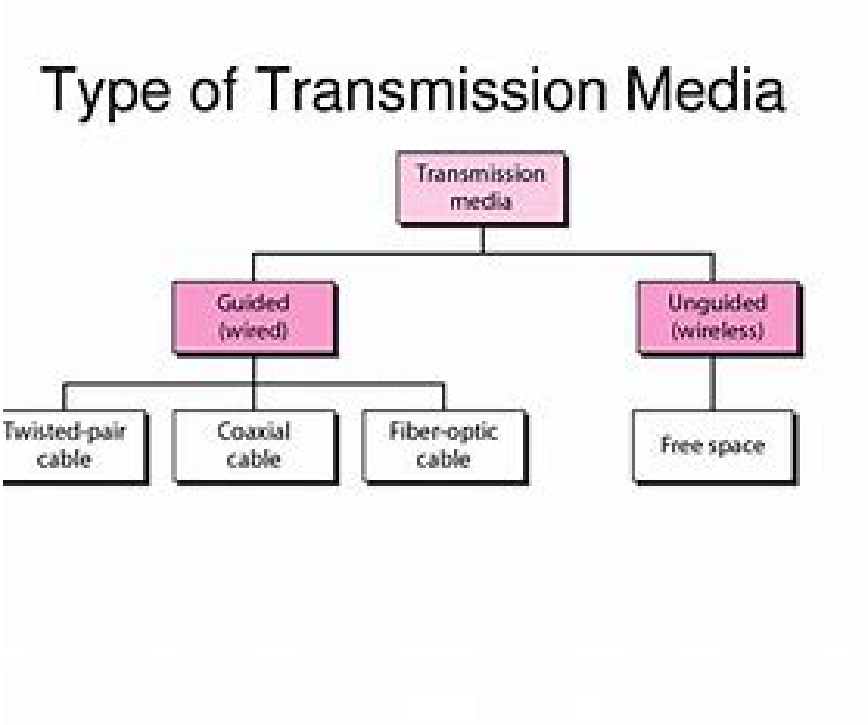
Hello Network

▼ *What is a Network?*

A *network* is a connection between two or more devices that communicate with each other through a communication medium. This medium can be *wired* or *wireless*:

- *Wired*: Examples include twisted pair cables and fiber optic cables.
- *Wireless*: Examples include radio waves.



▼ *Key Concepts in Networking*

Before diving into how devices communicate, it's important to understand some essential concepts:

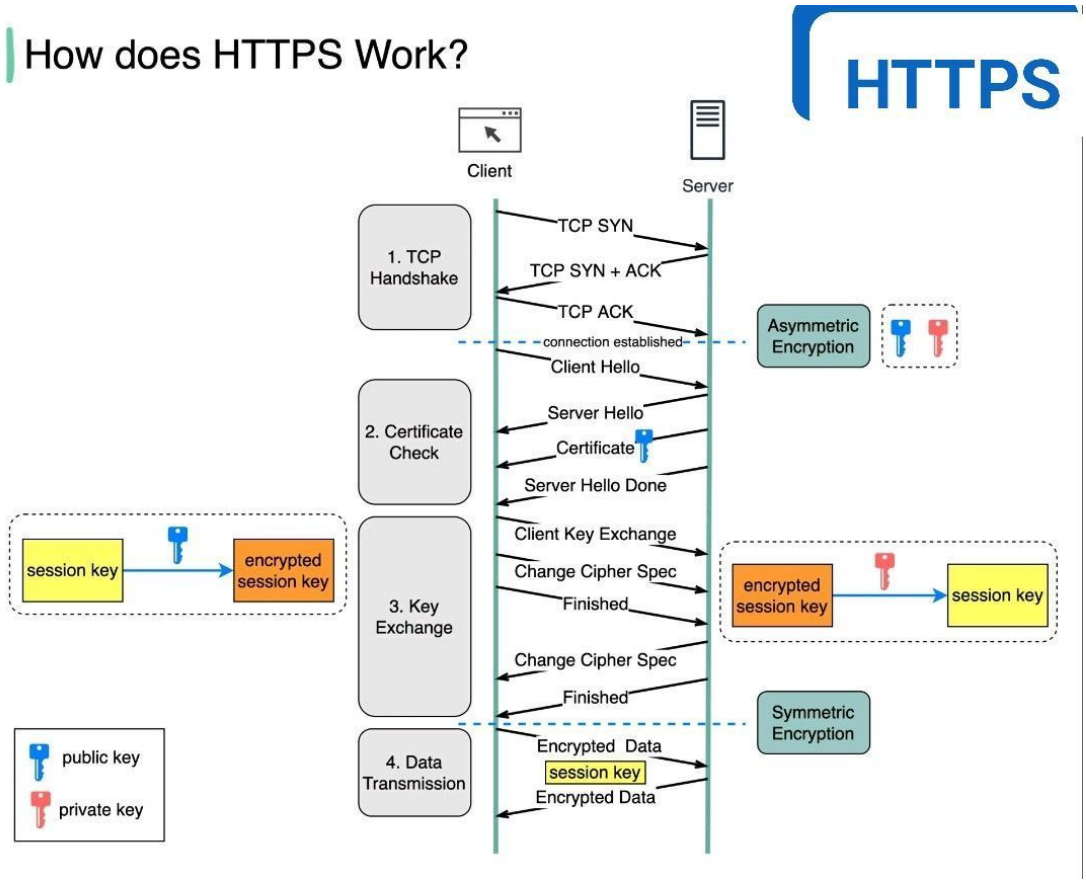
1. *Basic Network Components*:
    - *Device*: A computer, smartphone, or any other gadget communicating over a network.
    - *Network Card*: An adapter that allows a device to connect to a network.
    - *Router*: An optional device that directs data between networks. It is required for connecting different networks.
    - *Cable*: Required in wired networks to physically connect devices.
    - *Frequency*: Needed in wireless networks for communication.
2. *Online vs. Offline*:
    - *Online*: A device that is actively sending and receiving data on the network.
    - *Offline*: A device that is not sending or receiving any data.

3. *Up and Running*:
    - Indicates that a specific hardware component is functioning correctly.
4. *Local Network*:
    - A network where devices communicate with each other without leaving the same network. Example: LAN (Local Area Network).
5. *Remote*:
    - Refers to a device on one network communicating with a device on another network.
6. *Internet*:
    - It is a heterogeneous network that allows information exchange, meaning different devices and networks can communicate with each other.
7. *Bandwidth*:
    - The amount of data that can be transmitted over a network in a given time.

▼ *Understanding the OSI Model*

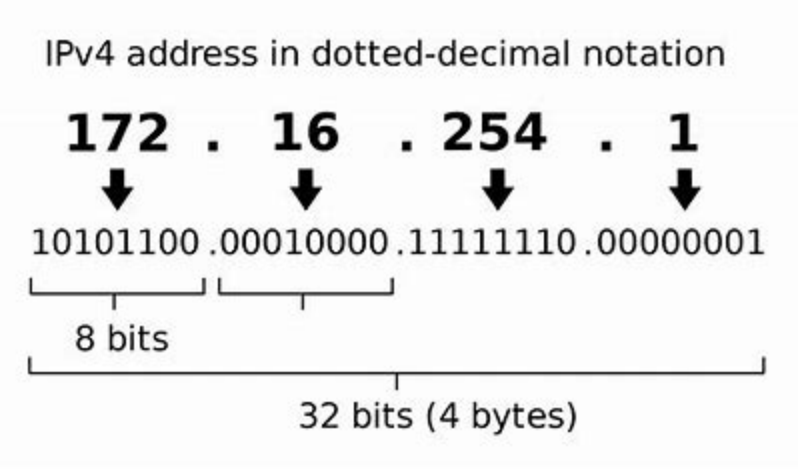
To transmit data from one device to another, the OSI (Open Systems Interconnection) model is used. The OSI model was developed after World War II when existing encryption methods were broken, and there was a need for a secure way to communicate over the Internet. Initially, it had seven layers, but it evolved to four layers.

1. *Application Layer*:
    - Includes protocols that allow you to interact with the network, like HTTP for browsing the web. A *protocol* is a set of rules that determine how data is transmitted and understood.
    - HTTPS “s” refers to secured data.

