

Hyderabad Karnataka Education Society's (HKE'S)

**POOJYA DODDAPPA APPA ENGINEERING COLLEGE  
KALABURAGI -585102**

**(An Autonomous Institution)**

*(Aiwan-E-Shahi Area, Kalaburagi, Karnataka 585102)*



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**COMPUTER NETWORK LAB MANUAL**

**Prepared By**

**Dr. Soumya M Anakal**

**Smt Jayanti K**

**Sri Prashant Devani**

**Sri Keval Andola**

### **VISION OF THE DEPARTMENT**

To become a premier department in computer education, research and to prepare highly competent IT professionals to serve industry and society at local and global levels.

### **MISSION OF THE DEPARTMENT**

- To impart high quality professional education to become a leader in Computer Science and Engineering.
- To achieve excellence in research for contributing to the development of the society.
- To inculcate professional and ethical behaviour to serve the industry.

### **PROGRAM EDUCATIONAL OBJECTIVES (PEOS)**

<b>PEO1:</b>	To prepare graduates with core competencies in mathematical and engineering fundamentals to solve and analyze Computer Science and Engineering problems.
<b>PEO2:</b>	To adapt to evolving technologies and tools for serving the society.
<b>PEO3:</b>	To perform as team leader, effective communicator and socially responsible computer professional in multidisciplinary fields following ethical values.
<b>PEO4:</b>	To encourage students to pursue higher studies, engage in research and to become entrepreneurs.

**Computer Network Lab**

**Rubrics for Assessment of Student's Performance in Laboratory: Evaluation Criteria**  
for each Experiment:

<b>Evaluation criteria for each lab Courses is as follows</b>			
<b>Sl.No</b>	<b>Evaluation Criteria</b>	<b>Weightage in percentage</b>	<b>Weightage in Marks</b>
1	Conduct of Experiments	60%	30
2	Open-ended Experiments	20%	10
3	Internal Assessments	20%	10

**Conduct of Experimental work: Thirty marks is distributed among all the experiments in the lab courses**

**Marking Criteria for conduct of experimental work**

<b>Marking Criteria for Conduct of experimental work</b>		
3	2	1
Student is able to develop a solution to implement and understand applications of the concept	Student can develop solution with moderate understanding of the concept	Student can implement the solution without involvement

**Marking Criteria for open ended experiment:**

<b>Marking Criteria for Open Ended Experiment</b>		
10-8	5-7	1-4

## Computer Network Lab

Student is able to successfully find the solution and analyze efficiently.	Student is able to design and develop the solution for identified problem	Student is able to identify, define and understand the problem
<b>Evaluation of Open End Experiment::</b> The purpose Open Ended Experiment is enabling the students to apply theoretical concepts to develop real world applications.		

### Marking Criteria for internal Assessment test

**Internal Assessments:**Two Internal Assessments tests are conducted each carrying five marks based on the lab experiments within the lab

Marking criterion for Internal Assessment Tests				
5	4	3	2	1
Student is able to successfully execute and Interpret results and develop alternative Solutions	Student is able to successfully execute and interpret results	Student is able to execute the programs	Student is able to write the program and execute partially	Student is able to write the program

**Table of Contents**

S.No	Experiments
	<b><u>Module I</u></b>
1.	a. Experimental Study of various network components and devices(StudyCAT6UTPEIA/TIA568A/Bstraightandcross-overcable, crimpandtest and/verifyits connectivity).
	b. Install and configure wired and wireless NIC . Demonstrate file transfer in wired and wireless LAN.
	c. Installandconfigurenetworkdeviceslikehub, switch,androuter
2	Use CISCO packet tracer to
	a. Build a Local Area Network of 4 to 6 nodes using hub /repeater.
	b. Build a peer to peer network
	<b><u>Module II</u></b>
1.	Implement sliding window protocol
2.	Implement go backN protocol
	<b><u>Module III</u></b>
1.	Install & Configure network devices switch
2.	Use CISCO packet tracer to a. Build a local area network of 4 to 6 nodes using switch b. Build a local area network of 4 to 6 nodes using hub & a switch & Study the differences between repeater,hub & Switch c. Identify Broadcast & Collision Domain
3.	Use wireshark to examine Ethernet packets and ARP packets
4.	To study Performance of CSMA/CD Prtocol
	<b><u>Module IV</u></b>
1.	Install & configure network devices routers
2.	Use Cisco packet tracer to a. Design and apply IP addressing scheme for a given topology b. Connect two or three LAN's via a router. Trace how routing happens via Simulation, and study the working of router.

## Computer Network Lab

	c. Design multiple subnets with suitable number of hosts d. Demonstrate static routing and dynamic routing for given topology e. Configure DHCP server f. Create subnets , Configure Host IP, Subnet Mask and Default Gateway in a LAN g. Configure RIP/OSPF
3.	Use Wireshark to a. analyze IP Datagram and IP fragmentation received during the execution of trace route command. b. Run ping command and examine ICMP packets using wireshark
	<b><u>Module V</u></b>
1.	Use wireshark to a. Examine UDP and TCP ports and handshake segments b. Use packet tracer to configure DHCP server, DNS server, SMTP server
2.	Implement client server program in C/Java

### **Course Outcomes**

**After successful completions of the course the students will be able:**

- Demonstratetheuseofdifferentnetworkcablingcomponentsand devices
- AnalysisperformanceofLANandwirelessLAN
- Illustratebasicnetworksutilitiesanddemonstrateclientserver communication.
- Demonstrateworkingofroutingalgorithms.
- Performpacketcaptureanalysisisthepacketcontents.

**SOFTWARES USED:** CISCOpackettracer. Wireshark & C/Java

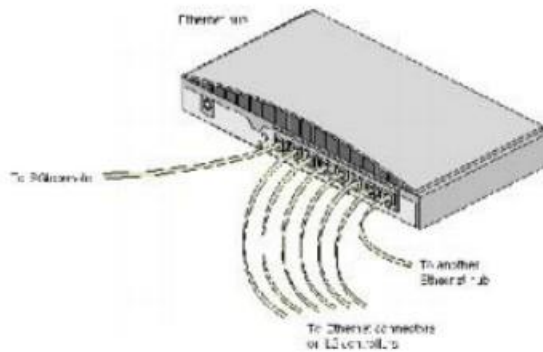
# **MODULE : I**

## **1. Study of various network components devices**

**Network Devices** : Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, router, and NIC, etc.

**AIM** : - Familiarization with Networking components and devices: LAN Adapters ,Hub, Switches, Routers.

**LAN ADAPTERS**: - A LAN adapter is a device used to allow a computer to interface with a network. Many computers may have some sort of LAN adapter already installed, but others may require a special installation, which is accomplished by adding a network interface card to the system or possibly connecting the adapter to a USB port. Most networks that are used in an office or home environment are known as local area



**SWITCHES**: - A network switch is a computer networking device that links network segments or network devices. The term commonly refers to a multi - port 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 called layer - 3 switches or multilayer switches. A switch is a telecommunication device which receives a message from any device connected

to it and then transmits the message only to the device for which the message was meant. This makes the switch a more intelligent device than a hub (which receives a message and then transmits it to all the other devices on its network). The network switch plays an integral part in most modern Ethernet local area networks (LANs).



**HUB** : - A special type of network device called the hub can be found in many home and small business networks. Hub is a small rectangular box, often made of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers (or other network devices) together to form a single network segment.

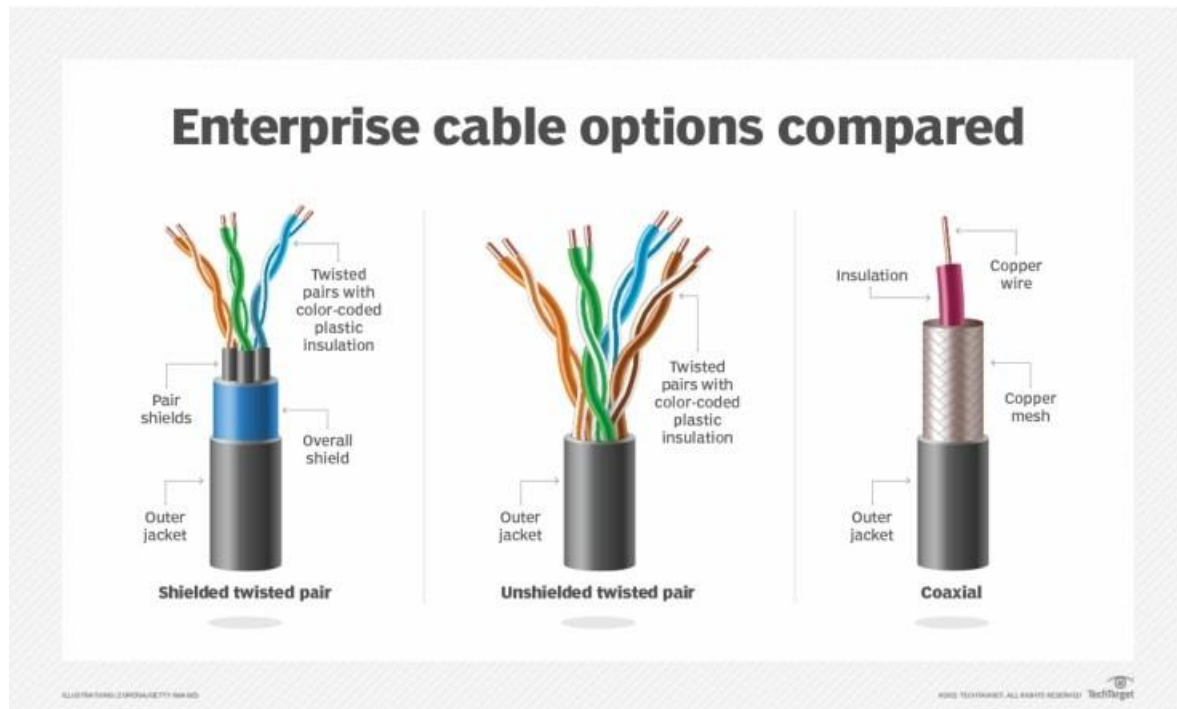


**Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.





**1 A) Study different network cables and prepare , test straight over and cross over cabling using crimping tool.**



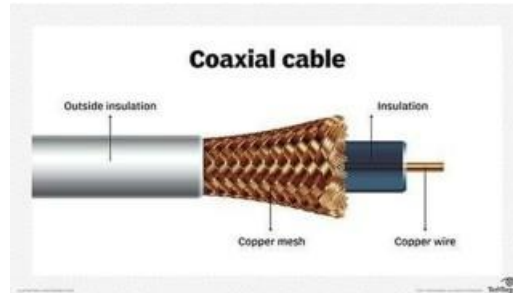
### 1. Coaxial Cables

Coaxial cables contain a centre conductor and a metal shield insulated by a plastic layer placed in between. The metal shield in coaxial cables blocks any elements or interferences from the outside.

In a coaxial cable, the outer layer, known as sheath, protects the cable from physical damage. Meanwhile, the metal shield protects the cable from any external interference, and the insulation between the metal shield and the conductor protects the conductor – the core of the coaxial cable.

Coaxial cable conductors carry electromagnetic signals and can come either in single - core or multi - core models. While a single - core coaxial cable has only one central metal, multi - core cables have many metal wires.

Coaxial cables were used in the earlier days of computer networks.



### 2. Shielded Twisted Pair Cables

These ethernet cables, also known as STP cables, are widely used for business installations. They were developed for computer networks and are an excellent choice for areas with high interference. Shielded twisted pair cables are also used to expand any distance between cables.

STP cables consist of coloured wires twisted around one another, forming pairs. Usually, shielded twisted pair cables are composed of four colourful pairs of wires wrapped with metal shields and a singular plastic sheath.

### 3. Unshielded Twisted Pair Cables

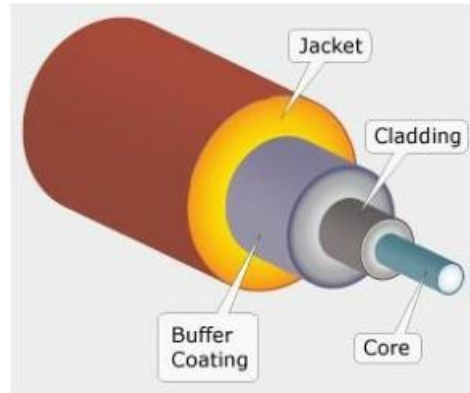
Unshielded twisted pair cables, or UTP cables, are widely used in industrial computers and telecommunication companies. The conductors present in UTP cables form a circuit that stops any EMI. Similarly to STP cables, unshielded twisted pairs are colourful wires wrapped around each other and then wrapped altogether in a plastic sheath.

