3RD SEMESTER

B.C.A

COMPUTER NETWORKS LAB

Prepared By:

Bhavya.C

Dept of CSA

St.Francis College

1. Execute the following commands:

arp, ipconfig, hostname, netdiag, netstat, nslookup, pathping, ping route, tracert

These commands are typically executed in a command-line interface (CLI) environment, such as Command Prompt.

1. **arp**: The arp -a command displays the ARP (Address Resolution Protocol) table on your computer. In simple terms, this table shows the list of devices on your local network that your computer has communicated with recently. It maps IP addresses (like a house address) to their corresponding MAC addresses (like a unique ID for each device).

arp -a

2. **ipconfig**: provides a comprehensive overview of your computer's network settings and configurations.

- **IP Address:** It tells you the unique address assigned to your computer on the network. It's like a house number for your computer.
- **Subnet Mask:** This defines the network segment your computer is on, helping to organize and manage networks.
- **Default Gateway:** This is the device (like a router) that your computer uses to connect to other networks, like the internet.
- **DNS Servers:** These are the servers your computer contacts to translate website names into IP addresses, making it easier to connect to websites.
- **MAC Address:** This is a unique identifier for your computer's network hardware, like a fingerprint for your network card.
- **Other Details:** It can also show information about other network settings, like whether DHCP (a system that automatically assigns IP addresses) is enabled.

ipconfig /all

3. **hostname**: Displays the name of the current host (computer).

hostname

4. **netdiag**: It's a useful command for identifying network problems like connectivity issues, incorrect configurations, or domain-related problems. To use it, you typically need to open a command prompt and run netdiag with the desired options. However, in more recent versions of Windows, this command has been largely replaced by other tools like **ipconfig, ping, and tracert.**

netdiag

5. **netstat**: The netstat -an command is used to display network connections and listening ports on your computer.

- **netstat**: This stands for "network statistics" and is a command used to view network connections and statistics.
- **-a**: This option tells netstat to show all active connections and listening ports.
- **-n**: This option makes netstat display the addresses and port numbers in numerical form rather than resolving them to hostnames and service names.

netstat -an

6. **nslookup**: The `nslookup` command is a tool used to find out the IP address associated with a domain name (like `example.com`) or to look up information about a domain name based on its IP address.

- What is the IP address of a website?

- What domain names are associated with a particular IP address?

nslookup www.google.com

7. **ping**: The ping command is like sending a quick "hello" to another computer or device on a network to see if it's there and how long it takes to respond.

1. **Send a Message**: When you use ping, your computer sends a small packet of data to another computer or server.
2. **Wait for a Response**: The receiving computer sends a reply back to your computer.
3. **Measure Time**: ping measures the time it takes for the packet to travel to the other computer and back. This is called latency or ping time.

ping www. google.com

8. **route**: The route print command is used to display the current routing table on a Windows-based computer. It shows the routes that the computer uses to send network traffic to various destinations.

- **Destination Network:** The target network or IP address.
- **Subnet Mask:** Defines the network's size and how addresses within it are allocated.
- **Gateway:** The IP address of the next hop or router to reach the destination network.
- **Interface:** The network interface through which the route is used.
- **Metric:** A value that indicates the cost of using a route (lower values are preferred).

This information helps you understand how your computer is routing traffic and troubleshoot network connectivity issues if they arise.

```
route print
```

9. **tracert**: The `tracert` command (short for "trace route") is used to find out the path data takes from your computer to another computer or website on the internet. It shows each step, or "hop," the data makes along the way, including the time it takes to reach each step. This helps you see if there's a problem with the connection and where it might be occurring.

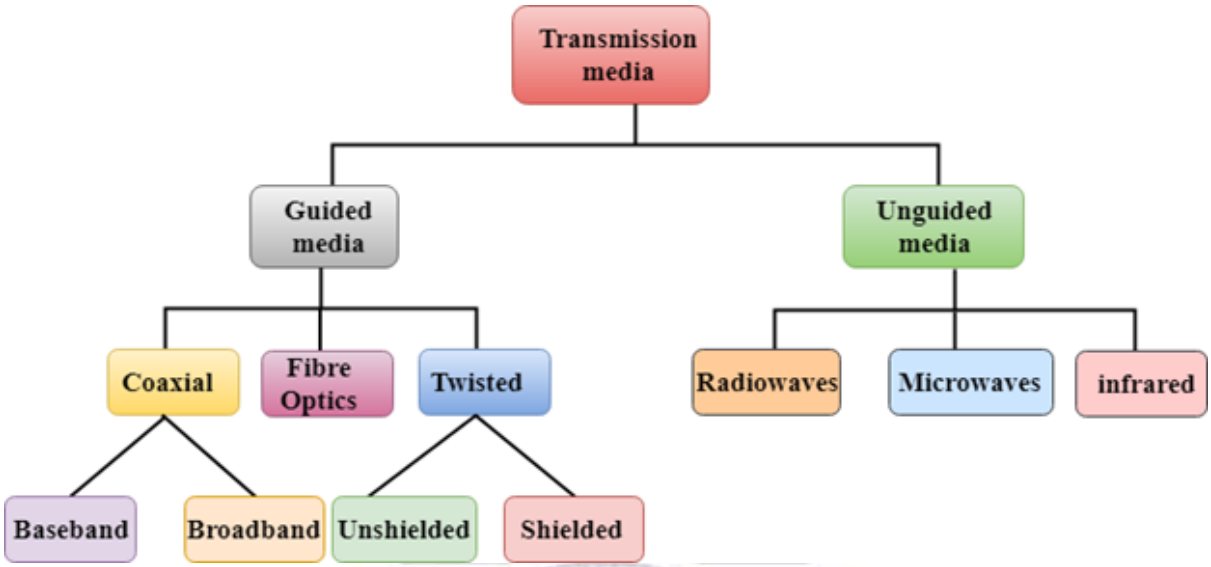
```
tracert www. google.com
```

10. **pathping**: The pathping command is a network diagnostic tool used in Windows. It combines the features of **ping** and **tracert** to help identify problems with network connections.