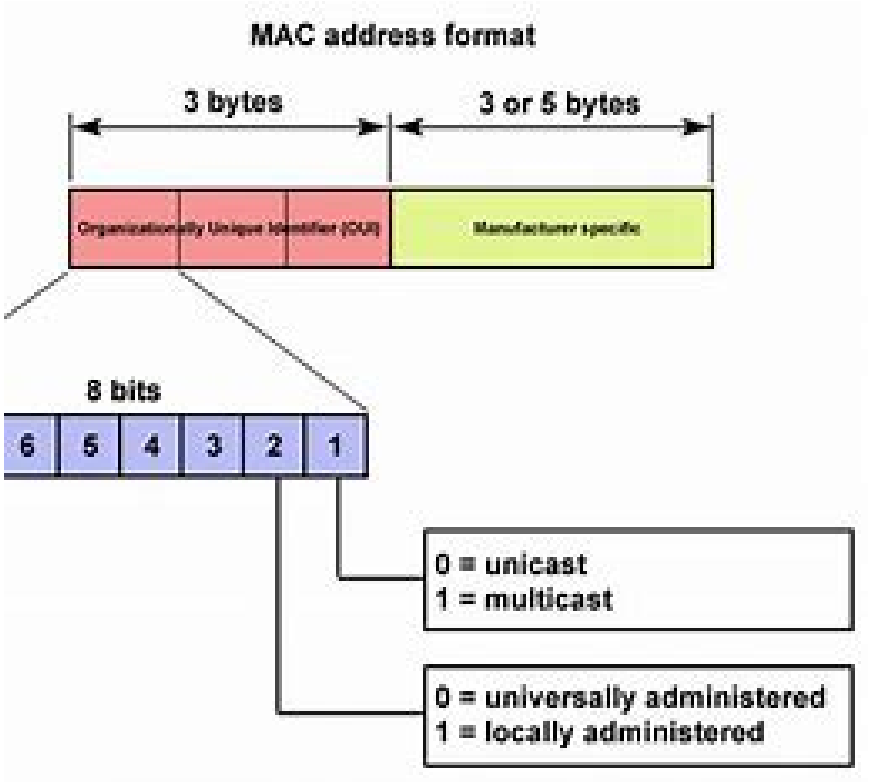


2. *Presentation Layer*:
    - Responsible for ensuring that the data is presented in the same way across different devices. For example, how the data appears on a laptop should be the same as on a mobile phone.
3. *Session Layer*:
    - Manages sessions, ensuring that different tabs or sessions do not interfere with each other.
4. *Transport Layer*:
    - Handles the transfer of data between devices. This is where protocols like TCP (connection-oriented, reliable, used for email) and UDP (connectionless, faster, used for streaming) come in.
    -

5. *Network Layer*:
    - Handles routing and forwarding of data. It deals with logical addresses like IP addresses. Routers operate here, using a *routing table* to determine the best path for data.
    -



6. *Data Link Layer*:
    - Responsible for node-to-node data transfer. Switches operate here, dealing with MAC addresses (unique identifiers for network interfaces) to forward data to the correct device.
    - MAC Format

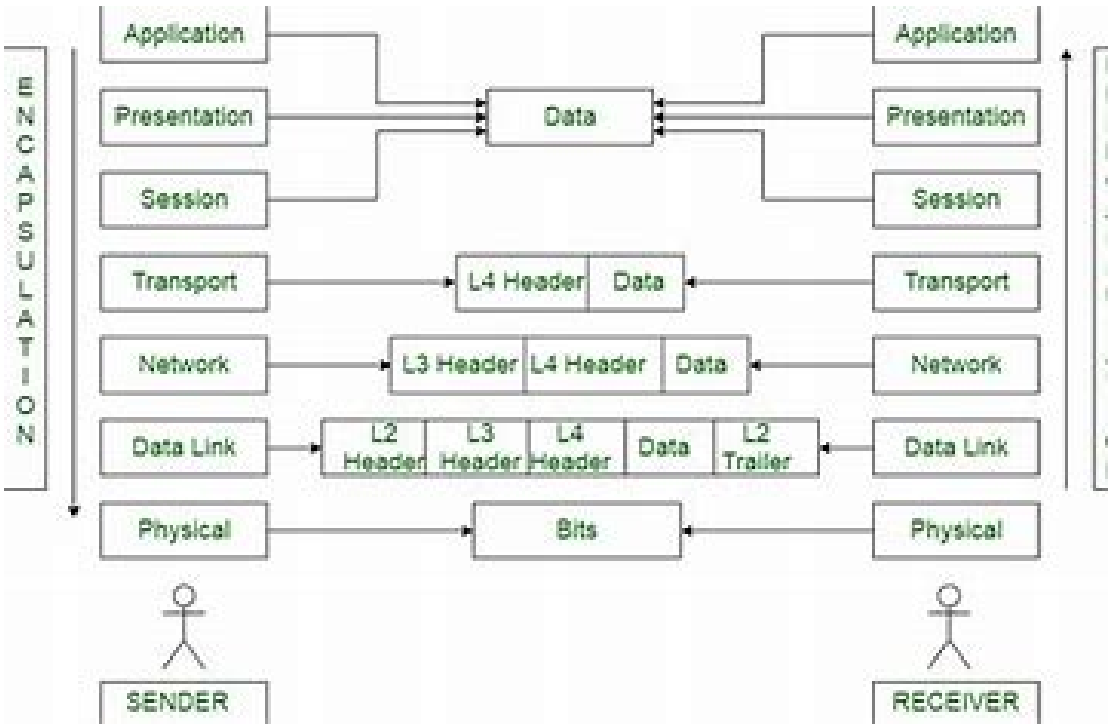


7. *Physical Layer*:

- Defines the physical aspects of the network, such as cables and the electrical signals used to transmit data.

▼ *Data Encapsulation*

When sending data, it starts at the application layer and moves down the OSI layers. At each layer, the data is encapsulated with additional information necessary for its transmission, such as routing information, ensuring it reaches its destination correctly.



▼ *What is the IP Address?*

The IP Address is a special address for each device on the network, and it consists of four numbers separated by dots. Each number is from 0 to 255. For example, your IP is 10.10.10.1.

2. *What is the Subnet Mask?*

The Subnet Mask determines which part of the IP Address is the network (Network) and which part is the device connected to the network (Host).

- For example, if you have a Subnet Mask like 255.255.255.0
- *The first part* (255.255.255) represents the Network.
- *The last part* (0) represents the Hosts.

3. *How do we get to the Network ID (the body of the network)?*

To know the Network ID, you take the IP Address and do an AND operation with the Subnet Mask.

Example:

- IP Address: 10.10.10.1
- Subnet Mask: 255.255.255.0

When we apply the AND operation, the result will be:

- *Network ID:* 10.10.10.0
- *Host ID:* 1 (the remaining part is the Host)

4. *Why is the Network ID 0?*

Because the 0 in the last part of the Network ID indicates that we are talking about the network as a whole, not a specific device within the network.

5. *And the Subnet?*

The Subnet is a part of the large network that is divided so that we can manage the devices better.

Summary:

- The Subnet Mask determines which part of the network and which part of the devices.
- The Network ID is determined by the AND operation between the IP Address and the Subnet Mask.

> **شرح مفصل لل IP Address وال Subnet Mask, الفرق بين Public IP Vs Private IP**

https://youtu.be/Nnv36wG_iCI?si=XipuMSN_aFopC8TF

▼ OSI Model Explained | OSI Animation

https://youtu.be/vv4y_uOneC0?si=QmWOr0QeN9kHeMtD

https://youtu.be/0y6FtKsg6J4?si=Nprko2lrFb0It-B_

▼ Wireshark

is a potent tool for monitoring and analyzing data traveling over a network. Let me explain it to you more clearly:

Wireshark: A program for monitoring and analyzing data

> *Wireshark* is an open-source program that allows you to monitor traffic on your network. This program enables you to "eavesdrop" on the data traveling over the network. It displays it to you in detail, as it is written in *Hexadecimal* or other forms such as plain text (ASCII) if the data can be read normally.

Graphical Interface (GUI) in Wireshark

- *Wireshark* has a graphical interface that makes it easy to view the captured data. Once you start monitoring, the program will start displaying all the data traveling over the network you have selected.
- *Red Button*: As you were explaining, the program can display indicators or alerts (such as the red button) to show you that you are currently capturing and monitoring data.

Using Wireshark to monitor the router

- Wireshark allows you to monitor traffic on your router. Through it, you can see all the data that is transferred to and from the devices connected to the router. This allows you to know what devices are searching for or communicating with on the network.

- https://youtu.be/Mj0YMh0yrEM?si=d6uKKkp4Jzpaeq-y

▼ *DNS and its relationship to obtaining the IP Address*

DNS (Domain Name System) is the system that translates website names (such as facebook.com) into *IP Addresses* so that devices can communicate with each other. When you buy a new device and you can't log in to Facebook, for example, the device sends a request to the DNS server to know Facebook's IP Address. When the DNS receives the request, it returns to you the IP Address that will enable you to access the site.

