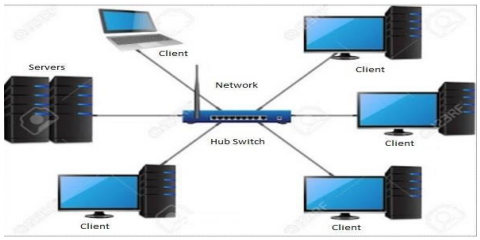
BAYELSA STATE POLYTECHNIC

SCHOOL OF APPLIED SCIENCES

DEPARTMENET OF COMPUTER SCIENCE (NETWORKING AND CLOUD COMPUTING)



PRACTICAL MANUAL / WORKBOOK

ON

NETWORKING ESSENCIAL

COURSE CODE: NCC 312

Name:	
Matric No.	
Department:	
Course:	
Group:	

Introduction Guide for Computer Practical Exercises

Welcome to your computer-based practical sessions! These exercises are designed to help you apply theoretical knowledge and develop hands-on skills that are crucial for your academic and professional success. To ensure that you get the most out of these sessions, it's important to approach each task with focus, preparation, and attention to detail. This guide will walk you through essential steps to help you handle the exercises in your practical manuals effectively.

Why is this important

Computer practical exercises often involve complex software tools, programming environments. The objective is not just to complete the task but to learn and understand the process. By following the right approach, you can maximize your learning, minimize mistakes, and ensure that you can solve problems efficiently and independently.

Steps to Handle Your Computer Practical Exercises Effectively

1. Preparation is Key

Before your practical session, make sure your computer is set up and ready to go. Ensure that all necessary software is installed and updated, and all peripherals are functioning properly. Taking the time to set up your workstation will save your time during the session and allow you to focus on the tasks.

2. Familiarize Yourself with the Manual

Read through the practical manual and the instructions for the exercise thoroughly before you begin. Make sure you understand the objectives, the steps involved, and the tools or software you'll need. If any part of the manual is unclear, take note of your questions and ask your instructor for clarification before starting.

3. Follow the Instructions Step-by-Step

Each practical exercise is structured to guide you through a sequence of steps. Pay close attention to these instructions and follow them in order. Skipping steps can result in errors or incomplete work, so it's crucial to proceed in the correct sequence to achieve the desired outcome.

4. Ask for Help When Needed

Don't hesitate to ask your instructor or classmates for assistance if you encounter difficulties. It's okay not to know everything, practical exercises are learning opportunities. Whether it's a technical issue or confusion about the task, getting help when needed will keep you on track.

5. Review Your Work

Once you've completed the practical exercise, take time to review your work. If applicable, test the program or functionality you've worked on. Debug any errors, recheck your results, and ensure everything meets the given specifications.

6. Ensure Timely Submission

Follow any instructions for submitting your work carefully. Save your files in the correct format and back them up if needed. Timely submission of your completed work ensures you meet the requirements and deadlines set by your instructor.

Final Thoughts

Your practical sessions are an opportunity to sharpen your skills, build confidence, and gain a deeper understanding of computer applications and tools. By preparing ahead, staying organized, and following the instructions carefully, you will ensure that you handle each exercise effectively and make the most out of your practical experience.

Good luck, and remember that consistent practice and attention to detail will lead to success!

Experiment-1

Aim of the experiment: Identify Network Devices

Objective:

To enable students to recognize, differentiate, and describe the function of common networking devices used in a LAN/WAN environment. List

Experiment-2

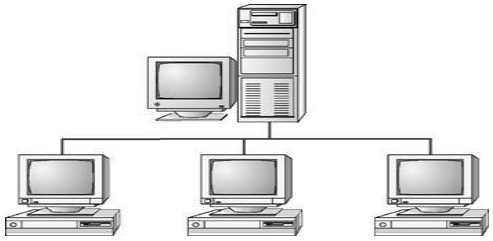
Aim of the experiment: Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.

A. ……

……

……

……



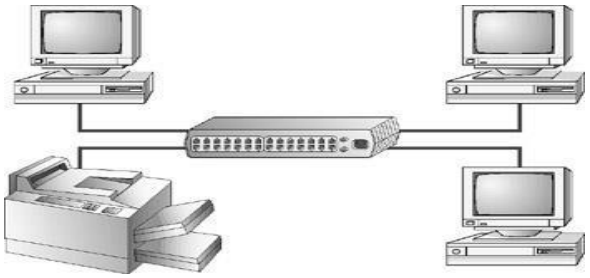
……

……

B. ……

……

……



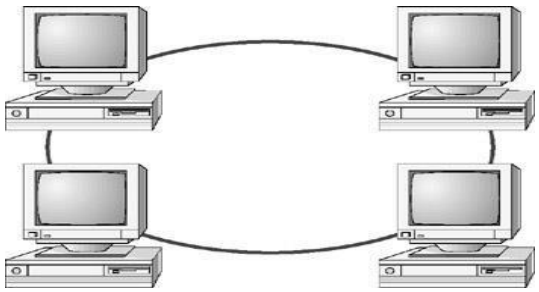
……

……

……

……

C. ……



……

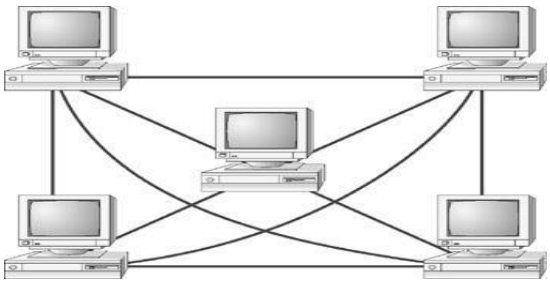
……

……

……

D……

……



……

……

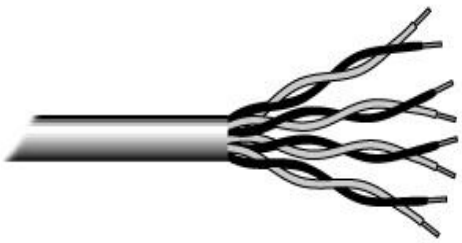
……

……

Study of cables:

The following cables are used in networking. Explain

E……



……

……

……

……

F……..

……

……..