When compared to STP cables, UTP cables are more affordable.

### 4. Fibre Optic Cables

Fibre optic cables are networking cables that contain either a glass or a plastic core, shielded by a cladding, a buffer and a jacket. These layers protect fibre optic cables from potential damage and from external interference. This networking cable is the perfect choice for carrying data around long distances and the standard cable for connecting networks in different locations.

Fibre optic cables can be single - mode fibre or multi - mode fibre. SMF cables support longer distances, while MMF cables carry more data.



## Types of cabling

### Standard Cabling:

1. 10BaseT and 100BaseT are most common mode of LAN. You can use UTP category-5 cable for both modes.
2. A straight cable is used to connect a computer to a hub

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

### Cross Cabling:

A cross cable is used to connect 2 computers directly (with ONLY the UTP cable). It is also used

then you connect 2 hubs with a normal port on both hubs

**Diagram shows you how to prepare straight through wired connection**

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

### Cable Crimping steps:

1. Remove the out most vinyl shield for 12mm at one end of the cable (we call this side A-side).
2. Arrange the metal wires in parallel
3. Insert the metal wires into RJ45 connector on keeping the metal wire arrangement.



4. Set the RJ45 connector (with the cable) on the pliers, and squeeze it tightly.
5. Make the other side of the cable (we call this side B -side) in the same way.
6. After you made it, you don't need to take care of the direction of the cable.

**IO connector crimping: Run the full length of Ethernet cable in place, from endpoint to endpoint, making sure to leave excess.**

At one end, cut the wire to length leaving enough length to work, but not too much

excess. Strip off about 2 inches of the Ethernet cable sheath.

Align each of the colored wires according to the layout of the jack. Use the punch down tool to insert each wire into the jack.

Repeat the above steps for the second RJ45jack.

**Testing the crimped cable using a cable tester:**

Step 1 : Skin off the cable jacket 3.0 cm long cable stripper up to cable11

Step 2: Untwist each pair and straighten each wire 190 0 1.5 cm long.

Step 3 : Cut all the wires

Step4:Insert the wires into the RJ45connector right white orange left brown the pins facing up

Step 5 : Place the connector into a crimping tool, and squeeze hard so that the handle reaches its full swing.

Step6:Use a cable tester to test for proper continuity

**Result:**

Cable Crimping, Standard Cabling and Cross Cabling, IO connector crimping and testing the crimped cable using a cable tester are done successfully

## **1 B. Install and configure wired and wireless NIC. Demonstrate file transfer in wired and wireless LAN.**

**NICs (Network Interface Card):** Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

### **Procedure:**

#### **(a) Install the network card:**

Disconnect all cables connected to the computer and open the case. Locate an available PCI slot (white slots) and insert the network card and secure the card with the screw that came with it. Once the adapter has been installed and secured close the computer case, connect all the cables and turn it on.

After installing the adapter driver it should be working fine, now let's configure the card for use on a network.

Click on the Start button and select Settings then Control

Panel. Double click on the System icon

Click on the hardware tab.

Click on Device Manager.

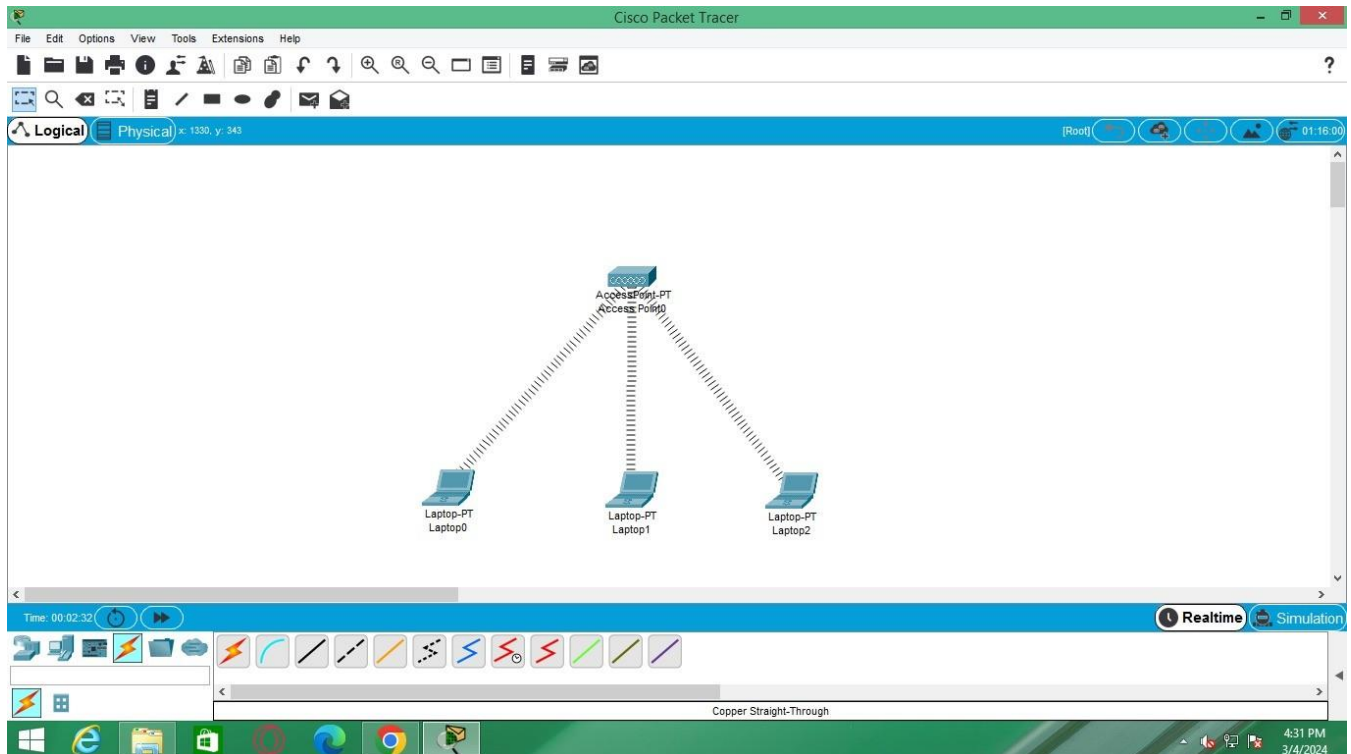
You will see a list of devices installed in your computer.

If necessary, click on the + sign next to Network Adapters to expand the list. Ensure that there is no yellow exclamation mark (!) next to the Network Adapter. This indicates a possible problem with the card or configuration. Double click on your network driver (e.g. NE2000 Compatible).

In the Device Status box you should see the message:  
This Device is working correctly.

If you do not see this message or if there is no Network Adapter displayed, then your Ethernet card will probably need configuring.

## Wireless LAN in cisco:



## Result:

Installation and configuration of Wired and Wireless (remotely) NIC and transfer files between systems in LAN and Wireless LAN between two systems in a LAN have been done successfully



## 1 C. Install and configure network devices HUB

### INSTALLING HUB STEPS:

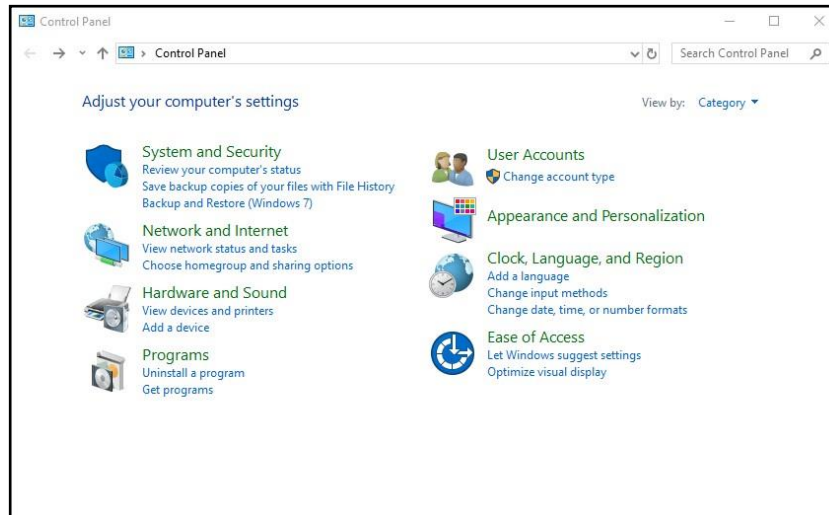
- 1 Stacking Hubs (if you are using more than one hub)
- 2 Connecting Hubs (if you are using more than one hub)
- 3 Connecting the Power and Turning the Hub On
4. Connecting Other Network Devices to the Hub
- 5 Connecting the CONSOLE Port (Micro Hub 1503 only)



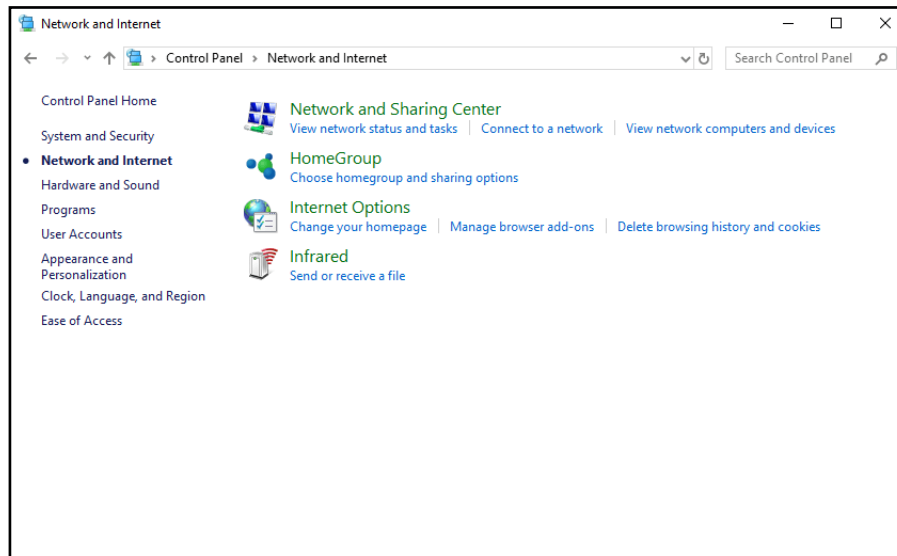
### CONFIGURE STEPS:

1. Open the **Control Panel** from the Windows® icon in the lower left corner of your monitor.  
In the Control Panel window, make sure **View by** is set to *Category*.
2. Click **Network and Internet**.

