routing and link state vector routing protocol

Objectives

- To familiarize students with distance vector routing and link state vector routing protocols and their use in configuring computer networks.
- To develop students' practical skills in configuring and managing a computer network using distance vector routing and link state vector routing protocols.

Theory:

- Distance vector routing and link state vector routing are two common routing protocols used in networking.
- In distance vector routing, routers only have information about the direction and distance to neighboring routers and the path to forwarding packets.
- In contrast, link state vector routing uses a complete map of network topology, which includes the links, nodes, and distances between them.
- Link state vector routing is more efficient and scalable for large networks compared to distance vector routing.

Requirements for Distance Vector Routing:

- Windows PCs – 3 Nos
- CISCO Packet Tracer Software (Student Version)
- PT switch – 3 No
- PT Router – 3 Nos

Requirements for Link State Routing:

- Windows PCs – 6 Nos
- CISCO Packet Tracer Software (Student Version)
- PT switch – 3 No
- PT Router – 3 Nos

Procedure for Distance Vector Routing

- Open the CISCO Packet tracer software
- Develop a Topology as shown in figure below
- Configure all routers

- Implement RIP protocol in Router to configure network
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Procedure for Link State Routing

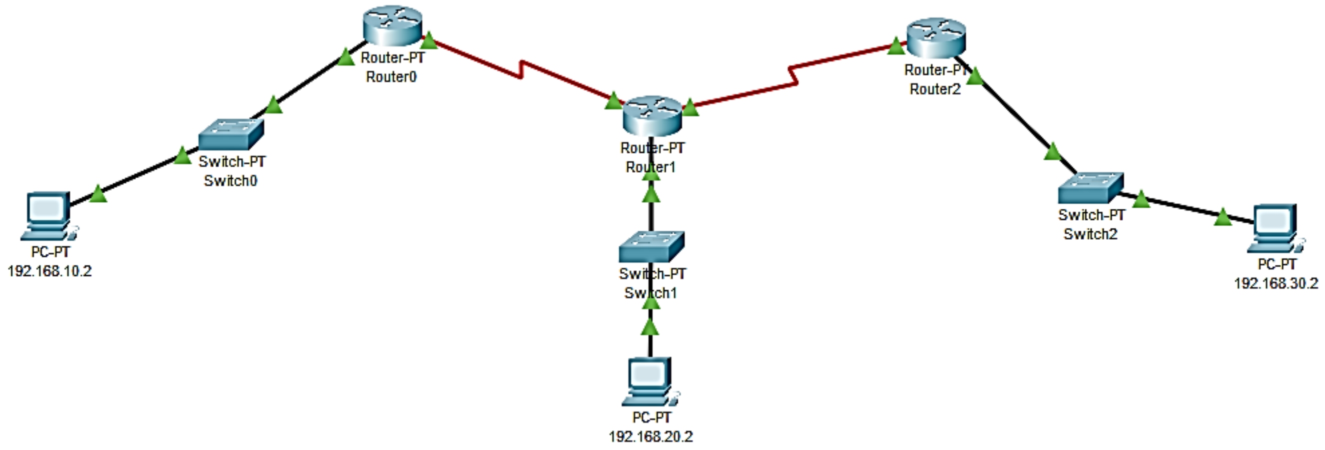
- Open the CISCO Packet tracer software
- Develop a Topology as shown in figure below
- Configure all routers, all workstations and all switches
- Implement OSPF protocol in Router to configure network
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory for RIP and OSPF

RIP(routing information protocol) is an intradomain routing protocol used inside an autonomous system. it is very simple protocol based on distance vector routing. RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain, but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exists: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn’t advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1. RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth. RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, this requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

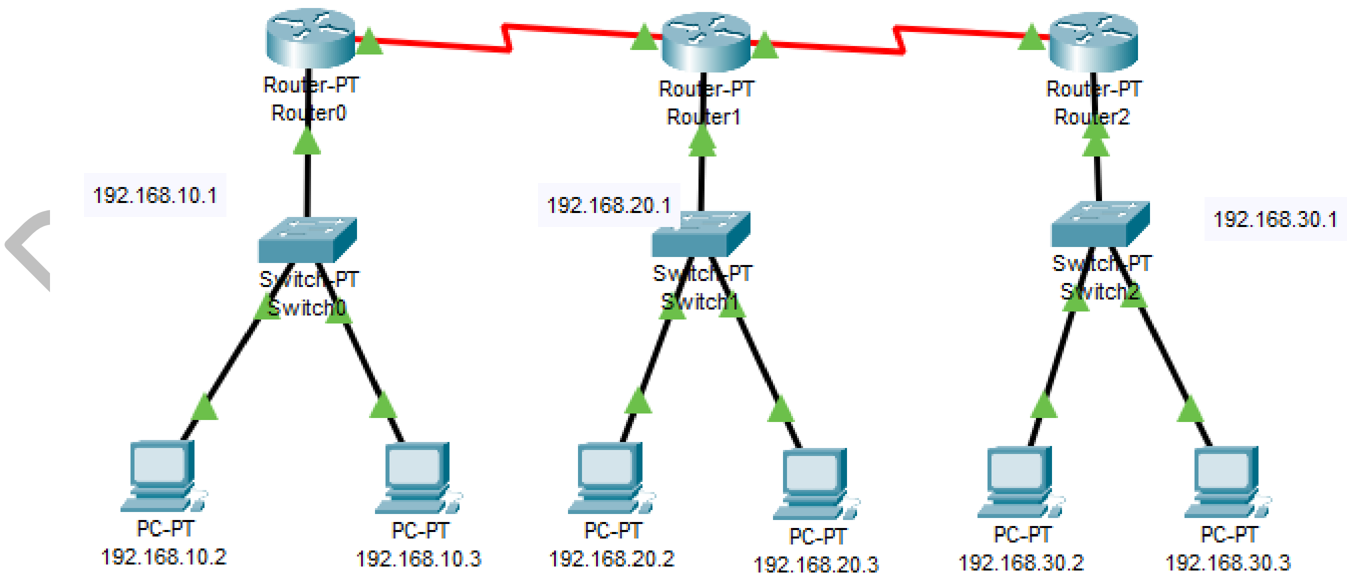
Network Topology Diagram for Distance Vector Routing



