**Deccan Education Society’s**

**Kirti M. Doongursee College of Arts, Science and Commerce**

**[NAAC Accredited: “A Grade”]**

****

**T.Y.B.Sc. [Computer Science]**

# **Practical Journal**

**25CSMJP52 : Data Communication and Networking**

# **Seat Number [ ]**

**Department of Computer Science and Information Technology**

**Department of Computer Science and Information Technology**

**Deccan Education Society’s**

**Kirti M. Doongursee College of Arts, Science and Commerce**

**[NAAC Accredited: “A Grade”]**

**C E R T I F I C A T E**

This is to certify that Mr. / Miss

of T.Y.B.Sc. (Computer Science) with Seat No. has completed **10**

Practicals of Paper- **25CSMJP52 : Data Communication and Networking** under my supervision in this College during the year **2025-2026**.

**Lecturer-In-Charge H.O.D.**

**Department of Computer Science & IT**

Date: / /2025 Date:

# Examined by: Remarks:

Date:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **25CSMJP52 : Data Communication and Networking** | | | | |
| **Sr.**  **No.** | **Date** | **Title** | **Page No.** | **Signature** |
| 1 |  | **Practical no: 1**  Understanding the working of NIC cards, Ethernet/Fast Ethernet/Gigabit Ethernet. | 4 |  |
| 2 |  | **Practical no: 2**  Crimping of Twisted-Pair Cable with RJ45 connector for Straight-Through, Cross-Over, Roll-Over. | 6 |  |
| 3 |  | **Practical no: 3**  To understand their respective role in networks/internet. | 6 |  |
| 4 |  | **Practical no: 4**  Problem solving with IPv4, which will include the concept of Classful addressing. (Supportive Hint: Use Cisco Binary Game) | 10 |  |
| 5 |  | **Practical no: 5**  Using Linux-terminal or Windows-cmd, execute following networking commands and note the output: ping, tracert, netstat, arp, ipconfig. | 15 |  |
| 6 |  | **Practical no: 6**  Create a basic network of two computers using appropriate network wire. | 22 |  |
| 7 |  | **Practical no: 7**  Connect multiple (min. 6) computers using a layer 2 switch. | 27 |  |
| 8 |  | **Practical no: 8**  Connect a network in triangular shape with three layer two switches and every switch will have four computers. Verify their connectivity with each other. | 33 |  |
| 9 |  | **Practical no: 9**  Create a wireless network of multiple PCs using appropriate access points. | 36 |  |
| 10 |  | **Practical no: 10**  Using Wireshark, network analyzer, set the filter for ICMP, TCP, HTTP, UDP, FTP, and perform respective protocol transactions to show/prove that the network analyzer is working. | 38 |  |

**Practical no 1: NIC/Ethernet/Fast Ethernet/Gigabyte Ethernet**

**Aim: Understanding the working of NIC/Ethernet/Fast Ethernet/Gigabite Ethernet**

The objective of this practical is to understand the operation and functionality of different types of Ethernet technologies, including NIC (Network Interface Cards), Ethernet, Fast Ethernet and Gigabit Ethernet.

**1. NIC (Network Interface Card)**

A Network Interface Card (NIC) is a hardware component that allows a device (like a computer, server, or printer) to connect to a network. It serves as the interface between the device and the network medium, whether that’s wired (Ethernet) or wireless (Wi-Fi). The NIC is responsible for sending and receiving data frames over the network.

It converts data from the device into a format that can be transmitted over the network and vice versa.

NICs are available in different speeds and formats, such as 10/100/1000 Mbps (Ethernet, Fast Ethernet, Gigabit Ethernet) and they can use different types of connectors (RJ-45, fibre optics, wireless).

**How it Works:**

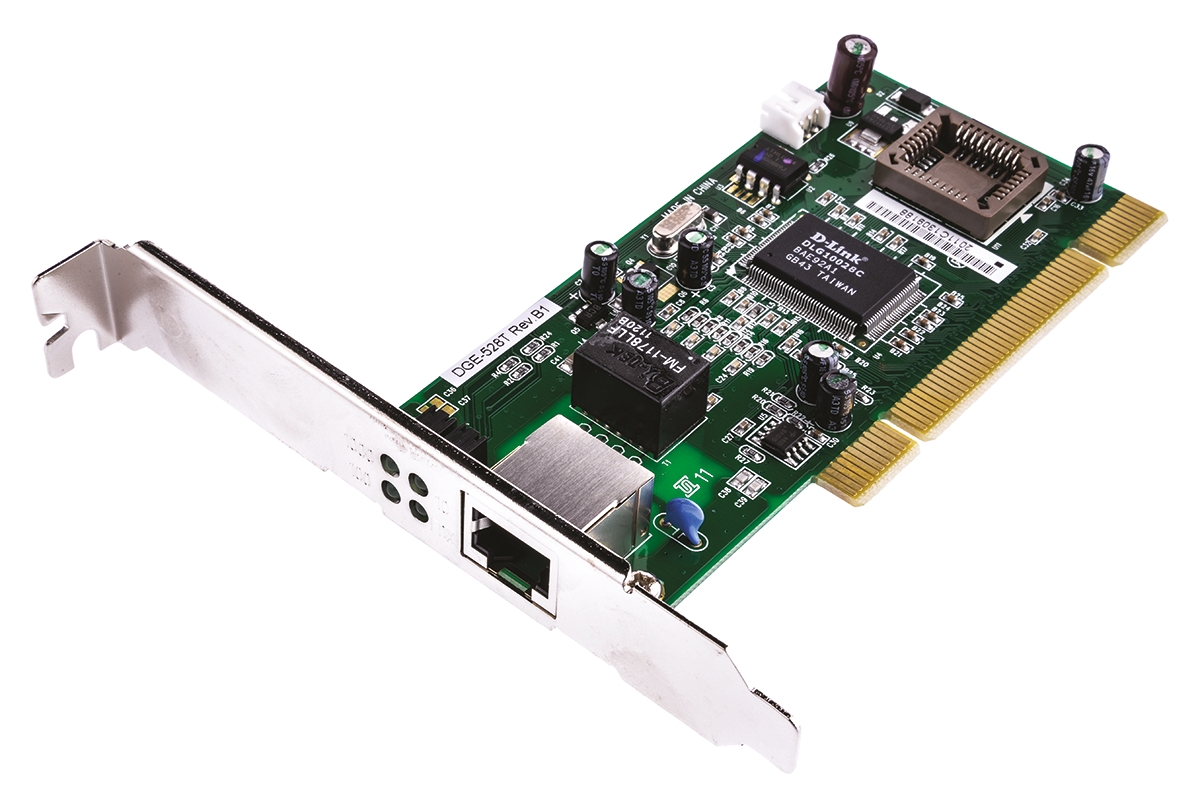
Connection: The NIC connects to the network via cables (Ethernet) or wireless signals (Wi-Fi).

Data Framing: It creates data packets and wraps them in frames with unique identifiers (MAC addresses).

Transmission: The NIC sends these frames over the network to the destination device.

Error Checking: It checks for transmission errors using CRC and ensures the data is intact.

Communication: Once received, the NIC passes the data to the operating system for further processing.



**2. Ethernet**

Ethernet is the most common LAN (Local Area Network) technology used to connect computers and other devices. It uses a physical medium (usually twisted-pair cables) and operates at a standard speed of 10 Mbps (original Ethernet).

Originally standardized as IEEE 802.3, Ethernet operates on a star topology, where each device is connected to a central switch or hub.

Ethernet uses a packet format called an Ethernet frame that includes source and destination MAC addresses, data and error-checking information.

Ethernet Characteristics:

|  |  |
| --- | --- |
| Speed | 10 Mbps |
| Cable | Coaxial (originally), twisted-pair cables (modern) |
| Range | Typically, 100 meters (for twisted-pair cables) |
| Uses | General purpose networking for small to medium-sized networks. |

**3. Fast Ethernet (100BASE-TX)**

Fast Ethernet is an enhancement of the original Ethernet standard, providing a higher data transfer rate of 100 Mbps.

Standard: IEEE 802.3u defines Fast Ethernet and it is widely used in most modern networking environments for general-purpose networking.

Speed: It provides a tenfold increase in speed compared to the original Ethernet standard.

Cable: Fast Ethernet typically uses Category 5 (Cat 5) or Category 5e (Cat 5e) cables for twisted-pair copper cabling.

Fast Ethernet Characteristics:

|  |  |
| --- | --- |
| Speed | 100 Mbps |
| Cable | Cat 5/5e (twisted-pair copper) |
| Range | 100 meters |
| Uses | Common for office networks, home networks and small businesses. |

**4. Gigabit Ethernet (1000BASE-T)**

Gigabit Ethernet is a further enhancement of Ethernet, providing speeds up to 1000 Mbps (1 Gbps). It’s the most widely deployed Ethernet standard in modern networks, offering fast data transfer rates ideal for high-demand applications.

Standard: Defined by IEEE 802.3ab (for copper wiring) and IEEE 802.3z (for fiber optic connections).

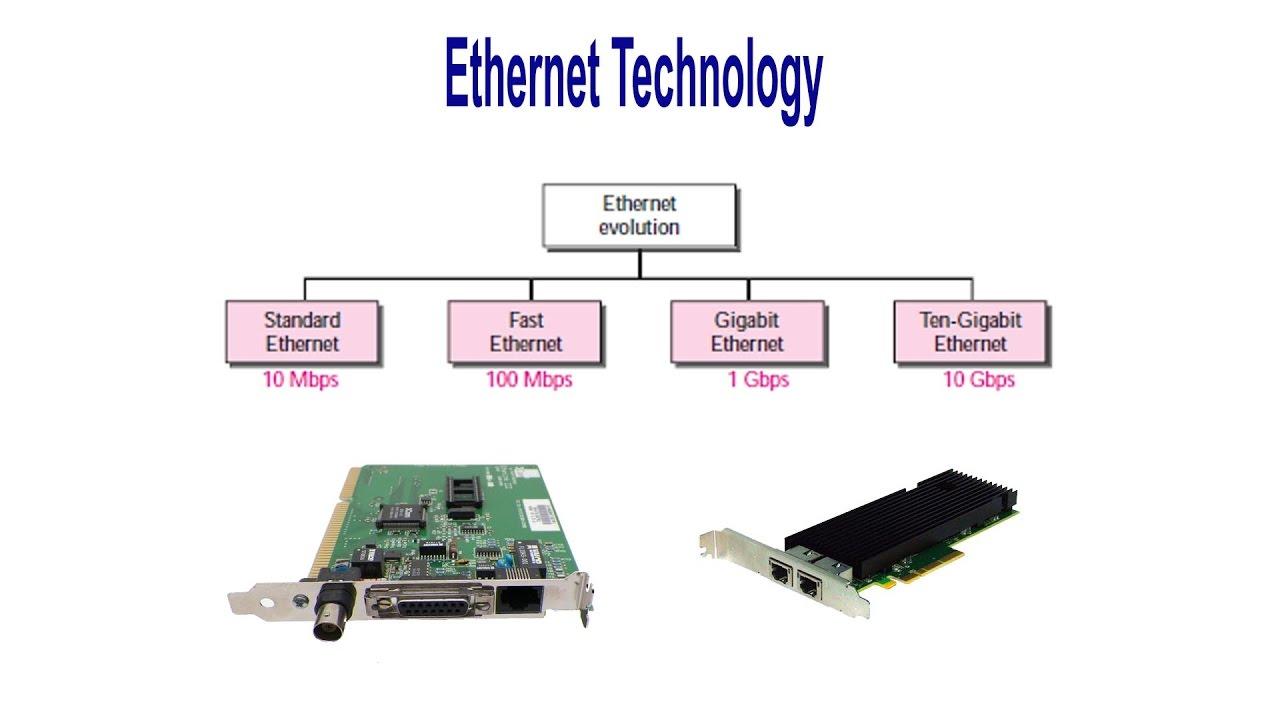
Speed: Gigabit Ethernet operates at 1000 Mbps, which is 10 times faster than Fast Ethernet.

Cable: Gigabit Ethernet typically uses Category 5e (Cat 5e), Category 6 (Cat 6), or fiber-optic cables.

Backwards Compatibility: Gigabit Ethernet is designed to be backward-compatible with lower-speed Ethernet standards like 10/100 Mbps, allowing devices to automatically adjust based on the speed supported.

Gigabit Ethernet Characteristics:

|  |  |
| --- | --- |
| Speed | 1000 Mbps (1 Gbps) |
| Cable | Cat 5e/6 (twisted-pair copper) or fiber optics |
| Range | 100 meters for copper; longer ranges for fiber optics |
| Uses | Common in enterprise networks, high-performance applications and data centers. |



**Practical no 2 & 3: Crimping of Twisted-Pair Cable & Roles of cable in network/internet**

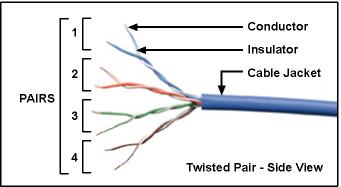
**Aim:**

* **Crimping of Twisted-Pair Cable with RJ45connector for Straight-Through, Cross-Over, Roll-Over.**
* **Understanding their respective roles in network/internet**

1. **Crimping Tool**



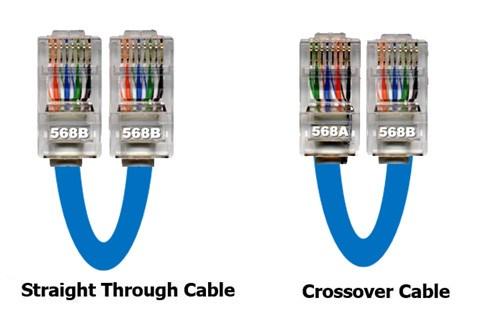
1. **Twisted pair cable**

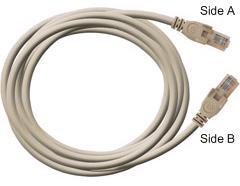


1. **Unshielded and Shielded twisted pair cable**

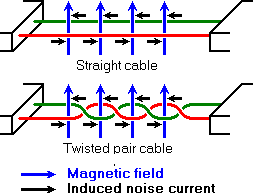


1. **Straight-Through, Cross-Over**

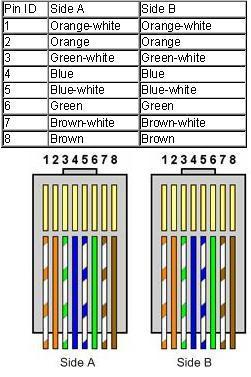
****

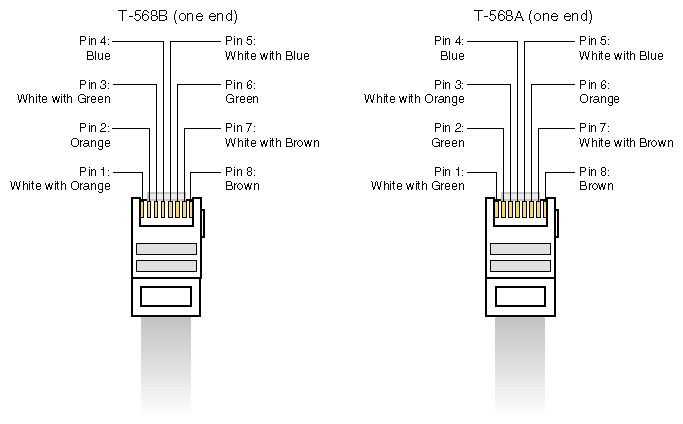


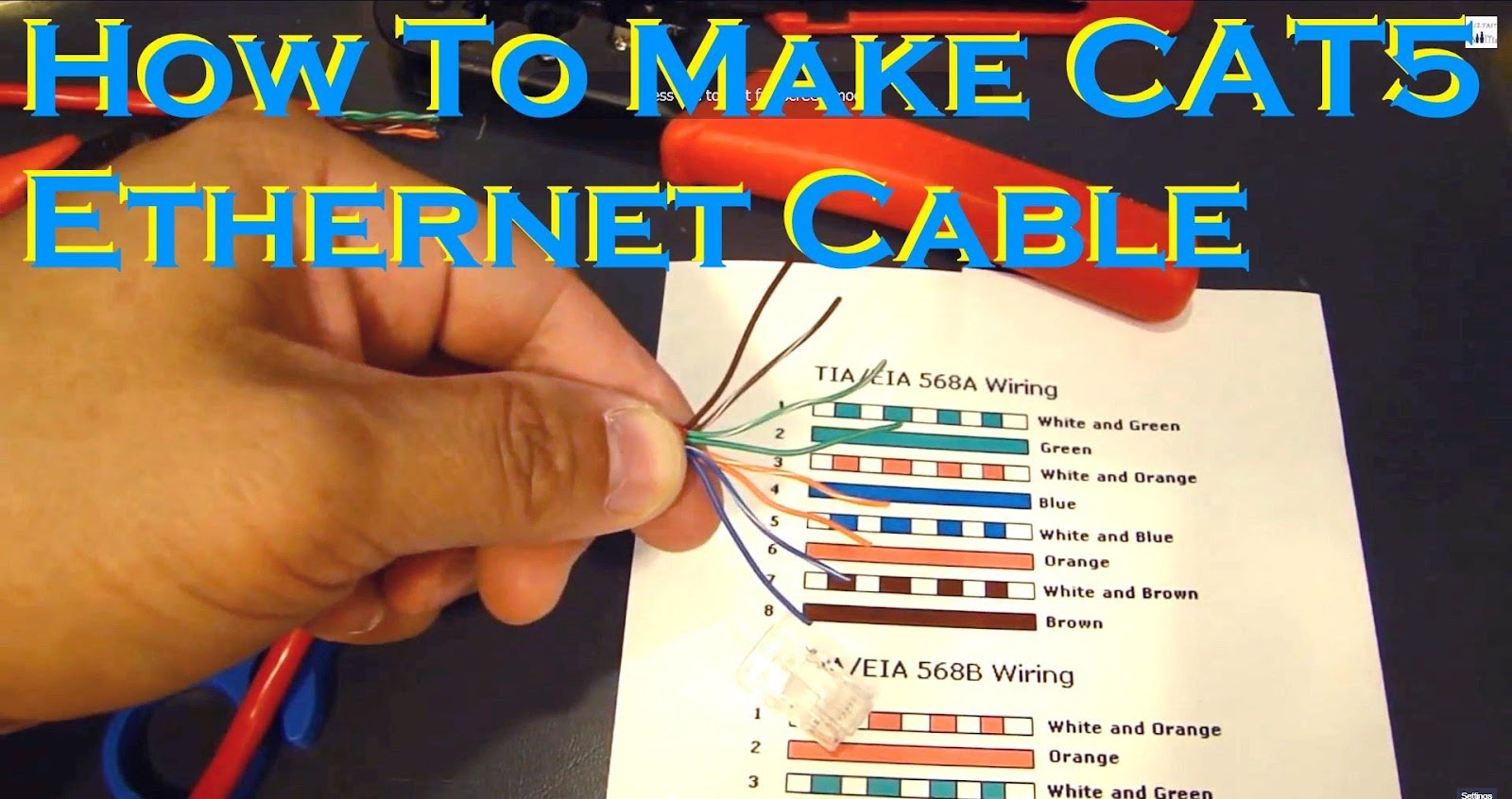
1. **Noise Reduction in twisted-pair cables due to Magnetic Field Cancellation**