1. **Ping Part:** It sends packets to each hop (or step) along the route to a target address, like a website.
2. **Tracert Part:** It maps out the path that these packets take from your computer to the target, showing each intermediate stop.

```
pathping www. google.com
```

2. Study of different types of network cables.



Network cables are essential for establishing connections and transmitting data within a network. Here are some common types of network cables used in various networking environments:

1. Guided Media:

- **Definition**: Guided media, also known as wired or bounded media, refers to transmission mediums where data signals are guided along a physical path.
- **Types**:
    - **Twisted Pair Cable**:
        - **Description**: Consists of pairs of insulated copper wires twisted together.
        - **Use**: Commonly used in telephone networks, Ethernet cables (Cat5e, Cat6).
    - **Coaxial Cable**:
        - **Description**: A single copper conductor surrounded by a plastic layer for insulation and a metallic shield.
        - **Use**: Used in cable television networks, and broadband internet connections.
    - **Fiber Optic Cable**:

        - **Description**: Uses light to transmit data through thin strands of glass or plastic fibers.
        - **Use**: High-speed data transmission over long distances, such as in internet backbone connections and cable television.

- **Characteristics**:
    - **Physical Path**: The data travels through a physical medium (cable).
    - **Security**: More secure from interception compared to unguided media.
    - **Speed**: Can support high data transmission speeds, especially with fiber optics.
    - **Distance**: Fiber optics allow for longer distances without significant signal loss.

2. Unguided Media:

- **Definition**: Unguided media, also known as wireless or unbounded media, refers to transmission mediums where data signals are transmitted without a physical path, typically through the air or space.
- **Types**:
    - **Radio Waves**:
        - **Description**: Electromagnetic waves used for wireless communication over short to long distances.
        - **Use**: Used in Wi-Fi, Bluetooth, AM/FM radio, and television broadcasting.
    - **Microwaves**:
        - **Description**: Higher frequency radio waves, typically used for line-of-sight communication.
        - **Use**: Used in satellite communication, cellular networks, and point-to-point communication links.
    - **Infrared Waves**:
        - **Description**: Light waves with frequencies just below visible light.
        - **Use**: Used in remote controls, short-range communication, and some wireless sensors.

- **Characteristics**:

- **No Physical Path**: Data is transmitted through the air, space, or other non-physical mediums.
- **Flexibility**: More flexible in terms of device mobility and placement.
- **Range**: Can vary from short distances (Bluetooth) to long distances (satellite communication).
- **Security**: More susceptible to eavesdropping and interference compared to guided media.
- **Speed and Bandwidth**: Generally lower than guided media, but varies depending on the technology.

- **Baseband** transmission uses the entire bandwidth of the coaxial cable to transmit a single signal or data stream, often directly as digital data. It is typically used in Ethernet networks and other local area networks (LANs).

  Example:

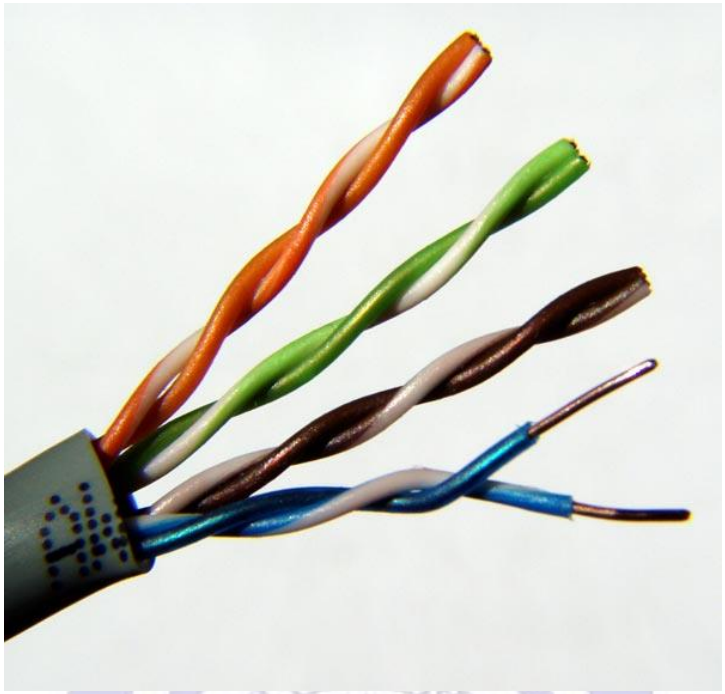
  Ethernet: Early Ethernet networks, particularly those using coaxial cables (like 10BASE2 or 10BASE5), are examples of baseband transmission, where the data is sent as digital signals directly over the cable.

- **Broadband** transmission divides the cable's bandwidth into multiple frequency channels, allowing the simultaneous transmission of multiple signals, such as in cable television and broadband internet services.

  Example:

  Cable Television (CATV): Coaxial cables used in cable TV systems are a common example of broadband transmission. Multiple television channels are transmitted simultaneously, each on a different frequency band.

1. Twisted Pair Cables



a. Unshielded Twisted Pair (UTP)

- Description: Comprises pairs of wires twisted together to reduce electromagnetic interference (EMI).

- Categories:

  - Cat 5: Up to 100 Mbps for 100 meters.

  - Cat 5e: Up to 1 Gbps for 100 meters.

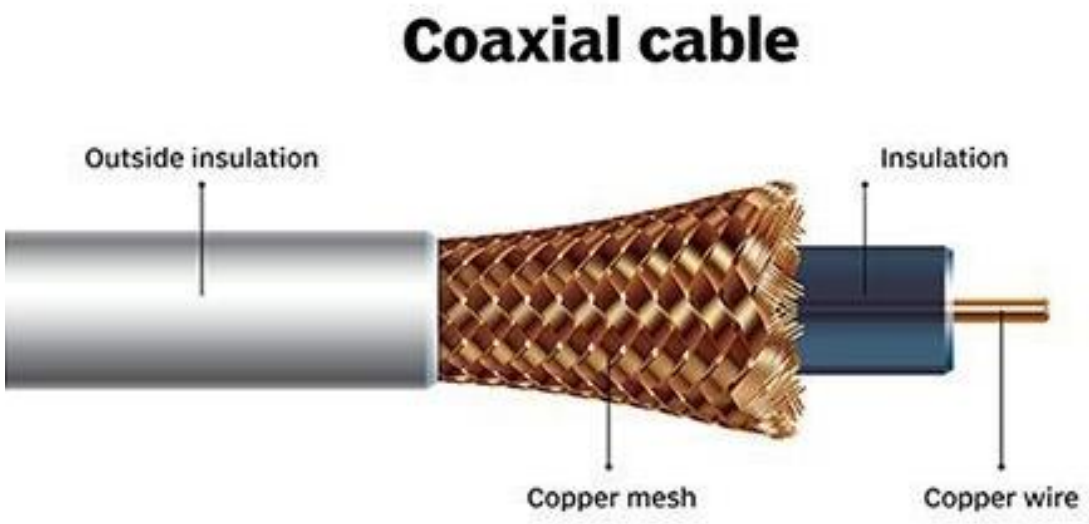
  - Cat 6: Up to 1 Gbps for 100 meters and 10 Gbps for 55 meters.