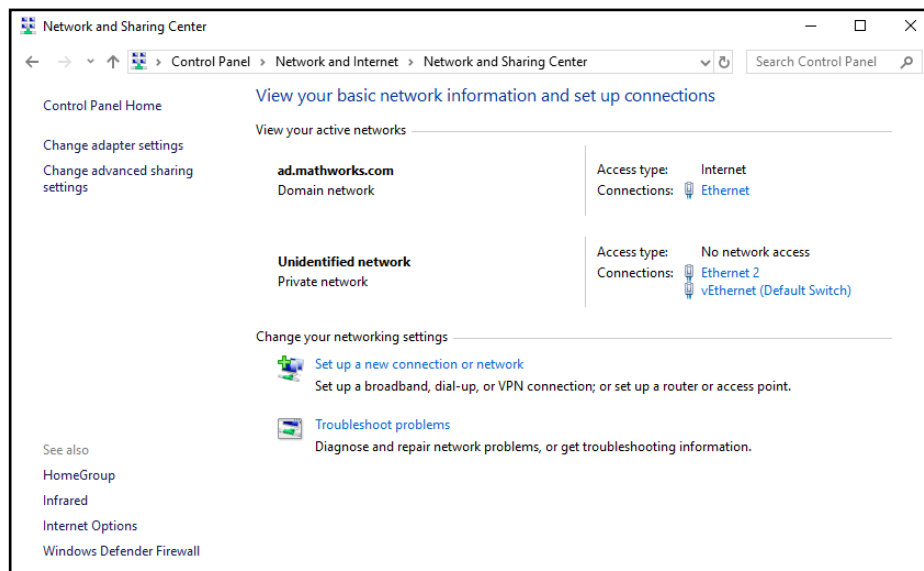




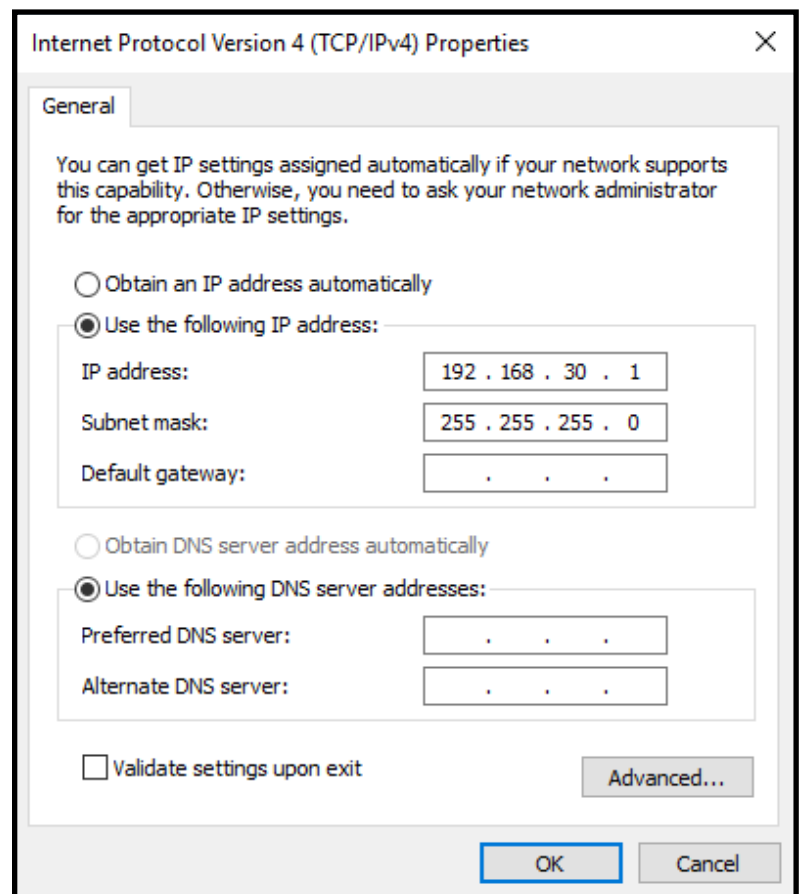
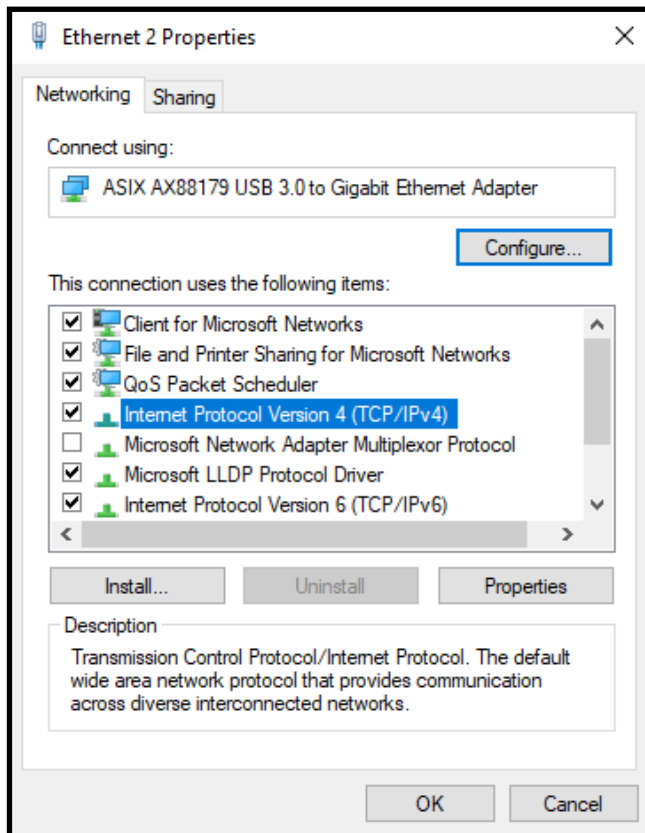
### 3. Click **Network and Sharing Center**.



### 4. Click **Change adapter settings** in the left pane.



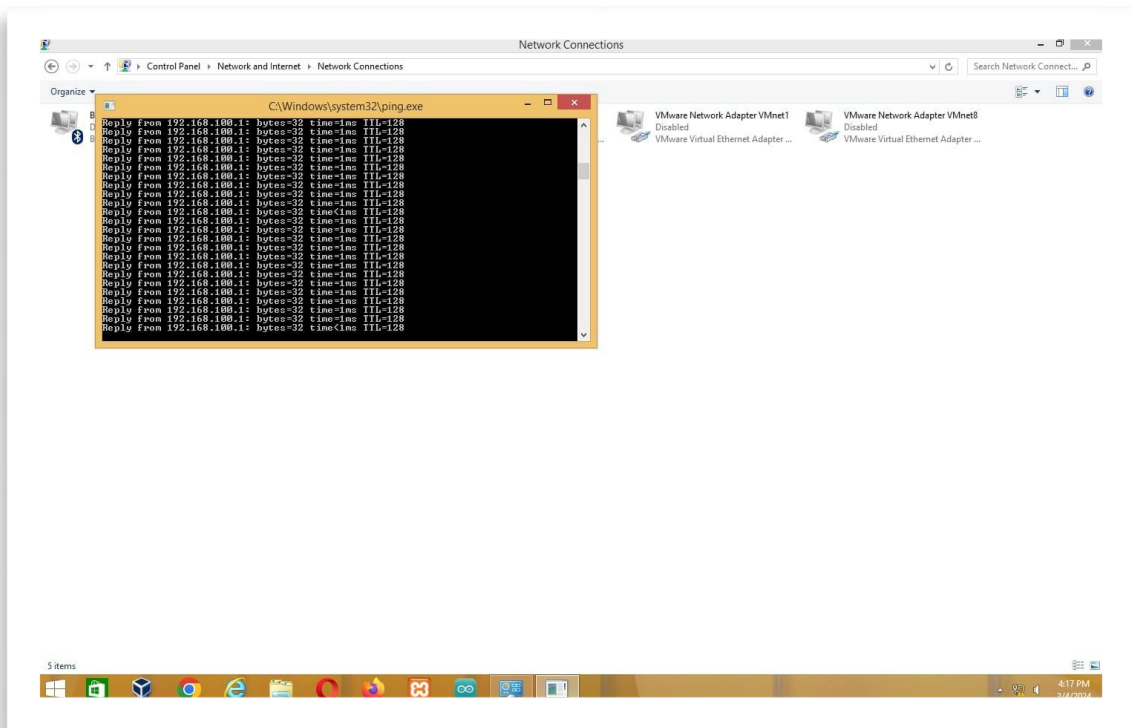
5. On the **Networking** tab, clear **Clients for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks**. These services can cause intermittent connection problems with USRP™ radios. To configure the IP address, double-click **Internet Protocol Version 4 (TCP/IPv4)**.



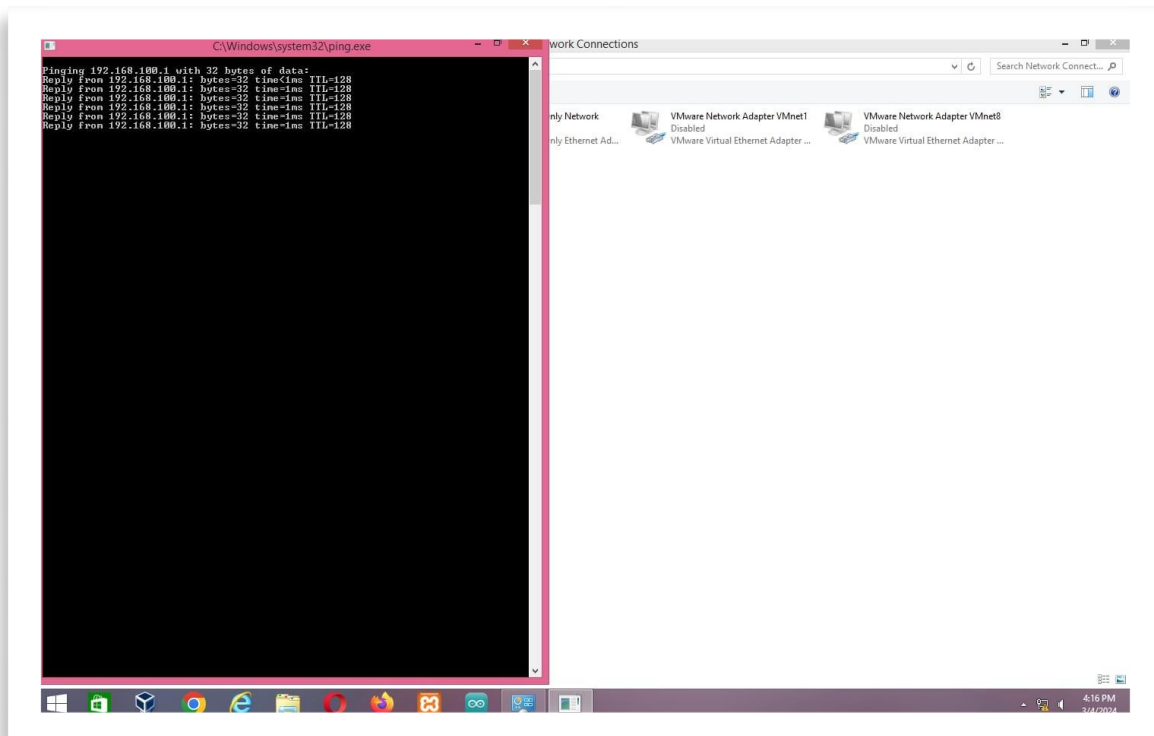
6. On the **General** tab, the default setting is typically set to **Obtain an IP address automatically**.

7. NOW press Windows + R and PING the system and you can share the files also

## Computer-1 After Ping

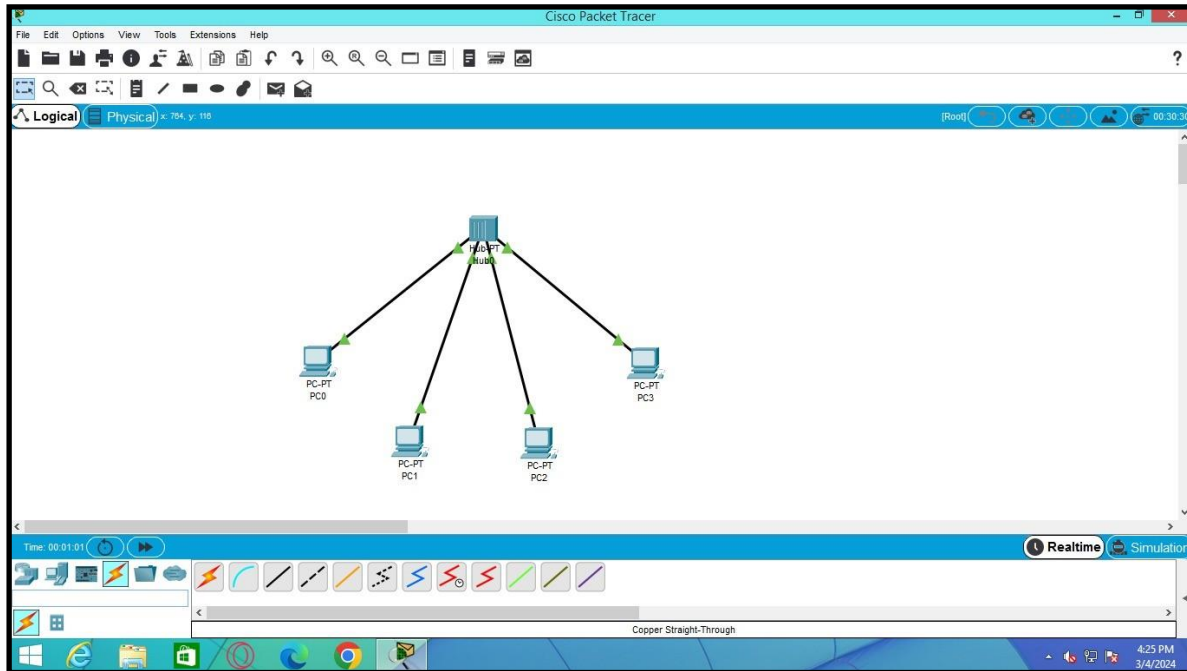


## Computer-2 After Ping



## 2. Use Cisco packet tracer to

### 2A. Build a local area network of 4 to 6 nodes using Hub/ Repeater



#### 1. Open Cisco Packet Tracer:

- Launch Cisco Packet Tracer on your computer.