……

……

……

……

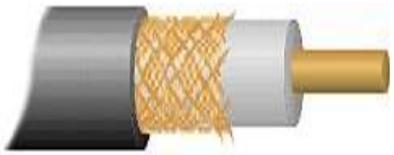
G……..

……

…….

……

……



H…….

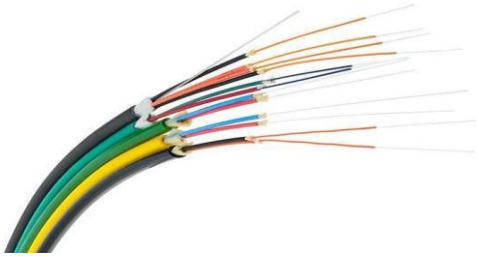
……

……

……

……

……



Experiment-3

Aim of the experiment: Making of cross over cable and straight cable.

Tools/Equipment/Components Required:

1. RJ-45 connector,
2. Crimping Tool,
3. Twisted pair Cable,
4. Cable Tester.

How to Terminate an Ethernet Cable (RJ-45) –
Step-by-Step

1. Strip the Outer Jacket

- Carefully strip about **2 inches (5 cm)** of the outer plastic jacket from the cable using a cable stripper or utility knife.
- **Important:** Avoid cutting or nicking the internal wires.
- **Check the wires:** If any inner wires are damaged, cut the end off and start again to ensure reliable performance.

2. Untwist and Prepare the Wires

- Gently untwist each pair of wires, keeping **no more than 1/2 inch (1.25 cm)** of untwisted wire exposed near the tip.
- Hold the cable jacket firmly to prevent the twist from unravelling inside the jacket.
- **Standard Cat5e/Cat6 cables** must maintain their twist as close to the connector as possible to preserve signal integrity.

3. Arrange the Wires in the Correct Order

- Choose the wiring standard: **T568A** or **T568B**.
- For **straight-through cables**, both ends use the **same standard**.
- For **crossover cables**, one end uses T568A, and the other uses T568B

Diagram shows you how to prepare **Diagram shows you how to prepare**

Cross 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	

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	

Step 4: Use a cable tester to test for proper continuity.

correct every grammatical error: Visit the Networking laboratory, and prepare a Cable Crimping, straight Cabling and Cross Cabling, and testing the crimped cable using a cable tester are done successfully.

Provide your experience:

……
……
……
……
……

Experiment-4

Aim of the experiment: Install and configure a network interface card in a workstation.

Apparatus/ Equipment Required:

1. NIC card
2. Desktop/PC
3. Computer Screw driver set
4. Driver Software

Theory:

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.

Every networked computer must also have a network adapter driver, which controls the network adapter.

Each network adapter driver is configured to run with a certain type of network adapter.

Procedure: Installing and Configuring the Network Card

1. Disconnect all cables and open the computer case. Insert the network card into an available PCI slot and secure it with the provided screw. Close the case, reconnect cables, and power on the system.
2. Install the driver for the network card. Once done, proceed to configure it for network use.
3. Click Start, go to Settings, and open Control Panel. Double-click the System icon.
4. Go to the Hardware tab and select Device Manager.
5. Expand Network Adapters by clicking the + sign.
6. Check for any yellow exclamation marks (!) next to the network adapter, indicating issues.
7. Double-click the network driver (e.g., NE2000 Compatible). The message This Device is working correctly should appear.
8. If the message doesn't appear or if no adapter is listed, the card may need further configuration.

State your Result: ……..

Experiment-5

Aim of the experiment: Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation.

Apparatus/ Equipment Required:

PC connected to internet.

Theory:

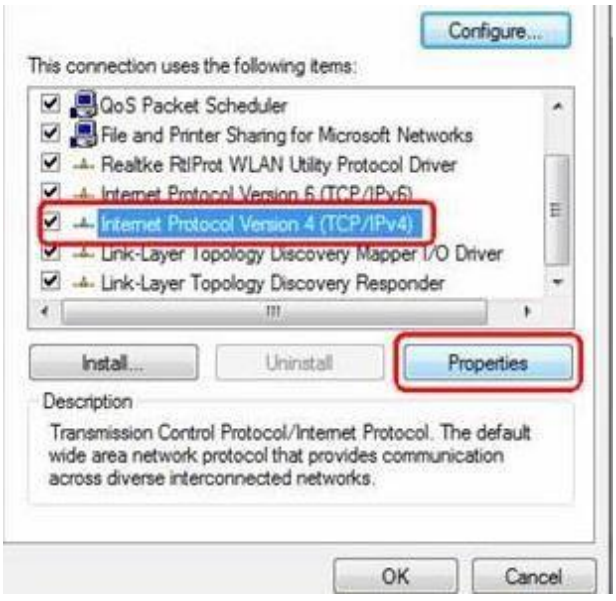
IP Address Identification:
An IPv4 address is a 32-bit number that uniquely identifies a device on the Internet. It's shown in dotted decimal notation, like this:

Example: 192.68.12.1
IP Address Classes:

- **Class A:** 1.0.0.1 to 126.255.255.254 – Supports 16 million hosts on 127 networks.
- **Class B:** 128.1.0.1 to 191.255.255.254 – Supports 65,000 hosts on 16,000 networks.
- **Class C:** 192.0.1.1 to 223.255.254.254 – Supports 254 hosts on 2 million networks.
- **Class D:** 224.0.0.0 to 239.255.255.255 – Reserved for multicast groups.
- **Class E:** 240.0.0.0 to 254.255.255.254 – Reserved.

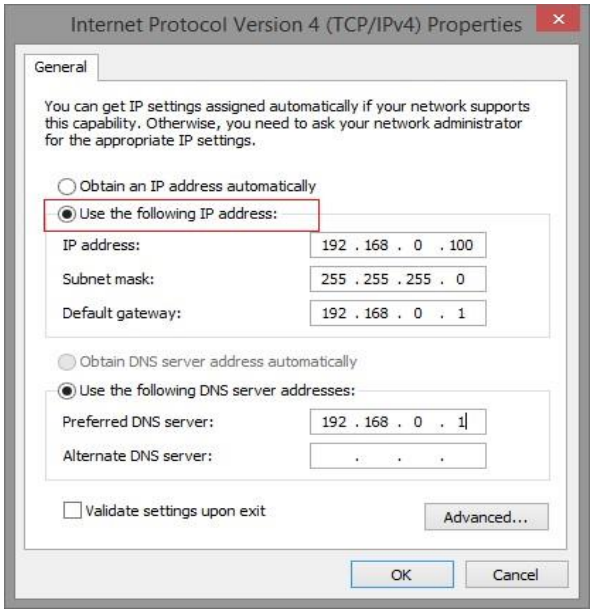
Steps to Configure IP Address:
Step 1:

1. Click the **Start** button and select **Control Panel**.
2. To view your IP address, go to **Network and Internet** > **Network and Sharing Center** > **Change Adapter Settings** (on the left).
3. Right-click **Ethernet** (or **Wi-Fi** for wireless) and select **Status** > **Details** to view the TCP/IP details.