- Cat 6a: Up to 10 Gbps for 100 meters.
- Cat 7: Up to 10 Gbps for 100 meters, with better shielding.
- Cat 8: Up to 40 Gbps for 30 meters, designed for data centres.

b. Shielded Twisted Pair (STP)

- Description: Similar to UTP but includes shielding to protect from EMI.
- Use Case: Environments with high interference (e.g., industrial settings).

2. Coaxial Cables



- Description: Consists of a central conductor, insulating layer, metallic shield, and outer insulating layer.
- Types:
  - RG-6: Used for cable television, satellite, and broadband internet.
  - RG-59: Used for older cable TV systems, CCTV, and short-run baseband video.

3. Fiber Optic Cables

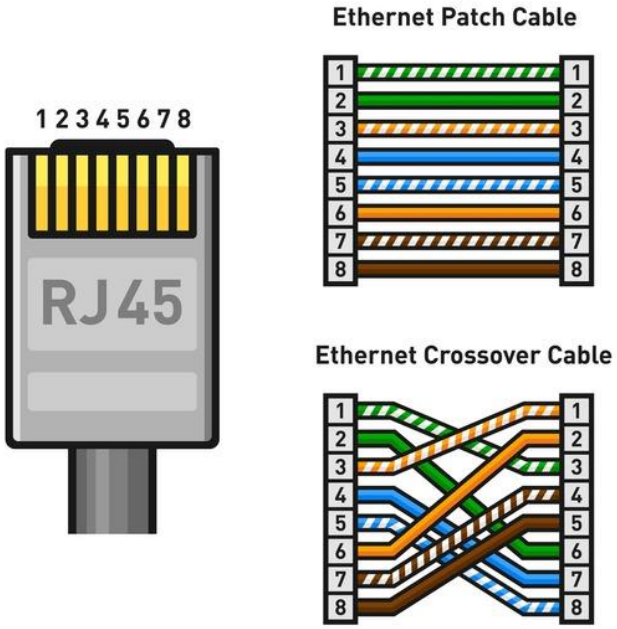
- Description: Transmits data as light pulses through glass or plastic fibers, offering high bandwidth and long-distance transmission.

- Types:

  - Single-mode Fiber (SMF): Small core (8-10 microns), long-distance communication, higher cost.

  - Multi-mode Fiber (MMF): Larger core (50-62.5 microns), shorter distances, lower cost.

4. Ethernet Crossover Cable



- Description: Special type of Ethernet cable used to connect two devices of the same type directly (e.g., two computers without a switch).

- Use Case: Direct device-to-device communication

5. USB Cables

- Description: Universal Serial Bus cables used for data transfer and power supply between computers and peripheral devices.

- Types: USB-A, USB-B, USB-C, USB 3.0, USB 3.1, USB 3.2, USB4.

7. Power over Ethernet (PoE) Cables

- Description: Ethernet cables that also carry electrical power to devices such as IP cameras, wireless access points, and VoIP phones.

- Standards: IEEE 802.3af (PoE), IEEE 802.3at (PoE+), IEEE 802.3bt (PoE++).

Choosing the Right Cable

When choosing a network cable, consider factors such as:

- Data Transfer Speed: Higher categories of UTP cables (Cat 6 and above) or fiber optic cables for high-speed requirements.

- Distance: Fiber optic cables for long distances, UTP/STP for shorter distances.

- Environment: STP cables for high interference areas, rugged cables for industrial environments.

- Cost: Balance between performance requirements and budget constraints.

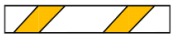
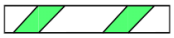
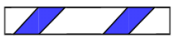
3. Practically implement the cross-wired cable and straight wired cable using crimping tool.

To study different types of network cables and implement cross-wired and straight-through cables using a crimping tool.

Requirements:
Crimping tool, UTP cable, RJ-45 connectors, cable tester.

Steps:

1. **Understand the Cable Types:**
    - Straight-through cable: Both ends are wired using the same standard (T568A or T568B).
    - Cross-wired cable: One end uses T568A, and the other uses T568B.
2. **Cut the Cable:**
    - Measure and cut the UTP cable to the desired length using a cable cutter.
3. **Strip the Cable:**
    - Remove about 1 inch of the cable jacket from both ends using a cable stripper.
4. **Untwist and Arrange Wires:**
    - **For straight-through:** Arrange wires on both ends in the same sequence (T568A or T568B).
    - **For cross-wired:** Arrange one end as T568A and the other as T568B.
    - **Wire Colors in the Cable:**
        1. **White-Orange**
        2. **Orange**
        3. **White-Green**
        4. **Blue**
        5. **White-Blue**
        6. **Green**
        7. **White-Brown**
        8. **Brown**

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	

Crossover Ethernet Cable Pin Outs

- **T568A and T568B Arrangements:**

  T568A Wiring Order (from left to right, pins 1 to 8 on the RJ45 connector):

  1. White-Green
  2. Green
  3. White-Orange
  4. Blue
  5. White-Blue
  6. Orange
  7. White-Brown
  8. Brown

- **T568B Wiring Order (most common for general use):**

  1. White-Orange
  2. Orange
  3. White-Green
  4. Blue
  5. White-Blue
  6. Green

7. White-Brown
8. Brown

- **Choosing Between T568A and T568B:**

✓ Use **T568A** if you are following a structured cabling standard, as it's often used in government and residential installations.

✓ Use **T568B** for most commercial and general networking setups.

✓ If both ends of your cable follow the same standard, you'll create a **straight-through cable**. If one end uses T568A and the other uses T568B, you'll create a **crossover cable**, used for connecting similar devices directly.

5. **Trim and Insert Wires:**
   - Trim the wires to the same length and insert them into the RJ-45 connectors.
6. **Crimp the Connector:**
   - Place the RJ-45 connector into the crimping tool and press firmly to secure the wires.
7. **Repeat for the Other End:**
   - Follow the same steps to attach the connector to the other end of the cable.
8. **Test the Cable:**
   - Use a cable tester to verify continuity and proper wiring for the straight-through or cross-wired cable.