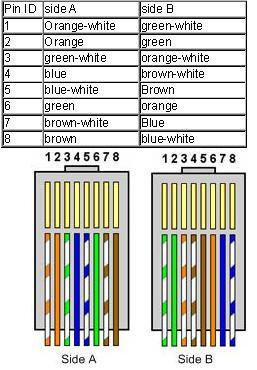
1. **Straight Cable**

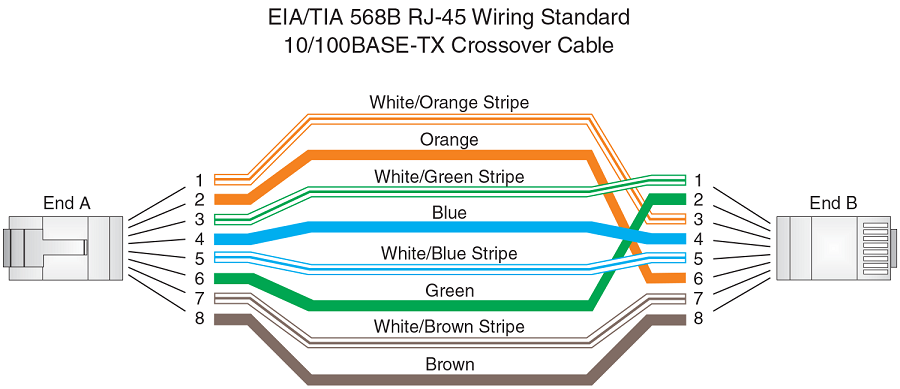






1. **Crossover Cable**





**Practical no 4: Classful Addressing**

**Aim: Problem solving with IPV4, which will include the concept of Classful addressing**

**(Use Cisco Binary Game)**

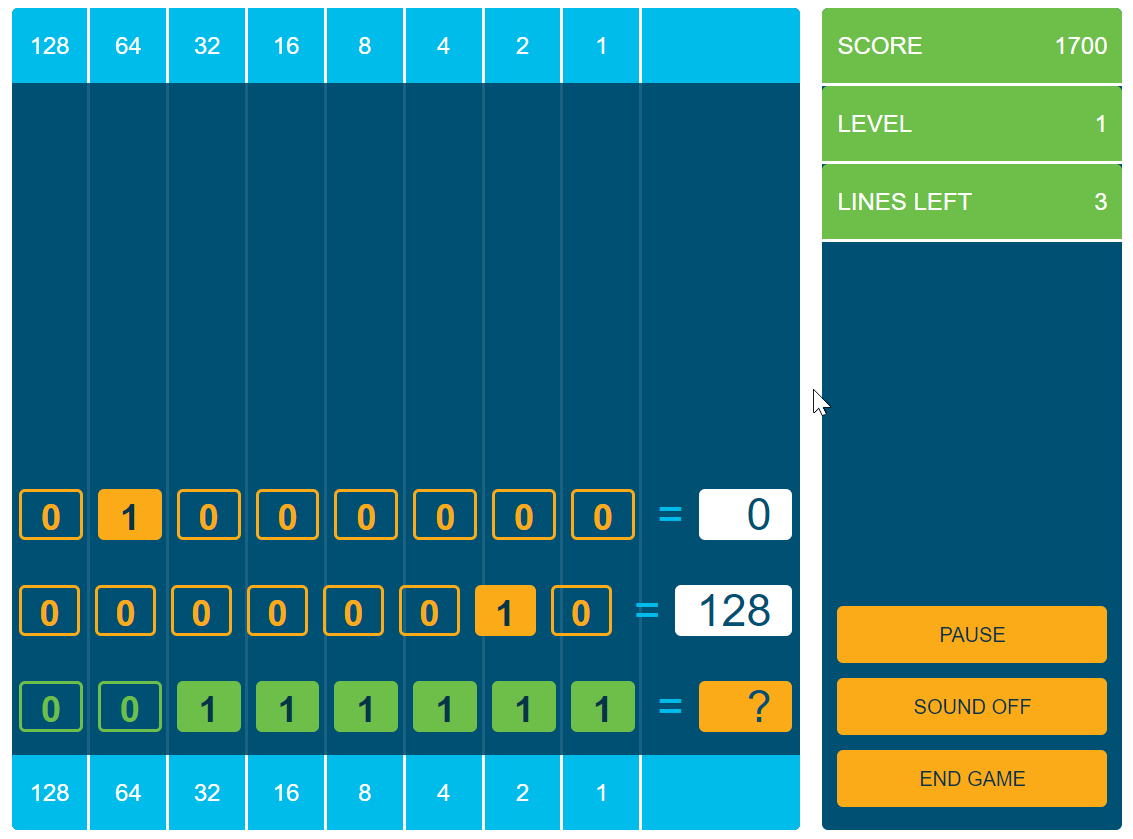
The objective of this practical is to understand and solve problems related to IPv4 addressing, specifically focusing on Classful Addressing. This practical aims to provide hands-on experience with the process of dividing and categorizing IP addresses into different classes (Class A, Class B, Class C, D and E), based on the networking requirements.

**The Cisco Binary Game** is an interactive, educational tool designed to help learners improve their understanding of binary-to-decimal conversion and IP address subnetting - both of which are crucial for networking and IP address management.

*https://learningnetwork.cisco.com/s/binary-game*

Key features:

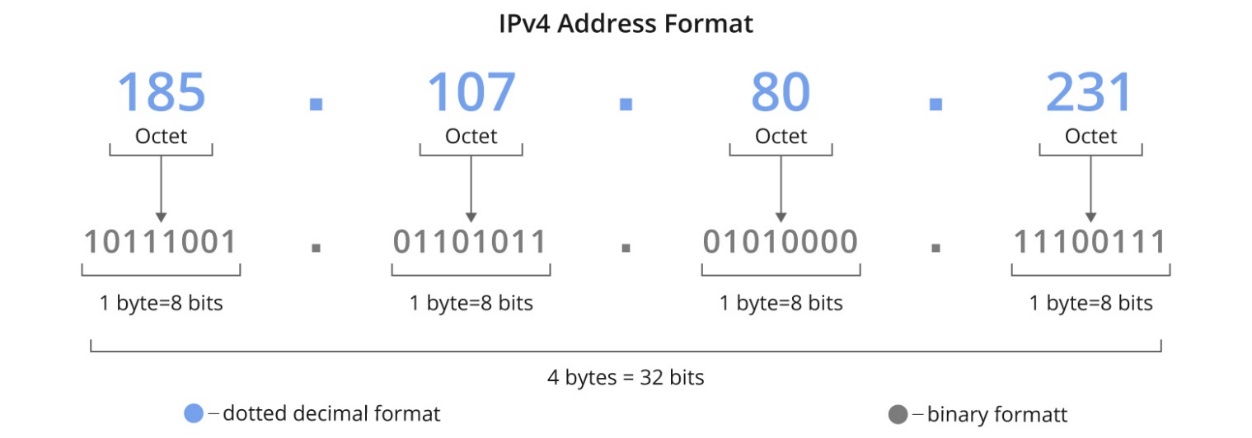
1. Binary-to-Decimal Conversion Practice
2. Interactive Gameplay
3. IP Address and Subnetting Challenges
4. Speed and Accuracy
5. Visual Representation
6. Progress Tracking
7. Fun and Engaging Learning Tool



**Classful addressing**

Classful addressing is an early method used to divide the IPv4 address space into fixed-sized address classes.

* It was designed to simplify IP address allocation based on the size of the network.
* An IP address is a 32-bit address that identifies a connection to the Internet.
* The IP address is made up of four parts, each of which is eight bits long (1 byte).
* The IP addresses are universally unique.
* The address space of IPv4 is 2^32 or 4,294,967,296.
* An IP address can be either in binary, decimal or hexadecimal notation and not a mixture of all.



It divided addresses into fixed classes (A, B, C, D, E) based on the first bits of the address.

Further, the 4 parts of the IP address is divided into parts: a network ID and a Host ID.

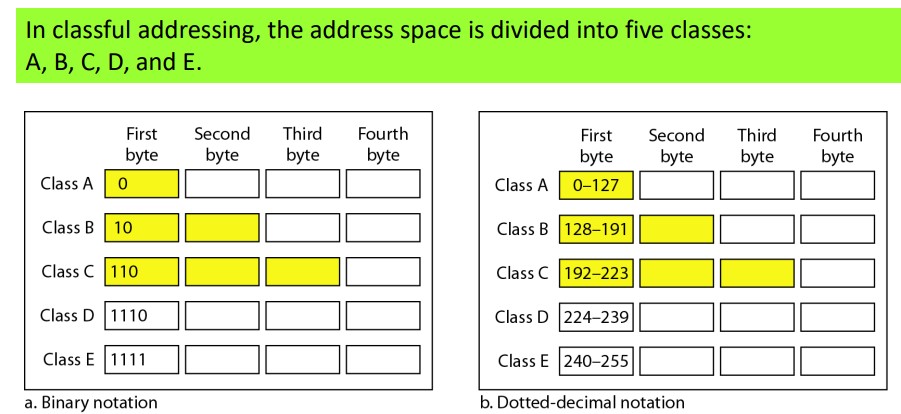
Class A: Large networks (like big organizations)

Class B: Medium-sized networks

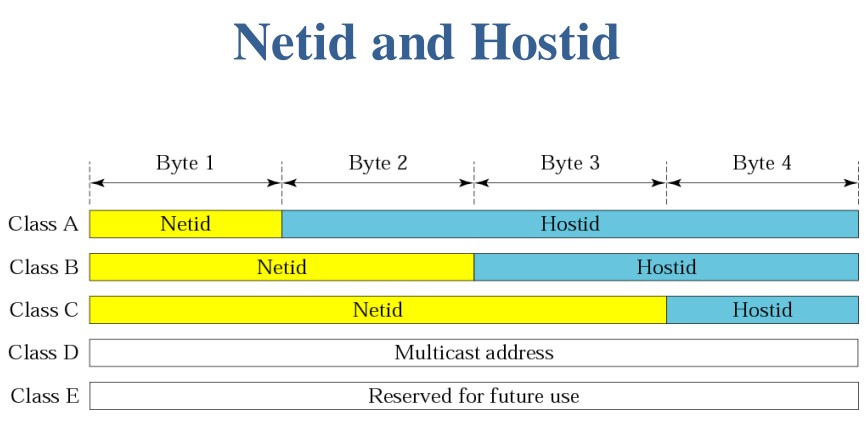
Class C: Small networks

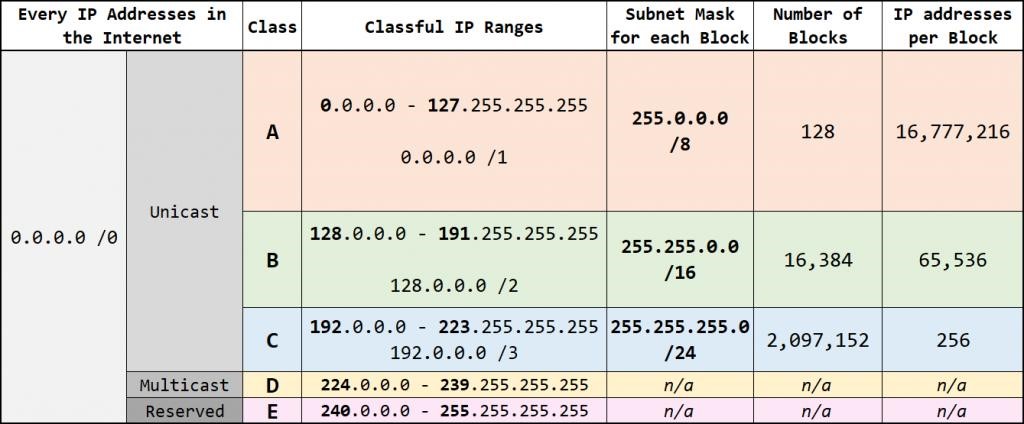
Class D: Reserved for multicast

Class E: Reserved for future or experimental use



Two addresses in each network are reserved: Network address (all host bits zero) and Broadcast address (all host bits one)





**Step 1: Setup Basic Network Topology**

Create a simple network with: 2 PCs (PC1 and PC2), 1 Switch.

Connect: PC1 to Switch (FastEthernet0/1) & PC2 to Switch (FastEthernet0/2)

**Step 2: Understand Classful IP Addressing**

**Step 3: Assign IP Addresses to PCs (Classful)**

On PC1:IP Address: 192.168.1.10 (Class C)

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1 (optional)

On PC2:IP Address: 192.168.1.20 (Class C)

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

**Step 4: Verify Connectivity with Correct Classful IPs**

On PC1, open the Command Prompt.

Type ping 192.168.1.20 and press Enter.

You should get successful replies showing connectivity.

**Step 5: Problem Scenario — Incorrect IP Class Assignment**

Change PC2’s IP address to 192.168.2.20 with subnet mask 255.255.255.0.

**Step 6: Test Connectivity Again**

On PC1, open Command Prompt.

Type ping 192.168.2.20.

The ping will fail because the two IPs are on different networks based on classful addressing.

**Step 7: Explanation & Troubleshooting**

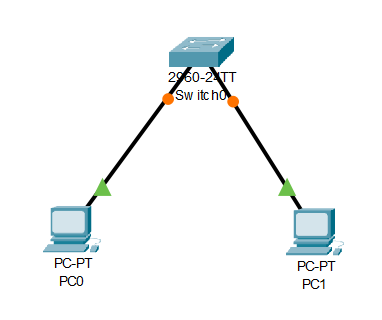
PC1's IP 192.168.1.10 is on network 192.168.1.0/24.

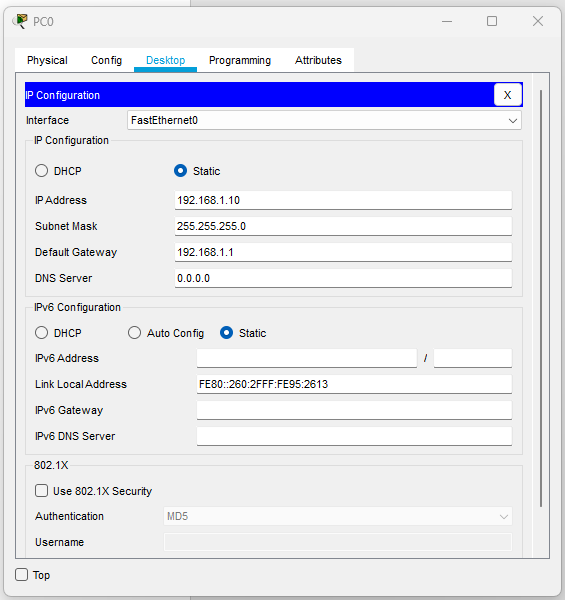
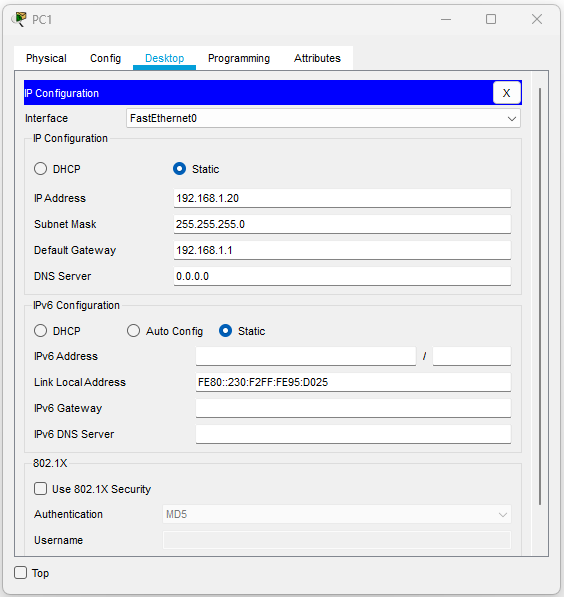
PC2's IP 192.168.2.20 is on network 192.168.2.0/24.