Step 2:

Right-click **Ethernet**, choose **Properties**, then select **Internet Protocol Version 4** and click **Properties**.



3: Select **Use the following IP address** and manually enter the IP or DNS address. Click **OK** and then **Close** to finish.

Provide your experience:

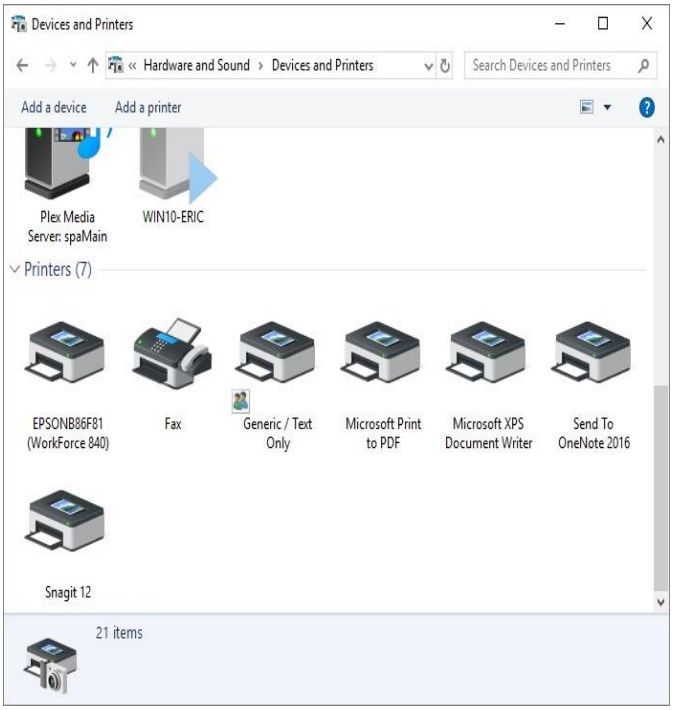
……
……
……
……
……

Experiment-6

Aim of the experiment: Sharing of Hardware resources in the network.

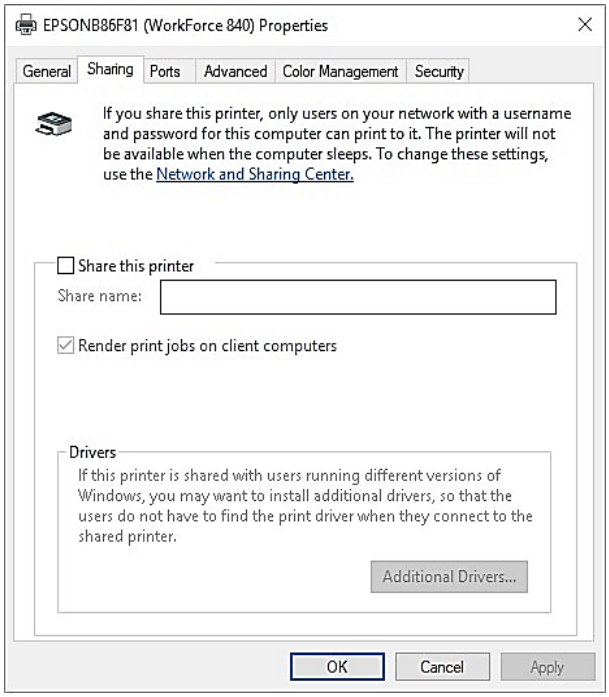
Apparatus/ Equipment Required:

1. Minimum 02 nos. of PCs
2. Printer



Procedure:

1. Network printer can be configured as shared devices so that others on the network can use them.
2. Follow the steps to share printer.
3. Go to the Control Panel from the Start Menu.
4. click View Devices and Printers (under the Hardware and Sound heading).
5. click the printer you want to share from Devices and Printers dialog box.
6. select Printer Properties from the Context menu.
7. Click on the Sharing tab of the printer's Properties dialog box.
8. Click the Share this Printer check box and optionally change the Share Name of the printer.
9. click OK to close the printer's Properties dialog box.

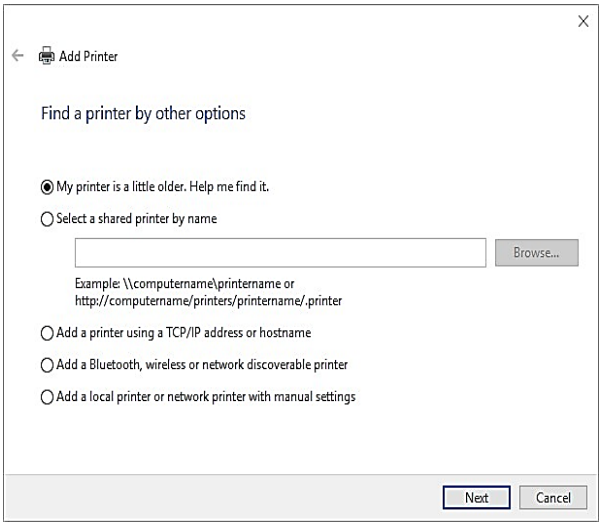


How to access the shared printer:

Now the shared printer is made available to others on your network. In order to access the shared printer from a different system, go to that system

1. Go to the Control Panel from the Start Menu.

2. click View Devices and Printers (under the Hardware and Sound heading).
3. click the Add a Printer option, at the top of the dialog box.
4. Click on The Printer I want isn't Listed if our printer isn't found. Windows displays the Find a Printer by Other Options section of the Add Printer wizard.



5. Click the second option, starts scanning the network for available printers.
6. After all of the printers have been found, select the printer name that you want to use and click Next.
7. The network printer is added to the computer's list of available printers.

