CITS CSA NOTES 2025-2026

Topic – Network Architecture

OS Installation

Steps to install an OS

Step-1

Download the OS ISO File

⬇

Go to the official website of the OS (Windows)

⬇

Download the ISO File for the version you want.

Step-2

Create a Bootable USB Drive

Use tools like:-

1. Rufus
2. Ventoy
3. Using the command prompt

Steps-3

Insert the bootable USB drive

⇩

Press the power button **ON**

⇩

Press key F2, F10, F11, F12. Esc or Delete.

⇩

Select Startup/Boot

CSM **Enable**

⇩

Boot mode **Auto**

Enter

⇩

Select UEFI: USB/Pen drive Name

⇩

Select windows

⇩

Boot in Normal mode

Step-4

Delete/Formal - Clicking this section will delete all data on the selected drive.

⇩

New - Clicking this section will create a new partition.

⇩

Extending - Clicking this section will add a partition.

System ON Work

How

1. Create New Divide Disk

2. Use for disk

3. Add disk

Follow the steps: -

Select This PC

⬇

Then Right Click.

⬇

Show more options

⬇

Click Manage

⬇

Select Storage

⬇

Disk Management

⬇

Select Disk (C)/(D)→ Right Click

Then you will see a lot of options: -

Open: Open all files and show all data

Format: Erase all data

Delete volume: This will erase all data

Shrink volume: - This creates a new device disk.

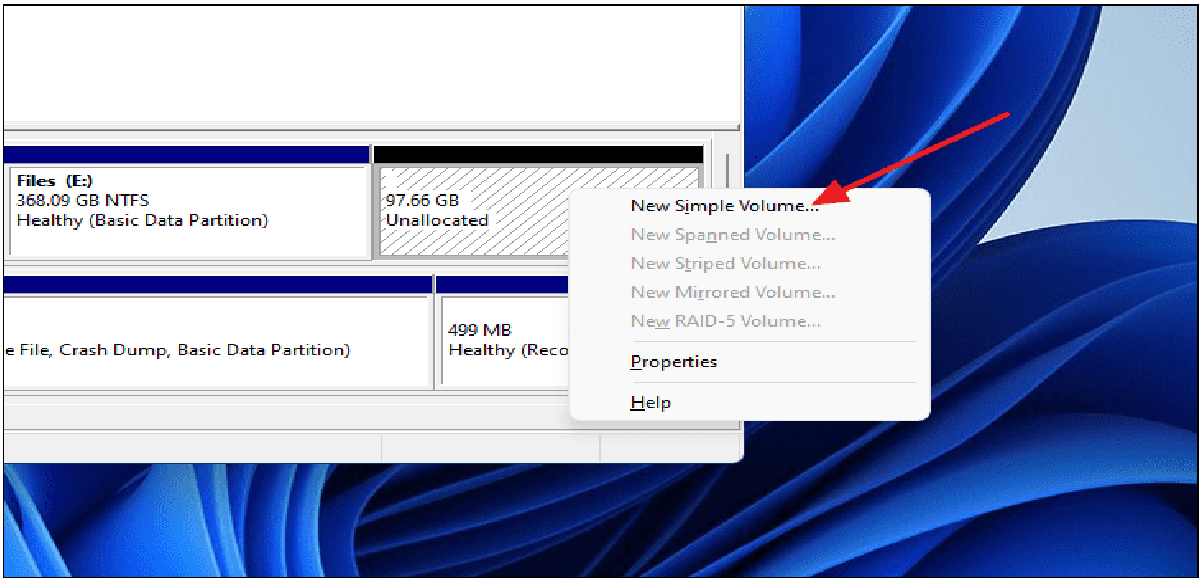
New Simple Volume: - use for disk

Extend volume: - Add divide a disk

New Divide disk बनाने के लिए

⇩

Shrink volume



Files (E:)
368.09 GB NTFS
Healthy (Basic Data Partition)

97.66 GB
Unallocated

e File, Crash Dump, Basic Data Partition)