#### 2. Create a New Project:

- Start a new project by clicking on "File" > "New" or by pressing Ctrl + N.

#### 3. Select Devices:

- Drag and drop a hub or a repeater from the "Connectivity" section of the device list onto the workspace.

#### 4. Connect Devices to the Hub/Repeater:

- Drag and drop PCs or laptops from the "End Devices" section of the device list onto the workspace.
- Connect each PC or laptop to the hub or repeater by clicking on the appropriate interface on the hub/repeater and then clicking on the interface of the PC or laptop.

#### 5. Assign IP Addresses (Optional):

- If you want to assign IP addresses to the devices, click on each device to open its configuration window.
- Navigate to the "Config" tab and assign IP addresses to each device according to your network requirements.

#### 6. Configure Interfaces (Optional):

- If needed, configure the interfaces on the hub or repeater. However, hubs and repeaters typically do not require any configuration as they operate at the physical layer.

#### 7. Verify Connectivity:

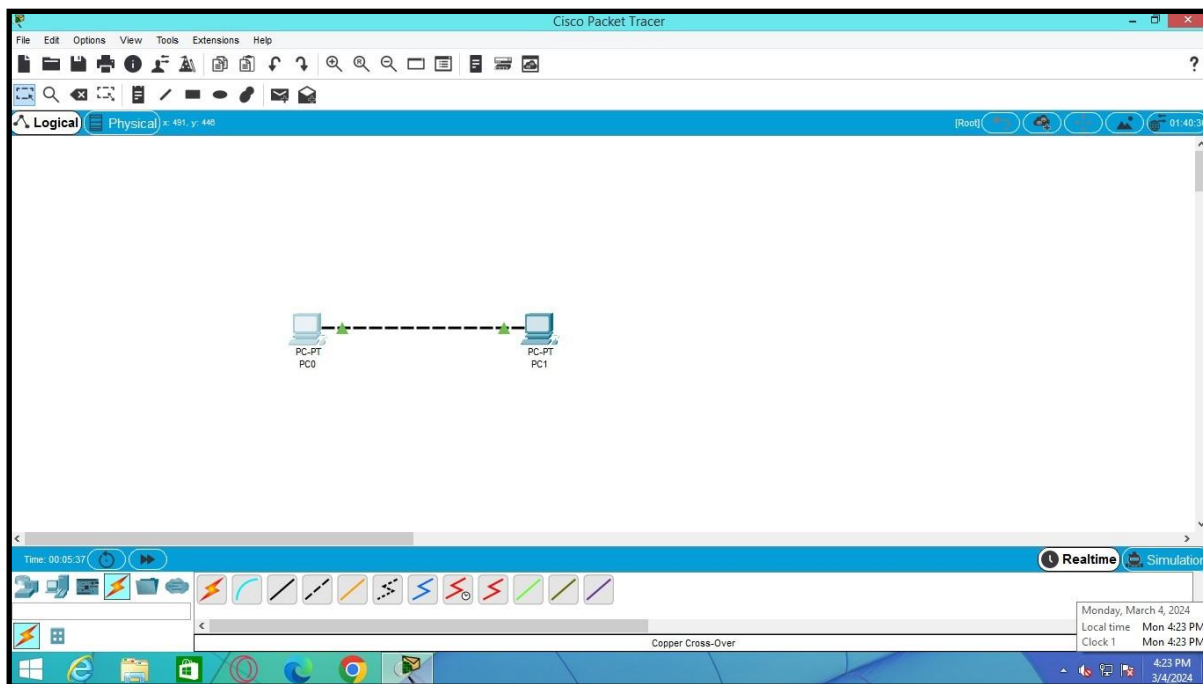
- Once the connections are made and devices are configured (if necessary), verify connectivity between the devices by sending ping commands between them.
- Click on a PC or laptop, go to the "Desktop" tab, open the Command Prompt or Terminal, and use the ping command to test connectivity to other devices in the network.

#### 8. Save Your Project:

## Computer Network Lab

- Save your project by clicking on "File" > "Save As" and providing a name for your project.
- 9. **Optional: Add Switches or Routers (Advanced):**
  - If you want to expand your network or add more complexity, you can replace the hub or repeater with a switch or router and connect devices accordingly. This step is optional and depends on your network requirements.
- 10. **Simulation (Optional):**
  - You can simulate the network to observe how traffic flows through the network and troubleshoot any issues that arise. Click on the "Simulation" tab and start the simulation to observe network behavior.

## 2B. Build a Peer to Peer network



1. **Open Cisco Packet Tracer:**
  - Launch Cisco Packet Tracer on your computer.
2. **Create a New Project:**
  - Start a new project by clicking on "File" > "New" or by pressing Ctrl + N.
3. **Select End Devices:**
  - Drag and drop PCs or laptops from the "End Devices" section of the device list onto the workspace.
  - You can add as many PCs or laptops as needed for your peer-to-peer network.
4. **Connect Devices:**
  - Connect each PC or laptop to the others using straight-through Ethernet cables.
  - Click on the appropriate Ethernet port on one device, then click on the Ethernet port of the device you want to connect it to.
5. **Assign IP Addresses:**
  - Optionally, you can assign IP addresses to each device to enable communication between them.

- Click on each PC or laptop to open its configuration window.
  - Navigate to the "Config" tab and assign IP addresses to each device. Make sure they are on the same subnet.
  - Alternatively, you can leave the devices to obtain IP addresses automatically using DHCP.
6. **Configure Interfaces (Optional):**
    - Since this is a peer-to-peer network, there are no intermediate devices like routers or switches that require configuration.
  7. **Verify Connectivity:**
    - Once the connections are made and devices are configured (if necessary), verify connectivity between the devices by sending ping commands between them.
    - Click on a PC or laptop, go to the "Desktop" tab, open the Command Prompt or Terminal, and use the ping command to test connectivity to other devices in the network.
  8. **Save Your Project:**
    - Save your project by clicking on "File" > "Save As" and providing a name for your project.
  9. **Simulation (Optional):**
    - You can simulate the network to observe how traffic flows through the network and troubleshoot any issues that arise. Click on the "Simulation" tab and start the simulation to observe network behavior.

## MODULE : II

### 1. Implement sliding window protocol

To implement the sliding window protocol in a simulated network environment, we'll use Cisco Packet Tracer to demonstrate the basic concepts. The sliding window protocol is a technique used in computer networks for reliable and efficient data transmission between sender and receiver.

#### 1. Sliding window Protocol

```
#include<stdio.h>

int main()
{
    int w,i,f,frames[50];

    printf("Enter window size: ");
    scanf("%d",&w);

    printf("\nEnter number of frames to transmit: ");
    scanf("%d",&f);

    printf("\nEnter %d frames: ",f);
```

## Computer Network Lab

```
for(i=1;i<=f;i++)
    scanf("%d",&frames[i]);

printf("\nWith sliding window protocol the frames will be sent
in the following manner (assuming no corruption of frames)\n\n");
printf("After sending %d frames at each stage sender waits for
acknowledgement sent by the receiver\n\n",w);

for(i=1;i<=f;i++)
{
    if(i%w==0)
    {
        printf("%d\n",frames[i]);
        printf("Acknowledgement of above frames sent is
received by sender\n\n");
    }
    else
        printf("%d ",frames[i]);
}

if(f%w!=0)
    printf("\nAcknowledgement of above frames sent is received
by sender\n");

return 0;
}
```

### OUTPUT:

Enter window size: 2

Enter number of frames to transmit: 5

Enter 5 frames: 1

2  
3  
4  
5

With sliding window protocol the frames will be sent in the following manner (assuming no corruption of frames)

After sending 2 frames at each stage sender waits for acknowledgement sent by the receiver

1 2

Acknowledgement of above frames sent is received by sender

3 4

Acknowledgement of above frames sent is received by sender

5

Acknowledgement of above frames sent is received by sender

-----  
Process exited after 11.14 seconds with return value 0

Press any key to continue . . .

In this example, we'll simulate a simple network with two devices: a sender and a receiver. We'll use the sliding window protocol to transmit data from the sender to the receiver.

Here's how you can implement it in Cisco Packet Tracer:

1. **Setup the Network:**

- Open Cisco Packet Tracer and create a new blank project.
- Add two end devices, representing the sender and the receiver. You can use PCs or laptops for this purpose.

2. **Connect the Devices:**

- Connect the sender and the receiver using a straight-through Ethernet cable.
- Ensure both devices are powered on and have appropriate IP configurations.

3. **Configure IP Addresses:**

- Assign IP addresses to both devices to enable communication between them. Make sure they are on the same subnet.
- Go to each device's configuration settings and set IP addresses, subnet masks, and default gateways if needed.

4. **Implement Sliding Window Protocol:**

- Use a programming language like Python to simulate the sliding window protocol.
- Write sender and receiver scripts that implement the protocol. The sender script should send data packets with sequence numbers, and the receiver script should acknowledge receipt of packets and handle any out-of-order packets.
- Simulate packet transmission and acknowledgment within the sender and receiver scripts based on the sliding window algorithm.

5. **Testing:**

- Run the sender and receiver scripts simultaneously.
- Observe the packet transmission and acknowledgment process.
- Monitor the window size, sequence numbers, and acknowledgments to ensure they follow the sliding window protocol rules.

6. **Debugging and Optimization:**

- Debug any issues encountered during testing, such as packet loss, out-of-order delivery, or incorrect acknowledgments.



- Optimize the implementation for efficiency and reliability, considering factors like window size, timeout intervals, and error handling mechanisms.
7. **Documentation:**
- Document the implementation details, including the sliding window algorithm used, any optimizations made, and the results of testing and debugging.

## 2. go back N Protocol

```
#include<stdio.h>
int main()
{
    int window size, sent=0, ack, i;
    printf("enter window size\n");
    scanf("%d", &window size);
    while(1)
    {
        for(i = 0; i<window size; i++)
        {
            printf("Frame %d has been transmitted.\n", sent);
            sent++;
            if(sent == window size)
                break;
        }
        printf("\nPlease enter the last Acknowledgement received.\n");
        scanf("%d", &ack);

        if(ack == window size)
            break;
        else
            sent = ack;
    }
    return 0;
}
```

### OUTPUT :

enter window size

7

Frame 0 has been transmitted.

Frame 1 has been transmitted.

Frame 2 has been transmitted.

Frame 3 has been transmitted.

Frame 4 has been transmitted.

Frame 5 has been transmitted.

Frame 6 has been transmitted.

Please enter the last Acknowledgement received.

4

Frame 4 has been transmitted.

Frame 5 has been transmitted.

Frame 6 has been transmitted.

Please enter the last Acknowledgement received.

7

-----

Process exited after 10.15 seconds with return value 0

Press any key to continue . . .

### 1. Run the Scripts:

- a. Run both the sender and receiver scripts simultaneously.

### 2. Observations:

- a. Observe the packet transmission, acknowledgment, and window sliding behavior based on the Go-Back-N protocol.
- b. The sender will send packets within the window size and wait for acknowledgments. If a timeout occurs, it will retransmit packets from the base.
- c. The receiver will send acknowledgments for correctly received packets and discard out-of-order packets.

### 3. Testing and Optimization:

- a. Test the implementation under various network conditions and packet loss scenarios.
- b. Optimize the implementation for efficiency and reliability, considering factors like window size, timeout intervals, and error handling mechanisms.