   Click Finish to finish the process.

Provide your experience:

……
……
……
……
……

Experiment-7

Aim of the experiment: Use of Netstat and its options.

Apparatus/ Equipment Required:

PC connected with internet connection.

The **netstat** command is used to display the TCP/IP network protocol statistics and information.

Procedure:

1. **Netstat is a command for checking network and Internet connections.**
2. **Netstat command uses following syntax and switches.**

Syntax and switches:

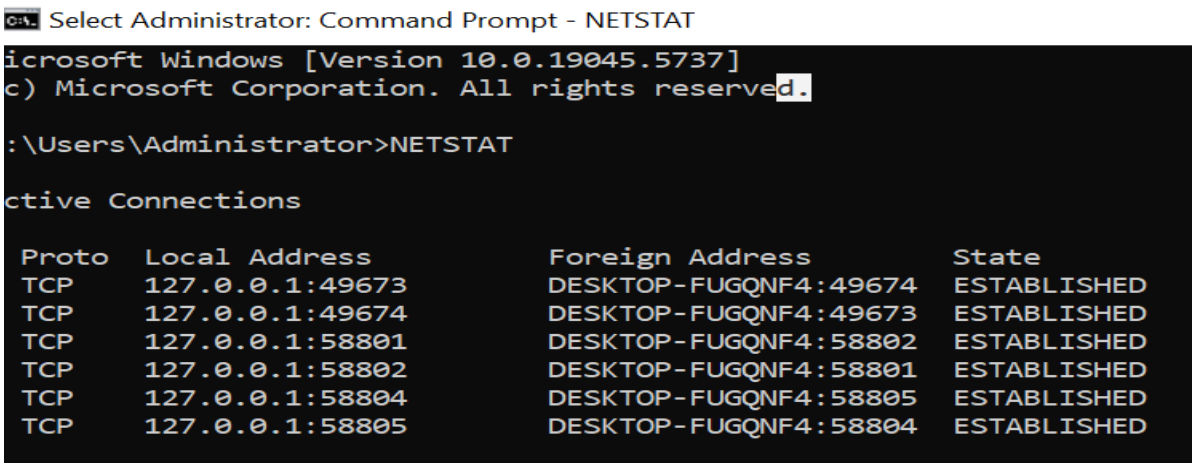
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

Switches	Description
-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases, well-known executables host multiple independent components, and in these cases, the sequence of components involved in creating the connection or listening port is displayed. In this case, the executable name is in [] at the bottom. Note that this option can be time-consuming and fails unless you have sufficient permissions.
-e	Displays Ethernet statistics. This option may be combined with the -s option.
-f	Displays FQDN (fully qualified domain names) for foreign addresses.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may
	be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays NetworkDirect connections, listeners, and shared endpoints.
-y	Displays the TCP connection template for all connections. Cannot be combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics. If omitted, netstat prints the current configuration information once.

Command:

C:\>NETSTAT



Enter this Command C:\>NETSTAT -S and produce the output:

Enter this Command C:\>NETSTAT -E and produce/paste the output here:

Experiment-8

Aim of the experiment: Connectivity troubleshooting using PING, IPCONFIG

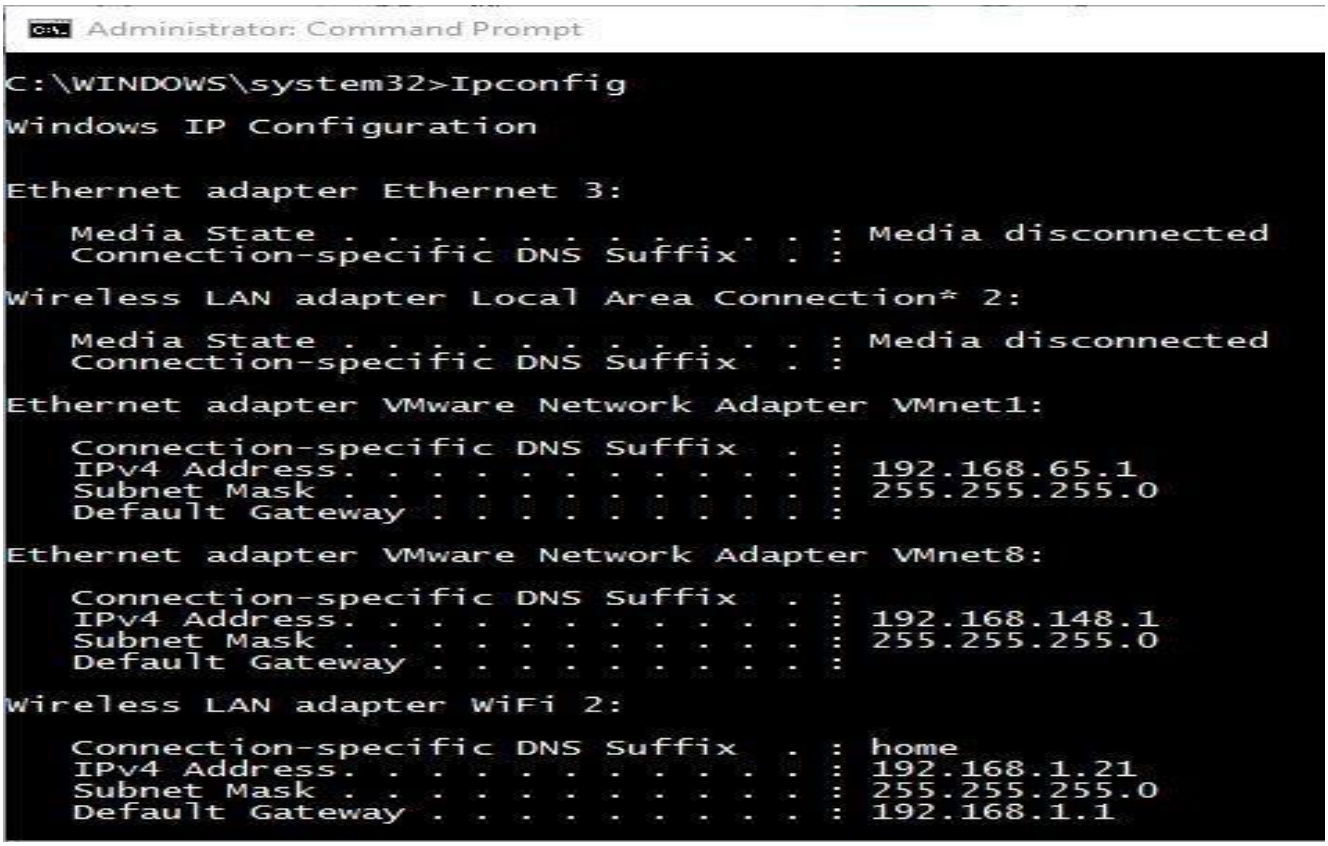
Apparatus/ Equipment Required:

PC connected with internet connection.