Input Details for Distance Vector Routing

	PC0	PC1	PC2
IP address:	192.168.10.2	192.168.20.2	192.168.30.2
Gate Way	192.168.10.1	192.168.20.1	192.168.30.1
	Router 0	**Router 1**	**Router 2**
Fast Ethernet 1	192.168.10.1	192.168.20.1	192.168.30.1
Serial 2/0	10.0.0.2 Clock Rate: 64000	10.0.0.3 Clock Rate: Not set	20.0.0.3 Clock Rate: Not set
Serial 3/0	-NA-	20.0.0.2 Clock Rate: 64000	-NA-
RIP	**Add Network Address:** 192.168.10.1 10.0.0.2	**Add Network Address:** 192.168.20.1 10.0.0.3 20.0.0.2	**Add Network Address:** 192.168.30.1 20.0.0.3

Network Topology Diagram for Link State Routing



Input Details for Link State Routing

	PC0 and PC1	PC2 and PC3	PC4 and PC5
IP address:	192.168.10.2, 192.168.10.3	192.168.20.2, 192.168.20.3	192.168.30.2, 192.168.30.3
Gate Way	192.168.10.1	192.168.20.1	192.168.30.1
	Router 0	**Router 1**	**Router 2**
Fast Ethernet 1	192.168.10.1	192.168.20.1	192.168.30.1
Serial 2/0	10.0.0.2 Clock Rate: 64000	10.0.0.3 Clock Rate: Not set	20.0.0.3 Clock Rate: Not set
Serial 3/0	-NA-	20.0.0.2 Clock Rate: 64000	-NA-

- Double-click on each router to open the configuration window.
- In the router configuration window, go to the "CLI" tab to access the Command Line Interface.
- Repeat the above two steps for each router.

ROUTER0 CLI:

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? ……Press enter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.0 0.0.0.255 area 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
00:19:21: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

ROUTER1 CLI:

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? ……Press enter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 2
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
00:19:07: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

```
Router(config-router)#network 20.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
%SYS-5-CONFIG_I: Configured from console by console
00:25:52: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.1 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

ROUTER2 CLI:

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.30.0 0.0.0.255 area 2
Router(config-router)#network 20.0.0.0 0.255.255.255 area 2
00:25:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
Router(config)#exit
```

OUTPUT:

Paste Screenshots of simulation mode by sending message from PC0 to PC1, PC1 to PC3, PC1 to PC5 for Link state routing.

Result:

Understood the concept and operation of RIP and pinged from PC in are networks to PC to another network

Understood the concept and operation of OSPF and obtained the routing table and observe transfer data packets in real and simulation time.

Experiment No. 10

Implement dijkstra's shortest path algorithm in network routing.

Objectives

- To understand the concept of Dijkstra's shortest path algorithm and its application in network routing.
- To gain hands-on experience in configuring and simulating network routing using Dijkstra's algorithm in Cisco Packet Tracer.