## **MODULE : III**

### **1. Install & Configure network devices switch**

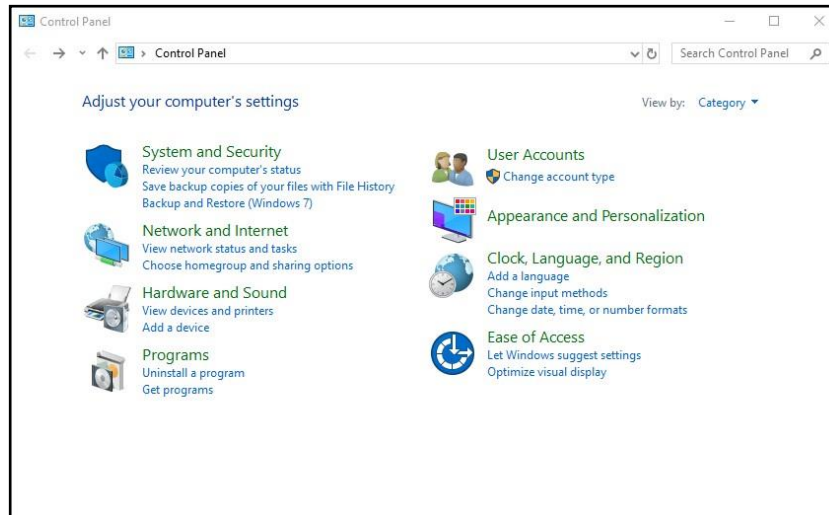
#### **INSTALLING A SWITCH STEPS:**

1. Stacking Switch (if you are using more than one switch)
2. Connecting Hubs (if you are using more than switch)
3. Connecting the Power and Turning the Switch On
4. Connecting Other Network Devices to the Hub
- 5 Connecting the CONSOLE Port

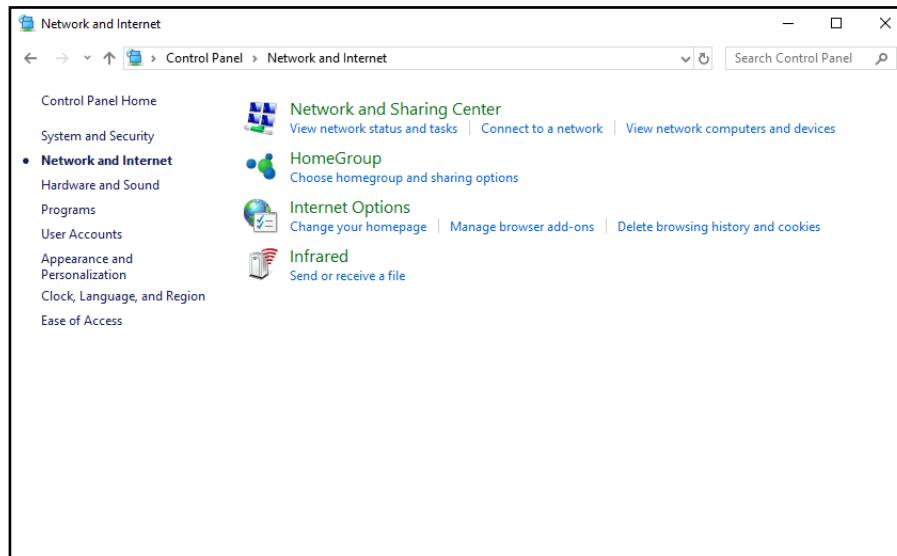


#### **CONFIGURE STEPS:**

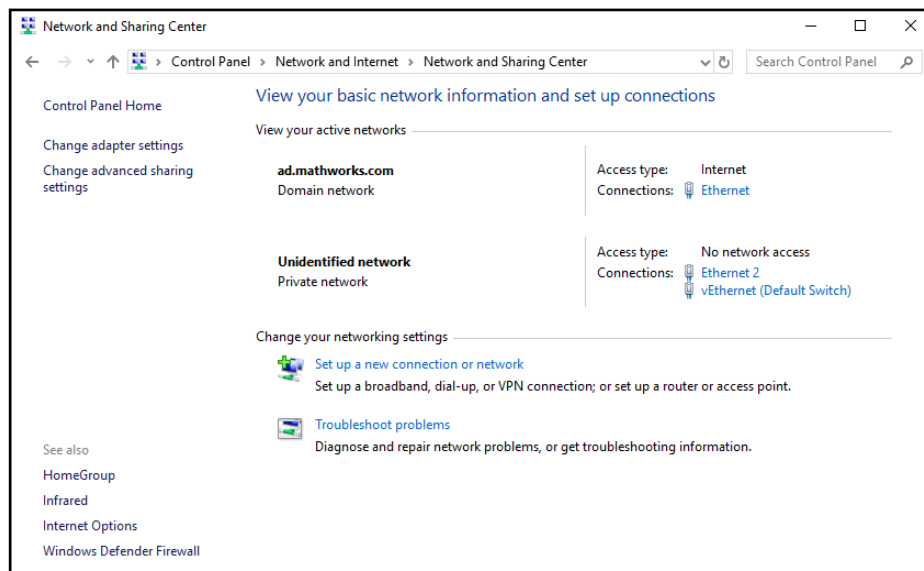
1. Open the **Control Panel** from the Windows® icon in the lower left corner of your monitor.  
In the Control Panel window, make sure **View by** is set to **Category**.
2. Click **Network and Internet**.



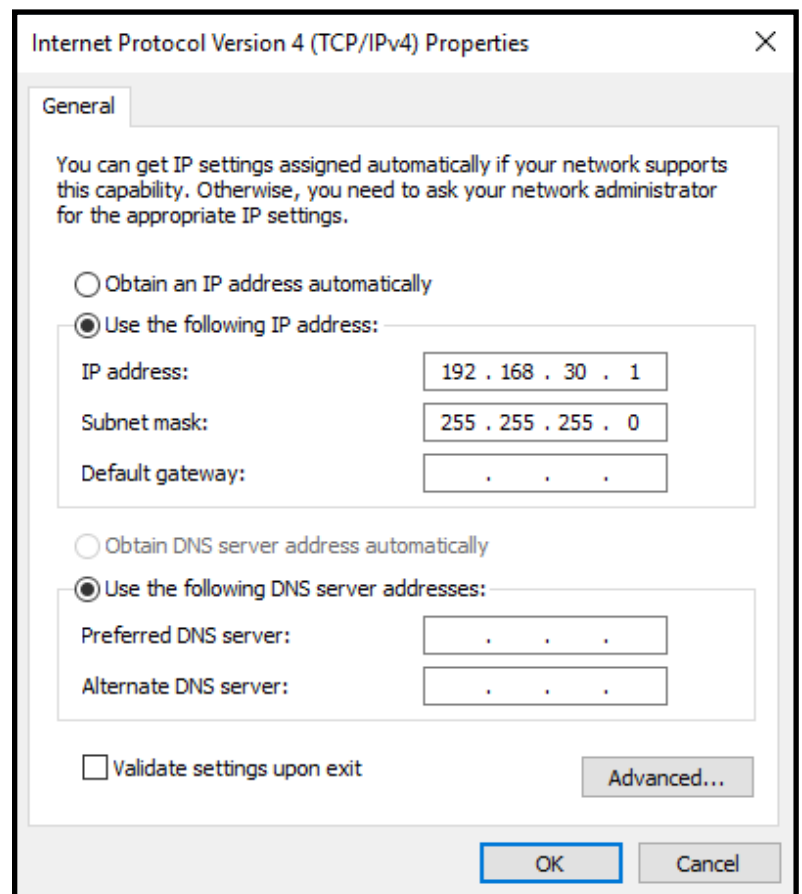
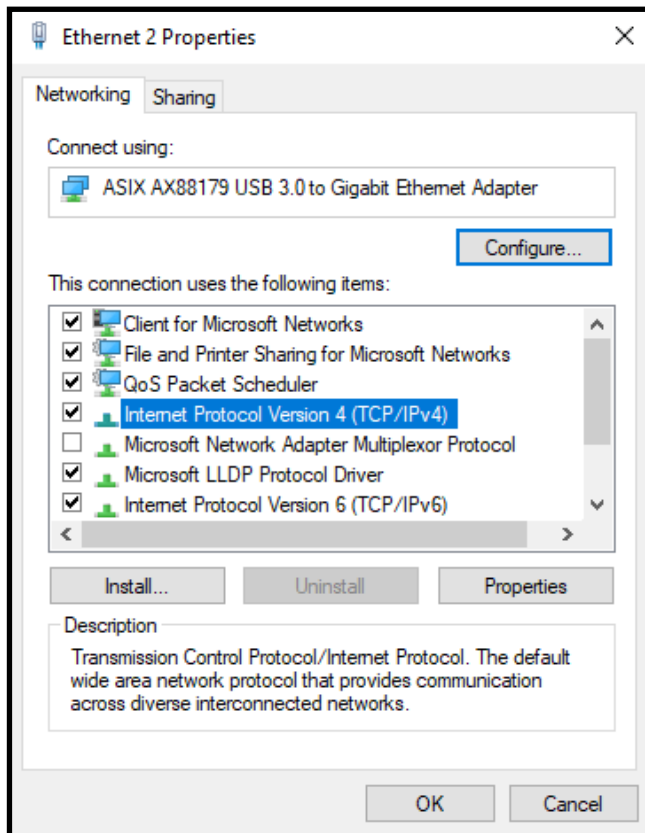
3. Click **Network and Sharing Center**.



4. Click **Change adapter settings** in the left pane.



5. On the **Networking** tab, clear **Clients for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks**. These services can cause intermittent connection problems with USRP™ radios. To configure the IP address, double-click **Internet Protocol Version 4 (TCP/IPv4)**.



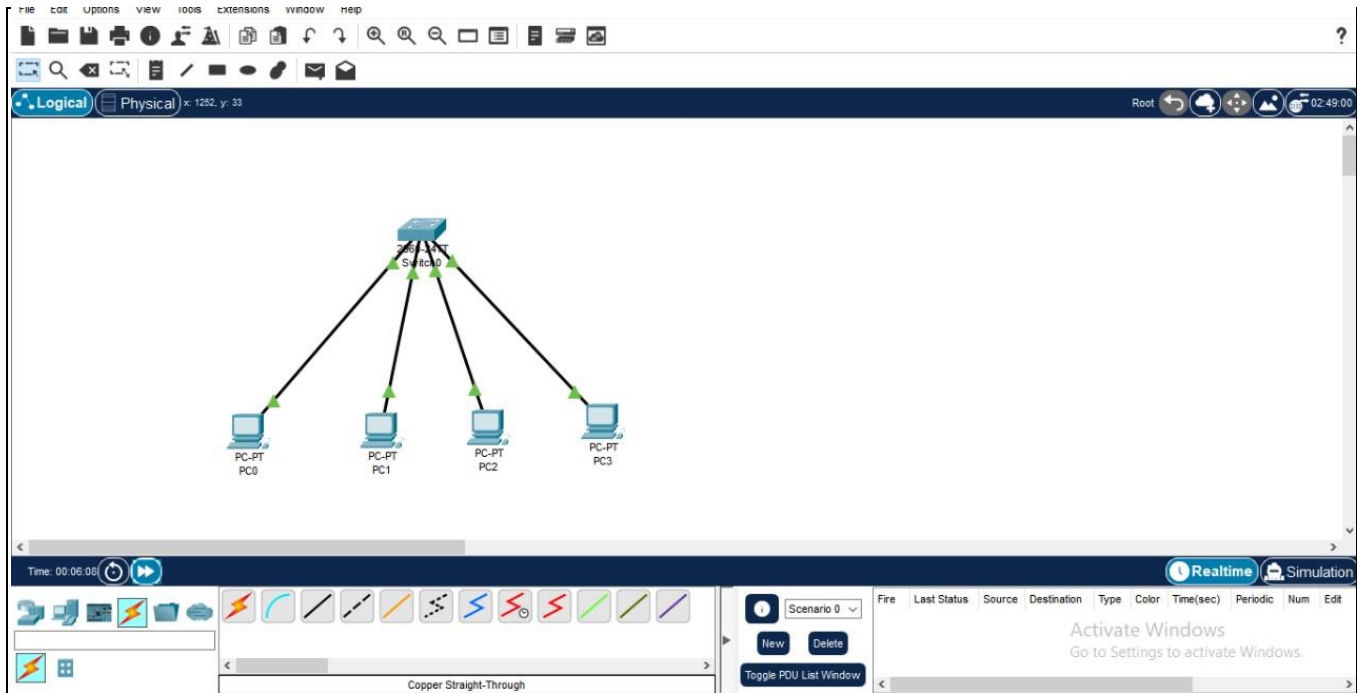
6. On the **General** tab, the default setting is typically set to **Obtain an IP address automatically**.