Procedure:

Troubleshoot the internet connectivity by using PING and IPCONFIG.

1. Open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.



3. At the command prompt, ping the loopback address by typing ping 127.0.0.1.

Command:

C:\>ping 127.0.0.1

4. Ping the IP address of the computer.

   Command:

   C:\> ping 192.168.1.1

5. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

Provide your experience:

……
……
……

6. Ping the IP address of a remote host (a host that is on a different subnet).

If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

Provide your experience:

……
……
……

7. Ping the IP address of the DNS server.

   If the ping command fails, verify that the DNS server IP address is correct that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

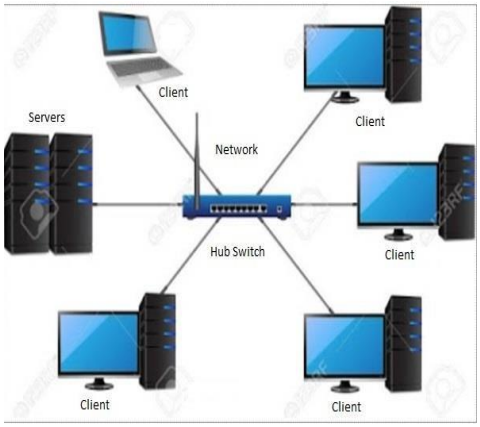
Provide your experience:

……
……
……

Experiment- 9

Aim of the experiment: Simple Steps to Set Up a Basic Server Network

Apparatus/ Equipment Required:



1. 06 NOS of computers (01 server and 05 clients)
2. Switch
3. Required Cables Procedure:

1. Insert a second LAN card into the computer you want to use as the server.
2. Plug your internet connection into the first (built-in) LAN port.
3. Enter the IP address provided by your ISP and confirm internet access on that system.
4. Ensure the second LAN card is detected and shows as "Unplugged."
5. Open **Properties** of the first LAN, go to the **Advanced** tab, check both sharing boxes, click **OK**, and close the window.
6. Use a straight-through Ethernet cable (same color pattern on both ends).
7. Connect one end to the second LAN port and the other to a network switch.
8. Open **Properties** of the second LAN, go to **TCP/IP settings**, and set:
   - IP Address: *192.168.0.1* (or any local IP),
   - Subnet Mask: *255.255.255.0*,
   - Gateway: *192.168.0.1*.
9. Once connected, you'll see a message like "Local Area Connection 2 is connected."
10. Connect another Ethernet cable from the switch to a second computer.
11. On that computer, set the IP as *192.168.0.2*, with the same Subnet Mask and Gateway as the server.

Provide your experience:

……

……

……

Experiment-10

Aim of the experiment: Investigate the TCP/IP and OSI Models in Action using packet tracer

Apparatus/ Equipment Required:

PC connected with internet connection.

Investigating TCP/IP and OSI Models in Action Using Packet Tracer

This guide will help you observe and understand how data travels through the different layers of the TCP/IP and OSI models using Cisco Packet Tracer. We'll create a simple network, capture packets, and analyze them to see the models in action.

Part 1: Understanding the Models

OSI Model (7 Layers)

1. **Physical Layer** - Deals with physical connections, cables, electrical signals
2. **Data Link Layer** - Handles MAC addresses, frames, switch operations
3. **Network Layer** - Manages IP addressing, routing, packet forwarding
4. **Transport Layer** - Provides TCP/UDP protocols, port numbers, segmentation
5. **Session Layer** - Manages sessions between applications
6. **Presentation Layer** - Handles data translation, encryption, formatting
7. **Application Layer** - Interfaces with user applications like HTTP, FTP, SMTP

TCP/IP Model (4 Layers)

1. **Network Access/Link Layer** - Combines OSI Physical and Data Link layers
2. **Internet Layer** - Equivalent to OSI Network layer
3. **Transport Layer** - Equivalent to OSI Transport layer
4. **Application Layer** - Combines OSI Session, Presentation, and Application layers

Part 2: Setting Up a Test Network in Packet Tracer

Create a Simple Network

1. Launch Packet Tracer
2. Create the following topology:
   - 2 PCs (PC1 and PC2)
   - 2 Switches (Switch1 and Switch2)

- 2 Routers (Router1 and Router2)

Connect the Devices

1. Connect PC1 to Switch1 using straight-through cable
2. Connect Switch1 to Router1 using straight-through cable
3. Connect Router1 to Router2 using serial cable
4. Connect Router2 to Switch2 using straight-through cable
5. Connect Switch2 to PC2 using straight-through cable

Configure IP Addresses

1. PC1: 192.168.1.10/24, Gateway: 192.168.1.1
2. Router1:
   - Fa0/0: 192.168.1.1/24
   - S0/0/0: 10.0.0.1/30
3. Router2:
   - S0/0/0: 10.0.0.2/30
   - Fa0/0: 192.168.2.1/24
4. PC2: 192.168.2.10/24, Gateway: 192.168.2.1

Configure Routing

1. On Router1:
2. Router1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
3. On Router2:
4. Router2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1

Part 3: Observing the Models in Action

Scenario 1: Ping from PC1 to PC2

1. Start a simple ping from PC1 to PC2:
   - On PC1, open Command Prompt
   - Type ping 192.168.2.10
2. Use Simulation Mode:
   - Click the "Simulation" tab at the bottom right
   - Click "Edit Filters" and select only ICMP
   - Click "Auto Capture/Play"
3. Observe the packet flow:
   - Watch as the packet travels from PC1 through the network to PC2 and back