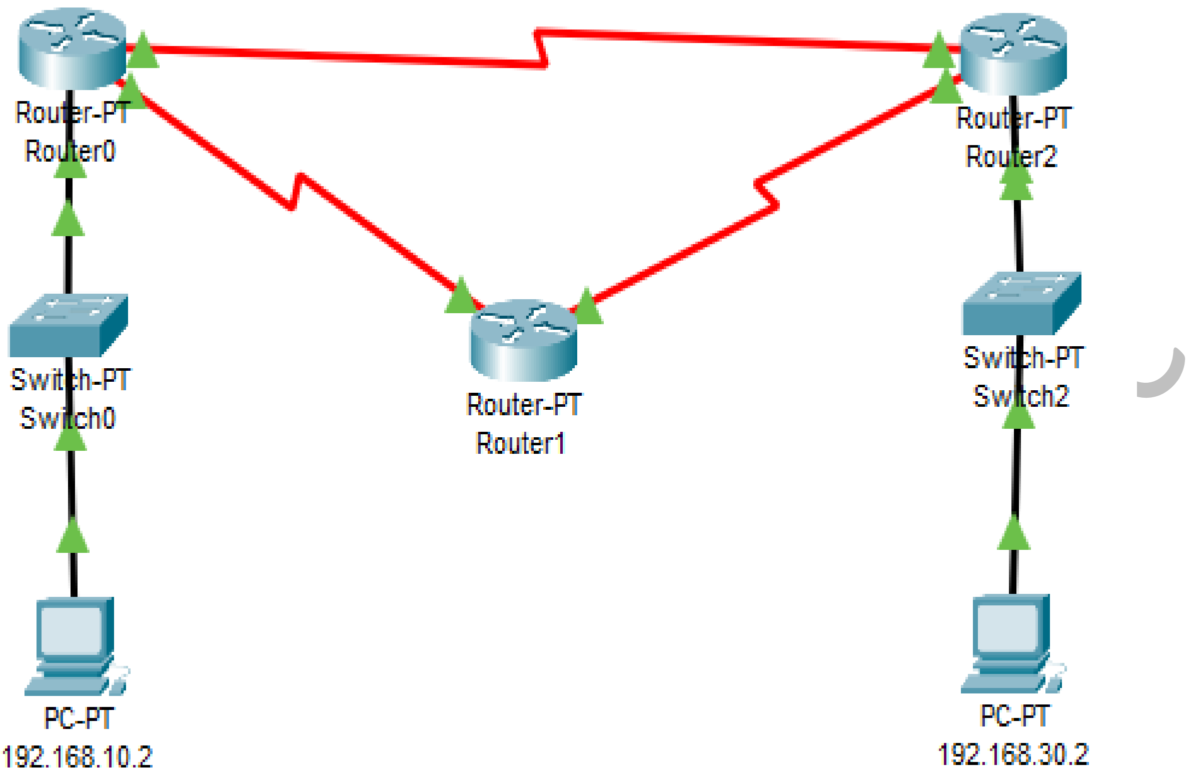
Theory:

- Dijkstra's algorithm is a popular algorithm used for finding the shortest path in a weighted graph.
- In the context of network routing, this algorithm enables efficient determination of the optimal path for transmitting data packets from a source node to a destination node.
- The algorithm assigns a cost value to each network link based on factors such as bandwidth, delay, or other metrics.
- By iteratively evaluating and updating the cost values, Dijkstra's algorithm determines the shortest path from the source to all other nodes in the network.
- The practical implementation of Dijkstra's algorithm in network routing involves configuring routers with appropriate IP addresses, enabling routing protocols, and simulating data transmission using Cisco Packet Tracer.
- Through this practical, understanding of how routing tables are dynamically updated based on the shortest path calculations, and gain proficiency in configuring network topologies using Dijkstra's algorithm is done.

Procedure

- Launch Cisco Packet Tracer and create a new network topology.
- Add routers to the network topology by selecting "Router" from the "End Devices" section in the sidebar and placing them on the workspace.
- Connect the routers using appropriate connections (e.g., Ethernet cables) by selecting the "Copper Straight-through" or "Copper Cross-over" cables from the "Connections" section in the sidebar and clicking on the router interfaces to connect them.
- Double-click on each router to open the configuration window.
- In the router configuration window, go to the "CLI" tab to access the Command Line Interface.

Network Topology Diagram for Implementing Dijkstra Shortest Path algorithm



Input Details for Implementing Dijkstra Shortest Path algorithm

		PC0	PC1
IP address:		192.168.10.2	192.168.30.2
Gate Way		192.168.10.1	192.168.30.1
	Router 0	**Router 1**	**Router 2**
Fast Ethernet 1	192.168.10.1	192.168.20.1	192.168.30.1
Serial 2/0	10.0.0.2 Clock Rate: 64000	10.0.0.3 Clock Rate: Not set	20.0.0.3 Clock Rate: Not set
Serial 3/0	30.0.0.2 Clock Rate: 64000	20.0.0.2 Clock Rate: 64000	30.0.0.3 Clock Rate: Not Set

- Double-click on each router to open the configuration window.
- In the router configuration window, go to the "CLI" tab to access the Command Line Interface.
- Repeat the above two steps for each router.

ROUTER0 CLI:

```
Router#enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.0 0.0.0.255 area 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#network 30.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

ROUTER1 CLI:

```
Router#enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.20.0 0.0.0.255 area 2
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#network 20.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

ROUTER2 CLI:

```
Router#enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.30.0 0.0.0.255 area 2
Router(config-router)#network 20.0.0.0 0.255.255.255 area 2
Router(config-router)#network 30.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

OUTPUT:

Paste Screenshots of simulation mode by sending message from PC0 to PC1, router 0 to router 2 and router 2 to router 1.

Result:

- Configured Dijkstra's algorithm by selecting an appropriate routing protocol such as Open Shortest Path First (OSPF).
- Network was tested by sending data packets from a source node to a destination node and observing the routing decisions made by the routers using the simulation mode in Cisco Packet Tracer to monitor the flow of data packets and the routing updates.