[illegible]

## A screenshot of a Windows desktop environment. In the foreground, a command prompt window titled 'C:\Windows\system32\ping.exe' is open, displaying the results of a ping command to 192.168.100.1. The output shows five successful replies with 32 bytes of data, each taking approximately 1ms and having a TTL of 128. In the background, a 'Network Connections' window is visible, showing a list of network adapters. Under the 'Ethernet' section, two 'VMware Virtual Ethernet Adapter' entries are listed, both marked as 'Disabled'. The Windows taskbar at the bottom shows various application icons, including File Explorer, Edge, and several instances of other applications. The system clock in the bottom right corner indicates the time is 4:10 PM on 3/1/2024.

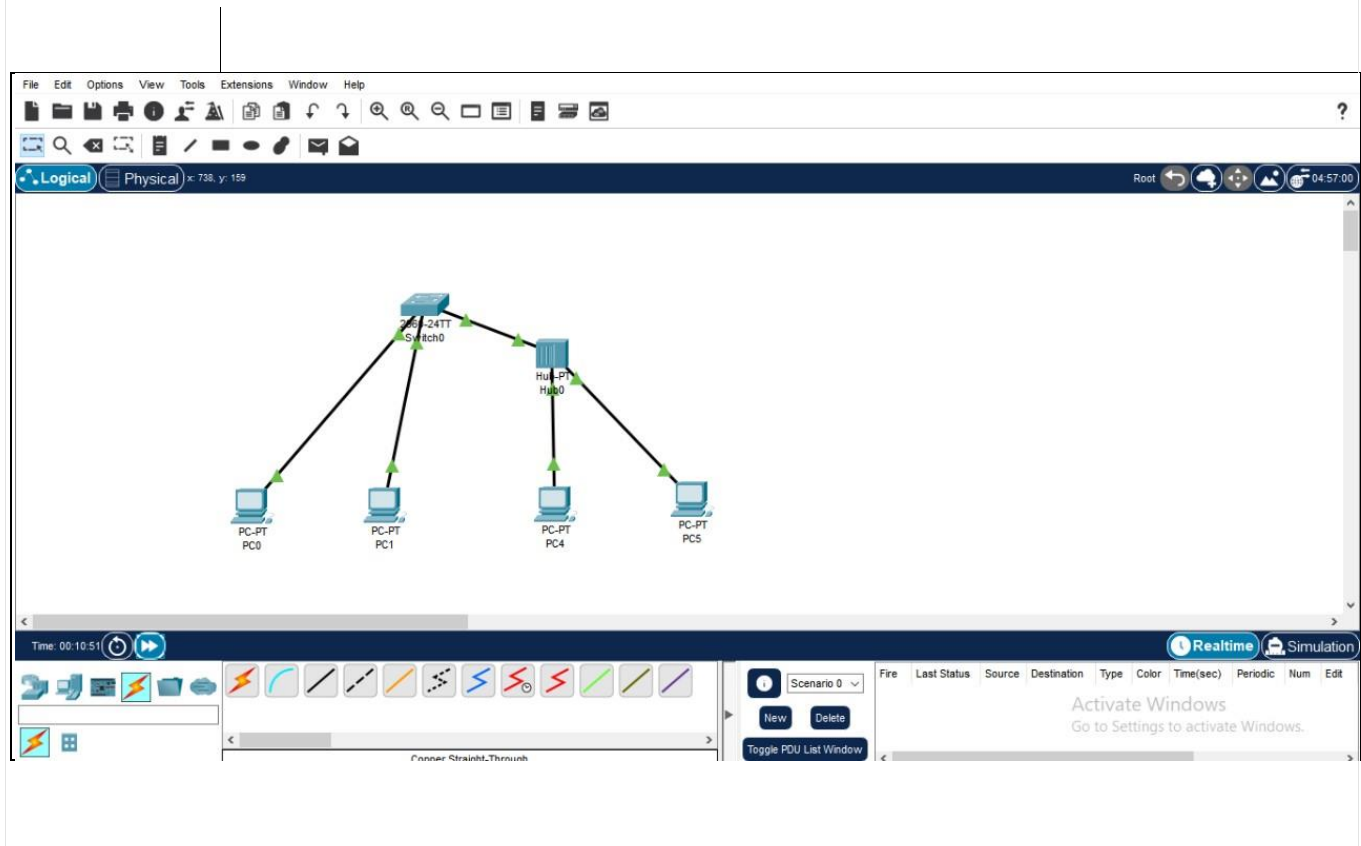
## 2. Use Cisco Packet Tracer to

### 2.A Build a local area network of 4 to 6 nodes using Switch



1. **Open Cisco Packet Tracer:** Launch Cisco Packet Tracer on your computer.
2. **Add Devices:** Drag and drop a switch from the device list onto the workspace. You can add multiple switches if you want to create a larger network.
3. **Connect Devices:** Use the appropriate cables to connect the devices. You can connect PCs to the switch using Ethernet cables. Drag cables from the available ports on the switch to the Ethernet ports on the PCs.
4. **Configure IP Addresses:** Right-click on each PC and select 'Configure' to set their IP addresses. Ensure that each PC has a unique IP address within the same subnet. For example, you can use the subnet 192.168.1.0/24 and assign IP addresses like 192.168.1.1, 192.168.1.2, etc., to each PC.
5. **Test Connectivity:** Once you've configured the IP addresses, you can test connectivity between the PCs by using the 'Command Prompt' or 'Terminal' in the PCs to ping each other.
6. **Optional:** If you want to configure VLANs or any other advanced settings, you can do so by accessing the switch's configuration interface. Right-click on the switch and select 'CLI' or 'Console' to access the command-line interface (CLI) of the switch.
7. **Save Configuration:** Once you're satisfied with your network setup, save your project in Cisco Packet Tracer.

**2b. let's create a basic local area network (LAN) using both a hub and a switch in Cisco Packet Tracer. We'll use four nodes (PCs) to keep it simple. Here are the steps:**



1. **Open Cisco Packet Tracer:** Launch Cisco Packet Tracer on your computer.
2. **Add Devices:** Drag and drop a switch and a hub from the device list onto the workspace. You can find them under the "Connectivity" section.
3. **Connect Devices to the Hub and Switch:** Connect two PCs to the hub and the remaining two PCs to the switch. To do this, select the appropriate cable type (Ethernet straight-through cable for switch connections and Ethernet crossover cable for hub connections) and drag from the available ports on the devices to the Ethernet ports on the PCs.
4. **Configure IP Addresses (Optional):** You can optionally configure IP addresses for the PCs to enable communication between them. Right-click on each PC, select 'Configure,' and set their IP addresses. Ensure that each PC has a unique IP address within the same subnet.
5. **Study the Network:** You can study the behavior of both the hub and the switch in this setup. Hubs operate at the physical layer of the OSI model and forward data to all devices connected to them, whereas switches operate at the data link layer and forward data only to the device it

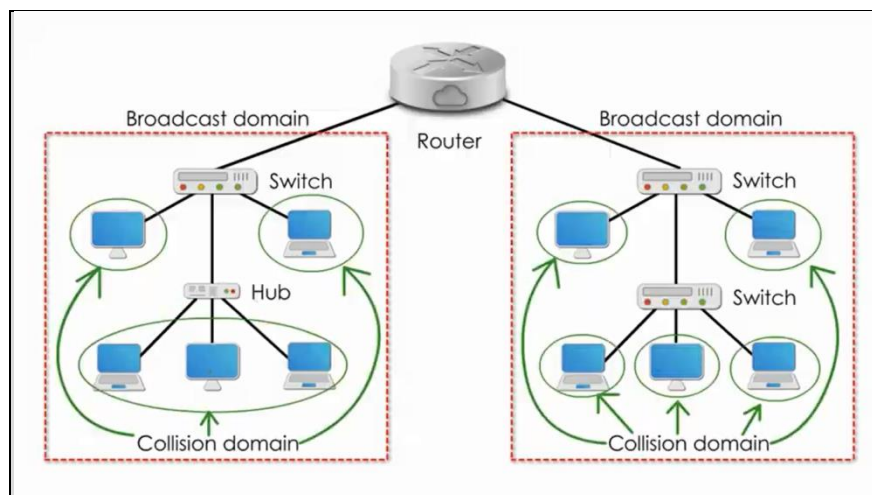


is intended for. You can observe the differences in traffic handling between the hub and the switch by monitoring the traffic flow and collision rates.

6. **Test Connectivity:** If you've configured IP addresses, you can test connectivity between the PCs by using the 'Command Prompt' or 'Terminal' in the PCs to ping each other.
7. **Optional:** You can also try adding more nodes or configuring VLANs to further study network segmentation and traffic isolation.
8. **Save Configuration:** Once you're satisfied with your network setup, save your project in Cisco Packet Tracer.

### 2c. Identify Broadcast & Collision Domain

In a network, understanding broadcast and collision domains is crucial for optimizing performance and troubleshooting issues. Let's use Cisco Packet Tracer to identify these domains in a simple network setup.



We'll create a network with a switch, a hub, and multiple PCs to demonstrate broadcast and collision domains.

1. **Open Cisco Packet Tracer:** Launch Cisco Packet Tracer on your computer.
2. **Add Devices:** Drag and drop a switch, a hub, and several PCs onto the workspace.
3. **Connect Devices:** Connect the PCs to both the switch and the hub. PCs connected to the switch should be connected using Ethernet straight-through cables, while PCs connected to the hub should use Ethernet crossover cables.
4. **Study Broadcast Domains:**
  - The switch creates separate broadcast domains for each port. Since a switch forwards traffic only to the port where the destination device is connected, broadcast packets

sent from one PC are not forwarded to all other PCs connected to the switch. Each PC connected to the switch is in its broadcast domain.

- However, the hub forwards all incoming packets to all connected devices, so all PCs connected to the hub are in the same broadcast domain.

## 5. Study Collision Domains:

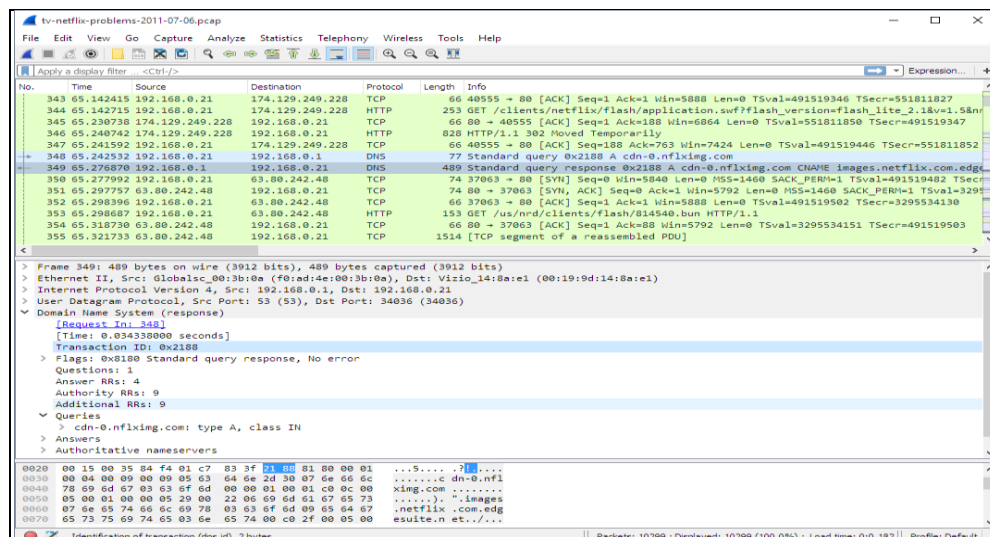
- In Ethernet networks, collision domains represent the set of devices whose frames could collide with each other. Collisions occur on shared media segments, such as those connected to hubs.
- With a switch, each port is in its collision domain, meaning collisions are limited to the devices connected to that port. Since a switch separates collision domains by default, there are no collisions between devices connected to the switch.
- However, all devices connected to the hub share the same collision domain. When multiple devices transmit data simultaneously, collisions can occur, leading to performance degradation.