Because no router or Layer 3 device connects these two networks, they can't communicate.

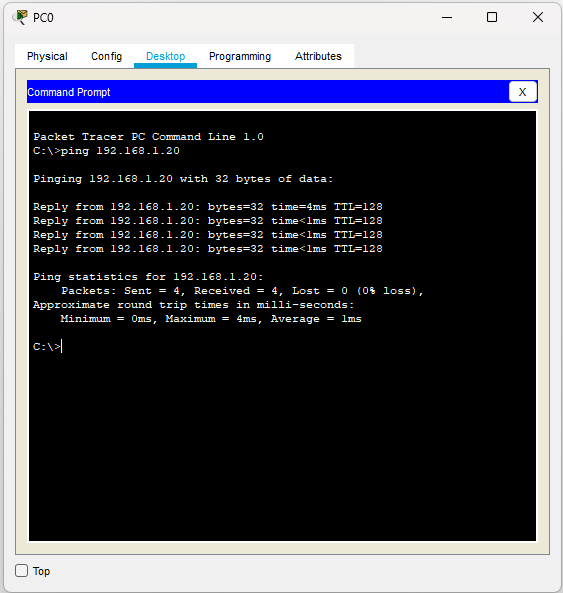
***According to classful addressing, networks with different third octets are separate Class C networks.***

**Step 1: Setup Basic Network Topology**

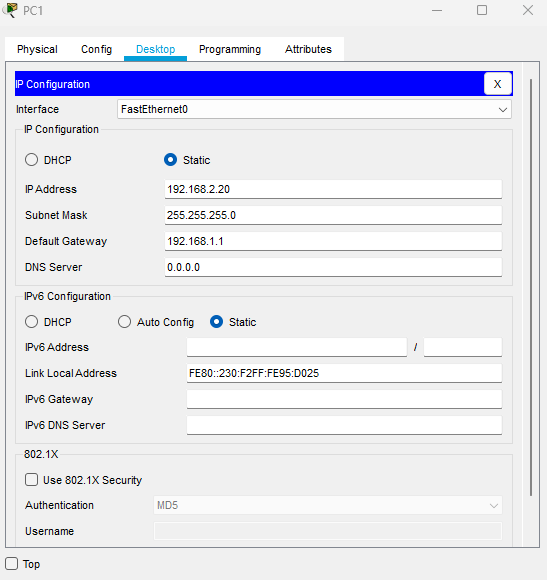


**Step 3: Assign IP Addresses to PCs (Classful)**

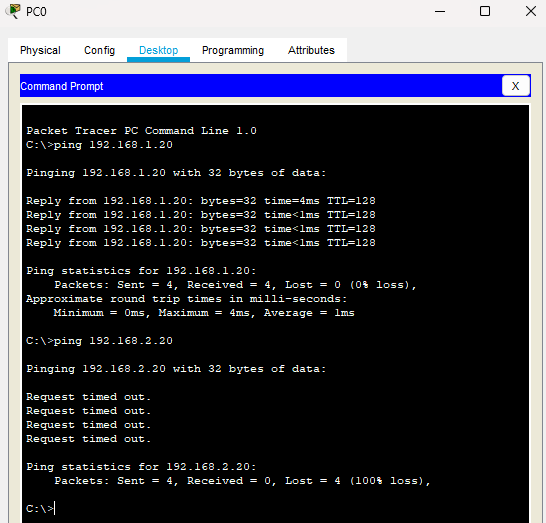
**Step 4: Verify Connectivity with Correct Classful IPs**



**Step 5: Problem Scenario — Incorrect IP Class Assignment**



**Step 6: Test Connectivity Again**



**Practical no 5: Networking commands**

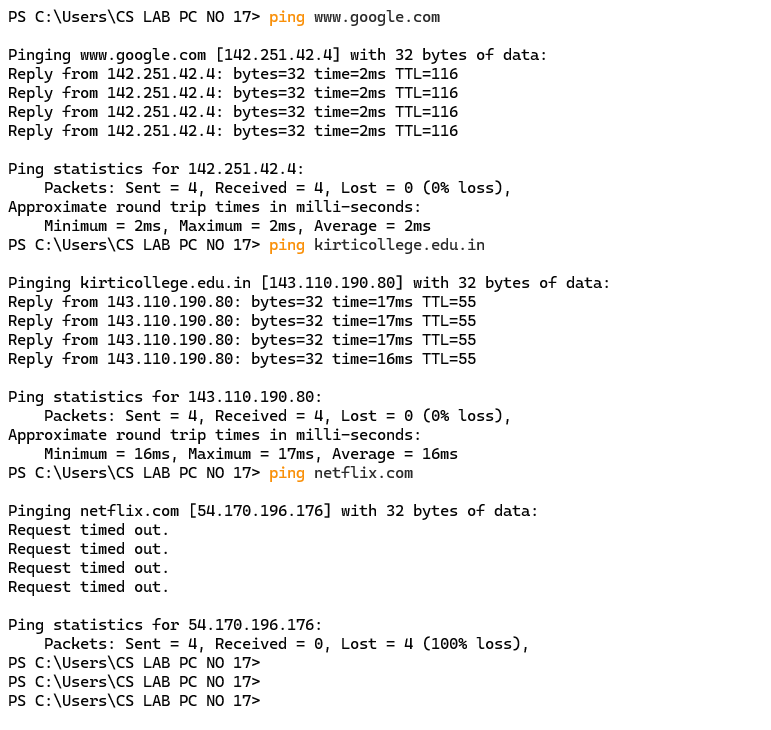
**Aim: Using Windows-cmd, execute following networking commands and note the output:ping, tracert, netstat, arp, ipconfig**

The objectives of using windows-based cmd commands:

1. To learn how to verify network connectivity using ping.
2. To trace the path packets take to a destination using tracert.
3. To identify active network connections and listening ports using netstat.
4. To view the IP-to-MAC address mappings in the ARP cache using arp.
5. To display current IP address, subnet mask, default gateway, and other network configuration details using ipconfig.

|  |  |  |  |
| --- | --- | --- | --- |
| **Command** | **Purpose** | **Syntax** | **Example** |
| ping | Test connectivity to an IP or hostname | ping <IP/hostname> | ping 8.8.8.8 |
| hostname | Show current device’s hostname | hostname | hostname |
| getmac | Display MAC addresses of local network adapters | getmac | getmac |
| SystemInfo | Show detailed system info (Windows only) | systeminfo | systeminfo |
| ipconfig | Show IP config of network interfaces (Windows) | ipconfig | ipconfig |
| ipconfig /all | Show detailed IP config including DNS, MAC | ipconfig /all | ipconfig /all |
| nslookup | Query DNS to resolve hostname/IP | nslookup <hostname/IP> | nslookup www.google.com |
| tracert | Show route path packets take | tracert <hostname/IP> | tracert google.com |
| netstat | Show active network connections and ports | netstat [options] | netstat -an |
| arp | Show IP-to-MAC mappings  (ARP table) | arp -a | arp -a |

1) Ping



2)hostname



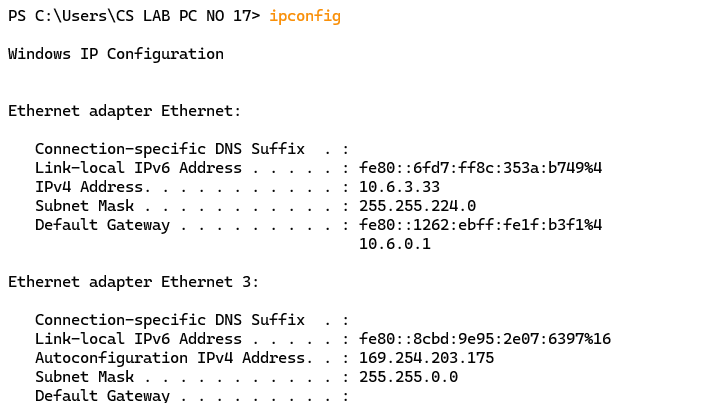
3)getmac



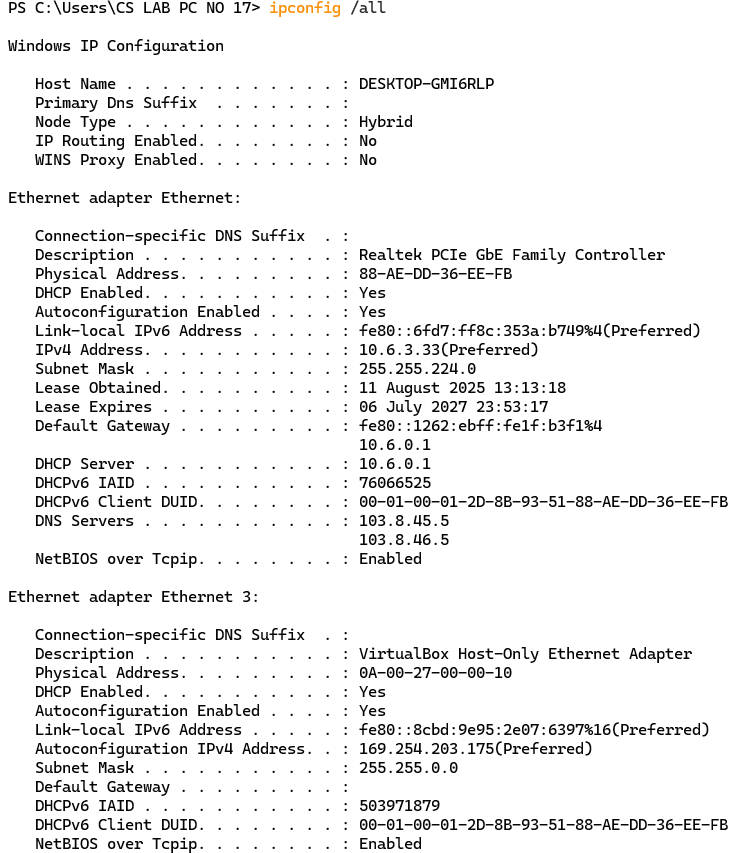
4)SystemInfo



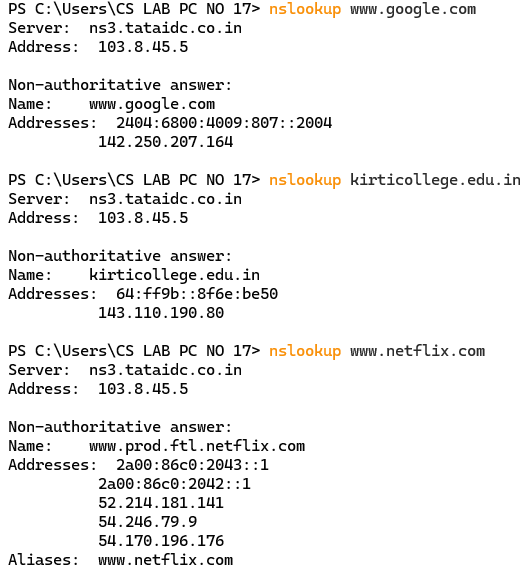
5)ipconfig



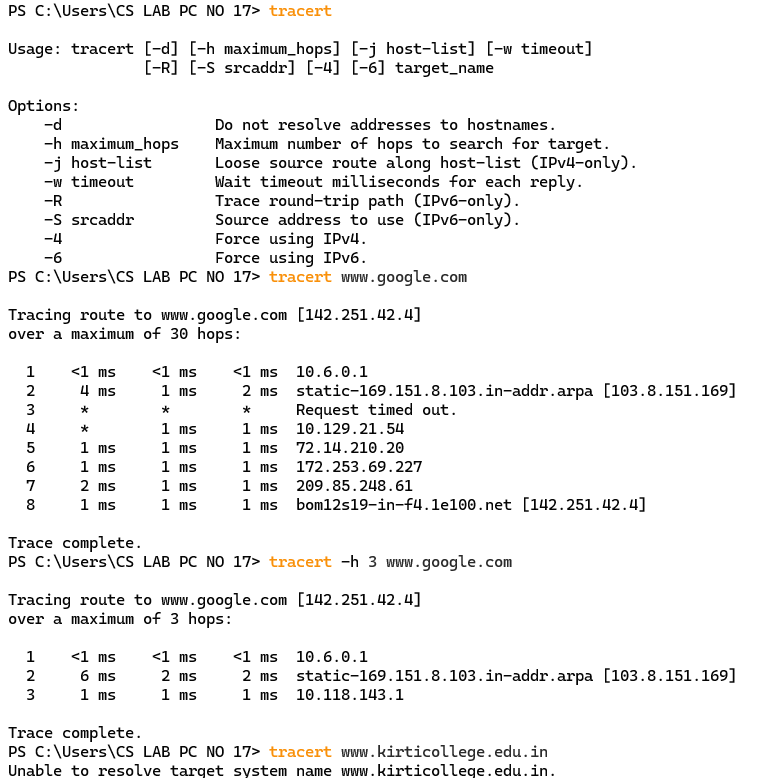
6)ipconfig /all



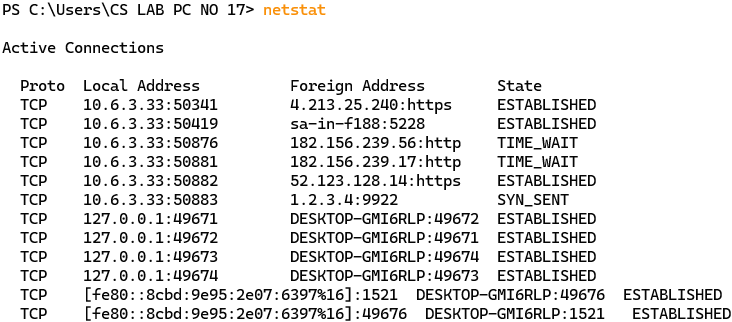
7) nslookup

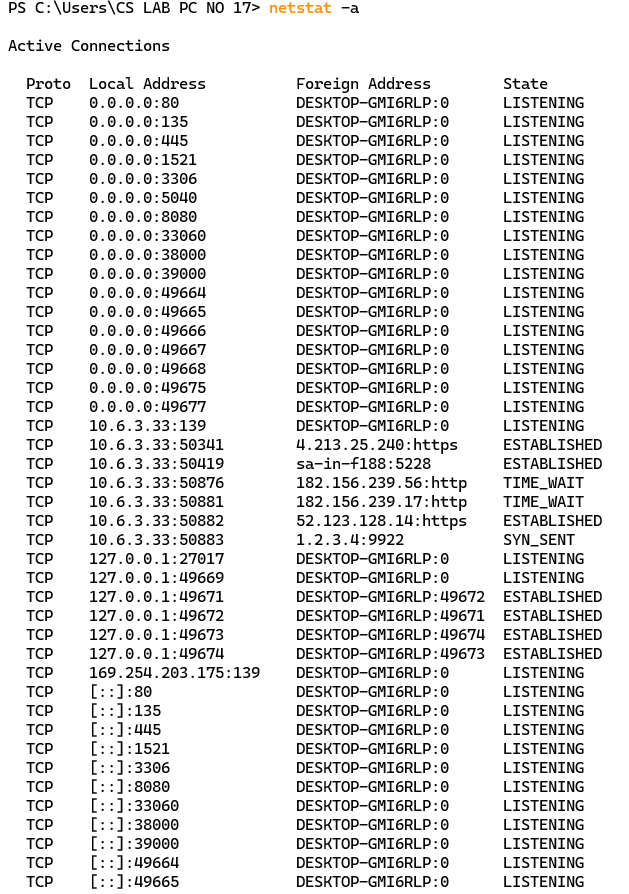


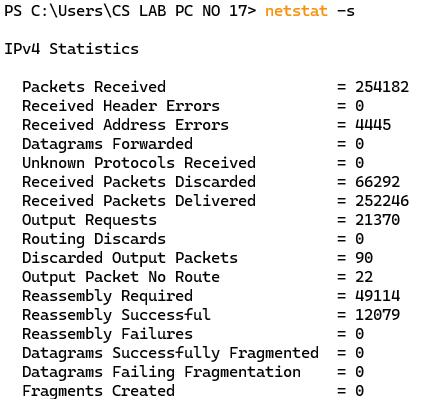
8)tracert



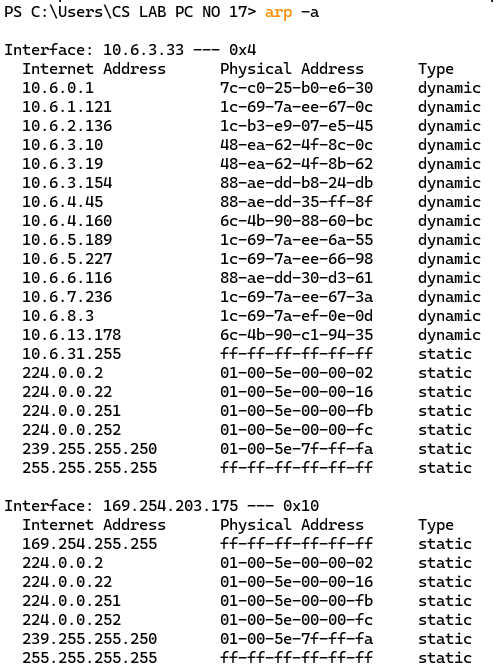
9)netstat







10)arp



**Practical no 6: Network of two computers**

**Aim: Create a basic network of two computers using appropriate network wire.**

The objective of this practical is to establish a basic network between two computers (PC0 and PC1), configure IP addresses and test communication between the devices using a ping command. The steps also include simulating the packet transfer between the two devices to visualize how data flows in a network.