Scenario 2: Web Page Request

1. Set up a Simple HTTP Server:
   - Place a Server device in the network connected to Switch2
   - Configure it with IP 192.168.2.20/24, Gateway 192.168.2.1
   - Configure HTTP service on the server
2. From PC1, access the web server:
   - Go to Web Browser
   - Enter http://192.168.2.20
3. Use Simulation Mode:
   - Set filters for HTTP, TCP, IP
   - Observe the packet flow

Part 4: Detailed PDU Analysis - Examining the Layers in Action

Analyzing an ICMP Ping Packet

1. In Simulation Mode, capture a ping packet
2. Click on the packet to view PDU (Protocol Data Unit) details
3. Observe how data is encapsulated through each layer:

OSI Layer 7-5 (Application, Presentation, Session) / TCP/IP Application Layer

- ICMP message type and code (Echo Request/Reply)

OSI Layer 4 (Transport) / TCP/IP Transport Layer

- Protocol: ICMP
- No port numbers (ICMP doesn't use ports)

OSI Layer 3 (Network) / TCP/IP Internet Layer

- Source IP: 192.168.1.10
- Destination IP: 192.168.2.10
- TTL value
- Protocol: 1 (ICMP)

OSI Layer 2 (Data Link) / TCP/IP Network Access Layer

- Source MAC address
- Destination MAC address

- Frame type: 0x0800 (IPv4)

OSI Layer 1 (Physical) / TCP/IP Network Access Layer

- Electrical signals (not directly visible in Packet Tracer but simulated)

Analyzing an HTTP Request

1. Capture an HTTP packet
2. Examine each layer:

OSI Layer 7-5 / TCP/IP Application Layer

- HTTP GET request
- Headers and content

OSI Layer 4 / TCP/IP Transport Layer

- Protocol: TCP
- Source Port: (ephemeral port on PC)
- Destination Port: 80 (HTTP)
- Sequence/Acknowledgment numbers
- Flags (SYN, ACK, etc.)

OSI Layer 3 / TCP/IP Internet Layer

- Source IP: 192.168.1.10
- Destination IP: 192.168.2.20
- TTL value
- Protocol: 6 (TCP)

OSI Layer 2 / TCP/IP Network Access Layer

- Source MAC address
- Destination MAC address
- Frame type: 0x0800 (IPv4)

Part 5: Focusing on Specific Layer Operations

Layer 2 (Data Link) Operations

1. Observe ARP process:
    - Clear the ARP cache on PC1 (arp -d * in Command Prompt)
    - Filter for ARP packets
    - Ping PC2 from PC1
    - Watch how PC1 discovers Router1's MAC address

2. Switch MAC learning:
    - Check Switch1's MAC address table before and after communication

Layer 3 (Network) Operations

1. Observe routing decisions:
    - Enable "Show Simulation Panel"
    - Watch how Router1 determines the next hop for packets to 192.168.2.0/24

Layer 4 (Transport) Operations

1. Observe TCP handshake:
    - Filter for TCP packets
    - From PC1, access the web server
    - Watch the SYN, SYN-ACK, ACK process

Part 6: Practical Exercises

Exercise 1: Identify the Layer Problem

1. Disable Fa0/0 on Router1
2. Try to ping from PC1 to PC2
3. Identify which layer is affected (Layer 1 - Physical)

Exercise 2: Change MAC Address

1. Change PC1's MAC address
2. Observe how this affects Layer 2 communication

Exercise 3: IP Addressing Issue

1. Change PC2's IP to 192.168.3.10/24 without updating routing
2. Observe how this affects Layer 3 communication

Exercise 4: Port Filtering

1. Configure an ACL on Router1 to block TCP port 80
2. Try accessing the web server from PC1
3. Observe how this affects Layer 4 communication

By understanding these models in action, you can better design, implement, and troubleshoot networks effectively.

Provide your experience:

.....

.....

Experiment-11

Aim of the experiment: Study of Routing and Switching, configuring of Switch and Routers, troubleshooting of networks.

Apparatus/ Equipment Required:

CISCO Packet Tracer software

Theory:

Routing and Switching:

Routing and switching are core functions in network communication, each serving a distinct purpose.

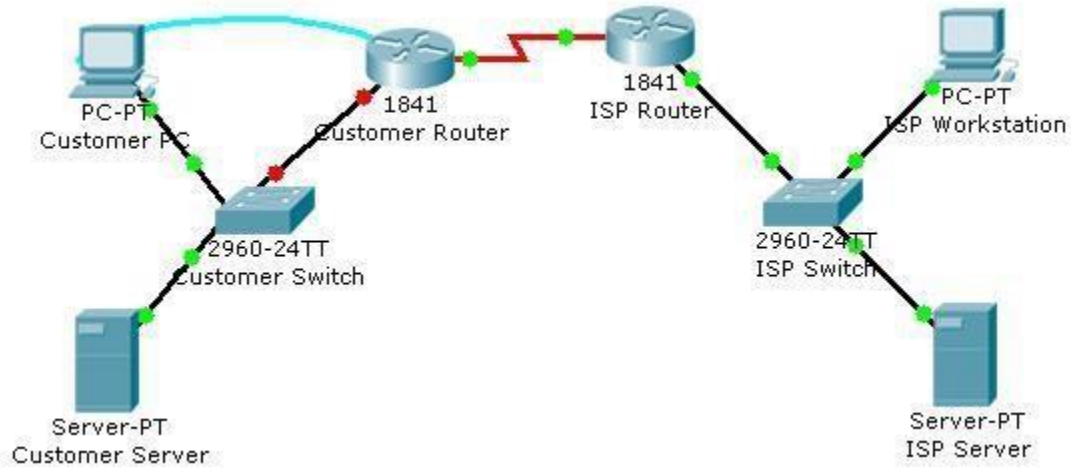
Switching involves moving data packets between devices within the same network, such as a Local Area Network (LAN). It ensures that data reaches the correct device inside a single network.

Routing, on the other hand, is responsible for directing data between different networks. It determines the best path for data to travel from one LAN to another.

In short, **switching connects devices within a network**, while **routing connects different networks together**.

Procedure:

Switch configuration (configuration of Cisco Catalyst 2960 switch.):



Topology Diagram

This guide will walk you through configuring the network shown in the above diagram, using Cisco Packet Tracer. This will cover basic device configurations to get the network operational.