## 6. Test Connectivity and Observations:

- Configure IP addresses on the PCs and test connectivity between them.
- Observe that broadcast traffic from a PC connected to the hub is received by all other PCs connected to the hub, while broadcast traffic from a PC connected to the switch is received only by the intended destination.
- Monitor the network traffic using Packet Tracer's simulation mode to observe collisions occurring on the hub-connected PCs.

7. **Save Configuration:** Once you're done studying the broadcast and collision domains, save your project in Cisco Packet Tracer.

## 3. Use Wireshark to examine Ethernet packets and ARP packets

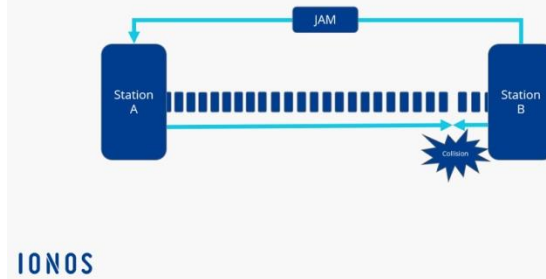


Wireshark to examine Ethernet packets and ARP (Address Resolution Protocol) packets. Here's how you can do it:

1. **Install Wireshark:** If you haven't already, download and install Wireshark from the official website: <https://www.wireshark.org/>.
2. **Start Wireshark:** Open Wireshark on your computer.
3. **Select Network Interface:** When you start Wireshark, it will ask you to select a network interface to capture packets. Choose the appropriate interface for your network connection and click on "Start" to begin capturing packets.
4. **Capture Packets:** Wireshark will start capturing packets on the selected interface. You'll see a list of captured packets in the main window.
5. **Filter for Ethernet Packets:** To filter for Ethernet packets, type "eth" in the display filter box at the top of the Wireshark window. This will filter the captured packets to only show Ethernet frames.
6. **Filter for ARP Packets:** To filter for ARP packets, type "arp" in the display filter box. This will filter the captured packets to only show ARP packets.
7. **Analyze Packets:** You can now examine the captured Ethernet and ARP packets in Wireshark. Click on a packet in the list to view its details in the packet details pane below. You can analyze various aspects of the packets, such as source and destination MAC addresses, source and destination IP addresses, ARP request and reply messages, etc.
8. **Stop Capturing:** Once you're done examining packets, you can stop the packet capture by clicking on the "Stop" button in Wireshark.
9. **Save Capture:** If you want to save the captured packets for further analysis or reference, you can save the capture file by clicking on "File" > "Save As" and choosing a file format (e.g., pcap).

### 4. To study Performance of CSMA/CD Protocol

To study the performance of the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol, we can simulate a network environment using tools like Cisco Packet Tracer or Wireshark. Unfortunately, Packet Tracer does not provide direct support for simulating CSMA/CD behavior explicitly. However, we can use Wireshark to analyze network traffic and infer the behavior of CSMA/CD.

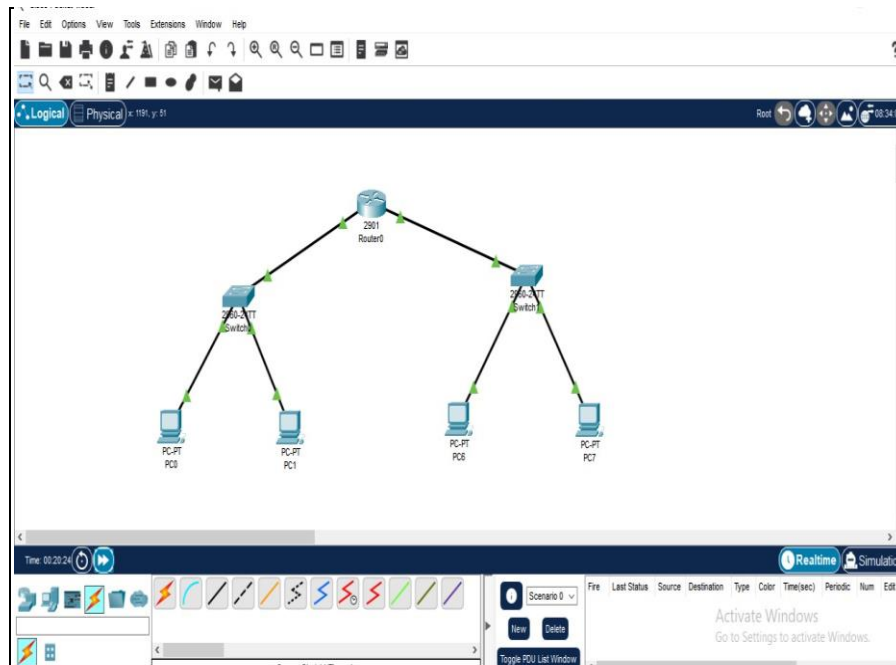


Here's how you can study the performance of CSMA/CD using Wireshark:

1. **Setup:** Create a small network topology in Packet Tracer with multiple nodes (PCs or laptops) connected via a hub or a shared medium like Ethernet. Ensure that the devices support Ethernet connectivity.
2. **Capture Packets:** Open Wireshark on a computer connected to the network. Start capturing packets on the network interface connected to the network.
3. **Generate Traffic:** Initiate data transfers between different nodes in the network. You can use various methods to generate traffic, such as file transfers, pings, or continuous data streams.
4. **Analyze Packets:** Analyze the packet capture in Wireshark. Look for instances of collision events. In a CSMA/CD environment, collisions occur when two or more devices attempt to transmit data simultaneously, leading to data corruption. You can identify collision events by observing packets with a high number of retransmissions, or packets with error flags indicating collisions.
5. **Study Performance Metrics:** Measure the performance of the CSMA/CD protocol by analyzing key metrics such as throughput, latency, and collision rates. Throughput refers to the rate at which data is successfully transmitted across the network. Latency measures the time taken for a packet to travel from the source to the destination. Collision rates indicate the frequency of collisions occurring in the network.
6. **Adjust Parameters:** Experiment with different network parameters, such as the number of nodes, data transmission rates, and network topology, to observe how they affect the performance of CSMA/CD.
7. **Draw Conclusions:** Based on your observations, draw conclusions about the effectiveness of the CSMA/CD protocol in managing network traffic and minimizing collisions. Consider factors such as network load, congestion, and the number of active nodes in the network.

# MODULE : IV

## 1. Install & configure network devices routers



1. **Choose a Router:** Select a router suitable for your network requirements. Consider factors such as the size of your network, desired features (e.g., wireless connectivity, VPN support), and budget.
2. **Physical Installation:**
  - Unpack the router and its accessories.
  - Place the router in a central location for optimal coverage.
  - Connect the router to a power source using the provided power adapter.
  - Connect the router to your modem using an Ethernet cable if you're setting up an internet connection.
3. **Connect Devices:**
  - Connect your devices (computers, printers, etc.) to the router using Ethernet cables or via Wi-Fi if the router supports wireless connectivity.
4. **Access Router Configuration:**
  - Open a web browser on a connected device.
  - Enter the router's IP address in the browser's address bar. The default IP address is often printed on a label on the router or provided in the router's manual. Common IP addresses include 192.168.0.1 or 192.168.1.1.

## Computer Network Lab

- Log in to the router's administration interface using the default username and password. This information is also provided in the router's manual.

### 5. **Configure Network Settings:**

- Once logged in, you can configure various network settings such as:
  - WAN (Wide Area Network) settings for connecting to the internet.
  - LAN (Local Area Network) settings including IP address, subnet mask, and DHCP (Dynamic Host Configuration Protocol) settings.
  - Wireless network settings (if applicable) including SSID (network name), security mode, and password.
  - Port forwarding, firewall settings, and other advanced configurations as needed.

### 6. **Save Configuration:**

- After making changes, be sure to save the configuration settings. This is usually done by selecting a "Save" or "Apply" button within the router's configuration interface.

### 7. **Test Connectivity:**

- Once configuration is complete, test connectivity by accessing the internet from connected devices and verifying that they can communicate with each other on the local network.

### 8. **Update Firmware:**

- Check for firmware updates for your router and install them if available. Firmware updates often include bug fixes, security patches, and performance improvements.

### 9. **Secure Your Router:**

- Change the default login credentials to something more secure.
- Enable WPA2 or WPA3 encryption for Wi-Fi networks.
- Disable remote administration if not needed.
- Consider enabling additional security features such as MAC address filtering or guest networks.

## 2. Use Cisco packet tracer to

- a. Design and apply IP addressing scheme for a given topology
- b. Connect two or three LAN's via a router. Trace how routing happens via Simulation, and study the working of router.
- c. Design multiple subnets with suitable number of hosts
- d. Demonstrate static routing and dynamic routing for given topology
- e. Configure DHCP server
- f. Create subnets , Configure Host IP, Subnet Mask and Default Gateway in a LAN

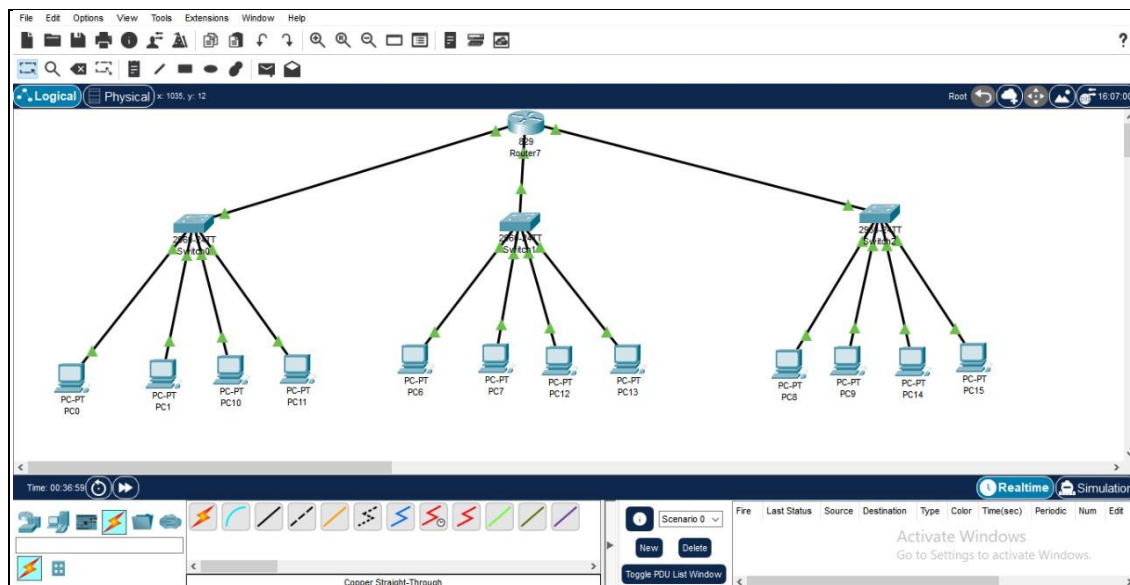
g. Configure RIP/OSPF

**Follow these instructions within Cisco Packet Tracer:**

## 2A. Design and apply IP addressing scheme for a given topology:

- Define the network topology using routers, switches, and PCs.
- Assign IP addresses to each device based on the network requirements, ensuring they belong to the same subnet.
- Use the appropriate subnet mask to define the size of each subnet.
- Verify connectivity between devices within the same subnet.