**Step 1: Device Setup**

Place two computers (PC0 and PC1) in the workspace of network simulator

These devices will represent the two PCs that will communicate with each other.

**Step 2: Connection Between Devices**

Choose a Copper Cross-Over Cable from the available cables in network simulation software.

connect the FastEthernet0 port of PC0 to the FastEthernet0 port of PC1.

A cross-over cable is required because both devices (PCs) are being connected directly without a switch or hub.

**Step 3: Configuring IP Addresses**

Assigning IP Address to PC0:

Click on PC0, go to the Desktop menu and select IP Configuration.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Assigning IP Address to PC1:

Click on PC1, go to the Desktop menu and select IP Configuration.

Assign the following IP address to PC1:

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

**Step 4: Testing Communication**

Ping from PC0 to PC1:

On PC0, open the Command Prompt from the Desktop menu.

Type the following command and press Enter:

ping 192.168.1.2

This command sends an ICMP (Internet Control Message Protocol) request from PC0 to PC1 to check if communication between the two devices is possible.

If the ping is successful, you will see a reply indicating that PC0 can communicate with PC1.

Ping from PC1 to PC0:

On PC1, open the Command Prompt from the Desktop menu.

Type the following command and press Enter:

ping 192.168.1.1

This command sends an ICMP request from PC1 to PC0 to check communication in the reverse direction.

If the ping is successful, it confirms that PC1 can communicate with PC0 as well.

**Step 5: Simulating Packet Transfer**

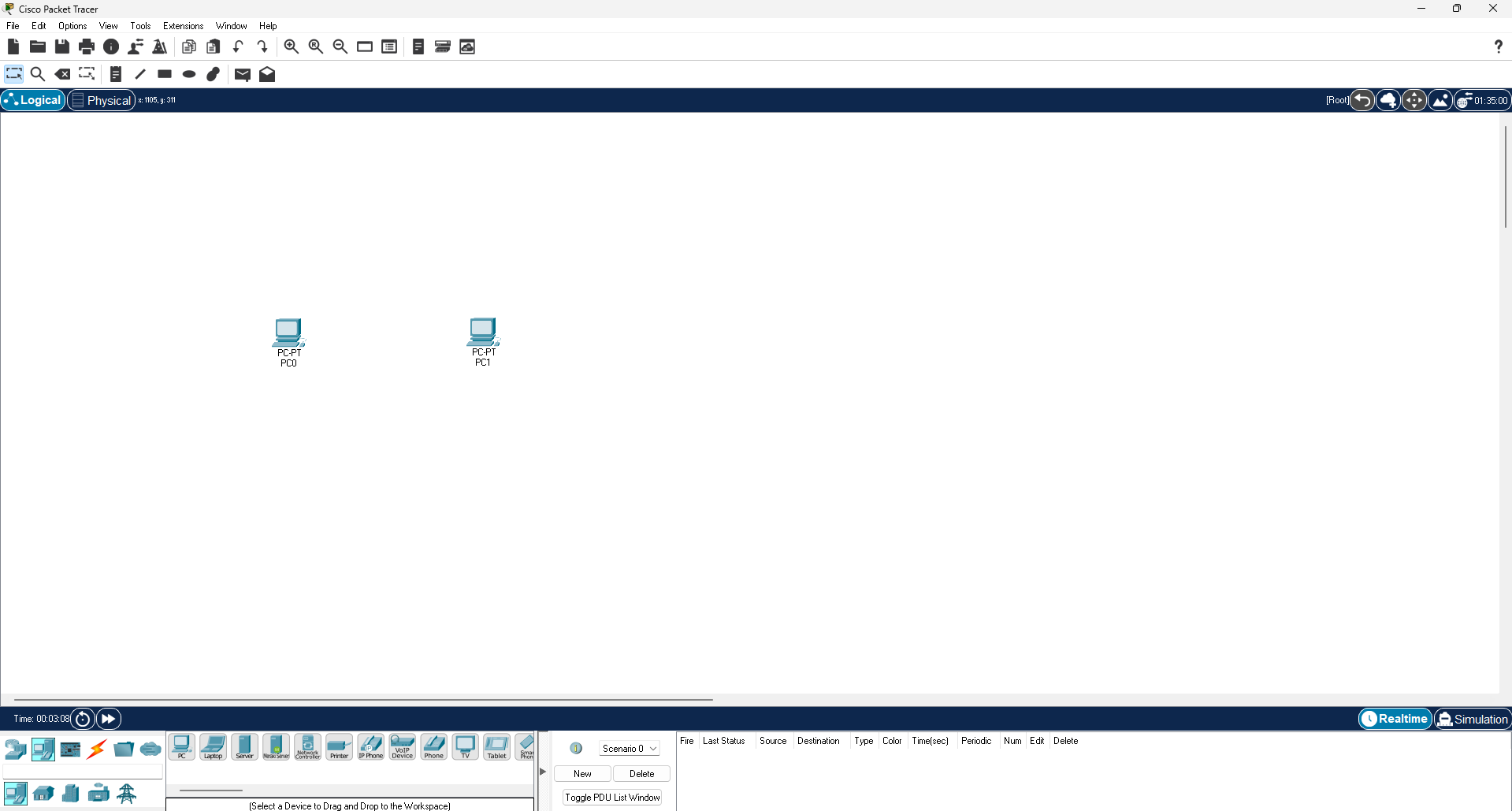
switch to Simulation Mode.

Initiate the ping from PC1 to PC0 again.

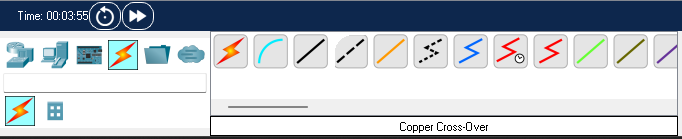
Watch the packet travel from PC1 to PC0 and observe how the data moves step-by-step between the devices.

This simulation allows you to visualize the packet’s journey, showing how the network protocol handles the data transfer.

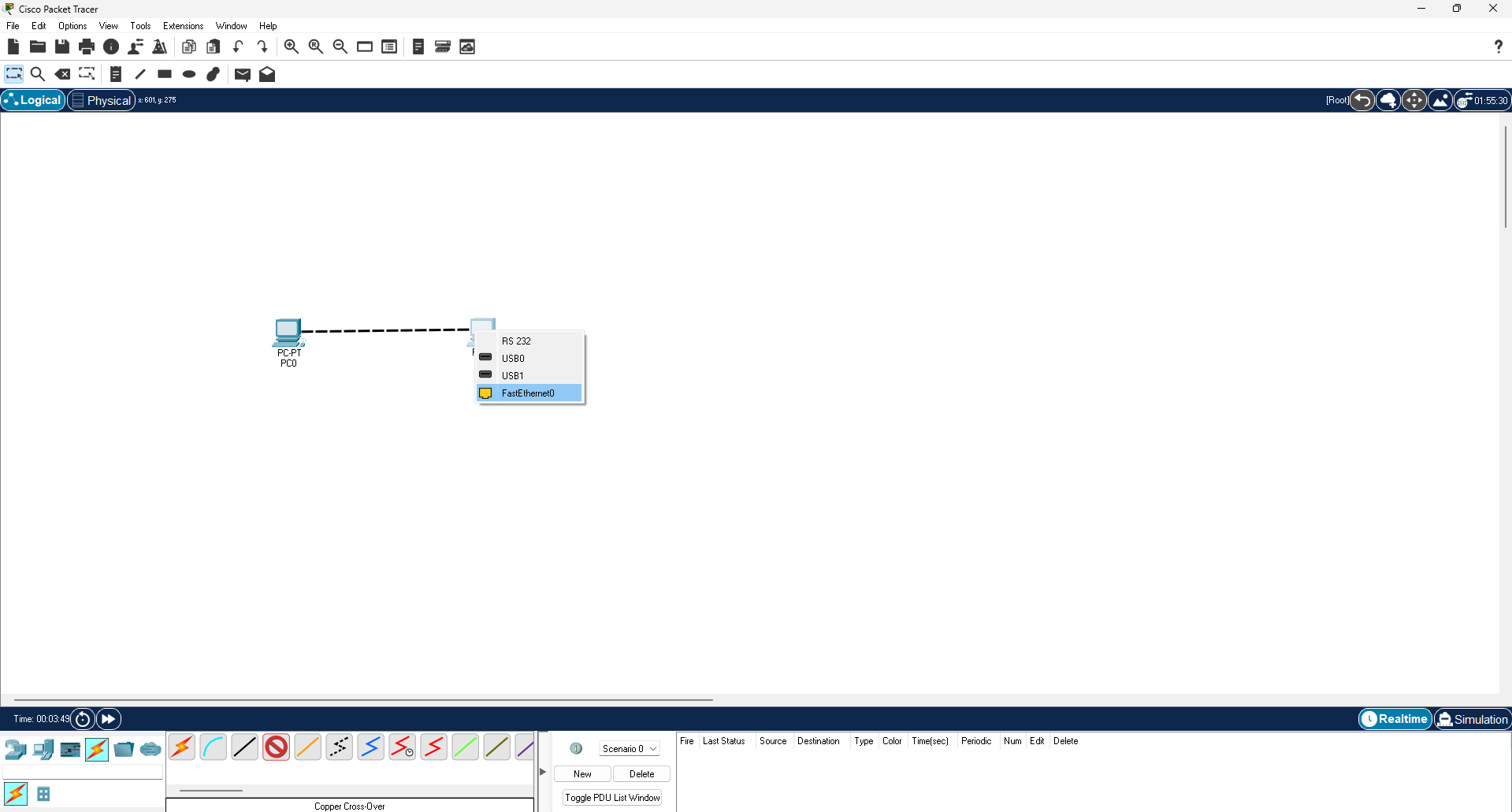
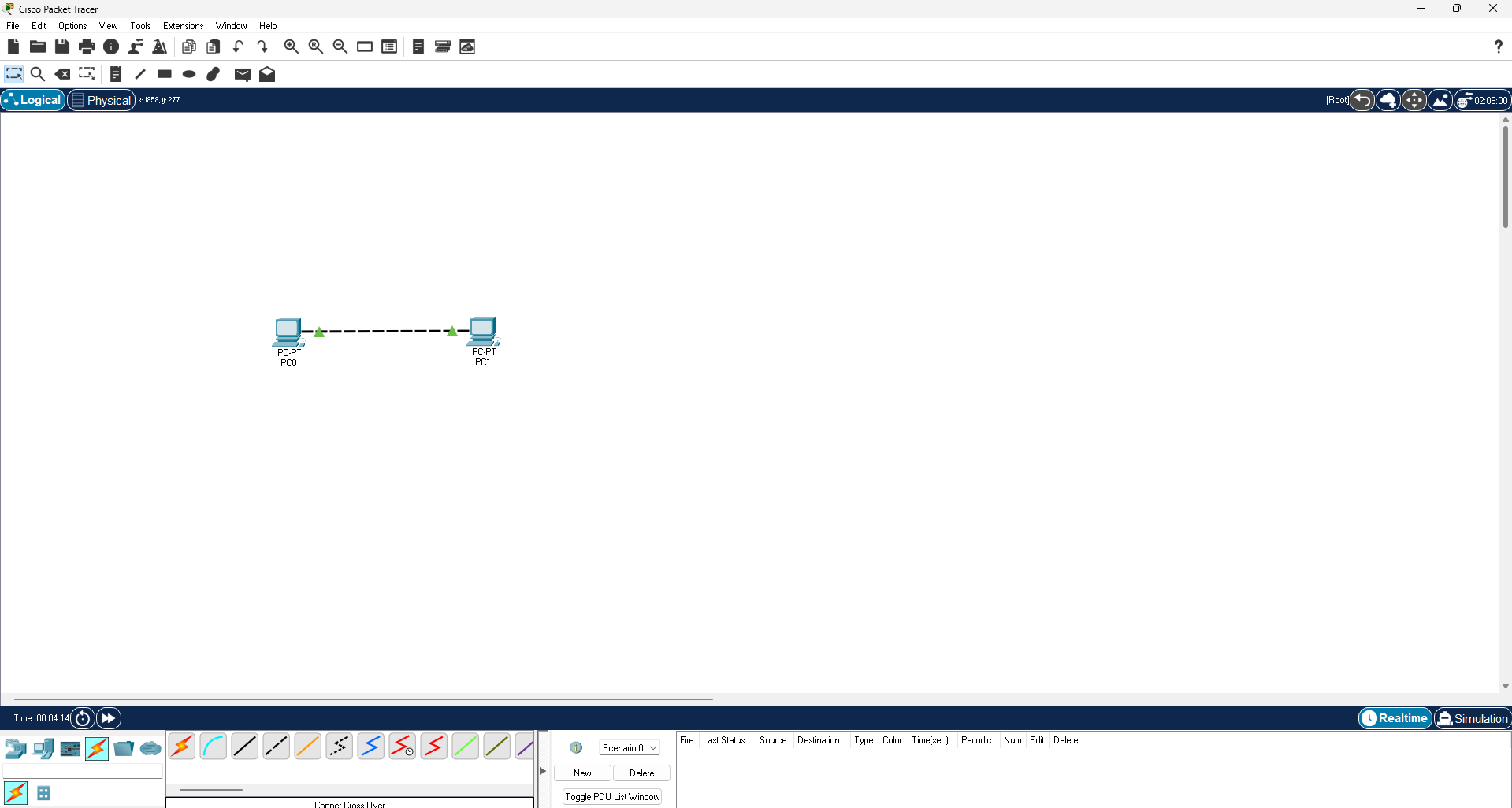
**STEP 1 : Taking PC0 And PC1 to connect.**



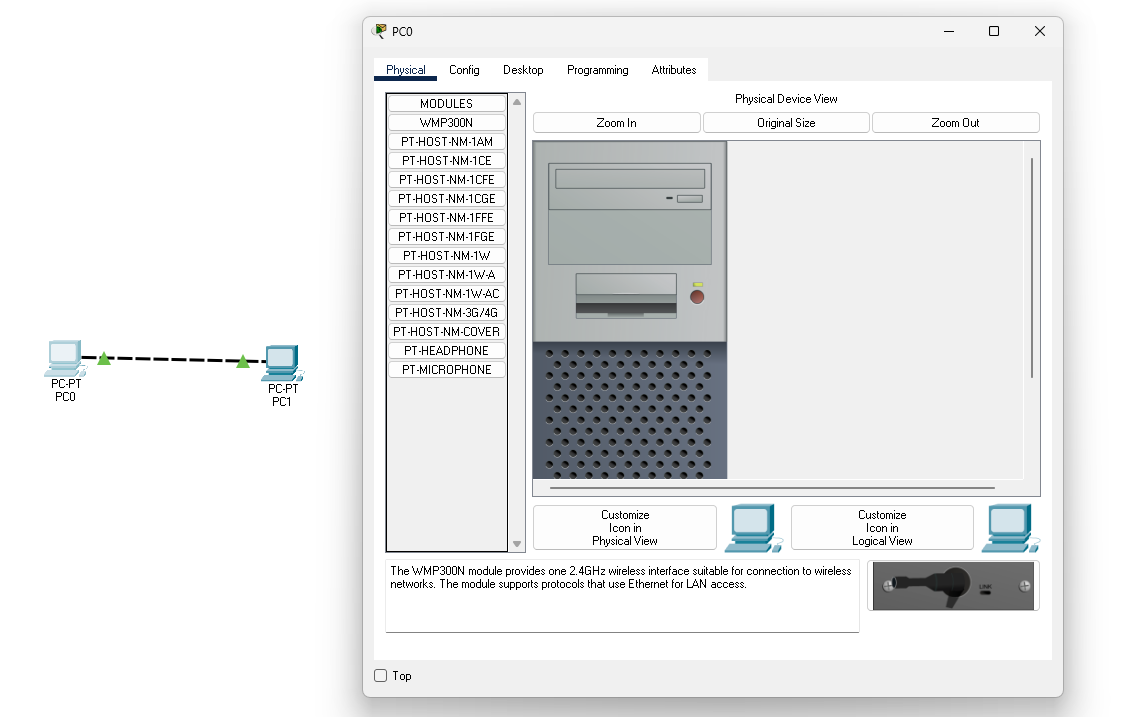
**Step 2 : Take Copper cross-over wire.**