499 MB
Healthy (Reco

Use में Disk को लाने के लिए

⇩

↳ New simple volume

Disk Add करने के लिए

⇩

↳ Extend volume

File Sharing के लिए

Select Setting ⚙

↓

Network & Internet

↓

Advanced Network Settings

↓

Advanced Sharing Setting

↓

private Networks

↓

Network discovery ON

↓

File and printer Sharing ON

↓

Network discovery ON

↓

Public folder sharing ON

Error handling when accessing another system

Step1

Open Registry Editor

⇩

Computer

⇩

HKEY-MACHINE

⇩

SYSTEM

⇩

CurrentControlSet

⇩

Services

⇩

Lanaman Workstation

⇩

Parameters

⇩

Create a new file

⇩

DWORD (32-bit) value

⇩

File Name - AllowInsecureGuestAuth

⇩

Value-1

Step-2

Search on PC→ PowerShell Run as Administrator

⇩

```
Set-SmbClientConfiguration -RequireSecuritySignature $false
```

Straight Cable and Cross Cable

Straight Cable: - (Straight-Through cable)

A Straight cable is a type of Ethernet networking cable used to connect different types of devices in a network.

Definition

A Straight-through Cable is one where the wiring order (colour sequence) on both ends of the cable is exactly the Same.

That means the wire connected to pin 1 on one connector is also connected to pin 1 on the other connector.

Uses:-

Straight Cables are used to connect different types of devices, such as:-

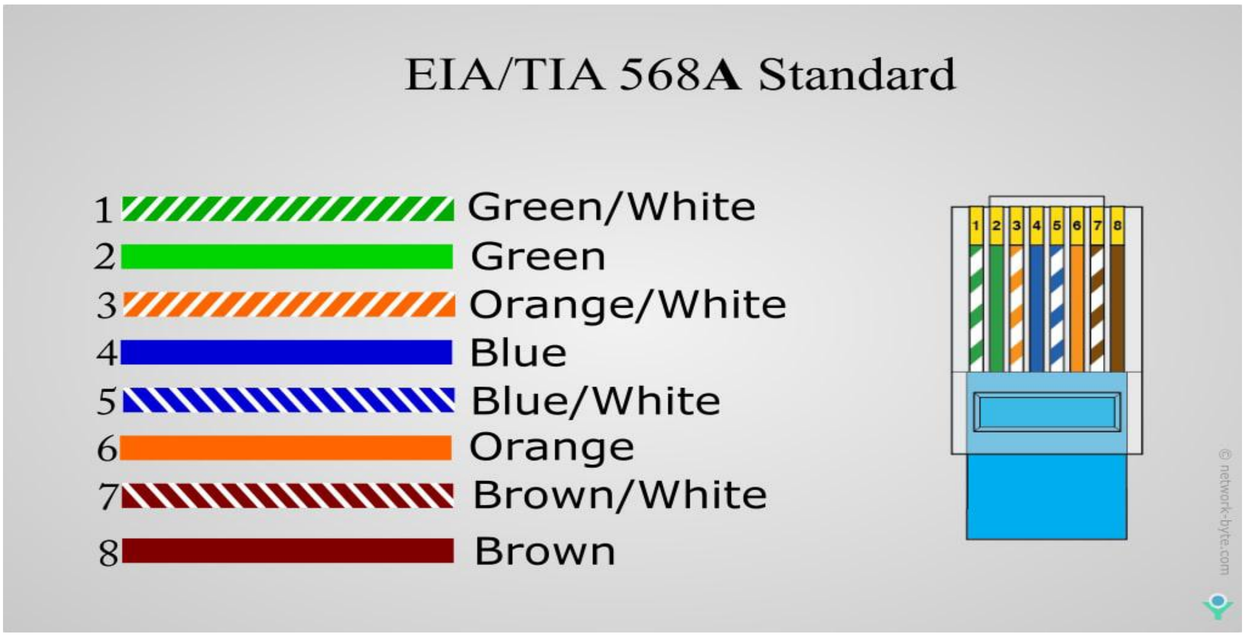
1. Computer - Switch/Hub
2. Computer - Routes.
3. Switch - Router
4. Printer - Switch