Observation:

- Straight-through cable: Pins match on both ends (e.g., Pin 1 to Pin 1).
- Cross-wired cable: Certain pins are crossed (e.g., Pin 1 to Pin 3, Pin 2 to Pin 6).

Conclusion:

You have successfully created and tested straight-through and cross-wired network cables!

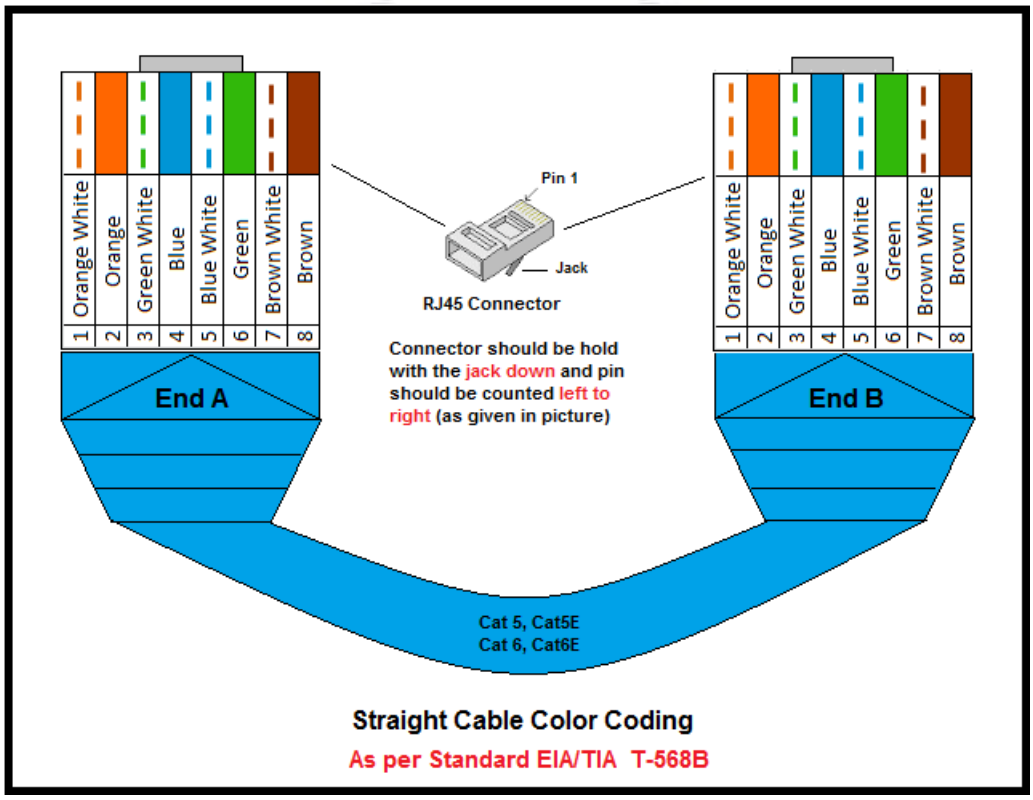
Crimping Tools:

UTP Cables:

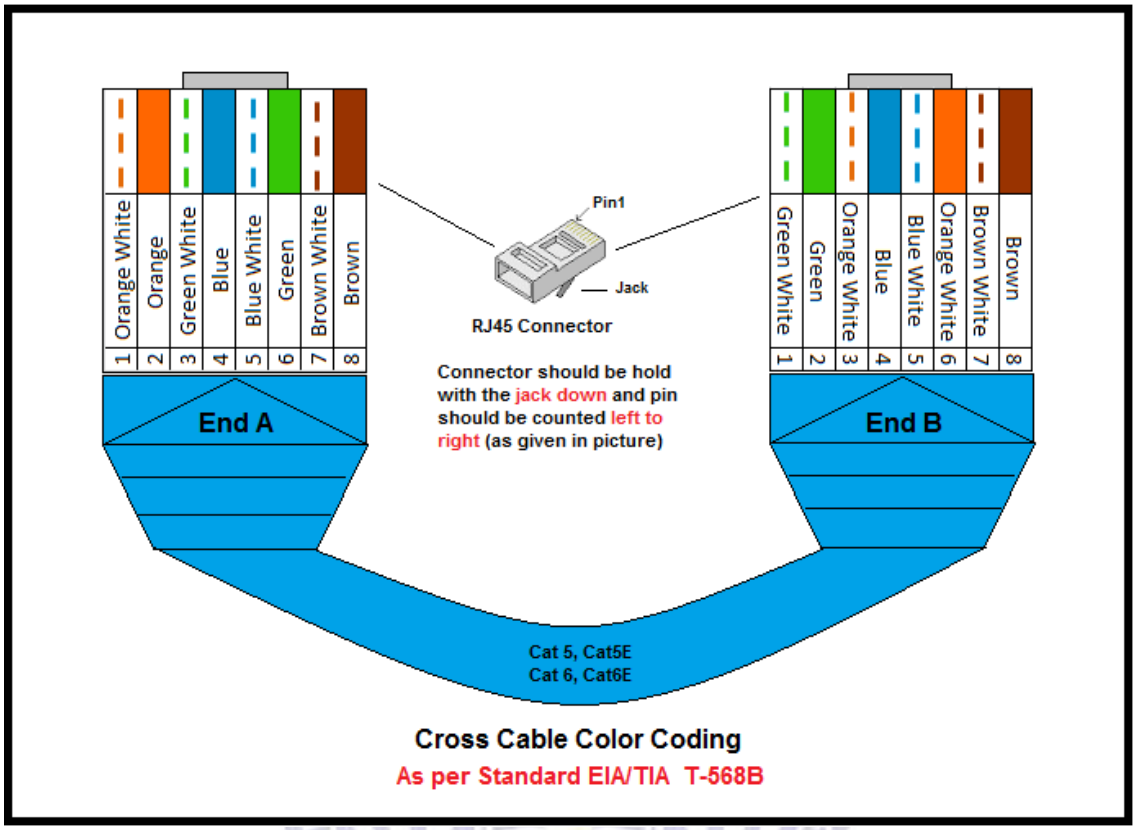
RJ-45 Connector:

Cable test:

Straight cable:



Cross cable:


Orange White
Orange
Green White
Blue
Blue White
Green
Brown White
Brown
1 2 3 4 5 6 7 8
End A
Pin1
Jack
RJ45 Connector
Connector should be hold with the jack down and pin should be counted left to right (as given in picture)
Green White
Green
Orange White
Blue
Blue White
Orange White
Brown White
Brown
1 2 3 4 5 6 7 8
End B
Cat 5, Cat5E
Cat 6, Cat6E
Cross Cable Color Coding
As per Standard EIA/TIA T-568B

4. Study of network IP address configuration: (Classification of address, static and dynamic address)

What is an IP Address?