Encapsulation and Decapsulation Operations

- After you get the IP Address from the DNS, the data that you will send to reach Facebook is filled in layers or what is known as *Encapsulation*. In each layer of the OSI Model, information specific to this layer is added.
- When the data reaches Facebook, these layers are decomposed in order (decapsulated) until they reach the original content.

https://prod-files-secure.s3.us-west-2.amazonaws.com/021cfc11-08f0-41f7-9bbc-ab9b826020da/8d39fab7-dbf0-4847-ba04-822573a6923e/SecurityTrybe-1820188151278686433-01.mp4

▼ *Dealing with server access problems*

If you encounter a problem accessing the company's server, there are steps you can take:

1. Ping: The first thing you should do is send a **Ping* to the server. Ping sends small packets of data to the server to make sure it is running and can receive data. If all packets arrive successfully, the connection is fine.

2. Troubleshooting with Traceroute: If there is a connection problem, you can use **Traceroute*. This is a tool that helps you know the path the data takes to reach the server and shows you where the problem is or any step that is delayed.

▼ *IP Address and Subnet Mask*

When you make *AND* between IP Address and Subnet Mask, you will know the *Network ID* which represents the name of your network or family. This Network ID determines the number of devices that can be on this network.

▼ *The difference between Switch, Hub, Router, and Access Point*

- *Switch*: It works on the Data Link Layer (the second layer in OSI) and works to transmit data between devices on the same network using MAC Addresses.
- *Hub*: A simpler device than the Switch, it sends data to all devices connected to it without discrimination.
- *Router*: It works on the Network Layer (the third layer in OSI) connects different networks and uses IP Addresses to direct data.
- *Access Point*: It provides a wireless connection to devices, meaning it acts as a bridge between the wired network and the wireless network.

▼ *Packet Tracer and working with the console*

Packet Tracer is an educational tool from Cisco that allows you to simulate and design networks. This tool helps you learn and understand how networks work by creating and working on virtual network models.

Cables and network connection

- *The correct cable*: When connecting devices to the network, you must use the appropriate cables so that the data is transmitted properly. If you use

an inappropriate cable, the connection between the devices will not be effective.

▼ *Switch and connecting devices*

- *Switch*: The switch works to connect the devices on the same network to each other. When you have more than one switch on the network, you can connect them to each other without having to make complicated settings.

▼ *Home Router in Egypt*

- In every Egyptian home, the router is a comprehensive device that combines:
- *Modem*: Converts the Internet signal coming from the service provider (ISP) into a signal that devices in the home can use.
- *Switch*: Connects devices in the same home network.
- *Router*: Connects the home network to the external Internet, and uses IP Addresses to direct data.
- *Access Point*: Provides a wireless connection (Wi-Fi) for devices in the home.

Details of each part of the router

- *Modem*: Converts the Internet signal from the service provider into a digital signal that devices can understand.
- *Switch*: Connects devices in the same local network.
- *Router*: Determines the best path for data and connects the local network to the external Internet.
- *Access Point*: Provides a wireless connection for devices using Wi-Fi technology.

▼ *Default Gateway and the importance of the router*

- *Default Gateway*: It is the router address that devices in the local network use to access the external Internet.
- You must adjust the router settings, such as the network name and password, to maintain the security of the network.

Cisco router and memory management

- *Cisco Routers*: Cisco routers use RAM (temporary memory) to store temporary settings and data that are currently being used.
- When you do *Save* for the settings, the settings are transferred from RAM to *NVRAM* (Non-Volatile RAM) so that they remain saved even after restarting the router.

ROM in the router

- ROM (Read-Only Memory): It is the read-only memory in the router, and it contains a copy of the basic operating system, which is **Mini IOS*. This system helps the router to operate basic functions even if there is a problem in the basic system.
- *Mini IOS*: It helps you if there is a malfunction in the basic system, so you can enter maintenance commands and fix the problem without having to completely restart the device.

POST (Power-On Self-Test)

- *POST*: This is a dynamic process that occurs when the router starts up. It tests all hardware parts to make sure they are working properly before starting the operating system.
- This is like a quick check of all parts of the router to make sure they are ready for use.

Router Operating System (IOS)

- *IOS (Internetwork Operating System)*: This is the operating system that the router runs on, and this is what allows you to manage and control all the functions of the router.

- Some routers have a graphical user interface (GUI) that you can use to manage the router, but in most cases, control is through the command interface (CLI).

Flash Memory in the router

- *Flash Memory*: This flash is like the hard disk in the computer. System settings and copies of the operating system are stored on it.
- If you make settings and want to save them permanently even after restarting the router, the settings are saved on the flash memory.

▼ *Modes in the router*

- There are several *Modes* or modes to control the router, and each mode is used for different purposes:

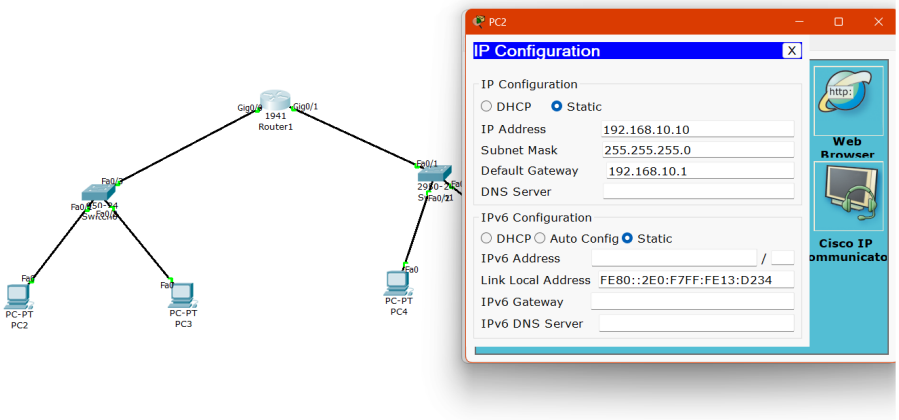
1. *User EXEC Mode*: The basic mode when you enter the router, this allows you to see some information but you will not be able to make changes.
2. *Privileged EXEC Mode*: This mode gives you greater permissions and you can enter more commands and make changes to the system.
3. *Global Configuration Mode*: This is the mode you enter to change the general settings of the router.
4. *Interface Configuration Mode*: In this mode, you can make changes to the communication interfaces (Interfaces) in the router.

▼ *Tasks in Packet Tracer*

1. *Connecting Devices:*

- Start by connecting devices such as a router, a switch, and a computer. Ensure the connections are properly made using the appropriate cables.

2. *Static IP Configuration:*
   - Open the *Desktop* tab on the computer, then go to *IP Configuration*.
   - Manually enter the *IP Address, **Subnet Mask, and **Default Gateway*.
   -



3. *Network Name vs. IP Address:*
   - *Network Name (SSID)*: This typically refers to the name of the wireless network you connect to. It is used for identification and connection purposes, particularly in Wi-Fi networks.
   - *IP Address*: This is a unique address assigned to each device in a network, allowing it to communicate with other devices. It is divided into two parts:
     - *Network Portion*: Identifies the specific network.
     - *Host Portion*: Identifies the specific device within that network.

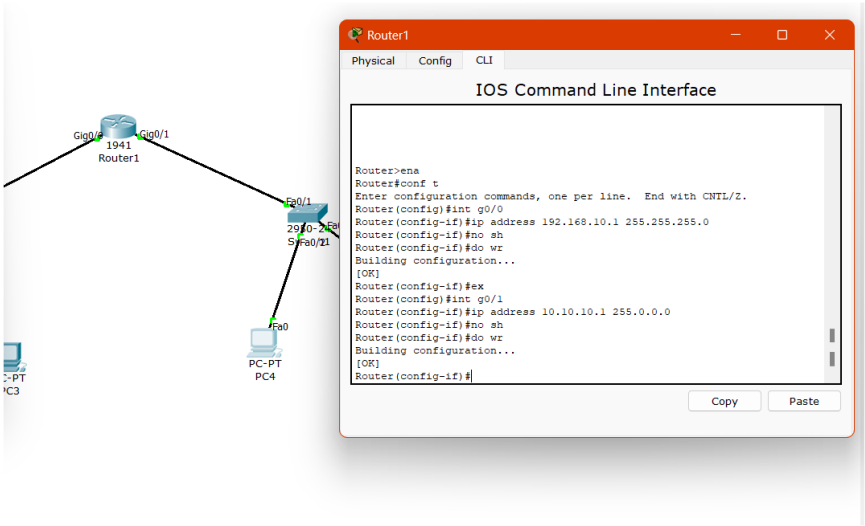
▼ *Connecting and Configuring a Router to Communicate with Another*

Network:

1. *Accessing the Router Command Line:*
    - *Command:* enable (shortened to ena)
        - *Explanation:* This command switches the router to "Privileged EXEC mode," which allows you to enter more advanced commands and configurations.
2. *Entering Configuration Mode:*
    - *Command:* configure terminal (shortened to conf t)
        - *Explanation:* This command puts the router into "Global Configuration Mode," where you can make changes to the router’s configuration.
3. *Selecting an Interface to Configure:*
    - *Command:* interface g0/0
        - *Explanation:* This selects the Gigabit Ethernet interface 0/0 on the router for configuration. The interface you choose will depend on the physical port you're using to connect to the network.
4. *Assigning an IP Address, Subnet Mask, and Default Gateway:*
    - *Command:* ip address [IP Address] [Subnet Mask]
        - *Explanation:* Here, you replace [IP Address] and [Subnet Mask] with the appropriate values for your network. This assigns the interface an IP address and subnet mask, allowing it to communicate on the network.
        - *Note:* The Default Gateway isn't directly set in this step but is understood as the router's role in directing traffic to external networks.
5. *Activating the Interface:*
    - *Command:* no shutdown (shortened to no sh)

- *Explanation:* This command activates the interface. By default, interfaces are shut down (turned off), so this command is essential to bring the interface online and make it functional.