**Connecting PC0 And PC1 with the wire on FastEthernet0 connection.**

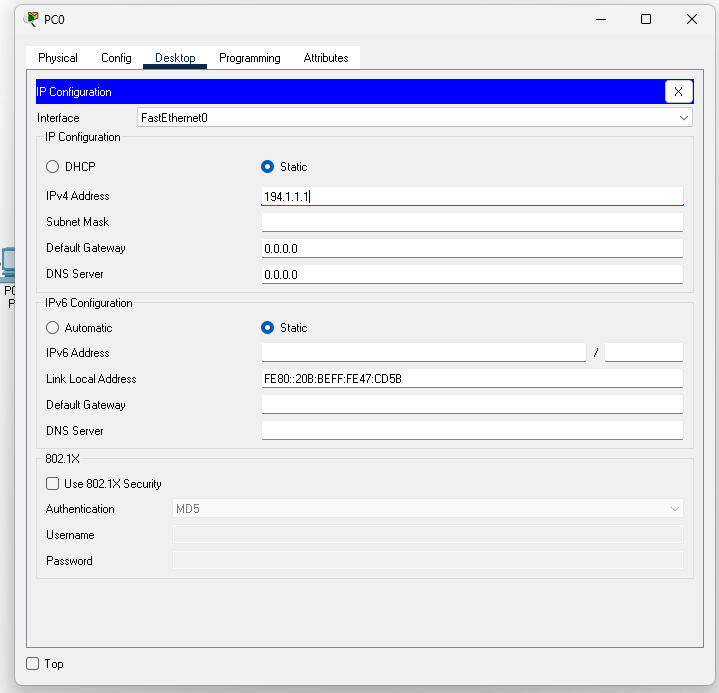
 

**Step 3 : Click on the device to set up the IP address from the Desktop menu.**

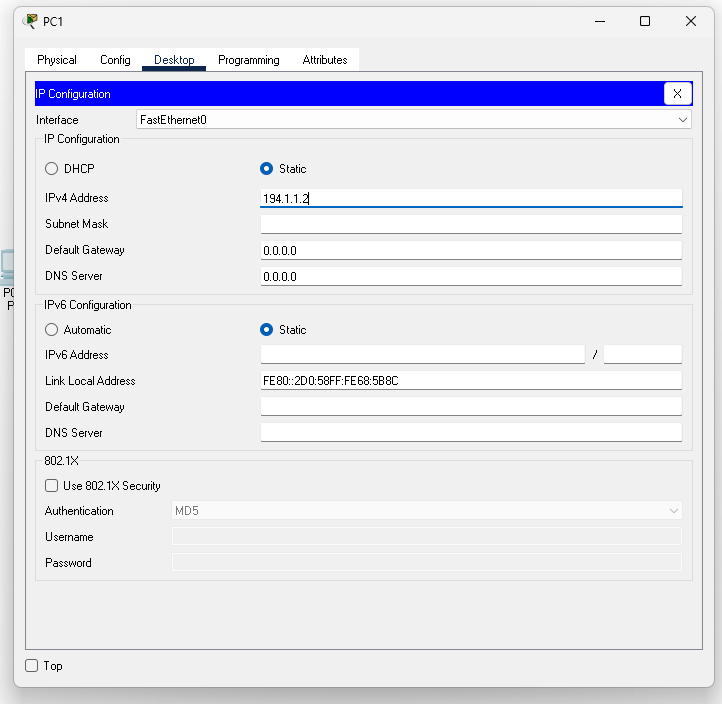


**Step 4 : Assigning the IP Address to both the devices.**

**PC0:**



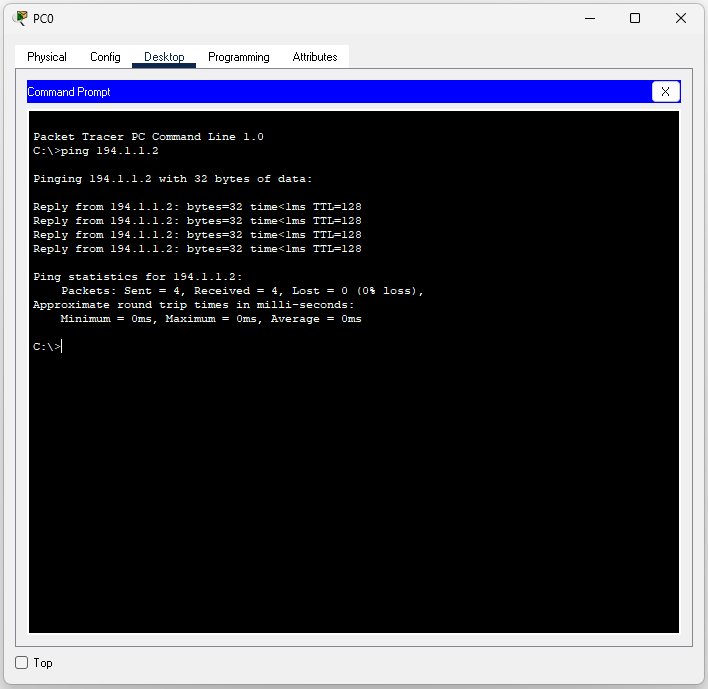
**PC1:**



**Step 5: Establishing communication between devices.**

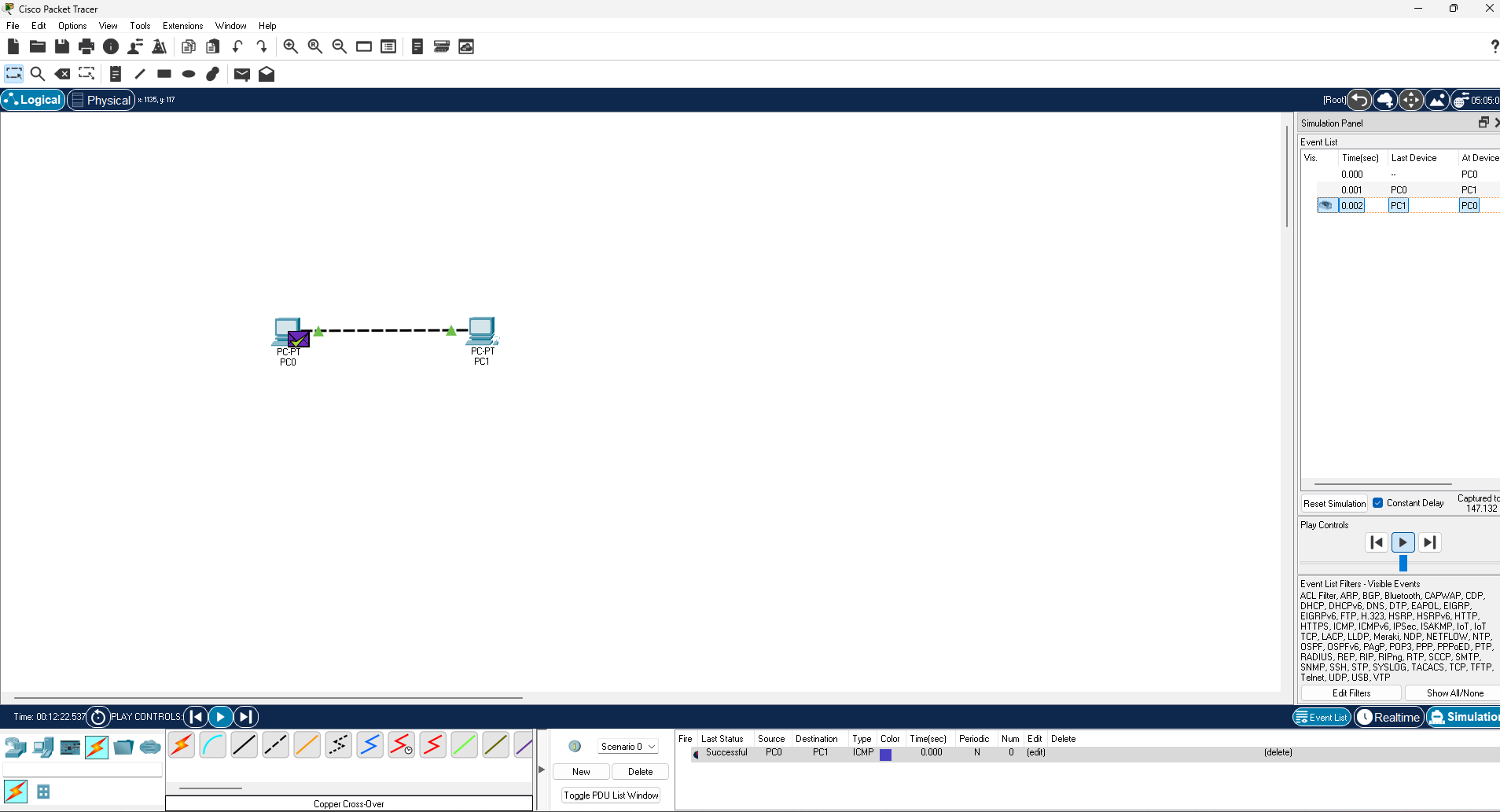
**1.PC0 To PC1**

**Step 1 : Ping PC0 to PC1**

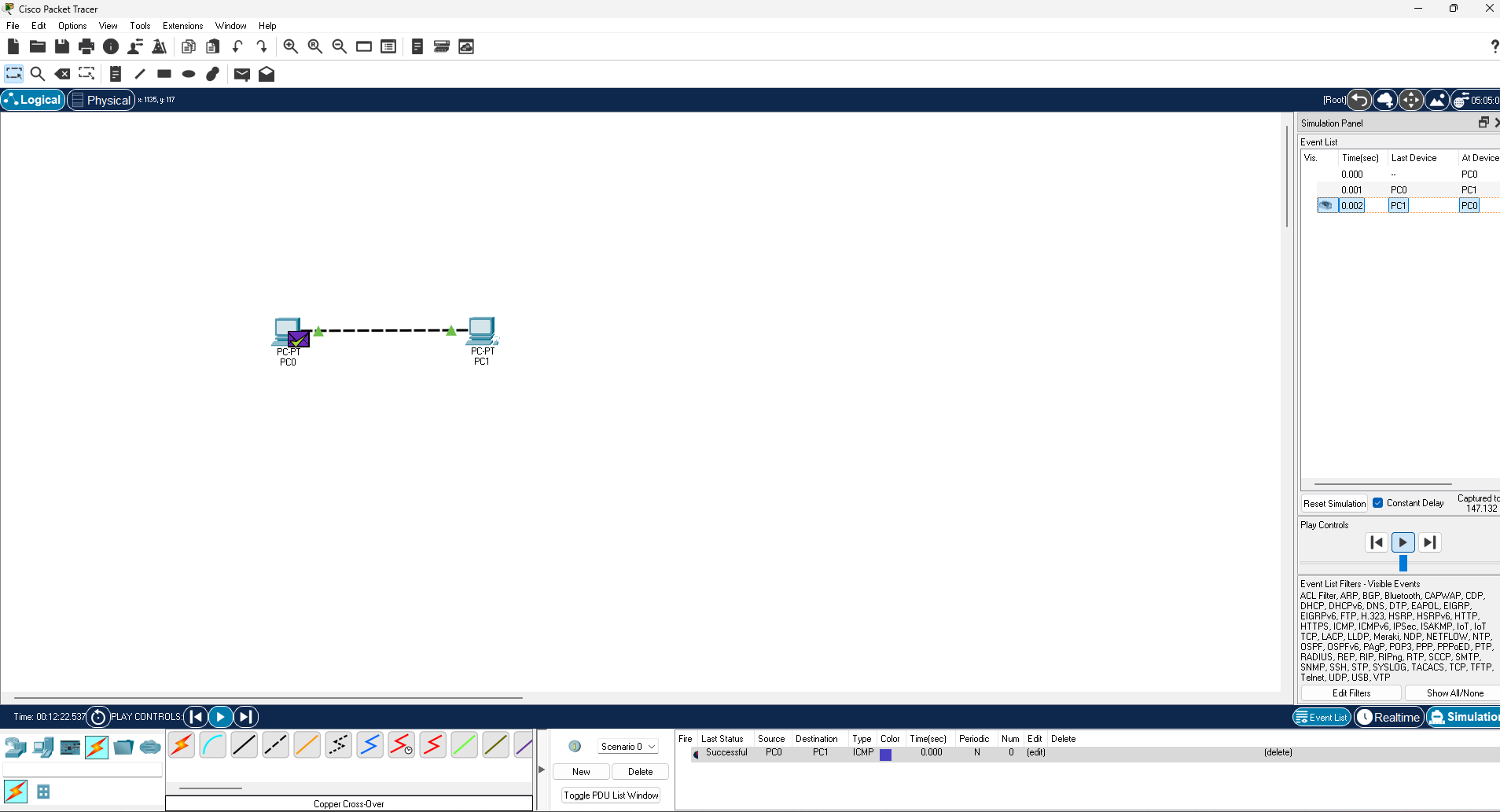


**Step 2: Packet Passing (PC0 to PC1)**



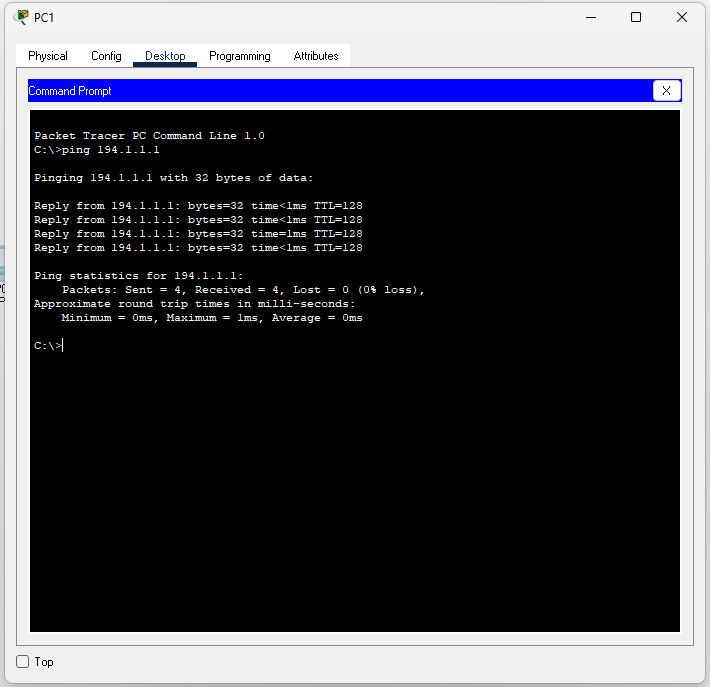


**Step 3: Simulation (PC0 to PC1)**

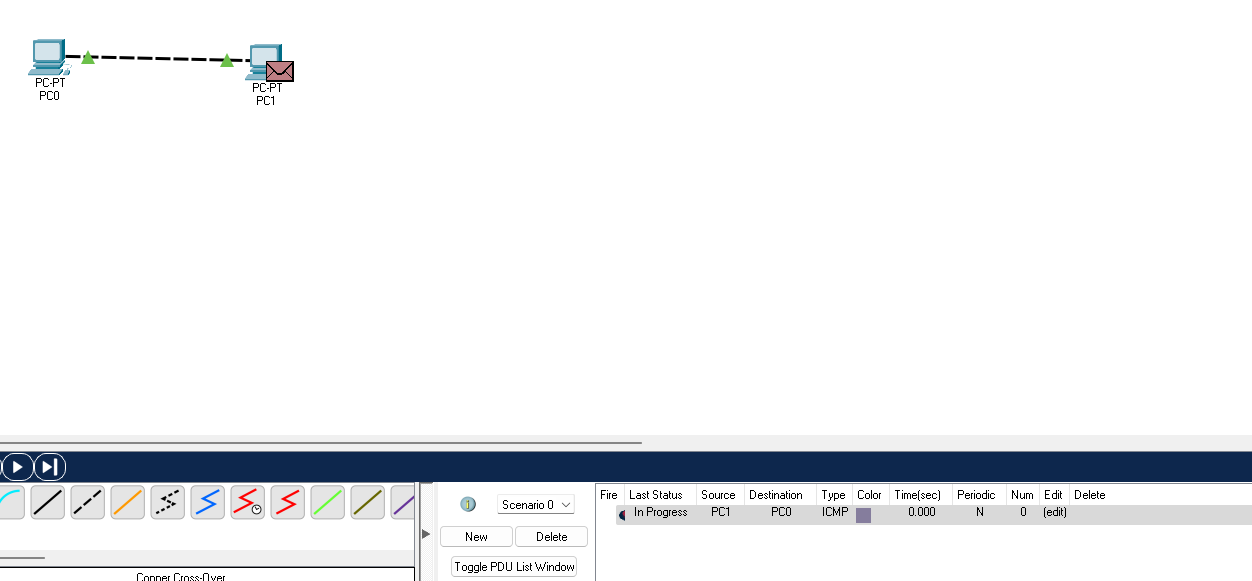


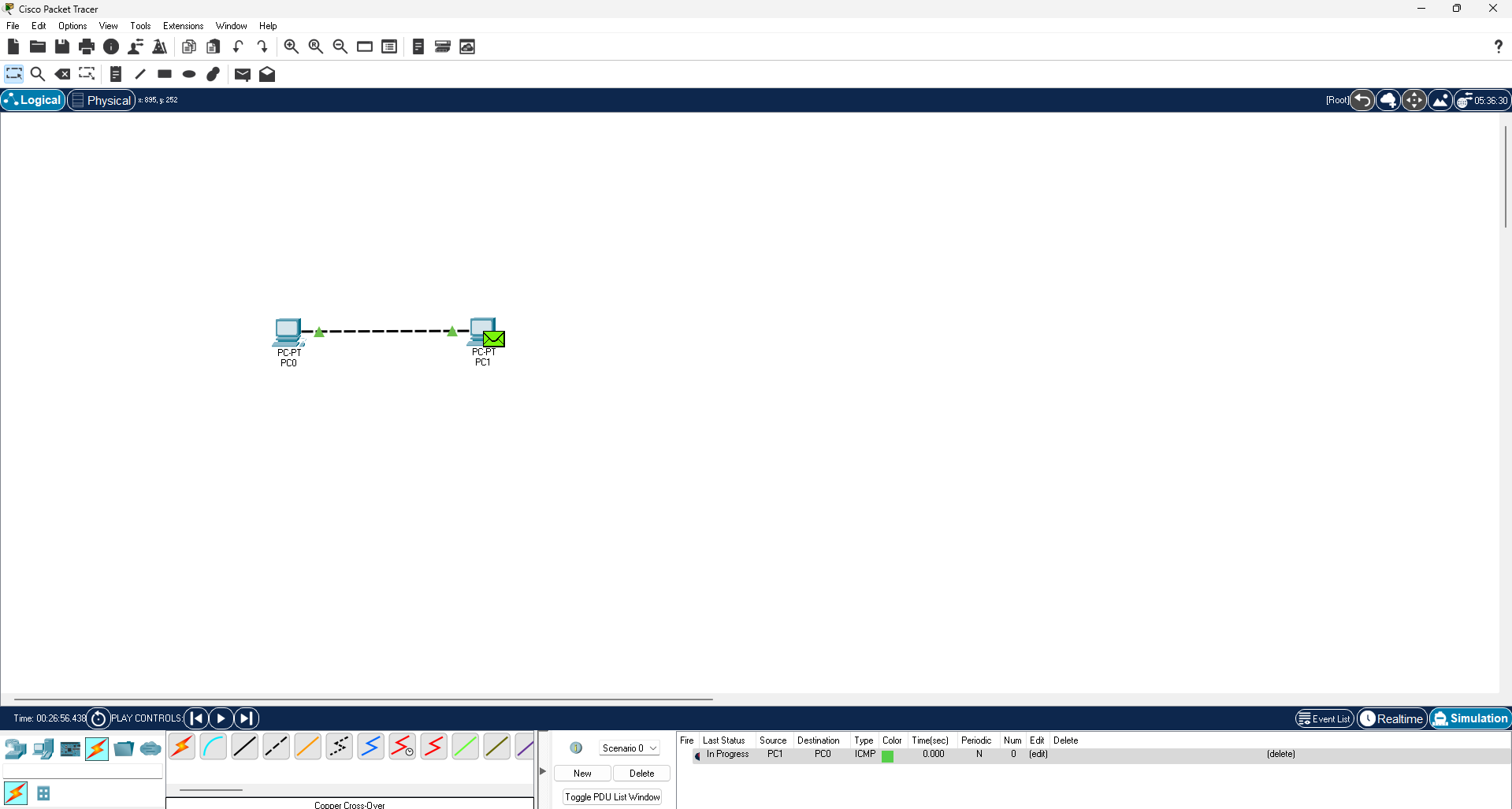
**2. PC1 To PC0**

**Step 1 : Ping PC1 to PC0**

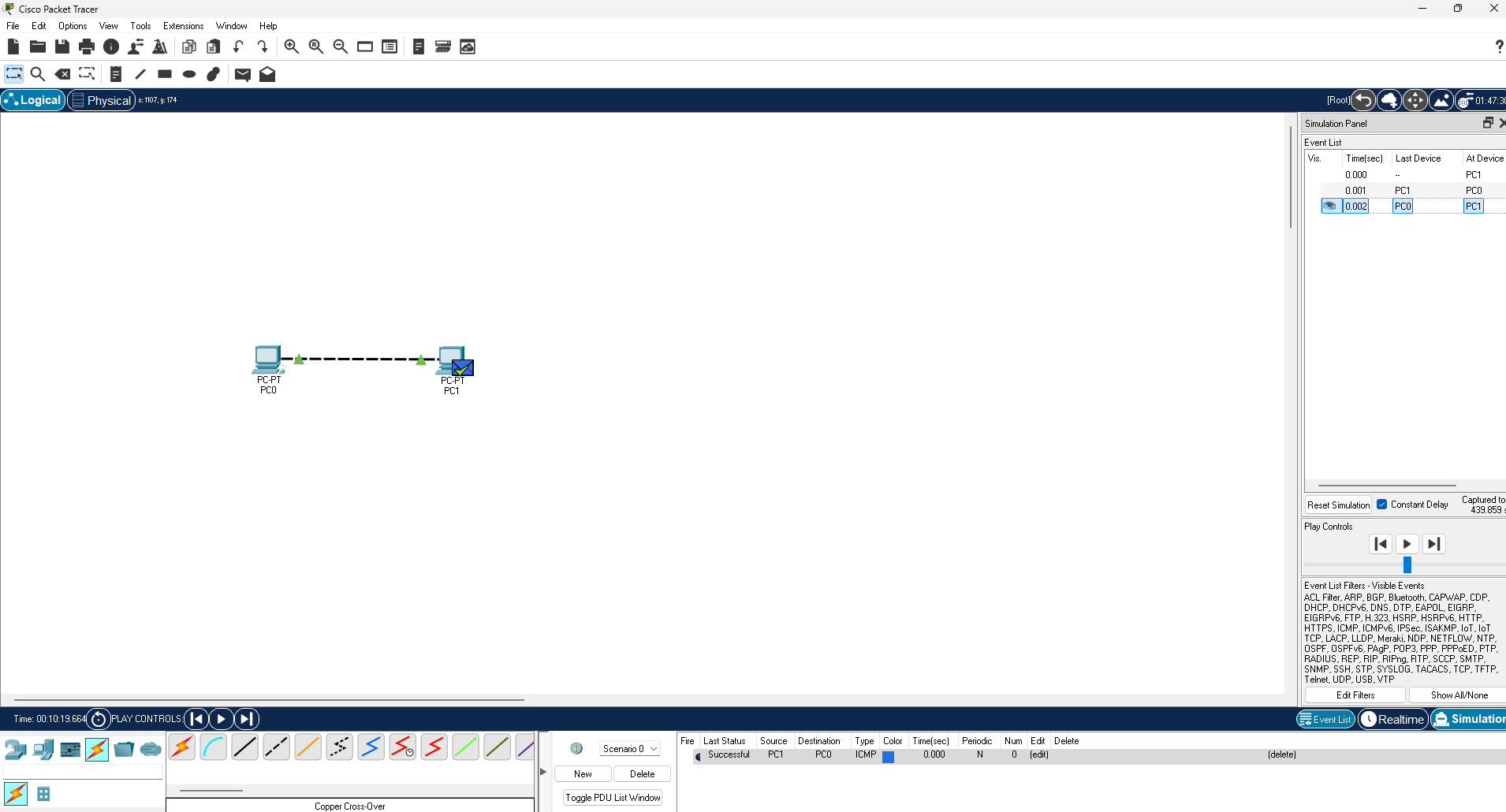


**Step 2 : Packet Passing (PC1 to PC0)**





**Step 3 :**  **Simulation (PC1 to PC0)**



**Practical no 7: Connection of min(six) devices using layer 2 switch**

**Aim: Create a network of 2 PC’s, 2 Laptops, A server and A Printer with the help of a layer 2 switch.**

The objective of this practical is to set up and test a small LAN using a Layer 2 switch, connecting 2 PCs, 2 laptops, 1 server, and 1 printer so they can share data and resources.