The network consists of:

a. Customer side: PC, Router, Switch, Server

b. ISP side: Workstation, Router, Switch, Server

Step-by-Step Configuration

1. Set Up the Physical Connections

1. Open Packet Tracer and drag all devices onto the workspace
2. Connect them as follows:
   - Customer PC → Customer Switch (FastEthernet)
   - Customer Server → Customer Switch (FastEthernet)
   - Customer Switch → Customer Router (FastEthernet)
   - Customer Router → ISP Router (Serial connection - use DCE cable on one side)
   - ISP Router → ISP Switch (FastEthernet)
   - ISP Switch → ISP Server and Workstation (FastEthernet)

2. Configure End Devices (PCs and Servers)

Customer PC:

1. Click on the PC → Desktop tab → IP Configuration
2. Set:
   - IP Address: 192.168.1.10
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.1.1

Workstation:

1. Click on the Workstation → Desktop tab → IP Configuration
2. Set:
   - IP Address: 203.0.113.20
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 203.0.113.1

Servers:
Configure both servers with IP addresses in their respective networks (Customer: 192.168.1.5, ISP: 203.0.113.10)

3. Configure Switches (Basic Configuration)

For both 2960 switches:

1. Click on the switch → CLI tab
2. Enter these commands:

enable
configure terminal
hostname Customer-Switch (or ISP-Switch for the other)
exit

4. Configure Routers

Customer Router:

1. Click on the router → CLI tab
2. Enter these commands:

enable
configure terminal
hostname Customer-Router
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface Serial0/0/0

ip address 10.0.0.1 255.255.255.252

clock rate 64000 (only if you're using the DCE end of the cable)

no shutdown

exit

ip route 0.0.0.0 0.0.0.0 10.0.0.2

exit

ISP Router:

1. Click on the router → CLI tab
2. Enter these commands:

```
enable
configure terminal
hostname ISP-Router
interface FastEthernet0/0
ip address 203.0.113.1 255.255.255.0
no shutdown
exit
interface Serial0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
exit
ip route 192.168.1.0 255.255.255.0 10.0.0.1
exit
```

5. Test Connectivity

1. From the Customer PC, open Command Prompt (Desktop tab)
2. Try pinging:
   - The Customer Server (192.168.1.5) - should work
   - The ISP Router (10.0.0.2) - should work
   - The ISP Server (203.0.113.10) - should work if all is configured correctly

Troubleshooting Tips

1. If pings fail:
   - Check all cables are properly connected
   - Verify all interfaces are "up" with show ip interface brief on routers
   - Ensure no IP addresses overlap
   - Check default gateways on end devices
2. Useful commands:
   - show running-config - view current configuration
   - ping [IP] - test connectivity
   - tracert [IP] - see path packets take

This basic configuration establishes connectivity between the customer network and ISP network. You can expand on this by adding security (passwords, ACLs), services (DHCP, DNS), or more complex routing protocols.

Experiment-12

Aim of the experiment: To capture and analyze Ethernet frames using Wireshark and understand what happens.

What You'll Need:

- A computer with Wireshark installed.
- Internet access or a network connection.
- Optional: Two PCs connected in a LAN environment for more direct control.

Using Wireshark to Examine Ethernet Frames

This guide will show you how to use Wireshark to capture, analyze, and understand Ethernet frames. By examining frames at the data link layer (Layer 2), you'll gain insights into how networking works at the fundamental level.

Part 1: Wireshark Installation and Setup

Installing Wireshark

1. Download Wireshark from wireshark.org
2. Run the installer with default options
3. When prompted, install WinPcap or Npcap (packet capture libraries)
4. Complete the installation and launch Wireshark

Configuring Wireshark for Ethernet Capture

1. From the Wireshark main screen, select your active network interface (usually Ethernet or Wi-Fi)
2. Click the shark fin icon in the toolbar to start capturing packets
3. Generate some network traffic (browse websites, ping devices, etc.)
4. Click the red square icon to stop the capture

Part 2: Understanding Ethernet Frame Structure

Before diving into analysis, let's understand what components make up an Ethernet II frame:

- **Preamble & SFD**: Signal to receivers that a frame is coming (not shown in Wireshark)
- **Destination MAC**: The hardware address of the intended recipient
- **Source MAC**: The hardware address of the sender
- **Type/Length**: Indicates what protocol is encapsulated in the frame (e.g., 0x0800 for IPv4)
- **Payload**: The actual data being carried (typically an IP packet)
- **FCS**: Frame Check Sequence for error detection (usually not shown in Wireshark)

Part 3: Basic Ethernet Frame Analysis

Identifying and Filtering Ethernet Frames

1. In Wireshark, all captured packets are Ethernet frames by default (on Ethernet networks)
2. Apply a display filter to focus on specific frame types:
    - eth.type == 0x0800 (IPv4 frames)
    - eth.type == 0x0806 (ARP frames)
    - eth.type == 0x86dd (IPv6 frames)

Examining an Ethernet Frame

1. Select any packet in the top pane
2. In the middle pane, expand the "Ethernet II" section
3. You'll see details about:
    - Source MAC address
    - Destination MAC address
    - Type field

Analyzing MAC Addresses

1. Find packets with your computer as the source:
    - Look for your MAC address in the "Source" column
    - Or filter with eth.src == xx:xx:xx:xx:xx:xx (replace with your MAC)
2. Identify broadcast frames:
    - Look for destination MAC ff:ff:ff:ff:ff:ff
    - Or filter with eth.dst == ff:ff:ff:ff:ff:ff
3. Identify multicast frames:
    - First octet has the least significant bit set to 1
    - Filter with eth.dst[0] & 1

Part 4: Practical Frame Analysis Exercises

Exercise 1: Capture and Analyze ARP Frames

1. Clear your ARP cache:
    - Windows: arp -d * in Command Prompt
    - Linux/Mac: sudo arp -d -a in Terminal
2. Start a Wireshark capture
3. Ping a device on your network
4. Stop the capture
5. Filter for ARP packets: arp
6. Examine the:
    - ARP Request: Broadcast frame asking "Who has IP x.x.x.x?"
    - ARP Reply: Unicast frame responding "x.x.x.x is at MAC xx:xx:xx:xx:xx:xx"

Exercise 2: Analyze DHCP Frame Encapsulation

1. Release your IP address:
    - Windows: ipconfig /release in Command Prompt

- Linux: sudo dhclient -r in Terminal
- Mac: System Preferences > Network > Advanced > DHCP > Renew DHCP Lease