6. *Verifying the Configuration:*
   - *Command:* do show ip interface brief (shortened to do show ip int br)
     - *Explanation:* This command shows a brief summary of the IP addresses and the status of all interfaces on the router. It helps verify that the interface is up and has the correct IP address assigned.



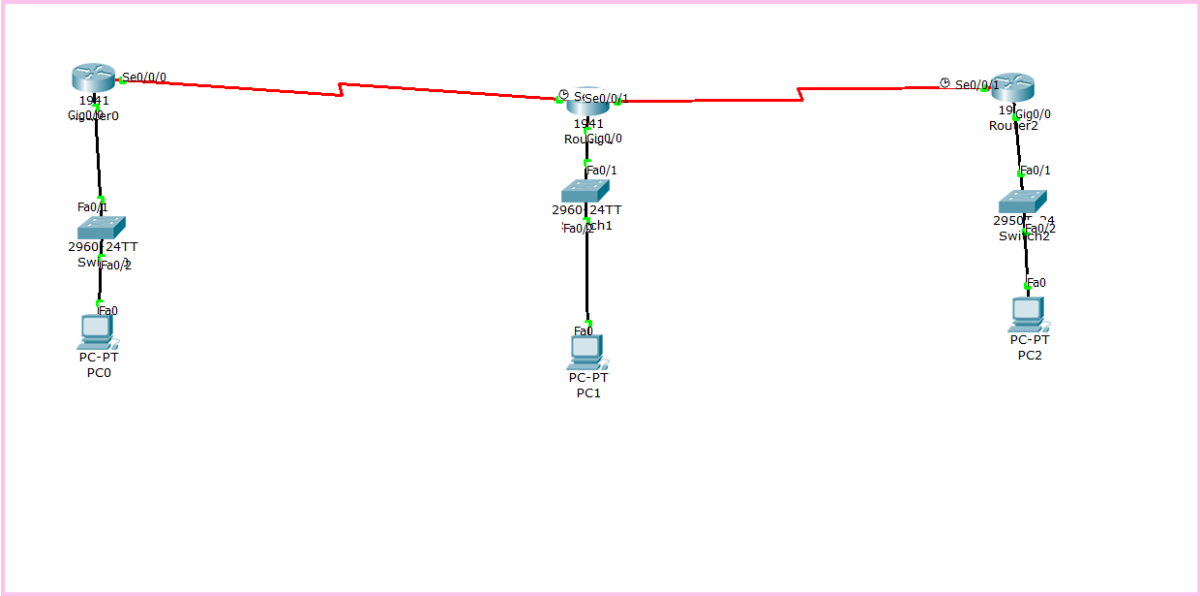
▼ *Connecting Routers Using Serial DCE Cable and Configuring Static Routing:*

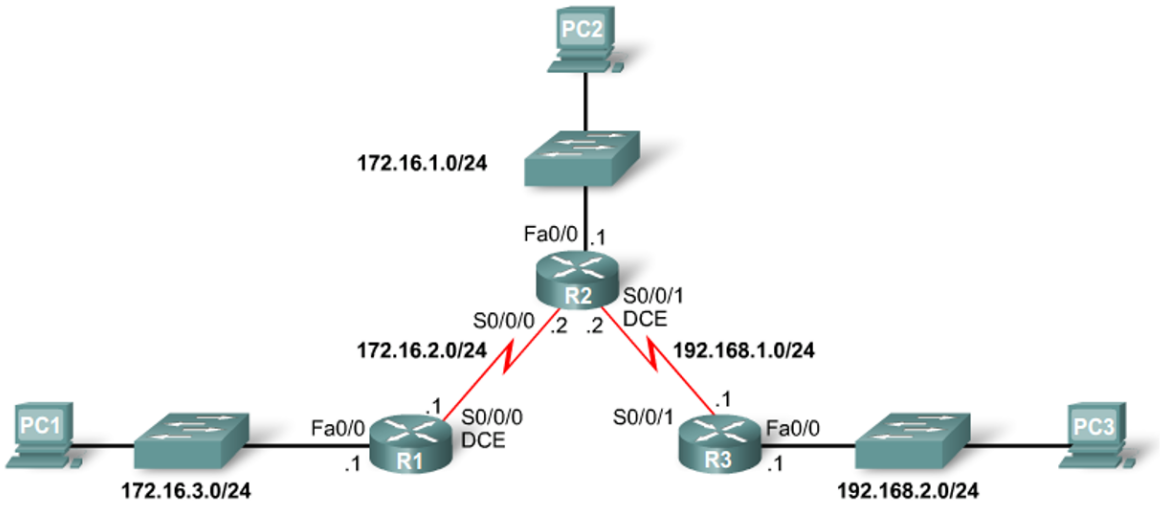
1. *Connecting the Routers:*
   - Use a *Serial DCE (Data Communications Equipment)* cable to connect the routers. This type of cable is used because it allows one router to control the timing of the data flow.
2. *Configuring the Serial Interface:*

- After connecting the cable, access the router's interface configuration to activate and configure the serial connection.
- *Command:* interface serial 0/0 /0(or the correct serial interface)
- *Assign IP Address:*
  - *Command:* ip address [IP Address] [Subnet Mask]
- *Activate the Interface:*
  - *Command:* no shutdown

3. *Static Routing:*
   - *Purpose:* In Static Routing, you manually enter the routes to other networks into the routing table. This is useful for small or simple networks where the routes don't change often.
4. *Adding a Static Route:*
   - *Command:* ip route [Destination Network] [Subnet Mask] [Next Hop IP Address]
     - *Explanation:*
       - *[Destination Network]:* The IP address of the network you want to reach.
       - *[Subnet Mask]:* The subnet mask associated with that network.
       - *[Next Hop IP Address]:* The IP address of the next router or device that will forward the packet towards the destination.

5. *Verifying the Configuration:*
   - *Command:* show ip route
     - *Explanation:* This command shows the routing table of the router, where you can verify that the static route has been correctly added.






```
R1#conf t
R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2
```

```
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
R2(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