An IP address (Internet Protocol address) is a unique number assigned to every device connected to a network, whether it's a computer, smartphone, printer, or router.

Static IP Address

A **static IP address** is manually assigned to a device and does not change unless manually modified. It's like assigning a permanent home address to a device.

Features:

- **Manual Assignment**: Requires an administrator to configure it.
- **Doesn't Change**: Once assigned, the device keeps the same IP address.
- **Common Uses**:
    - Servers that need to be consistently reachable (e.g., web servers, file servers).
    - Devices that need to maintain a fixed identity in the network, such as printers or security cameras.

Dynamic IP Address

A **dynamic IP address** is automatically assigned by a **DHCP server** (Dynamic Host Configuration Protocol) whenever a device connects to the network. Most home networks and small offices use dynamic IP addresses.

Features:

- **Automatic Assignment**: Devices automatically receive an IP address from the DHCP server.
- **Can Change**: The IP address may change after the device disconnects or if the DHCP lease expires.
- **Common Uses**:
    - Home and office devices like laptops, smartphones, and tablets that don't require a fixed IP address.
    - Any device that doesn't need to be consistently reachable at the same address.

5. Study of network IP address configuration: (IPv4 and IPv6 , Subnet, Supernet)

IPv4 (Internet Protocol version 4): IPv4 is the most commonly used version of the Internet Protocol and has been the foundation of network communication for decades.

Key Characteristics of IPv4:

- **Address Format:** IPv4 addresses are 32-bit numbers, represented as four octets (8-bit blocks) separated by dots (also called dotted decimal notation).
    - Example: 192.168.1.1
- **Address Space:** IPv4 supports around 4.3 billion unique addresses (2^32).
- **Depletion of Addresses:** Due to the rapid growth of devices connected to the internet, IPv4 addresses have become scarce. Techniques like NAT (Network Address Translation) and private IP addressing have been implemented to extend the life of IPv4.
- **Common Use:** Despite the development of IPv6, IPv4 is still widely used in most networks today, especially in private networks.
- **Example of IPv4 Address:**

    192.168.0.1: A typical home router IP.

    Subnet Mask: Common subnet mask 255.255.255.0

IPv6 (Internet Protocol version 6): IPv6 was developed to overcome the limitations of IPv4, particularly the exhaustion of addresses.

Key Characteristics of IPv6:

- **Address Format:** IPv6 addresses are 128-bit numbers, represented in hexadecimal format and separated by colons.
    - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- **Address Space**: IPv6 supports an enormous number of addresses (approximately 340 undecillion addresses, or 2^128), making it virtually impossible to run out of addresses.
- **No NAT Needed:** Since there are plenty of addresses, IPv6 doesn't rely on NAT (Network Address Translation) as IPv4 does.

What is Subnetting?

Subnetting is the process of dividing a large network into smaller, more manageable subnetworks, or subnets. This helps improve network efficiency, security, and address management.

Efficient IP Address Usage: Subnetting allows better allocation of IP addresses. For example, instead of wasting addresses in a large network, you can divide it into subnets based on the actual number of devices (hosts) needed.

Example:

- **Original Network**: You have the IP address block **192.168.1.0/24**. This means:
  - **Total Addresses**: 256 (from 192.168.1.0 to 192.168.1.255)
  - **Usable Addresses**: 254 (after subtracting 2 for network and broadcast addresses).
- **Subnetting**: You decide to divide this network into smaller subnets to keep things organized and manage traffic better. You want to create **2 subnets**:
  - **Subnet 1**:
    - **Network Address**: **192.168.1.0/26**
    - **Usable Addresses**: 62 (from 192.168.1.1 to 192.168.1.62)
    - **Broadcast Address**: 192.168.1.63
  - **Subnet 2**:
    - **Network Address**: **192.168.1.64/26**
    - **Usable Addresses**: 62 (from 192.168.1.65 to 192.168.1.126)
    - **Broadcast Address**: 192.168.1.127

What is Supernetting?

Supernetting is the opposite of subnetting. Instead of dividing a network into smaller subnets, supernetting combines multiple networks (subnets) into a larger network. This is also known as CIDR (Classless Inter-Domain Routing) aggregation.

Scenario: You manage multiple small networks for different departments in a company. Each department has its own network:

- Department A: 192.168.2.0/26 (64 addresses)
- Department B: 192.168.2.64/26 (64 addresses)

- Department C: 192.168.2.128/26 (64 addresses)
- Department D: 192.168.2.192/26 (64 addresses)

Total: You have 4 small networks that you want to combine to simplify management.

1. Supernetting: You decide to aggregate these four networks into a single larger network:
    - Combined Network:
        - Network Address: 192.168.2.0/24
        - Total Addresses: 256 (from 192.168.2.0 to 192.168.2.255)
        - Usable Addresses: 254 (after subtracting 2 for network and broadcast addresses).

6. Study of network devices: (Switch, Router, Bridge)

1. Router

- **What It Does:** A router directs data between different networks. It connects multiple networks together, such as a home network and the internet.
- **Example:** The device in your home that connects your computer or smartphone to the internet. It ensures that your request to visit a website is sent to the correct place.

2. Switch

- **What It Does:** A switch connects multiple devices within a single network, like a LAN (Local Area Network). It allows these devices to communicate with each other.
- **Example:** In an office, a switch connects all the computers so they can share files and access the same printer.

3. Bridge

- **What It Does:** A bridge connects two separate networks and allows them to function as a single network. It filters traffic between the two networks.
- **Example:** If you have two separate LANs in different parts of a building, a bridge can connect them so they act like one big network.

7. Configure and connect the computer in LAN.

1. Launch Cisco Packet Tracer:

Open the Cisco Packet Tracer application on your computer.

2. Create a Simple Network Topology:

- Select End Devices from the device types.
- Drag and drop PCs (end devices) onto the workspace. Place as many PCs as you want to connect.
- Drag and drop a Switch onto the workspace. Use the 2960 switch (which is common for LAN).