Layer 2 Switch works at the Data Link Layer (Layer 2) of the OSI model.

Main job: Connect devices in a LAN and forward data based on MAC addresses.

It learns the MAC address of each device connected to its ports and stores them in a MAC address table.

When a device sends data, the switch looks at the destination MAC and sends it only to the correct port (not to all devices like a hub).

This reduces network traffic and increases speed.

**Step 1 : Connecting all the devices to Switch by Using Copper Straight Through.**

**Step 2 : Assigning the IP Address to all the devices.**

**Step 3 : Establishing communication between devices.**

**1.PC0 To Laptop1**

**Step 1 :- Ping PC0 To Laptop1**

**Step 2 :- Packet sending**

**Step 3 :- Simulation**

**2. Server To PC1**

**Step 1 :- Ping Server To PC1**

**Step 2 :- Packet sending**

**Step 3 :- Simulation**

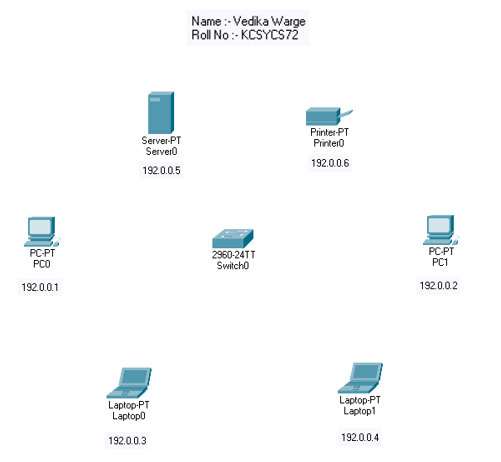
**3. Laptop0 To Printer**

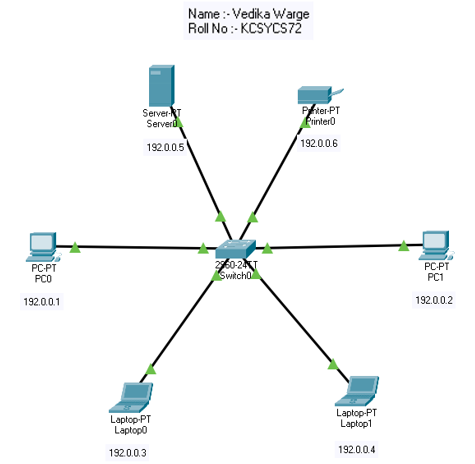
**Step 1 :- Ping Laptop0 To Printer**

**Step 2 :- Packet sending**

**Step 3 :- Simulation**

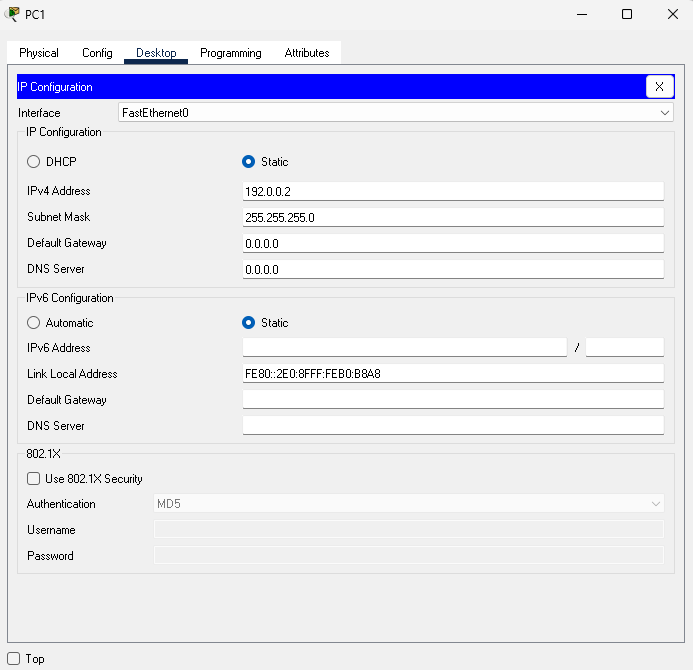
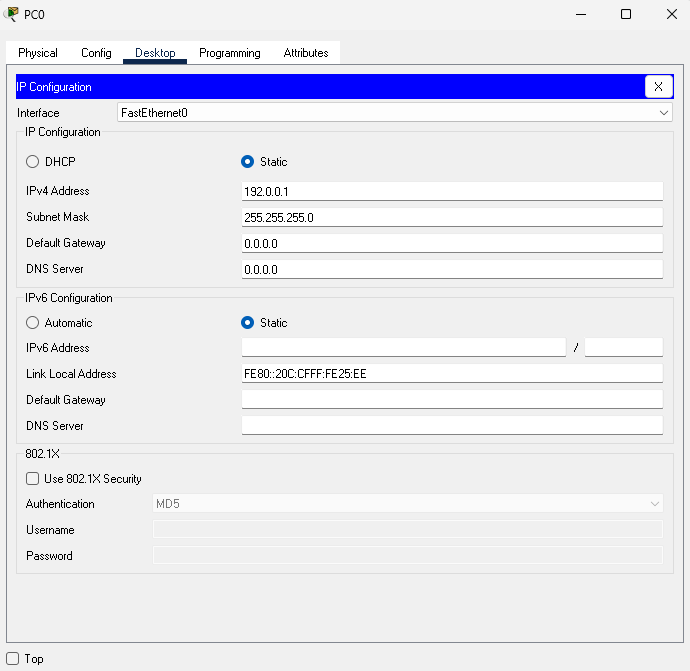
**STEP 1 : Connecting all the devices to Switch by Using Copper Straight Through.**



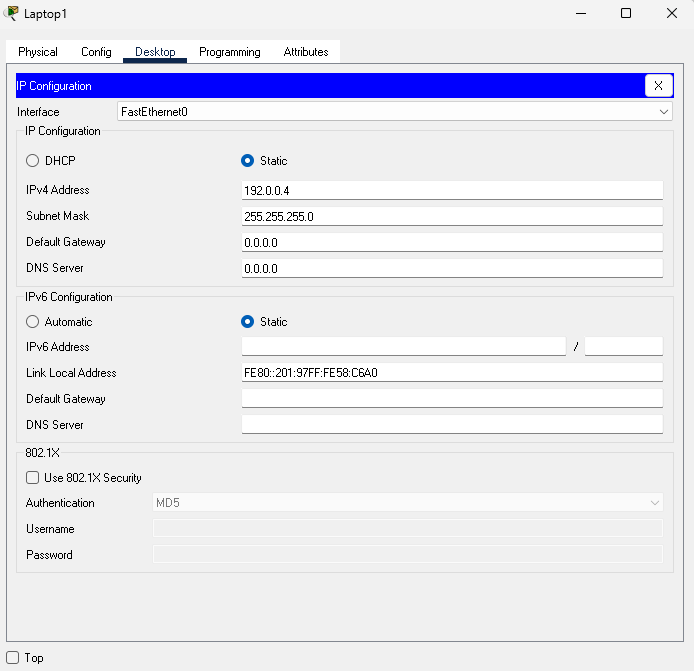
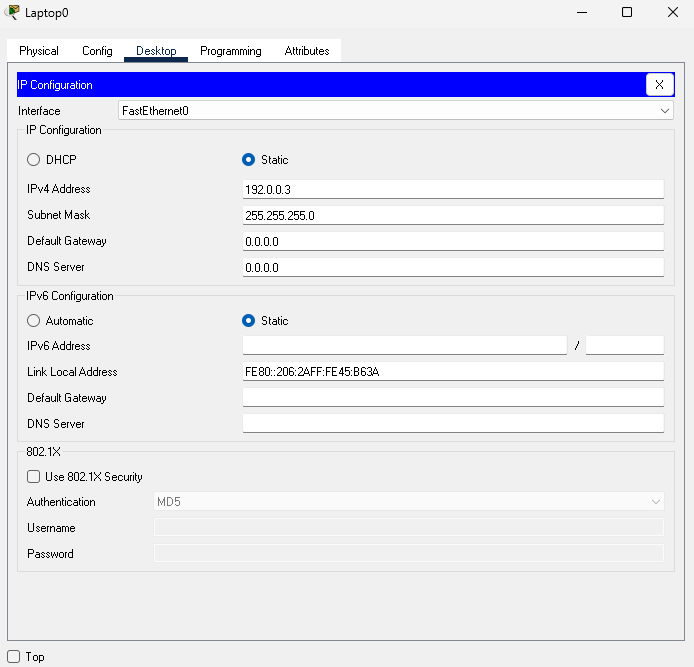
****