```
R3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.2
```

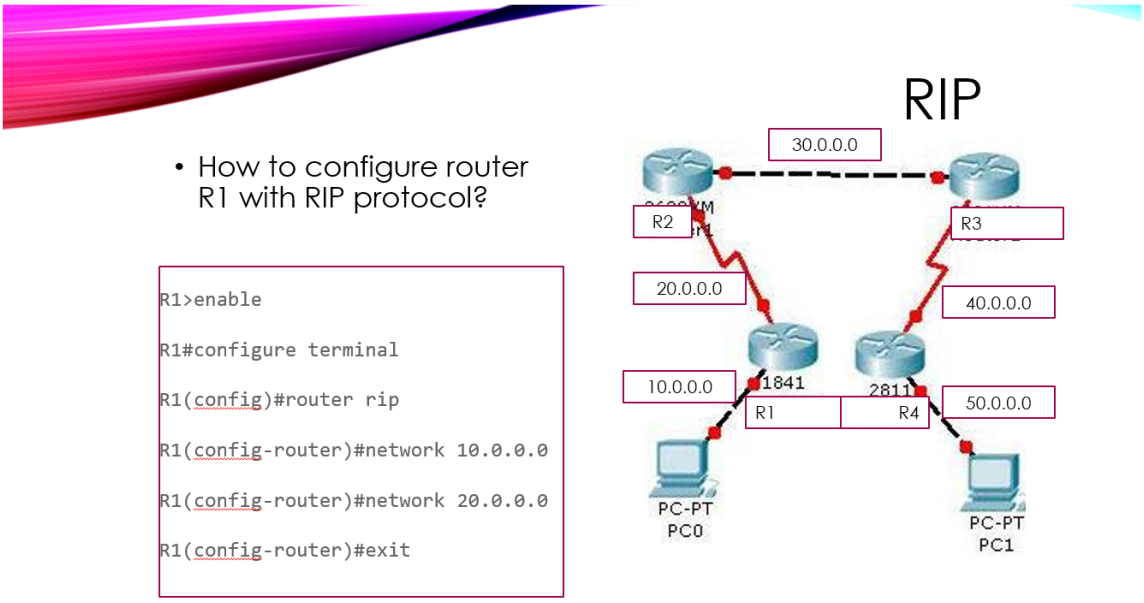
▼ *Configuring Dynamic Routing Between Routers*

1. *Introduction to Dynamic Routing:*
    - Unlike static routing, where routes are manually entered, dynamic routing allows routers to automatically exchange information about networks they know, adjusting the routes dynamically as the network topology changes. This is more efficient for larger or more complex networks.
2. *Enabling a Dynamic Routing Protocol:*
    - There are several dynamic routing protocols you can use, such as *RIP (Routing Information Protocol), **OSPF (Open Shortest Path First), and **EIGRP (Enhanced Interior Gateway Routing Protocol). Below, I'll use *_RIP_* as an example, but the steps are similar for other protocols.
3. *Steps to Configure RIP:*

- *Enter Router Configuration Mode:*
  - *Command:* router rip
  - *Explanation:* This command puts the router into RIP configuration mode.
- *Specify the Version of RIP:*
  - *Command:* version 2
  - *Explanation:* RIP has two versions, and version 2 supports classless IP addressing (which is more commonly used).
- *Advertise Networks:*
  - *Command:* network [Network Address]
  - *Explanation:* This tells the router which networks it should advertise to other routers using RIP. You need to enter the network addresses that are directly connected to the router.
  - *Example:*
    - If the router is connected to the 192.168.1.0 and 10.0.0.0 networks, you would enter:
      - network 192.168.1.0
      - network 10.0.0.0
- *End Configuration:*
  - *Command:* exit
  - *Explanation:* Exit the RIP configuration mode to return to the global configuration mode or privileged EXEC mode.

4. *Verifying Dynamic Routing Configuration:*
   - *Command:* show ip route
     - *Explanation:* This command will display the router's routing table, showing all the networks it knows about, including those learned via RIP. You'll see entries marked with an "R" indicating they were learned through RIP.

5. *How Dynamic Routing Works:*
    - Once configured, RIP will automatically exchange information with neighboring routers using periodic updates. If a route goes down, RIP will remove it from the routing table and find an alternative path if available.
    -



▼ Videos for configuration

https://youtu.be/V6c-6FUw7Y0?si=1K0Rv4-JPJki5_Wy

https://youtu.be/Kav17zx4RxA?si=ojWOvuxjqRnUxP5d

▼ *Bandwidth Utilization*

The *spectrum* is a natural resource the government allocates for various services like radio and television broadcasting. This spectrum is divided into different *bands* based on the service type. Each band is then divided into *frequencies* to carry *signals* that transmit *data* between devices.

It's not practical to assign a separate frequency for each user or device, as the available frequencies would quickly be exhausted. To address this, various

methods have been developed to manage access to channels more efficiently. One of the key methods is called *Multiplexing*.

Multiplexing allows multiple signals to be combined on the same channel, enabling several users to send data simultaneously over the same frequency. This process is carried out using a device called a Multiplexer (MUX), which is a digital switch that operates in the **Data Link Layer*.

There are several types of *Multiplexing*, including:

- *FDM (Frequency Division Multiplexing):* Assigning different frequencies to each signal.

▼ *FDM (Frequency Division Multiplexing):*

https://youtu.be/f52bwNbuMDA?si=UlNPvIwncrCuOe76

FDM is a technique that divides the bandwidth into several non-overlapping frequencies, where each signal is assigned a different frequency. This technique involves **Modulation* and *Bandwidth Filtering*.

- Modulation: This process uses *Carrier Waves* to carry and protect the signal during transmission.
- Bandwidth Filter: It determines the **low and high frequencies* to focus on, ignoring other irrelevant frequencies.

How *FDM* Works:

It divides the bandwidth into several *separate frequencies, leaving spaces between them called **Guard Bands*. These guard bands prevent interference between channels but reduce bandwidth utilization.

For example, downloading a video using *FDM* might take longer, depending on the number of users and how the channels are divided.

Applications:

FDM is used in:

- Radio broadcasting
- Television broadcasting
- Cable TV networks

Disadvantages of *FDM*:

- It requires a large number of *Modulators* and *Filters*.
- Low-speed channels need carrier waves, which reduces *Throughput*.
- It requires *complex hardware* and circuits.

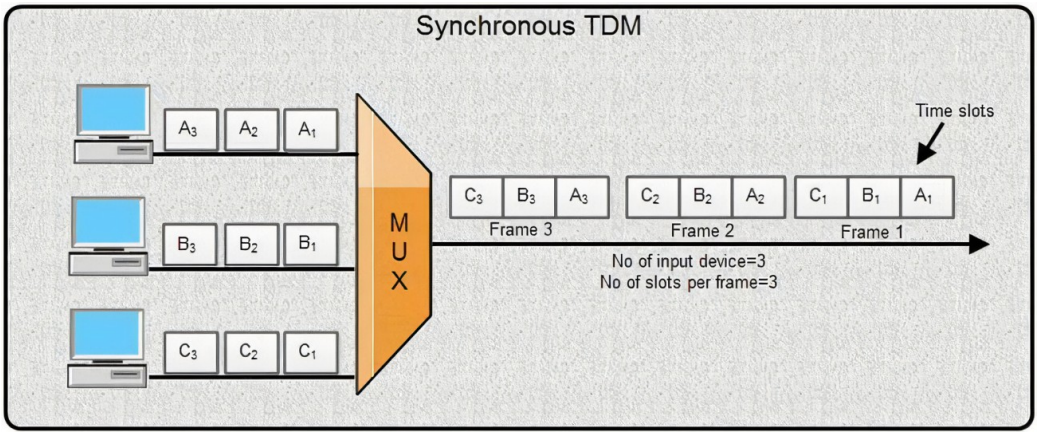
- *TDM (Time Division Multiplexing):* Assigning different time slots to each signal.

▼ Time Division Multiplexing (TDM)

TDM is a technique used to share a single communication channel among multiple devices by dividing the time into discrete intervals or slots. Each device is allocated a specific time slot in which it can send its data.

There are two main types of TDM:

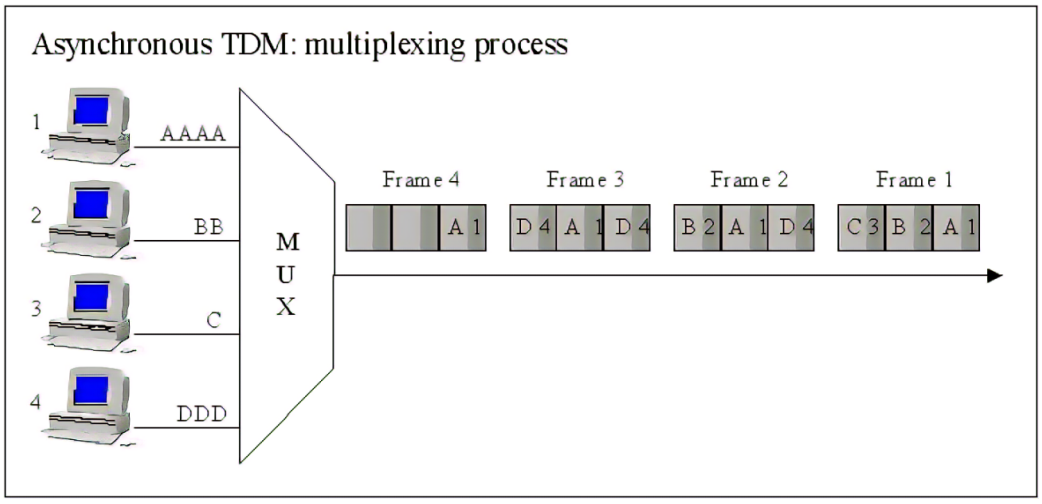
1. *Synchronous TDM*:



https://youtu.be/kcPgzI75RF0?si=r0NXfCoBnkphkFK8

- In *Synchronous TDM*, each device is assigned a fixed time slot in a repeating cycle.
- *Time Slots*: Each device gets a predetermined time slot to transmit data, regardless of whether it has data to send or not.
- *Fixed Allocation*: Even if a device has no data to transmit during its allocated time slot, that slot remains reserved for it. This can lead to inefficient use of bandwidth if some slots are empty.

2. *Asynchronous TDM*:



- *Asynchronous TDM* (also known as Statistical TDM) allocates time slots dynamically based on demand.
- *Dynamic Allocation*: Time slots are assigned based on the readiness of the devices to send data. If a device has data to send, it will use the time slot; otherwise, the slot can be allocated to another device that needs it.
- *Improved Utilization*: This method can better utilize the available bandwidth because it adapts to the varying data transmission needs of the devices.

Summary:

- *Synchronous TDM*: Each device gets a fixed, repeating time slot regardless of its data needs.
- *Asynchronous TDM*: Time slots are assigned dynamically based on the actual data transmission requirements of the devices, leading to more efficient bandwidth utilization.

- *CDM (Code Division Multiplexing):* Using unique codes for each signal.

▼ Code Division Multiplexing (CDM), also known as Code Division Multiple Access

Code Division Multiplexing (CDM)

https://youtu.be/BkThmLtjQpE?si=L1kOT92dZSd60HYJ

Code Division Multiplexing (CDM) is a method that uses unique codes to distinguish between different data streams on the same frequency channel. This technique allows multiple signals to be transmitted over the same channel without interfering with each other.

- ***How It Works***:
  - Unique Codes: Each data stream is assigned a unique code, known as a *code sequence*. These codes are used to modulate the data before transmission.
  - *Spread Spectrum*: The unique codes spread the data signal across a wider frequency band than the minimum required, which helps to minimize interference and noise.
  - *Signal Separation*: At the receiver end, the signals are separated using the same unique codes. The receiver uses these codes to demodulate and recover the original data streams.
- ***Applications***:

    - *Wireless Communication*: CDM is commonly used in cellular networks, such as 3G mobile networks, to allow multiple users to communicate simultaneously over the same frequency band.
    - *Satellite Communication*: CDM is used to handle multiple signals from different satellites or ground stations.
- ***Benefits***:
    - *Efficient Use of Spectrum*: CDM allows multiple users to share the same frequency band, leading to more efficient use of the available spectrum.
    - *Enhanced Security*: The unique codes used in CDM add a layer of security, as signals can be encrypted and separated using the codes.