1. **Connecting Devices:**

- Select the Connections tab.
- Choose the Copper Straight-Through Cable (represented by a solid line).
- Click on the first PC, then select FastEthernet0 (network interface) as the port.
- Next, click on the switch and select any FastEthernet port (e.g., FastEthernet0/1) to connect the PC to the switch.
- Repeat this process to connect all other PCs to the switch via different ports.

2. **Configure IP Addresses:** Assign each computer a unique IP address within the same network.

- Click on the first PC.
- Go to the Desktop tab and select IP Configuration.
- Enter the IP address and subnet mask. Example:
    - **IP address: 192.168.1.2**
    - **Subnet mask: 255.255.255.0**
- Repeat the process for each PC, assigning them different IPs (e.g., 192.168.1.3, 192.168.1.4, etc.), but use the same subnet mask.

3. Verify Connections:

- Use the Command Prompt on one of the PCs to verify connectivity.
- Open Command Prompt on one PC by selecting the Desktop tab -> Command Prompt.
- Type the following command to ping another PC's IP address: **ping 192.168.1.3**
- **If you receive replies, the connection is successful,** meaning the computers are properly connected in a LAN.

8. Block the website using "Windows Defender Firewall" in windows 10.

Step 1: Launch the Control Panel on your computer.

Step 2: Select System and Security.

Step 3 : Select "Windows Defender Firewall" followed by "Advanced Settings" on the left-side pane.

Step 4: Right-click on "Outbound Rules" from the menu on the left and select "New Rule."

Step 5: When a new window pops up, select the "Custom" option followed by "Next."

Step 6: On the next window, select "All programs" and again select "Next."

Step 7: Select the " These IP addresses " option under "Which remote IP addresses does this rule apply to?" and click next

Step 8: Open the Command Prompt as Administrator by entering "CMD" into the search box.

Step 9: Enter "nslookup www.facebook.com" and press the Enter button.

Step 10: Click on "Add" and enter the IP addresses you want to block. Then select "Next."

Step 11: Make sure to choose the "Block the connection" option and click on "Next."

Step 12: Step 11: Choose whether the rule applies to Domain, Private, or Public. You can also select all three.

Step 13: Select "Next," add a name or description for this rule, and select "Finish" to complete the action.

Step 14: Finish , Check for Blocked website

9. Share the folder in a system, and access the files of that folder from other system using IP address.

Windows to Windows Sharing

Step 1: Enable File Sharing

1. Open **Control Panel → Network and Sharing Center**.
2. Click on **Change advanced sharing settings**.
3. Under **Private**, ensure the following are enabled:
    - **Turn on network discovery**
    - **Turn on file and printer sharing**
    - **Turn off password-protected sharing** (optional if you want access without needing credentials)

Step 2: Share the Folder

1. Right-click the folder you want to share.
2. Select **Properties → Sharing** tab.
3. Click **Advanced Sharing**.
4. Check **Share this folder**, then click **Permissions** and configure the access permissions (e.g., Read, Write).
5. Click **OK** and close the window.

Step 3: Obtain the IP Address

1. Open **Command Prompt**.
2. Type **ipconfig** and press **Enter**.
3. Look for the **IPv4 Address** (e.g., 192.168.1.x).

Step 4: Access the Folder from Another System

1. On the second system, open **File Explorer**.
2. In the address bar, type **\\[IP Address]** (e.g., \\192.168.1.x) and press **Enter**.
3. You should now see the shared folder. You may need to enter credentials if password protection is enabled.

OR

1. On the second system, open **RUN / windows+R**.
2. Type **\\[IP Address]** (e.g., \\192.168.1.x) and press **OK**.
3. You should now see the shared folder. You may need to enter credentials if password protection is enabled.

10.Share the printer in Network, and take print from other PC.

Step 1: Set Up the Devices

1. **Add Devices to the Workspace:**
    - Drag and drop a printer (e.g., a generic printer) and two PCs onto the workspace.
    - Add a switch to the workspace to connect the devices.
2. **Connect the Devices:**
    - Use Copper Straight-Through cables to connect each PC and the printer to the switch.

Step 2: Assign IP Addresses

1. **Configure IP Addresses on Each PC:**
    - Click on PC0 > Desktop > IP Configuration.
        - Assign an IP address, such as 192.168.1.2.
        - Set the subnet mask to 255.255.255.0.
    - Repeat for PC1 with an IP address, e.g., 192.168.1.3.
2. **Assign IP Address to the Printer:**
    - Click on the Printer > Config > Settings.
        - Assign an IP address, such as 192.168.1.10.
        - Set the subnet mask to 255.255.255.0.

Step 3: Set Up Printer on PC0 and PC1

1. Test the Printer Connection on PC0 and PC1:
    - Go to PC0 > Desktop > Command Prompt.
    - Ping the printer using the command: **ping 192.168.1.10**
    - Ensure the printer is reachable.
    - Follow the same steps on PC1 also.

11.Configuration of wifi hotspot, and connect other devices (mobile / laptop).

Step 1: Set Up a Wireless Router

1. Add a Wireless Router:
    - In Cisco Packet Tracer, go to the Network Devices section and drag a Wireless Router (e.g., WRT300N) onto the workspace.
2. Configure the Wireless Router:
    - Click on the router, go to the Config or GUI tab.
    - Under the Wireless settings:
        - Set the SSID (e.g., "SFCwifi").
        - Choose a security mode (e.g., WPA2-PSK for stronger security).
        - Set a Pre-Shared Key (12345678).
    - Configure other parameters as needed (e.g., DHCP settings to provide IP addresses automatically to devices).

Step 2: Set Up a Device to Connect to Wi-Fi (e.g., Laptop or Smartphone)

1. Add a Laptop or Smartphone:
    - Go to the End Devices section and drag a Laptop or Smartphone onto the workspace.
2. Connect the Device to Wi-Fi:
    - Click on the device and go to the Desktop tab (for laptops) or Config tab (for smartphones).
    - Select the PC Wireless or Smartphone Wireless configuration.
    - Search for available networks. Select the SSID you configured (e.g., "SFCwifi") and enter the pre-shared key to connect.

Step 3: Test the Connection

1. Verify Connectivity:
    - Once connected, try pinging the router's IP address from the device to confirm it's connected to the Wi-Fi network.

12.Configuration of switches.