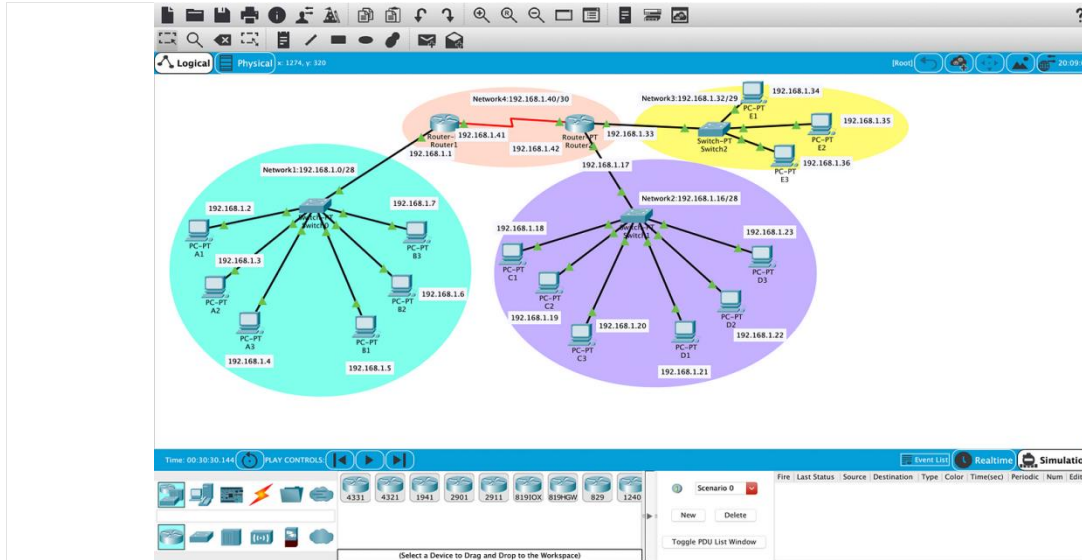
## 2B. Connect two or three LAN's via a router. Trace how routing happens via Simulation, and study the working of router:



- Connect multiple LANs using routers.
- Configure IP addresses on router interfaces and PCs according to the IP addressing scheme.
- Use Packet Tracer's simulation mode to trace the routing process:
  - Send a packet from a source PC to a destination PC on a different LAN.
  - Observe how the router forwards the packet based on its routing table.
  - Verify that the packet reaches the destination PC successfully.

## 2C. Design multiple subnets with suitable number of hosts:





- Determine the number of subnets required based on network requirements.
- Decide on the subnet sizes and subnet masks to accommodate the desired number of hosts in each subnet.

Assign IP addresses to devices within each subnet according to the subnetting scheme

## 2D. Demonstrate static routing and dynamic routing for given topology:

- Configure static routes on routers to manually specify the next-hop IP address for remote networks.
- Alternatively, configure dynamic routing protocols such as RIP or OSPF to allow routers to dynamically learn and share routing information.
- Verify routing functionality by sending packets between devices on different networks and observing how they are routed.

## 2E. Configure DHCP server:

- Add a DHCP server device to the network.
- Configure DHCP pools on the DHCP server, specifying the range of IP addresses to be leased to clients.
- Configure additional DHCP options such as default gateway, DNS server, and subnet mask.
- Connect DHCP clients to the network and verify that they receive IP addresses automatically.

## 2F. Create subnets, Configure Host IP, Subnet Mask, and Default Gateway in a LAN:

- Define the subnetting scheme and assign IP addresses to devices within each subnet.



- Configure the subnet mask and default gateway on each device according to the subnet they belong to.
- Verify connectivity between devices within the same subnet.

### 2G. Configure RIP/OSPF:

- Enable RIP or OSPF routing protocols on routers.
- Configure router interfaces to participate in the routing process.
- Verify routing table updates and communication between routers using the chosen routing protocol.

By following these steps, you can effectively design, configure, and test various network scenarios in Cisco Packet Tracer, gaining practical experience with IP addressing, routing, subnetting, DHCP, and routing protocols.


## 3. Use Wireshark to

**3A.** analyze IP Datagram and IP fragmentation received during the execution of trace route command.

Wireshark is a powerful tool for analyzing network traffic, including IP datagrams, fragmentation, and ICMP packets generated by commands like trace route and ping. Here's how you can analyze these packets using Wireshark:

### 3A. Analyze IP Datagram and IP Fragmentation Received During the Execution of Trace Route Command:

1. Start Wireshark on your computer and select the network interface connected to the network where you want to capture traffic.
2. Open the command prompt or terminal on your computer and execute the trace route command to a destination IP address. For example:


 Copy code

```
tracert www.example.com
```

3. Wireshark will start capturing packets on the selected network interface. Filter the captured packets to display only IP traffic by typing "ip" in the filter box.
4. Analyze the captured packets to observe the IP datagrams exchanged during the trace route command execution. You'll see ICMP Time Exceeded messages generated by routers along the path, indicating the route taken by packets to reach the destination.
5. Look for IP fragmentation by examining packets with the "Fragmentation" flag set. IP fragmentation occurs when packets exceed the Maximum Transmission Unit (MTU) of a network segment and need to be fragmented into smaller packets for transmission.

### 3B. Run Ping Command and Examine ICMP Packets Using Wireshark:

1. Start Wireshark on your computer and select the network interface connected to the network where you want to capture traffic.
2. Open the command prompt or terminal on your computer and execute the ping command to a destination IP address. For example:

 Copy code

```
ping www.example.com
```

3. Wireshark will start capturing packets on the selected network interface. Filter the captured packets to display only ICMP traffic by typing "icmp" in the filter box.
4. Analyze the captured packets to observe ICMP Echo Request and Echo Reply messages exchanged during the ping command execution. The Echo Request messages are sent by your computer, and the Echo Reply messages are generated by the destination host.
5. Examine the timestamps and sequence numbers of ICMP packets to calculate round-trip times (RTT) between your computer and the destination host.

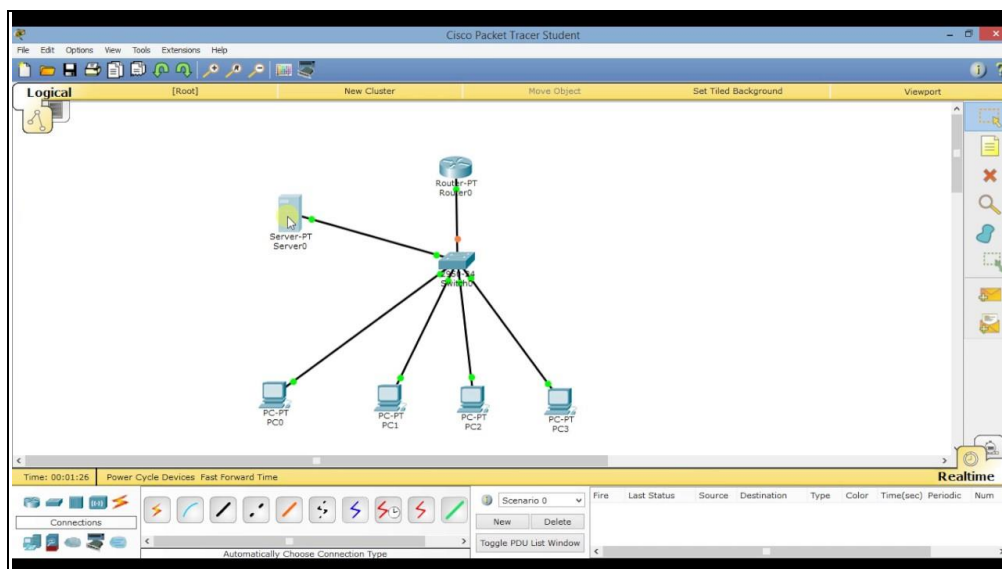
# MODULE : V

1. Use wireshark to
  - a. Examine UDP and TCP ports and handshake segments
  - b. Use packet tracer to configure DHCP server, DNS server, SMTP server

## **1A. Examine UDP and TCP Ports and Handshake Segments using Wireshark:**

1. Start Wireshark on your computer and select the network interface connected to the network where you want to capture traffic.
2. Apply filters to display only UDP or TCP traffic. Type "udp" or "tcp" in the filter box and press Enter. This will filter the captured packets to display only UDP or TCP packets.
3. Analyze the captured packets to observe UDP and TCP port numbers in the packet details pane. Look for source and destination port numbers to identify the communication endpoints.
4. To examine TCP handshake segments, focus on TCP connections. Look for packets with the SYN (synchronize), SYN-ACK (synchronize-acknowledgment), and ACK (acknowledge) flags set. This sequence represents the TCP three-way handshake used to establish connections.
5. Pay attention to the sequence and acknowledgment numbers exchanged during the handshake to understand the flow of data between the client and server.

## **1B. Use Packet Tracer to Configure DHCP Server, DNS Server, SMTP Server:**



1. Start Cisco Packet Tracer and create a new blank project.
2. Add devices to the workspace:
  - Add a router to act as the gateway for the network.
  - Add PCs or laptops to represent client devices.
  - Add a DHCP server device from the "End Devices" section.
  - Add a DNS server device from the "End Devices" section.
  - Add an SMTP server device from the "End Devices" section.
3. Connect the devices using appropriate cables. Connect the client devices to the router and the DHCP, DNS, and SMTP servers to the router as well.
4. Configure IP addresses for all devices:
  - Assign static IP addresses to the router, DHCP server, DNS server, and SMTP server.
  - Configure the DHCP server with a pool of IP addresses to lease to client devices.
5. Configure DHCP server:
  - Access the DHCP server configuration interface and configure DHCP settings such as IP address range, subnet mask, default gateway, and DNS server.
6. Configure DNS server:
  - Access the DNS server configuration interface and configure DNS settings such as domain names and IP addresses for hostnames.
7. Configure SMTP server:
  - Access the SMTP server configuration interface and configure SMTP settings such as domain name, email accounts, and SMTP relay settings.
8. Test the configuration:
  - Verify that client devices obtain IP addresses automatically from the DHCP server.
  - Test DNS resolution by accessing websites using domain names.
  - Test SMTP functionality by sending emails from client devices to external email addresses.

## 2. Implement client server program in C

Below are examples of simple client-server programs implemented in both C and Java. **C**

### Client-Server Program:

Server Program in C(TCP):

# Computer Network Lab

Server (TCP):

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <arpa/inet.h>

#define PORT 8080
#define BUFFER_SIZE 1024

int main() {
    int server_fd, new_socket;
    struct sockaddr_in address;
    int opt = 1;
    int addrlen = sizeof(address);
    char buffer[BUFFER_SIZE] = {0};
    const char *hello = "Hello from server";

    // Creating socket file descriptor
    if ((server_fd = socket(AF_INET, SOCK_STREAM, 0)) == 0) {
        perror("socket failed");
        exit(EXIT_FAILURE);
    }

    // Forcefully attaching socket to the port 8080
    if (setsockopt(server_fd, SOL_SOCKET, SO_REUSEADDR | SO_REUSEPORT, &opt, sizeof(opt)) < 0) {
        perror("setsockopt");
        exit(EXIT_FAILURE);
    }
    address.sin_family = AF_INET;
    address.sin_addr.s_addr = INADDR_ANY;
    address.sin_port = htons(PORT);

    // Forcefully attaching socket to the port 8080
    if (bind(server_fd, (struct sockaddr *)&address, sizeof(address)) < 0) {
        perror("bind failed");
        exit(EXIT_FAILURE);
    }
    if (listen(server_fd, 3) < 0) {
        perror("listen");
        exit(EXIT_FAILURE);
    }
    if ((new_socket = accept(server_fd, (struct sockaddr *)&address, (&addrlen))) < 0) {
        perror("accept");
        exit(EXIT_FAILURE);
    }

    read(new_socket, buffer, BUFFER_SIZE);
    printf("Client: %s\n", buffer);
    send(new_socket, hello, strlen(hello), 0);
    printf("Hello message sent\n");
    return 0;
}
```

Client Program in C (TCP):

```
Client (TCP):

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <arpa/inet.h>

#define PORT 8080
#define BUFFER_SIZE 1024

int main() {
    int sock = 0;
    struct sockaddr_in serv_addr;
    const char *hello = "Hello from client";
    char buffer[BUFFER_SIZE] = {0};

    if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0) {
        printf("\n Socket creation error \n");
        return -1;
    }

    serv_addr.sin_family = AF_INET;
    serv_addr.sin_port = htons(PORT);

    // Convert IPv4 and IPv6 addresses from text to binary form
    if (inet_pton(AF_INET, "127.0.0.1", &serv_addr.sin_addr) <= 0) {
        printf("\nInvalid address/ Address not supported \n");
        return -1;
    }

    if (connect(sock, (struct sockaddr *)&serv_addr, sizeof(serv_addr)) < 0) {
        printf("\nConnection Failed \n");
        return -1;
    }

    send(sock, hello, strlen(hello), 0);
    printf("Hello message sent\n");
    read(sock, buffer, BUFFER_SIZE);
    printf("Server: %s\n", buffer);
    return 0;
}
```

# Computer Network Lab