    - *Reduced Interference*: By using spreading codes, CDM helps to reduce the impact of interference from other signals.
- ***Challenges***:
    - *Code Management*: Proper management of the unique codes is essential to avoid collisions and ensure effective separation of signals.
    - *Complexity*: CDM systems can be more complex to design and implement compared to other multiplexing techniques.

▼ *Wavelength Division Multiplexing (WDM)*

https://youtu.be/2KsaTaAErDk?si=lFCg6AXEtnp4vX5T

is a technique similar to *Frequency Division Multiplexing (FDM)* but used in optical fiber communication.

- *How it Works*: WDM involves transmitting multiple data signals simultaneously through a single optical fiber by using different

wavelengths (or colors) of light. Each wavelength represents a different frequency and can carry a separate data stream.

- *WDM Types*:
  - *Dense Wavelength Division Multiplexing (DWDM)*: Used in high-capacity systems, allowing for hundreds of channels (e.g., up to 160 channels) to be transmitted over the same fiber.
  - *Coarse Wavelength Division Multiplexing (CWDM)*: Generally used for shorter distances and fewer channels.
- *Application*: WDM is used to increase the capacity of optical fiber networks by allowing multiple data streams to be carried simultaneously over the same fiber, each on a different wavelength.

- *SDM (Space Division Multiplexing):* Allocating channels based on spatial location.

▼ Space Division

- FDM can also refer to **Space Division Multiplexing* in some contexts, where multiple signals are transmitted over different physical channels or paths, such as in cellular networks.
- *Application in Cellular Networks*: In cellular networks, each cell (or antenna) covers a specific geographical area and uses FDM to avoid interference between cells. This allows multiple conversations to occur simultaneously over different frequencies.

▼ Spread Spectrum

Spread Spectrum Overview

Spread Spectrum is a technique used in telecommunications to spread a signal over a wider frequency band than the minimum required. This helps improve the signal's resistance to interference, enhances security, and allows multiple signals to coexist on the same frequency band.

▼ *Frequency Hopping Spread Spectrum (FHSS)*

- *What It Is*: FHSS is a method where the transmission frequency of a signal changes rapidly according to a specific pattern or sequence.
- *How It Works*: The signal "hops" from one frequency to another at regular intervals. This pattern of frequency hopping is predetermined and known only to the transmitter and receiver.
- ***Benefits*:**
  - *Reduced Interference*: Since the signal moves across different frequencies, it's less likely to experience consistent interference.
  - *Increased Security*: The hopping pattern makes it harder for unauthorized listeners to intercept or jam the signal.
- *Example*: Used in Bluetooth communication, where devices frequently change frequencies to avoid interference from other wireless devices.

▼ *Direct Sequence Spread Spectrum (DSSS)*

- *What It Is*: DSSS spreads the signal across a wide frequency band by combining the data signal with a higher frequency code sequence (also known as a spreading code).
- *How It Works*: The original data is multiplied by a pseudo-random code sequence. This spreads the data signal across a wider bandwidth than the minimum required. At the receiver, the same code sequence is used to retrieve the original data.
- *Benefits*:
  - *Better Noise Resistance*: Spreading the signal makes it less susceptible to interference and noise.
  - *Improved Security*: The spreading code adds a layer of security, making it harder for unauthorized users to decode the signal.

- *Example*: Used in older Wi-Fi standards (e.g., 802.11b), where data is spread over a wider frequency range to reduce interference.

▼ Interconnecting Devices in a Network

https://youtu.be/Hc_eZUWXxDg?si=SnXHeizq5c8tbzSk

▼ Hubs

▼ *1. Physical Layer and Hubs*

At the *Physical Layer* of networking, devices connect through hardware like hubs. A hub operates at this layer, dealing with the physical transmission of data. It handles:

- *Physical Store*: The hardware components that transmit and receive signals.
- *Topology*: The physical layout or arrangement of devices in the network.
- *Pathological Post*: Refers to how data travels through the network.

▼ *2. How Hubs Work*

Hubs use *Twisted Pair Cables* (such as Cat5e or Cat6) to transmit data between devices. Here's how they function:

- *Data Transmission*: When a device sends data to a hub, the hub broadcasts it to all other connected devices. It doesn’t filter or direct the data specifically to the intended recipient.
- *No Filtering*: The hub doesn’t know which device should receive the data; it simply sends it out to all connected devices.
- *Collision Domain*: A collision domain is a network segment where data collisions can occur. If two devices send data at the same time, a collision happens, leading to data retransmission and reduced network performance.

▼ *3. Collision Domains and Protocols Domains*

- *Collision Domain*: In a network segment where a hub is used, all connected devices share a single collision domain. This means if two devices transmit data simultaneously, it causes collisions, which can degrade performance.
- *Protocols Domain*: This term describes a network segment where devices can receive messages from other devices using different protocols. A hub doesn't segregate or manage these protocols.

▼ *4. Advantages and Disadvantages*

- *Advantages*:
  - *Extended Distance*: Hubs can extend the distance between network nodes since they can connect multiple devices over longer distances.
  - *Simplified Networking*: Hubs provide a straightforward way to connect multiple devices in a network.
- *Disadvantages*:
  - *Collision Reduction*: Because hubs broadcast data to all devices, they increase the likelihood of data collisions. This can significantly reduce network performance as devices must wait for collisions to resolve before retransmitting data.
  - *Performance Impact*: As the number of devices connected to a hub increases, performance can degrade due to increased collisions and network congestion.

▼ Layer 2 Switches

▼ *1. Layer 2 Switching Overview*

Layer 2 switches operate at the Data Link Layer (Layer 2) of the OSI model. They handle data based on *MAC addresses* (Media Access Control addresses) and manage *frames* (data packets at this layer).

▼ *2. Functions of Layer 2 Switches*

- *MAC Address Table*: Layer 2 switches maintain a MAC address table (also known as a forwarding table). This table maps MAC addresses to switch ports. Initially, this table is empty and is populated as the switch learns the addresses of devices on the network.
- *Learning Process*: The learning process involves:
  - *Learning*: When a switch receives a frame, it checks the source MAC address and updates its MAC address table with the port number where the device is connected.
  - *Forwarding*: When the switch receives a frame destined for a particular MAC address, it looks up the address in the MAC address table and forwards the frame only to the port associated with that address.
- *Collision Domains*: Unlike hubs, switches segment the network into multiple collision domains. Each port on a switch represents a separate collision domain, reducing the chances of collisions and improving network performance.
- *Protocol Domains*: A switch operates within a single broadcast domain (the protocol domain). This means that while it reduces collision domains, all devices connected to the switch are still part of the same broadcast domain.

▼ *3. Advanced Features and Benefits*

- *Enhanced Performance*: Switches improve performance by using the MAC address table to efficiently forward frames, reducing unnecessary traffic and collisions compared to hubs.