1. Configure password (For Login to Switch)

Enable for switch configuration steps

Step - 1 Switch> EN or Enable

Step - 2 Switch# Config t / configuration terminal

Step -3 Switch(config)#line console 0 / con 0

Step -4 Switch(config-line)#password 1234

Step -5 Switch(config-line)#login

Step -6 Switch(config-line)# Exit

Step -7 Switch(config)#Exit

Step -8 Switch# Exit

2. Configure password for configuration switch

Step - 1 Switch> EN or Enable

Step - 2 Switch# Config t / configuration terminal

Step -3 Switch(config)# enable secret 123456

Step -4 Switch(config)# Exit

Step -5 Switch# Exit

To check for configuration password (i.e Login to Switch) First need to enter console password

User Access Verification

Password: (Login password)

Switch> En /Enable

Password: (Configuration password i.e Secret password)

Switch#

3. Configure Switch hostname as St.Francis

Step -1 Switch# configure t

Step -2 Switch(config)# hostname **St.Francis**

Step -3 **St.Francis** (config)#

4. Configure the message of the day as "Welcome to St.Francis College"

Step -1 **St.Francis** (config)#banner motd #

" Welcome to St.Francis College "

Step - 2 **St.Francis** (config)# Exit (To check the message exit from the configuration)

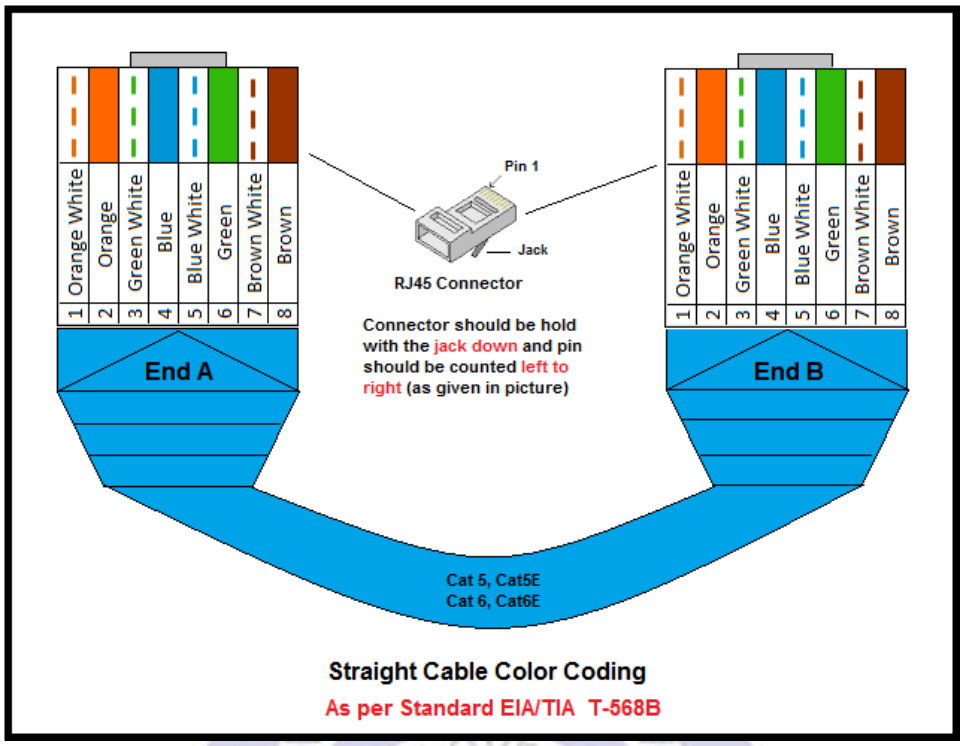
Step - 3 **St.Francis** # Exit

14.Making your own patch cord.

Making a Patch Cord focuses only on straight-through cables. "Patch Cord" emphasizes making a neat, standard connection for devices within a network.

For straight-through: Arrange wires on both ends in the same sequence (T568A or T568B).

1. **Gather Materials:**
   - Ethernet cable (e.g., Cat5e or Cat6).
   - RJ45 connectors.
   - Crimping tool.
   - Cable cutter/stripper.
   - Network tester (optional, but recommended).
2. **Cut Cable:**
   - Measure and cut the cable to the desired length using the cable cutter.
3. **Strip Cable Jacket:**
   - Remove about 1 inch of the cable jacket from both ends using a cable stripper.
4. **Organize Wires:**
   - Untwist and arrange the wires according to the T568A or T568B standard.
   - Ensure all wires are straight and cut to an even length.
   - **Wire Colors in the Cable:**
     1. **White-Orange**
     2. **Orange**
     3. **White-Green**
     4. **Blue**
     5. **White-Blue**
     6. **Green**
     7. **White-Brown**
     8. **Brown**



- **T568B Arrangements:**
- **T568B Wiring Order (most common for general use):**
    1. White-Orange
    2. Orange
    3. White-Green
    4. Blue
    5. White-Blue
    6. Green
    7. White-Brown
    8. Brown

5. **Insert Wires into RJ45 Connector:**
    - Push the wires into the RJ45 connector in the correct order until they reach the end.
6. **Crimp the Connector:**
    - Place the connector into the crimping tool and press firmly to secure the wires in place.

7. **Repeat for the Other End:**
    - Follow the same steps for the second connector on the other end of the cable.
8. **Test the Cable:**
    - Use a network tester to check for continuity and ensure the wiring is correct.

15.Configuration of VLAN using Packet Tracer/ GNS3

A VLAN (Virtual Local Area Network) is a way to divide a network into smaller, isolated sections, even though they all share the same physical hardware. It allows you to create separate "networks" within a single switch or network infrastructure.

In the example below:

- **We created two separate groups of devices: PCs on the 192.12.1.x network and PCs on the 192.12.20.x network.**
- **VLAN 20 was set up to logically separate PCs (PC2 and PC3) from the rest of the network.**
- **Devices on VLAN 20 can only communicate with other devices within the same VLAN unless a router allows traffic between VLANs.**

Step 1: Set up the hardware.

- Deploy four PCs, one router (Cisco 1841 model), and one switch (Cisco 2960) in the simulation environment.

Step 2: Connect PCs to the Switch.

- Use copper straight-through cables to connect each PC to the switch.
- Steps:
    - Select the cable.
    - Click on PC0, select FastEthernet 0.
    - Connect it to Switch on FastEthernet 0/1.
    - Repeat this process for the other PCs, connecting each to a different FastEthernet port on the switch.

Step 3: Connect the Router to the Switch.

- Connect the router to the switch using a copper straight-through cable.
- Steps:
    - Click on the switch, select FastEthernet 0/5.
    - Connect it to the router's FastEthernet 0/0.