2. Start a Wireshark capture
3. Renew your IP address:
    - Windows: ipconfig /renew
    - Linux: sudo dhclient
    - Mac: System Preferences > Network > Advanced > DHCP > Renew DHCP Lease
4. Stop the capture
5. Filter for DHCP: bootp
6. Analyze how the DHCP messages are encapsulated in Ethernet frames
7. Note the progression: DHCP Discover → Offer → Request → Acknowledge

Exercise 3: Compare Different Frame Types

1. Start a new capture
2. Generate diverse traffic:
    - Ping an IPv4 address: ping 8.8.8.8
    - Ping an IPv6 address: ping ipv6.google.com
    - Browse to a website
3. Stop the capture
4. Compare the Ethernet Type fields:
    - IPv4: Type = 0x0800
    - IPv6: Type = 0x86DD
    - ARP: Type = 0x0806

Part 5: Advanced Frame Analysis

Examining Frame Sizes

1. Add the "Length" column to your Wireshark display:
    - Right-click on any column header
    - Select "Column Preferences"
    - Click "+" to add a new column
    - Name it "Length"
    - Field type: "Frame length"
2. Observe different frame sizes:
    - Minimum Ethernet frame: 64 bytes (including headers)
    - Maximum standard frame: 1518 bytes
    - Jumbo frames: >1518 bytes (if supported by your network)
3. Use a filter to find small or large frames:
    - frame.len <= 64 (minimum sized frames)
    - frame.len >= 1518 (maximum sized or jumbo frames)

VLAN Tagged Frames

1. If your network uses VLANs, look for 802.1Q tagged frames:
    - Filter: vlan
2. Examine the VLAN tag:
    - VLAN ID
    - Priority (Class of Service)
    - Note that the Ethernet Type changes to 0x8100 for VLAN tagged frames

MAC Address Analysis

1. Identify the vendor of a device from its MAC address:
    - The first three bytes (OUI - Organizationally Unique Identifier)

- Wireshark resolves this automatically in the "Source" and "Destination" columns

2. Filter frames by vendor:
    - eth.addr contains 00:0c:29 (VMware devices)
    - eth.addr contains 00:50:56 (VMware devices)
    - eth.addr contains 3c:22:fb (Apple devices)

Part 6: Troubleshooting with Ethernet Frame Analysis

Identifying Duplicate MAC Addresses

1. Look for signs of duplicate MACs:
    - Filter: arp.duplicate-address-detected
    - Check for strange ARP behavior

Finding Packet Loss and Retransmissions

1. For TCP connections, look for retransmissions:
    - Filter: tcp.analysis.retransmission
2. Look for fragmentation:
    - Filter: ip.fragments

Analyzing Broadcast Storms

1. Look for excessive broadcast traffic:
    - Filter: eth.dst == ff:ff:ff:ff:ff:ff
2. Check broadcast packet rate:
    - Statistics > I/O Graph
    - Filter: eth.dst == ff:ff:ff:ff:ff:ff

Part 7: Wireshark Tips for Frame Analysis

Colorize Frame Types

1. Go to View > Coloring Rules

2. Create rules based on frame properties:
    - Name: "ARP Frames"
    - Filter: arp
    - Background: Light pink
3. Create similar rules for other Ethernet frame types

Use Statistical Tools

1. Statistics > Protocol Hierarchy
    - Shows distribution of protocols
    - Ethernet is at the top level
2. Statistics > Conversations
    - Select "Ethernet" tab
    - Shows all MAC address pairs communicating

Save and Export Specific Frames

1. Select frames of interest
2. File > Export Specified Packets
3. Choose file format (PCAPNG recommended)
4. Use for documentation or further analysis

Part 8: Advanced Wireshark Features for Frame Analysis

Display Filter Expressions for Ethernet

Common filters for Ethernet frame analysis:

- eth.dst == ff:ff:ff:ff:ff:ff (Broadcast frames)
- eth.addr == xx:xx:xx:xx:xx:xx (Frames to/from specific MAC)
- eth.lg == 0 (Locally administered MAC addresses)
- eth.ig == 1 (Multicast frames)
- eth.type == 0x0800 && ip.ttl < 10 (IPv4 packets with low TTL)

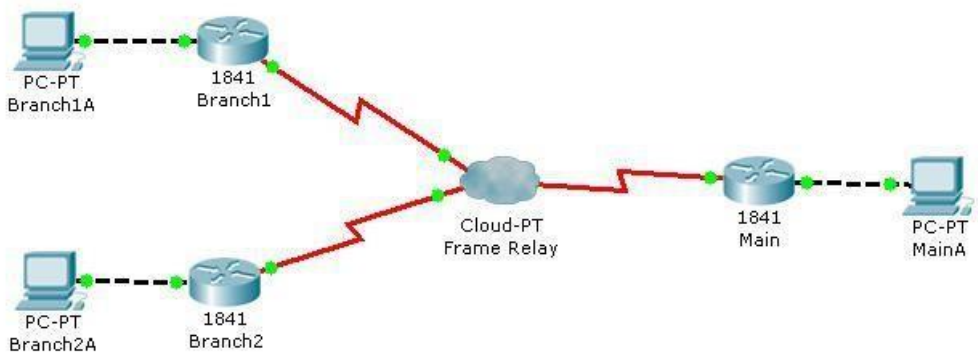
Experiment-13

Aim of the experiment: Study WAN concepts and Configure and forward Traffic in WAN.

Equipment Required:

CISCO Packet Tracer software **Theory:**

Wide Area Network, or WAN, is used to connect physically separated locations on a network. WANs can connect buildings that are across town or across the world on the same network. There are various techniques to do this, but two of the most common are hub and spoke and full mesh networks topologies. Configure and forward Traffic in WAN:



Step 1: Configuration of Branch1 and Branch2 (Switch).

a. Click on Branch1 and use various show commands to view the connectivity to the network. b. Use the show running-configuration command to view the router configuration. c. Use the show ip interface brief command to view the status of the interfaces.

d. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

e. Click on Branch 2 and use various show commands to view the connectivity to the network. f. Use the show running-configuration command to view the router configuration. g. Use the show ip interface brief command to view the status of the interfaces.

h. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.