- *Increased Reliability*: Switches provide better network reliability by reducing collisions and managing traffic more effectively.
- *Security*: Switches offer improved security over hubs because they send data only to the intended recipient rather than broadcasting it to all connected devices.
- *Geographical Flexibility*: Switches support various topologies and can be used to connect devices across different geographical locations within the same broadcast domain.

- *Plug-and-Play*: Many switches support plug-and-play functionality, allowing easy addition of new devices to the network with minimal configuration.
- *Full-Duplex Communication*: Switches support full-duplex communication, meaning data can be sent and received simultaneously, enhancing overall network efficiency.

▼ *4. Frame Forwarding*

- *Source MAC Address*: Used by the switch to learn and update the MAC address table.
- *Destination MAC Address*: Used to determine the port to which the frame should be forwarded.

▼ Routers

- Layer: Routers operate at the *Network Layer* (Layer 3) of the OSI model. They handle packets and use IP addresses to make routing decisions.
- *Collision Domains*: Routers separate traffic into multiple collision domains. Each interface on a router represents a different collision domain, reducing collisions and improving performance.
- *Broadcast Domains*: Routers also separate broadcast domains. Each interface on a router is in its broadcast domain, meaning broadcasts are not forwarded between interfaces, which helps in isolating traffic.
- *Traffic Isolation*: Routers provide traffic isolation by segmenting networks into separate collision and broadcast domains, ensuring efficient traffic management and reducing unnecessary traffic.
- *Plug-and-Play*: Routers typically do not offer plug-and-play functionality. They require configuration to set up routing protocols and manage network traffic effectively.
- *Optimal Routing*: Routers excel in optimal routing. They use routing algorithms and protocols to determine the best path for packets across different networks.

- *Cut-Through Switching*: Routers do not use cut-through switching. They perform a more complex process involving packet examination and routing, which can introduce some latency compared to cut-through switching.

Summary Comparison

Feature	Router	Switch
Collision Domains	Yes	Yes
Broadcast Domains	Yes	No (unless VLANs are used)
Plug-and-Play	No	Yes
Optimal Routing	Yes	No
Cut-Through Switching	No	Yes

▼ Virtual LANs (VLANs) and VRAM

▼ *1. What is VRAM?*

In the context of networking, *VRAM* typically refers to *VLAN (Virtual LAN)* rather than Video RAM. VLANs allow you to create logical groups within a physical network. These groups can be configured through software rather than requiring physical wiring changes.

▼ *2. VLAN Overview*

- *Network Segmentation*: VLANs enable you to segment a network into smaller, isolated segments. This is done purely through software configuration on network switches, without needing additional physical connections.
- *Broadcast Domains*: VLANs create separate broadcast domains within a network. This means that broadcast traffic sent within one VLAN is not forwarded to devices in another VLAN. This isolation helps in reducing unnecessary broadcast traffic and improves network efficiency.
- *Collision Domains*: VLANs also contribute to reducing collisions. Each VLAN is treated as a separate logical network segment, so

devices within the same VLAN communicate directly, minimizing collisions and improving performance.

▼ *3. Benefits of Using VLANs*

- *Cost Reduction*: By creating logical networks (VLANs) instead of adding more physical network hardware, you can reduce costs related to physical wiring and network equipment.
- *Increased Security*: VLANs enhance security by isolating sensitive traffic within specific VLANs. This prevents unauthorized access to different segments of the network and enhances overall security.
- *Efficient Grouping*: VLANs allow for the creation of virtual workgroups or departments within an organization. For instance, different teams (like HR, Finance, and IT) can be grouped into separate VLANs, improving network organization and management.
- *Simplified Network Management*: VLANs simplify network management by allowing changes to network structure to be made through software configuration rather than physical re-wiring.

4. Summary

- *VLANs*: Enable logical segmentation of a network into separate broadcast and collision domains through software configuration.
- *Benefits*: Reduce costs, increase security, facilitate efficient group creation, and simplify network management.

▼ Exercise: Find out how many Collision Domains and Broadcast domains

https://youtu.be/C2FrTZxi_NI?si=rYxdE8yrxg-Nc0vK

https://youtu.be/MfV-ha8Xnwo?si=7lmbqk_kXeI6cZb-

https://youtu.be/eIx49XNGUgk?si=MxNiI5jiBYexAKYs

▼ Basic Concepts

- Baseband: This system uses a *single data channel* to send data over the entire bandwidth. In other words, only *one channel* utilizes the full bandwidth, like in *LAMP* systems.
- Broadband: This system allows for *multiple data channels* to share the bandwidth simultaneously, making it more efficient than *Baseband* as it can handle *multiple channels* at once.

▼ *Antenna Considerations*

- *Antenna Usage*: In a cellular network, antennas are used to both transmit and receive signals. If an antenna is used only for transmission or reception, the coverage area needs careful management to ensure seamless connectivity.
- *Maintenance*: Proper maintenance of antennas is crucial for ensuring consistent coverage and network performance. If an antenna fails or is not maintained properly, it can affect the network's ability to transmit and receive signals effectively.

▼ Data Link Layer Overview

The Data Link Layer is the second layer in the OSI model, responsible for providing reliable communication over a physical network link. It sits between the Network Layer (Layer 3) and the Physical Layer (Layer 1). Its main functions include framing, error detection, error correction, flow control, and access control.

▼ Key Services of the Data Link Layer

1. *Framing*
    - *What it is:* Framing involves encapsulating Network Layer datagrams (or packets) into frames. This process adds a header and a trailer to the packet to create a frame.
    - *Purpose:* The header and trailer contain essential control information like source and destination addresses and error-checking data.

- *Formats:* Different protocols use different frame formats, but all frames generally include a header (with addresses and control information) and a trailer (for error detection).

2. *Link Access*
    - *What it is:* This service manages how devices on a network access the shared communication medium.
    - *Purpose:* It ensures that multiple devices can use the network without interfering with each other, typically handled by the MAC (Media Access Control) sub-layer.
3. *Error Detection*
    - *What it is:* Error detection techniques identify errors that occur during the transmission of frames.
    - *Techniques:* Common methods include checksums, cyclic redundancy checks (CRC), and parity bits.
4. *Error Correction*
    - *What it is:* Error correction involves techniques to fix errors detected in transmitted frames.
    - *Techniques:* Error correction methods may include retransmission requests (ARQ protocols) and forward error correction codes (FEC).
5. *Flow Control*
    - *What it is:* Flow control prevents the sender from overwhelming the receiver by sending frames too quickly.
    - *Purpose:* It ensures that data is transmitted at a rate that the receiver can handle, typically managed through mechanisms like acknowledgments and sliding window protocols.
6. *Access Control*
    - *What it is:* Access control determines how devices on a network take turns to use the communication medium.