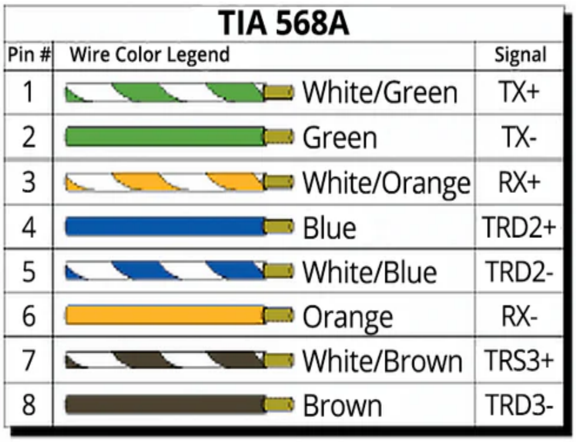
Wiring Standards:-

Ethernet cables follow two main wiring Standards-

T568 A   T568 B

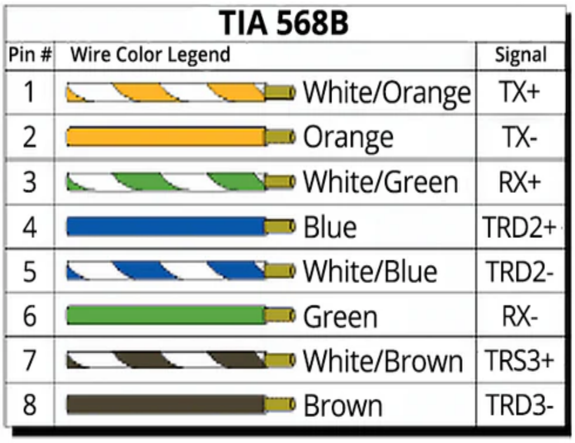
Colour Order





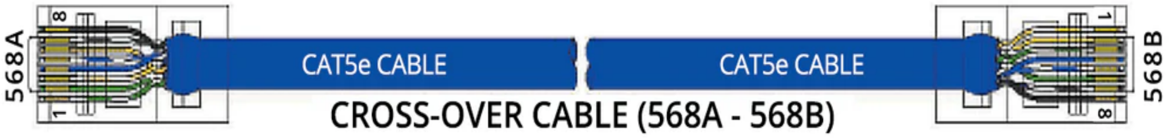
TIA 568A

Pin #	Wire Color Legend	Signal
1	White/Green	TX+
2	Green	TX-
3	White/Orange	RX+
4	Blue	TRD2+
5	White/Blue	TRD2-
6	Orange	RX-
7	White/Brown	TRS3+
8	Brown	TRD3-



TIA 568B

Pin #	Wire Color Legend	Signal
1	White/Orange	TX+
2	Orange	TX-
3	White/Green	RX+
4	Blue	TRD2+
5	White/Blue	TRD2-
6	Green	RX-
7	White/Brown	TRS3+
8	Brown	TRD3-



Cross cable (Crossover Cable)

Cross cable: - A cross cable (also called a Crossover cable) is a type of Ethernet Cable used to connect similar devices directly to each other without a hub. Switch or router.

Definition: -

A Crossover cable is a network cable in which the transmit (Tx) and receive (Rx) wires are swapped (crossed) at one end.

This allows data to be sent and received directly between two similar devices.

Purpose /uses:-

Crossover Cables are used to connect Similar types of network devices, such as:-

1. computer - computer

2. Switch - switch

3. Hub - Hub

A. Router - Router

Cross cable में 1326 में Colour को connect करना है।

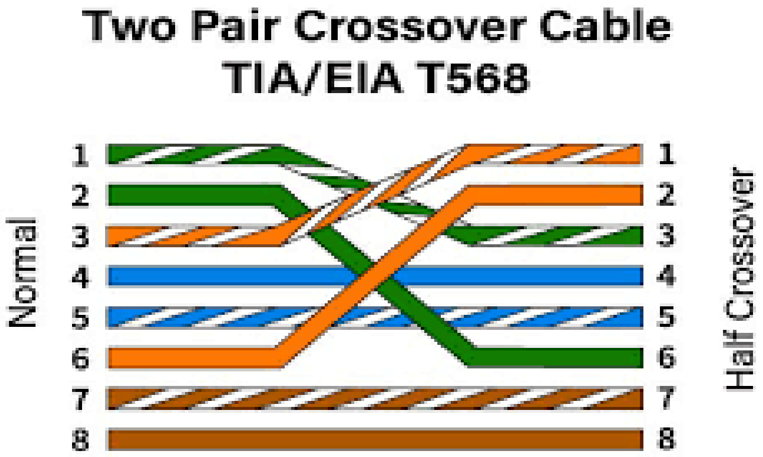
1 ⇄ 3 - Connect 1 to 3
2 ⇄ 6 - Connect 2 to 6