**Step 2 : Assigning the IP Address to all the devices.**

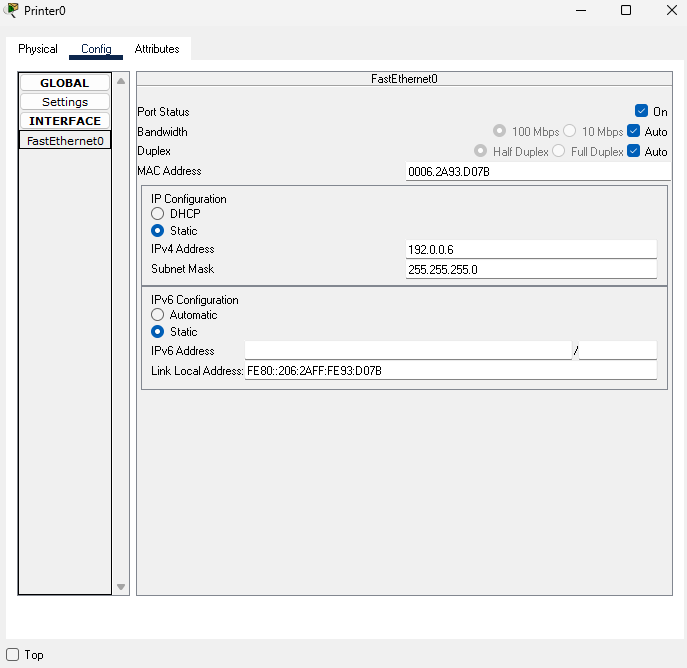
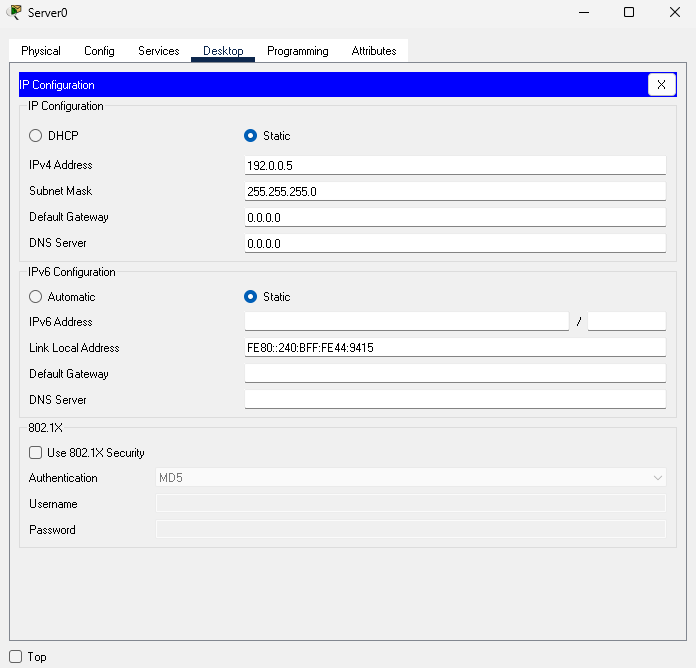
**PC0: PC1:**



**Laptop0: Laptop1:**



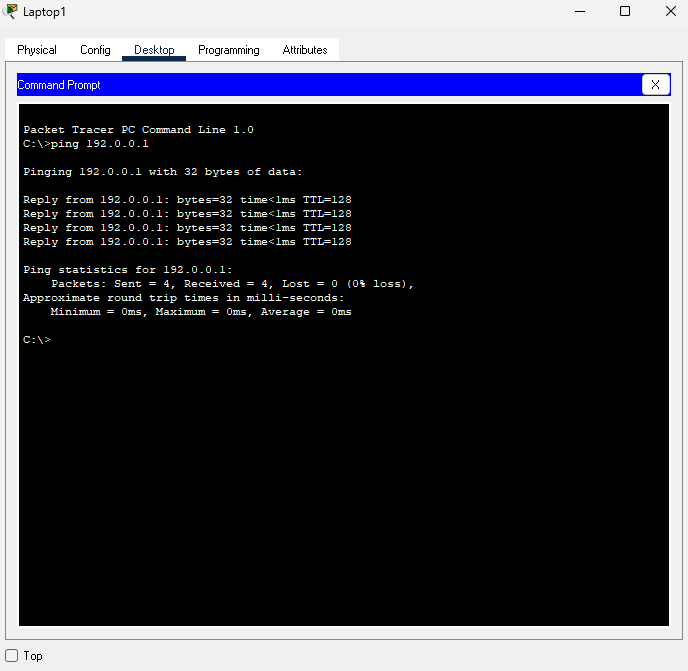
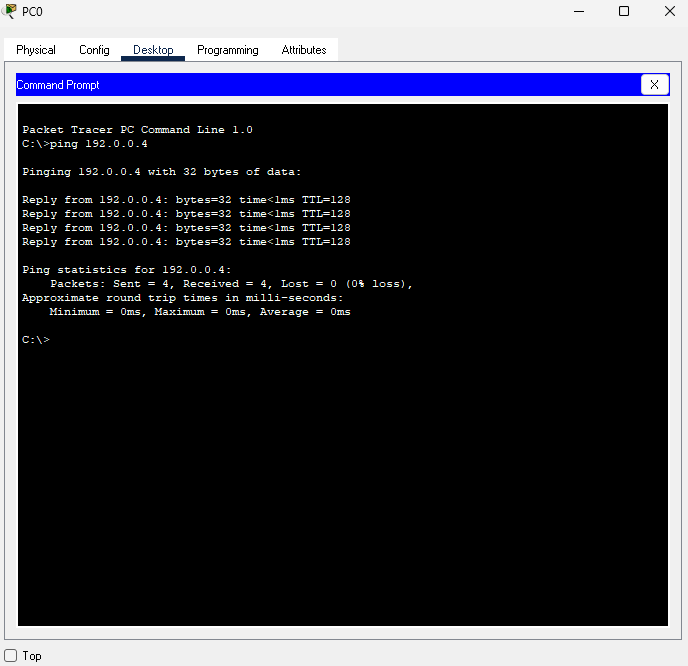
**Server: Printer:**



**Step 3 : Establishing communication between devices.**

**1.PC0 To Laptop1**

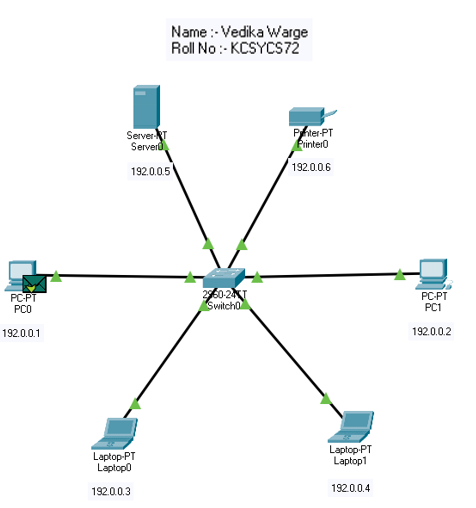
**Step 1 :- Ping PC0 To Laptop1**



**Step 2 :- Packet sending**

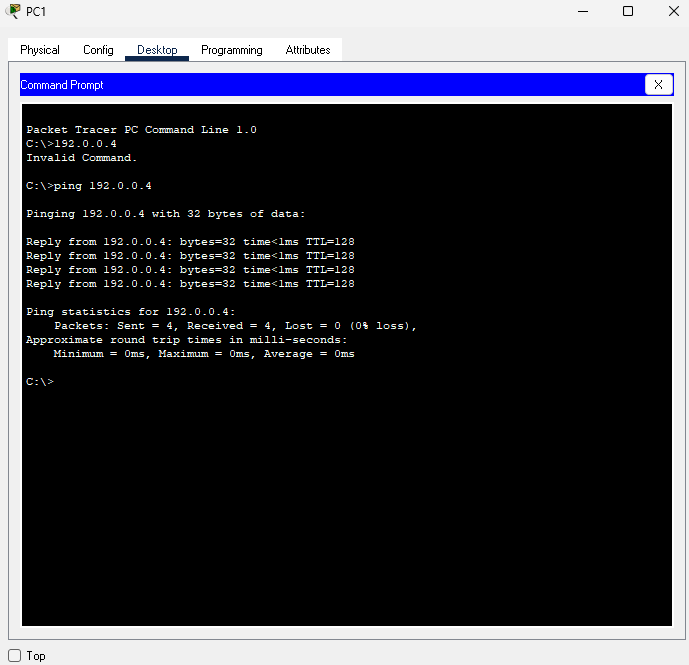
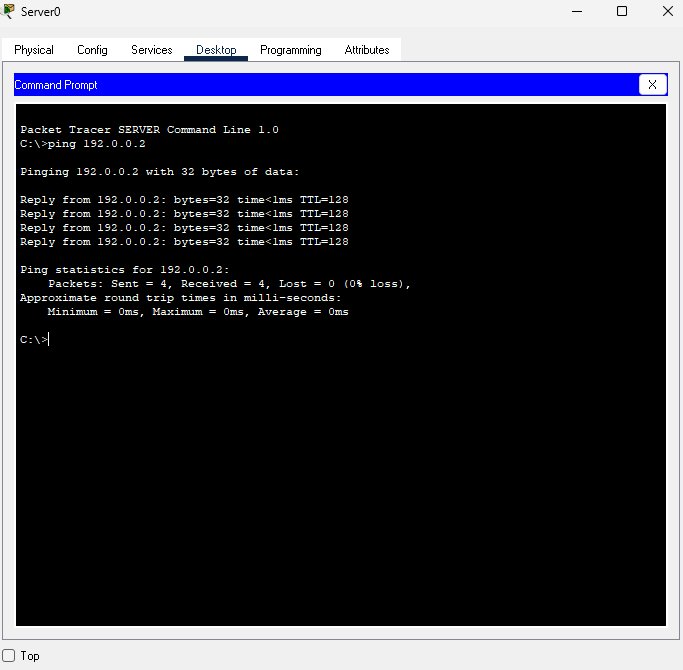


**Step 3 :- Simulation**

****

**2. Server To PC1**

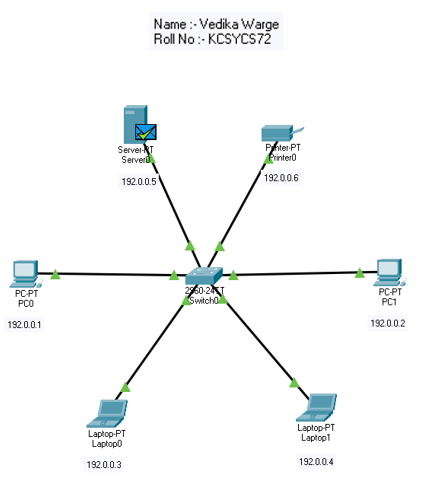
**Step 1 :- Ping Server To PC1**



**Step 2 :- Packet sending**

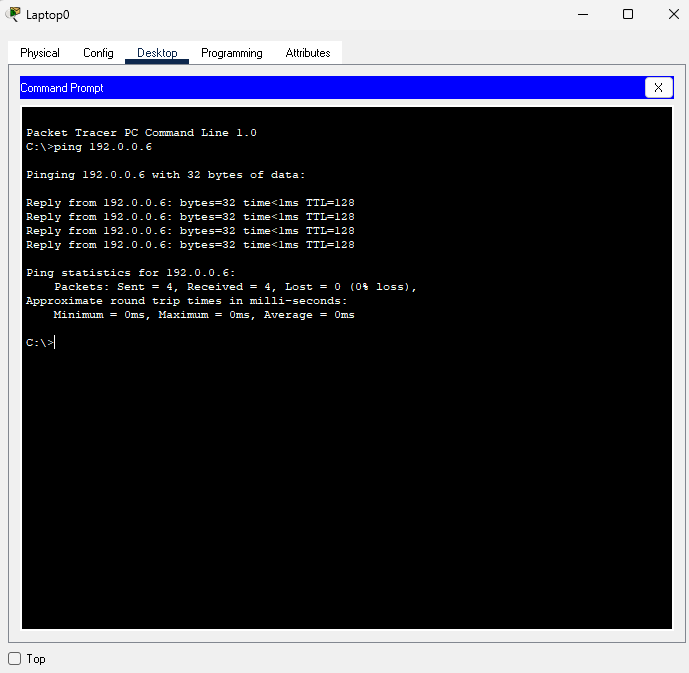


**Step 3 :- Simulation**

****

**3. Laptop0 To Printer**

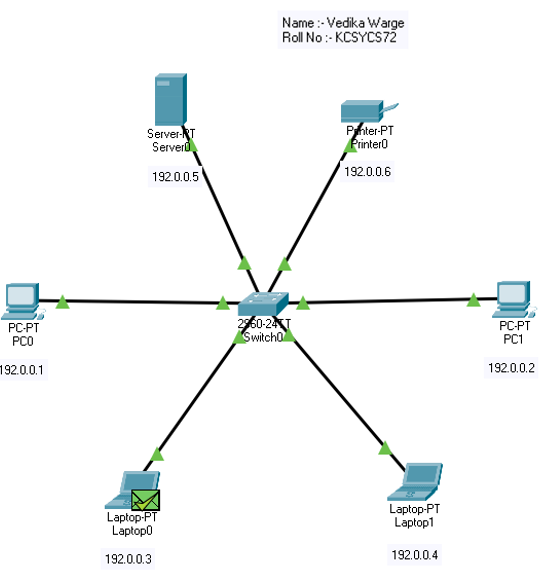
**Step 1 :- Ping Laptop0 To Printer**



**Step 2 :- Packet sending**



**Step 3 :- Simulation**

****

**Practical no 8: Connection of a network in triangular shape**

**Aim: Connect a network in triangular shape with three layer two switches and every switch will have four computers. Verify their connectivity with each other.**

The objective is to understand and implement a small switched network with redundancy then verify communication among all connected devices. Specifically:

* Learn to design and configure a Layer 2 network topology with redundancy by connecting three switches in a triangle, which can help prevent single points of failure.
* Understand how switches forward traffic within and across switches to enable devices on different switches to communicate.

**Step 1. Set up the physical devices**

**Step 2. Connect the switches in a triangle**

**Step 3. Connect computers to switches**

**Step 4. Assign IP addresses to computers**

**Step 5. Configure the switches (if necessary)**

**Step 6. Test connectivity between PCs on the same switch**

**Step 7. Test connectivity between PCs on different switches**

**Step 1. Set up the physical devices**

Use 3 Layer 2 switches.

Use 12 computers (4 per switch).

**Step 2. Connect the switches in a triangle**

Connect Switch 1 to Switch 2.

Connect Switch 2 to Switch 3.

Connect Switch 3 to Switch 1.

This forms a triangle, where each switch is connected to the other two.

**Step 3. Connect computers to switches**

Connect 4 computers to Switch 1.

Connect 4 computers to Switch 2.

Connect 4 computers to Switch 3.

**Step 4. Assign IP addresses to computers**

Assign IP addresses to all PCs in the same subnet or in different subnets if you want to test routing later (but for Layer 2, usually the same subnet).

Example:

PCs on Switch 1: 192.168.1.1 to 192.168.1.4 /24

PCs on Switch 2: 192.168.1.5 to 192.168.1.8 /24

PCs on Switch 3: 192.168.1.9 to 192.168.1.12 /24

**Step 5. Configure the switches (if necessary)**

By default, Layer 2 switches do not need complex configuration for basic switching.

Ensure all ports connecting to PCs and other switches are enabled.

If using Cisco switches or simulation tools like Packet Tracer, verify ports are up.

Optional: Enable Spanning Tree Protocol (STP) to avoid broadcast storms caused by loops in the triangle topology.

**Step 6. Test connectivity between PCs on the same switch**

From PC1 connected to Switch 1, ping other PCs on the same switch (e.g., PC2, PC3, PC4).

**Step 7. Test connectivity between PCs on different switches**

From PC1 on Switch 1, ping PCs on Switch 2 and Switch 3.

From PCs on Switch 2, ping PCs on Switch 3, etc.