    - *Purpose:* It avoids collisions and ensures fair access. Common protocols include Carrier Sense Multiple Access with Collision

Detection (CSMA/CD) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

7. *Addressing*
    - *What it is:* Addressing involves identifying devices on a network using unique identifiers.
    - *Types:*
        - *MAC Address (Physical Address):* Used within a Local Area Network (LAN) to uniquely identify devices.
        - *Layer 2 Address:* General term for addresses used at the Data Link Layer.
8. *Half Duplex vs. Full Duplex*
    - *Half Duplex:* Communication can occur in both directions, but not simultaneously. Devices take turns sending and receiving data.
    - *Full Duplex:* Communication can occur in both directions simultaneously, allowing for more efficient data transfer.

▼ Layers within the Data Link Layer

1. *Logical Link Control (LLC) Layer*
    - *Purpose:* The LLC layer manages the communication between the Network Layer and the MAC sub-layer. It provides error control and flow control services and interfaces with various network protocols.
2. *Media Access Control (MAC) Layer*
    - *Purpose:* The MAC layer controls access to the physical transmission medium and is responsible for frame delimiting, addressing, and access control.
    - *Interaction:* It interfaces directly with the Physical Layer, managing how frames are transmitted over the hardware.

▼ Multiple Access Protocols Overview

In a network where multiple nodes share the same communication channel, there is a risk of collisions if two or more nodes try to transmit data at the same time. To manage this, protocols are used to regulate access to the shared medium and minimize collisions.

▼ Types of Multiple Access Protocols

1. *Random Access Protocols*
    - *Overview:* These protocols allow nodes to transmit whenever they have data to send, without a predefined order. However, this can lead to collisions if multiple nodes transmit simultaneously.
    - *Example:* Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a well-known random access protocol.
2. *Controlled Access Protocols*
    - *Overview:* Controlled access protocols use mechanisms to prevent collisions by coordinating which node can transmit at any given time. This usually involves some form of scheduling or polling.
    - *Example:* Token Ring and polling-based methods are controlled access protocols.
3. *Channelization Protocols*
    - *Overview:* Channelization protocols divide the communication channel into separate channels or time slots, allowing nodes to transmit in their designated times or frequencies to avoid collisions.
    - *Example:* Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) are channelization techniques.

▼ Focus: Collision Detection (CD) – A Random Access Protocol

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a random access protocol designed to handle collisions in a shared network environment. Here's how it works:

1. *Carrier Sensing:*

- *Step 1:* Before transmitting, a node listens to the channel to check if it is clear (i.e., no other node is currently transmitting).
- *Step 2:* If the channel is clear, the node proceeds to transmit its data. If the channel is busy, the node waits for a random period before checking again.

2. *Collision Detection:*
   - *Step 1:* While transmitting, the node continues to monitor the channel to detect if another node has started transmitting at the same time (a collision).
   - *Step 2:* If a collision is detected (typically through changes in signal patterns), the node stops transmitting and sends a special signal (jam signal) to inform other nodes of the collision.
3. *Backoff Procedure:*
   - *Step 1:* After detecting a collision, the node waits for a random backoff period before attempting to transmit again. This helps in reducing the chances of repeated collisions.
   - *Step 2:* The backoff time is generally chosen from a range of times that increases exponentially with each subsequent collision.

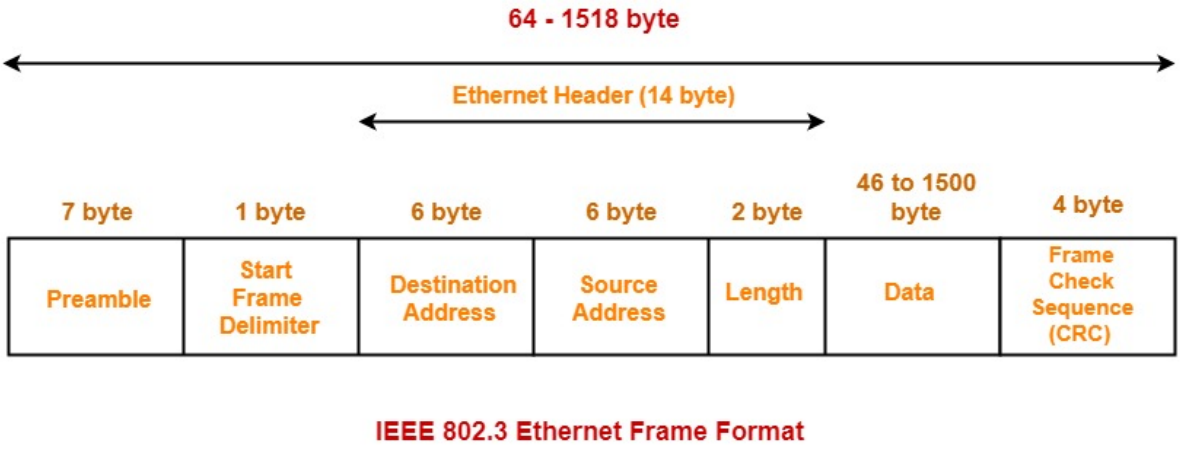
▼ Key Points

- *Collision Avoidance:* While CSMA/CD detects and manages collisions, it does not prevent them completely. The random backoff reduces the likelihood of repeated collisions.
- *Efficiency:* Random access protocols like CSMA/CD are efficient for networks with low to moderate traffic but can suffer from performance issues under high traffic conditions.

▼ Backoff Algorithm for CSMA/CD

https://youtu.be/N08RJ-aeUmY?si=jfWaFCtX_11xwMcV

▼ Ethernet Frame Format Explanation

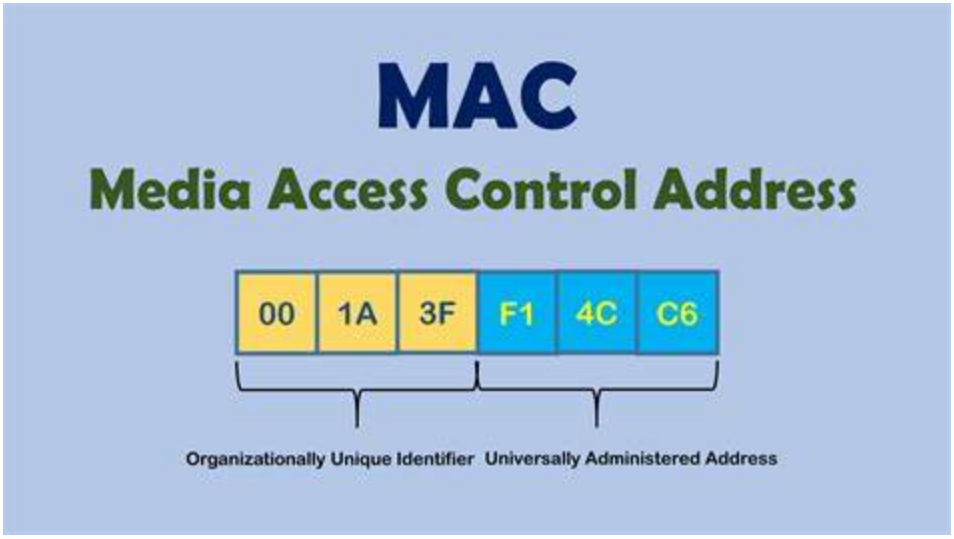


IEEE 802.3 Ethernet Frame Format

https://youtu.be/JsYqqDqmQaE?si=E2cN5rtzhge50kor

▼ MAC Address

https://youtu.be/TIiQiw7fpsU?si=5geVccWujLQWQxQ0



📌 The source MAC address must be unicast.

▼ Network Layer Basics

https://youtube.com/playlist?list=PLgwJf8NK-2e7oXV-CKsSFJfBUPas42gsQ&si=Y2_4k1LEdVhB3wYf

▼ Public vs Private IP Address

https://youtu.be/po8ZFG0Xc4Q?si=zLD_gy9mQMwlCGaJ

▼ Classful Addressing

https://youtu.be/VkgfyLf1raY?si=znAQMTvhqfeH3MlB

https://youtu.be/0MJmtjj0qCQ?si=mW_LbPsYj3nNie1A

https://youtu.be/KILaAaNWd8o?si=DfoYq1eBTx5pP_bx

▼ Calculate Network, Broadcast, and host addresses

https://youtu.be/hb2yTNT2rBU?si=1NXRh3ernzmc7pWX

▼ Variable Length Subnet Masking (VLSM) - Solved Problem 1

https://youtu.be/N7BEDtZ7G4g?si=nxx_o36dKn_vpaLm

▼ *Public and Private Network*

- ***Private Network:***
    - A private network is used within an organization or home. Devices connected to this network share resources like files, printers, and

internet access.

    - Typically, private IP addresses (e.g., 192.168.x.x or 10.x.x.x) are used, which cannot be directly accessed from the public internet.
    - *Example:* Your home Wi-Fi network is a private network. All devices connected to it, such as your phone, computer, and printer, can communicate with each other but are not visible to external devices on the internet.
- ***Public Network:***
    - A public network is used to connect to the internet. Any device connected to this network has a public IP address that can be accessed from the internet.
    - *Example:* When you connect to the Wi-Fi at a café, you're using a public network, meaning your device is visible and accessible on the internet.

https://youtu.be/po8ZFG0Xc4Q?si=1wXt-y2WMbjJUBuy

▼ *NAT (Network Address Translation)*

- *NAT* is a technology that translates private IP addresses from a local network into a public IP address (or multiple public IPs) when connecting to the internet.
- The main benefit is conserving IP addresses and reducing exposure of the internal network to internet threats.
- *Example:* When you browse the internet from your home device, the NAT in your router translates your device's internal IP address to the public IP of the router to connect to the internet.
-

https://youtu.be/FTUV0t6JaDA?si=ziZsTekhDsRStKjW

▼ *DHCP (Dynamic Host Configuration Protocol)*

- *DHCP* is a protocol that automatically assigns IP addresses to devices connected to a network, instead of setting them manually.
- A device like a router acts as a DHCP server that distributes IP addresses to each device connecting to the network.
- *Example:* When you turn on your computer and connect to your Wi-Fi, the router automatically assigns an IP address to your device using DHCP.

Difference Between DHCP and Static IP:

- *DHCP:* IP addresses change every time the device connects to the network.
- *Static IP:* A fixed IP address is assigned that does not change, usually used for devices that require a permanent address like servers.

Comprehensive Example:

- You have a home network (Private Network) with a router using NAT to translate private IP addresses to a public IP address. DHCP assigns IP addresses to devices automatically. When playing games online, you may have trouble connecting to other players if your NAT type is Strict, so you might need to adjust your router settings for better connectivity.
-

https://youtu.be/e6-TaH5bkjo?si=hMWkgLv7cZ7PE2AE