Step 4: Configure the Router Interface.

- Set up the IP address on the router.
- Steps:

- Click on the router, go to the Config tab, select FastEthernet 0/0.
- Set the IP address to 192.12.1.1.
- Enable the port status (turn it ON).

Step 5: Configure PC0.

- Set IP configuration on PC0.
- Steps:
  - Go to the Config tab, select FastEthernet 0.
  - Set the IP address to 192.12.1.2.
  - In the Settings tab, set the default gateway to 192.12.1.1 (router's IP).

Step 6: Configure PC1.

- Set IP configuration on PC1.
- Steps:
  - Set the IP address to 192.12.1.3.
  - Set the default gateway to 192.12.1.1(router's IP)..

Step 7: Configure PC2.

- Set IP configuration on PC2.
- Steps:
  - Set the IP address to 192.12.20.2.
  - Set the default gateway to 192.12.20.1.

Step 8: Configure PC3.

- Set IP configuration on PC3.
- Steps:
  - Set the IP address to 192.12.20.3.
  - Set the default gateway to 192.12.20.1.

Step 9: Create VLAN 20 on the Router.

- Set up VLAN 20 in the router's VLAN database.
- Steps:
  - Click on the router, go to the Switching menu, and select VLAN database.
  - Set VLAN number to 20 and VLAN name to LAN-1.

- Click Add to create the VLAN.

Step 10: Configure a Subinterface for VLAN 20 on the Router.

- Enable subinterface routing on the router for VLAN 20.
- Commands:

```
Router#config t
Router(config)#int f0/0.1
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.12.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
```

- Explanation:
  - int f0/0.1: Creates a subinterface for VLAN 20 on FastEthernet 0/0.
  - encapsulation dot1q 20: Tags the subinterface for VLAN 20.
  - ip address 192.12.20.1 255.255.255.0: Assigns an IP to the subinterface.

Step 11: Assign VLAN 20 to Switch Port FastEthernet 0/3.

- Go to the switch's configuration, set FastEthernet 0/3 to VLAN 20.
- Steps:
  - Click on the switch, go to the Config tab.
  - Select FastEthernet 0/3, set VLAN to 20, and click Add.

Step 12: Assign VLAN 20 to Switch Port FastEthernet 0/4.

- Repeat Step 11 for FastEthernet 0/4.

Step 13: Test Connectivity with Ping.

- Verify that devices on the same VLAN (VLAN 20) can communicate.(PC2 and PC3)
- Example: From PC2, ping 192.12.20.3 (PC3's IP).

16.Configuration of VPN using Packet Tracer/ GNS3

A VPN (Virtual Private Network) is a secure way to connect to the internet by creating a private "tunnel" for your data, protecting it from being seen by others. It also helps you access content and websites as if you are in a different location by masking your real IP address.

Step 1 : 02 PC's, 03 Routers (1841)

Step 2 : Connect PC0 to Router0 and PC1 to Router2 using copper straight-through cables and also connect Router1 with Router0 and Router2.

Step 3 : Assign IP Addresses to PCs
On **PC0**, configure the IP address as **192.168.1.2** and the gateway as **192.168.1.1**.
On **PC1,** configure the IP address as **192.168.2.2** and the gateway as **192.168.2.1**.

Step- 4: Router Interface Configuration

1. **Router0 Configuration:**
   Assign the following IPs:

- FastEthernet0/0: **192.168.1.1**
- FastEthernet0/1: **1.0.0.2**

- **Type the following in CLI:**

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 1.0.0.2 255.255.255.0
Router(config-if)# no shutdown
```

2. **Router1 Configuration:**
   Assign the following IPs:

- FastEthernet0/0: **1.0.0.1**
- FastEthernet0/1: **2.0.0.1**

- **Type the following in CLI:**

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 1.0.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 2.0.0.1 255.255.255.0
Router(config-if)# no shutdown
```

3. **Router2 Configuration:**
   Assign the following IPs:

- FastEthernet0/0: **192.168.2.1**
- FastEthernet0/1: **2.0.0.2**

- **Type the following in CLI:**

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 2.0.0.2 255.255.255.0
Router(config-if)# no shutdown
```

Step 5: Configure Static Routes

1. **Router0 Static Route:**
   Add a default route pointing to Router1:

   Network: 0.0.0.0

   Mask: 0.0.0.0

   Next Hop: 1.0.0.1

2. **Router2 Static Route:**
   Add a default route pointing to Router1:

   Network: 0.0.0.0

   Mask: 0.0.0.0

   Next Hop: 2.0.0.1

Step 6: Create a Tunnel

1. **Router0 Tunnel Configuration:**
   Create a tunnel interface with the following settings:
   - **IP Address: 172.16.1.1**
   - **Tunnel Source: FastEthernet0/1**
   - **Tunnel Destination: 2.0.0.2**

- **Type the following in CLI:**

  Router(config)# interface tunnel 1

  Router(config-if)# ip address 172.16.1.1 255.255.0.0

  Router(config-if)# tunnel source FastEthernet0/1

  Router(config-if)# tunnel destination 2.0.0.2

  Router(config-if)# no shutdown

2. **Router2 Tunnel Configuration:**
   Create a tunnel interface with the following settings:
   - **IP Address: 172.16.1.2**
   - **Tunnel Source: FastEthernet0/1**
   - **Tunnel Destination: 1.0.0.2**

- **Type the following in CLI:**

  Router(config)# interface tunnel 2

  Router(config-if)# ip address 172.16.1.2 255.255.0.0

  Router(config-if)# tunnel source FastEthernet0/1

  Router(config-if)# tunnel destination 1.0.0.2

  Router(config-if)# no shutdown

Step 7: Configure Static Routes for VPN Traffic

1. **Router0 VPN Route:**
   Add a static route to reach the 192.168.2.0/24 network via the tunnel:

   Network: 192.168.2.0

   Mask: 255.255.255.0

   Next Hop: 172.16.1.2
2. **Router2 VPN Route:**
   Add a static route to reach the 192.168.1.0/24 network via the tunnel:

   Network: 192.168.1.0

   Mask: 255.255.255.0

   Next Hop: 172.16.1.1

Step 8: Verification

1. **Ping Test from PC0:**
   On PC0, test connectivity to PC1: **ping 192.168.2.2**
2. **Traceroute Test:**
   On PC0, trace the route to PC1 to verify the VPN tunnel: **tracert 192.168.2.2**