**Step 1. 2. 3. 4. 5.**

192.168.1.1

192.168.1.11

192.168.1.10

192.168.1.9

192.168.1.7

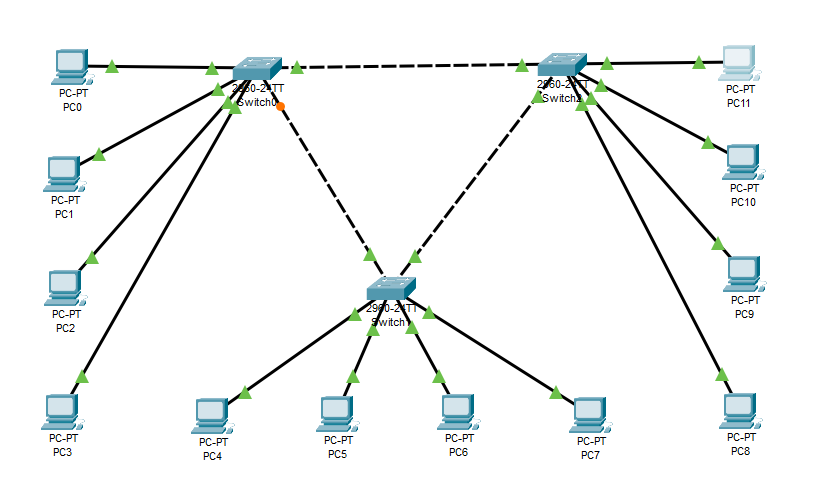
192.168.1.5

192.168.1.4

192.168.1.3

192.168.1.2

192.168.1.12

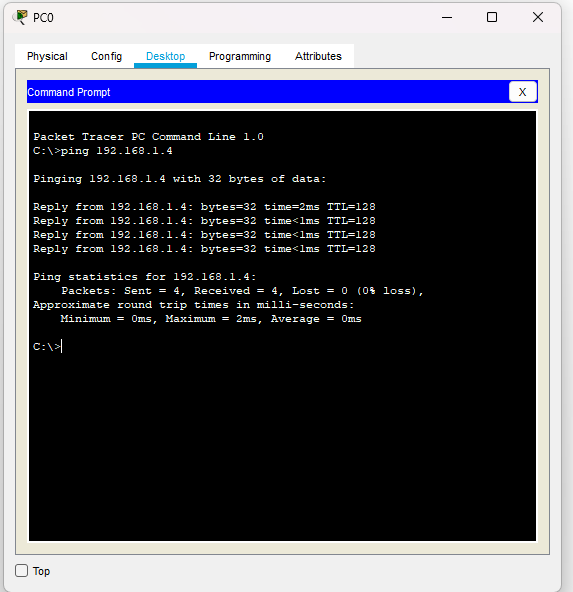
****

192.168.1.8

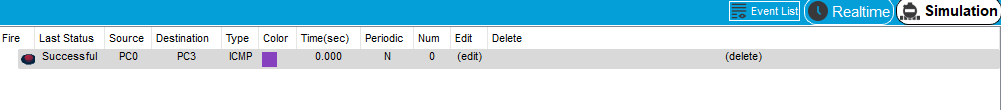
192.168.1.6

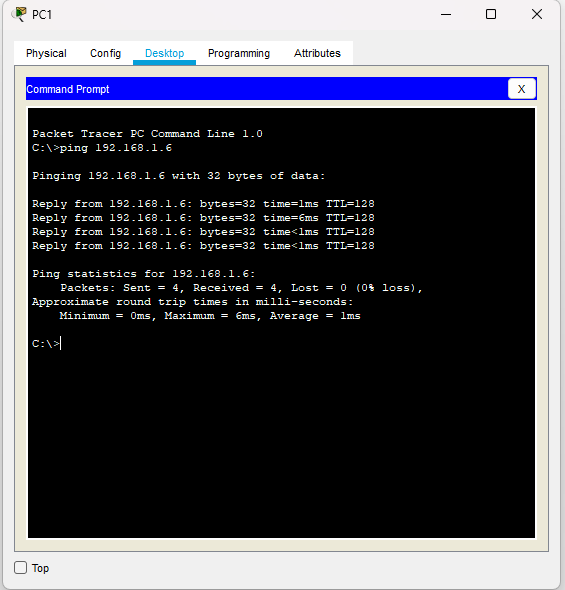
**Step 6. Test connectivity between PCs on the same switch**

**Ping PC3 from PC0**

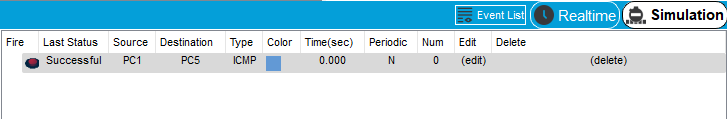


**Packet Simulation**

**Ping PC5 from PC1**



**Packet Simulation**



**Practical no 9: Wireless network of multiple PCs**

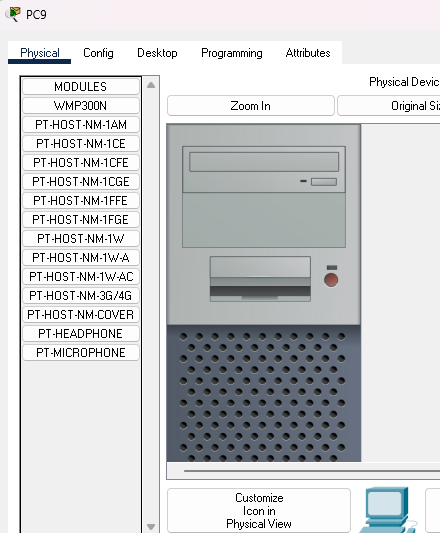
**Aim: Using Cisco Packet Tracer, create a wireless network of multiple PCs using appropriate access point.**

The objective of this practical is to build the foundational knowledge needed for designing and deploying wireless networks.

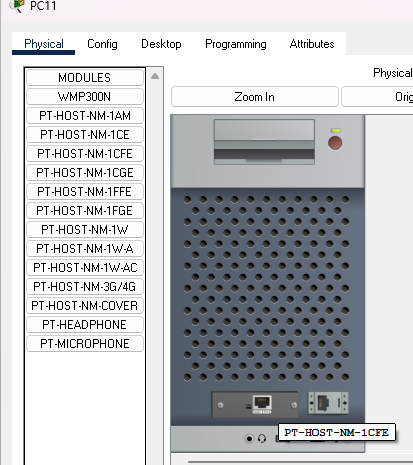
Understand wireless networking concepts: Learn how wireless communication works in a network, including the basic components such as access points, wireless routers and wireless devices.

Set up a wireless network using Cisco Packet Tracer: Create a wireless network with multiple PCs connected to an appropriate wireless access point (AP) to simulate real-world wireless connectivity.

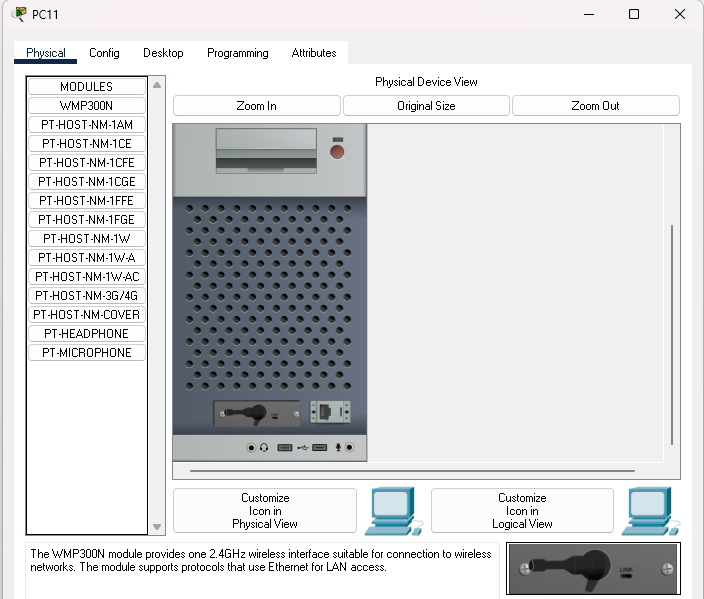
**STEP 1 : Turn off the P/C**



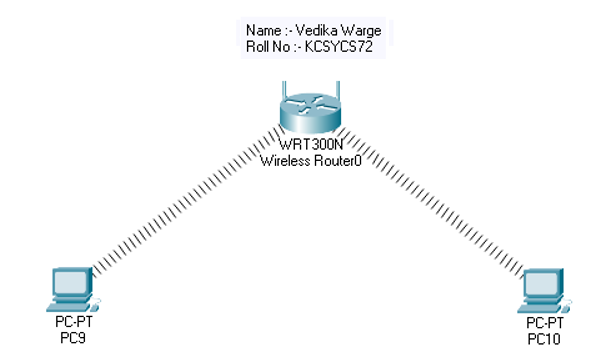
**STEP 2 : Remove the connect device**



**STEP 3 : Add the connector**

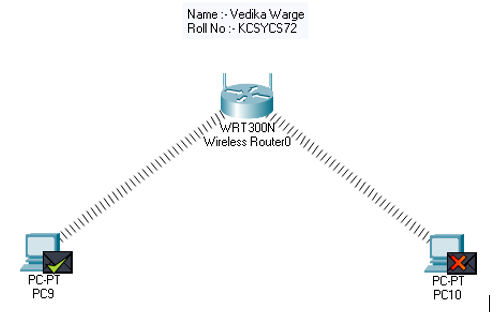


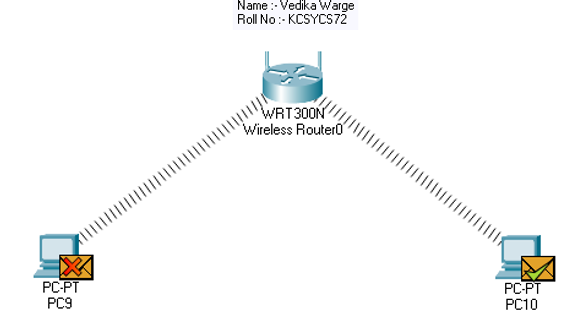
**STEP 4 : Establishing a wireless connection .**

****

**STEP 5 : Packet sending**



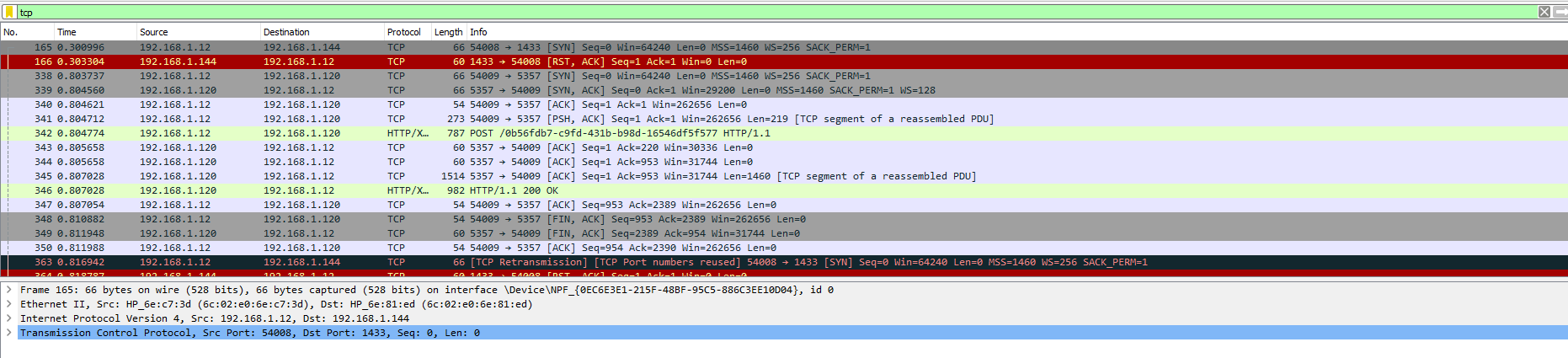
**Step 6 : Simulation**



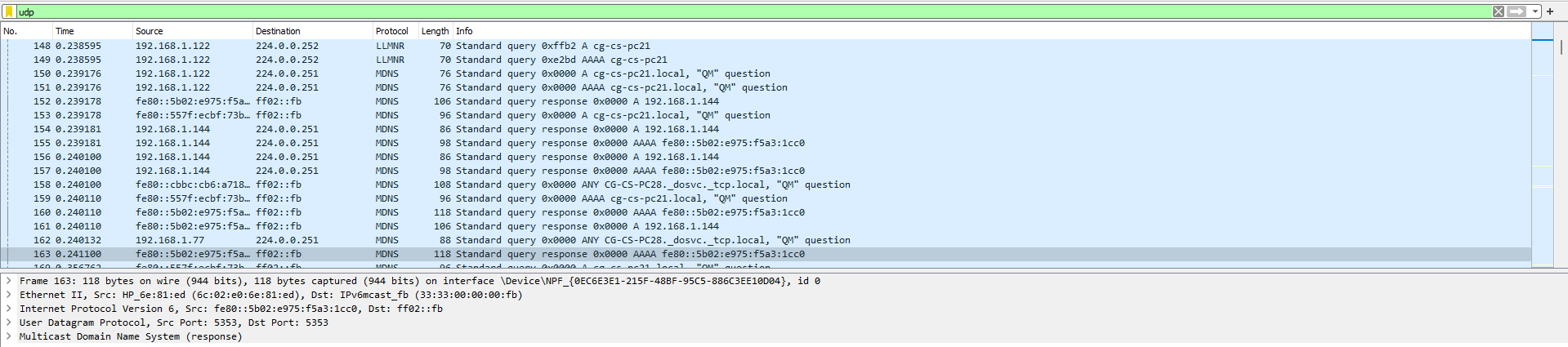
**Practical no 10: Using Wireshark, network analyser, set the filter**

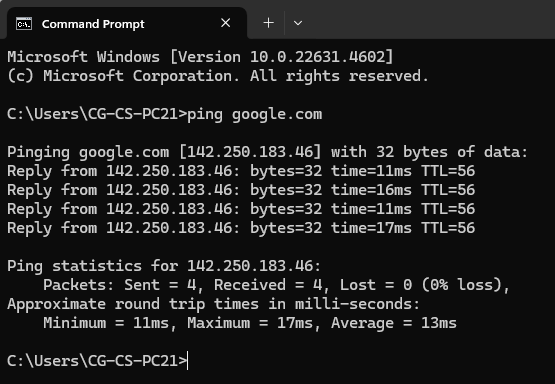
**Aim: Using Wireshark, network analyser, set the filter for ICMP, TCP, HTTP, UDP and perform respective protocol transactions to show/prove that the network analyser is working.**

**TCP :**

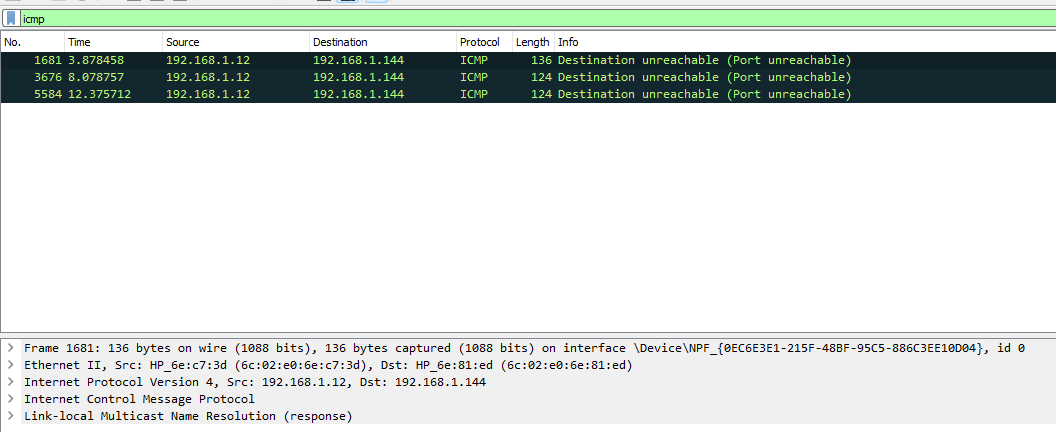


**UDP :**

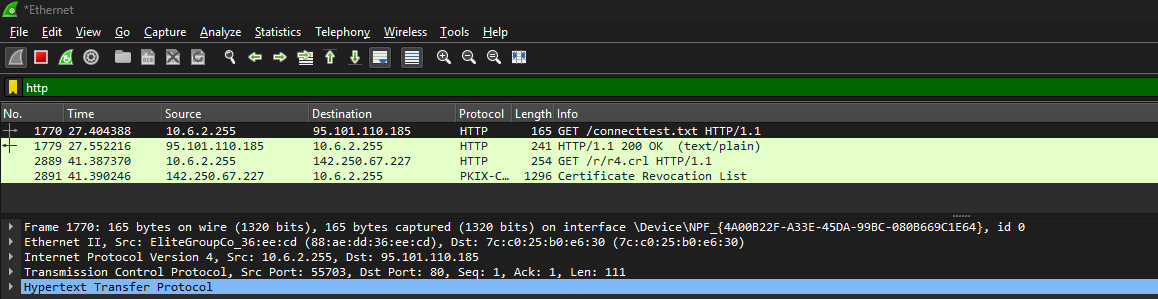




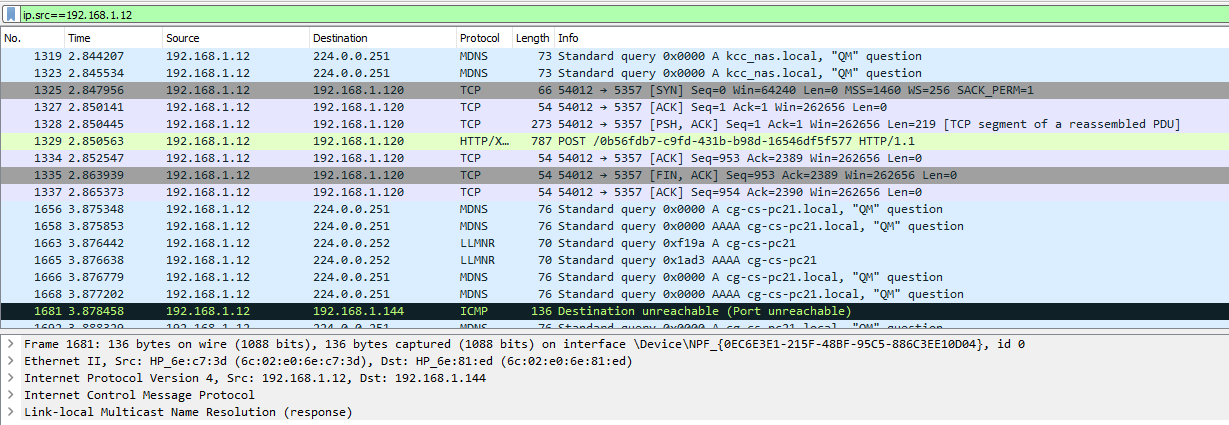
**ICMP :**



**HTTP :**

****

**IP SOURCE :**



**IP DESTINATION :**