1 को 3 में connect करें

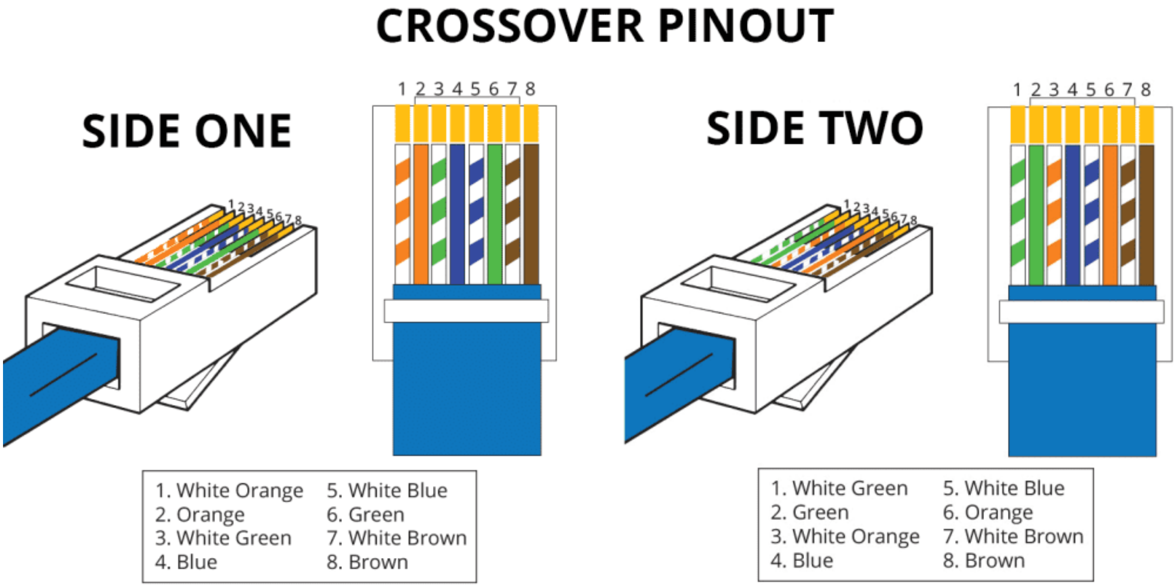
2 को 6 में connect करें

3 को 1 में connect करें

6 को 2 में connect करें



Colour Order



OSI MODEL

Layering: - Layering in Networking means breaking down the entire process of Communication in a network into different layers, where each layer has a specific function and interacts only with the layer directly.

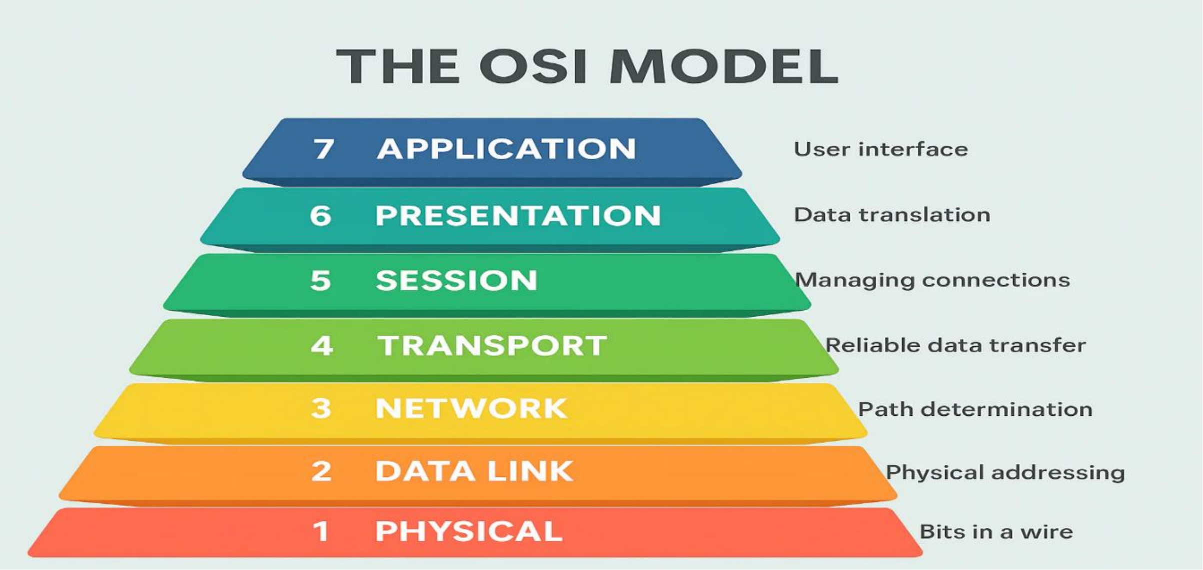
OSI Model

Open System Interconnection.

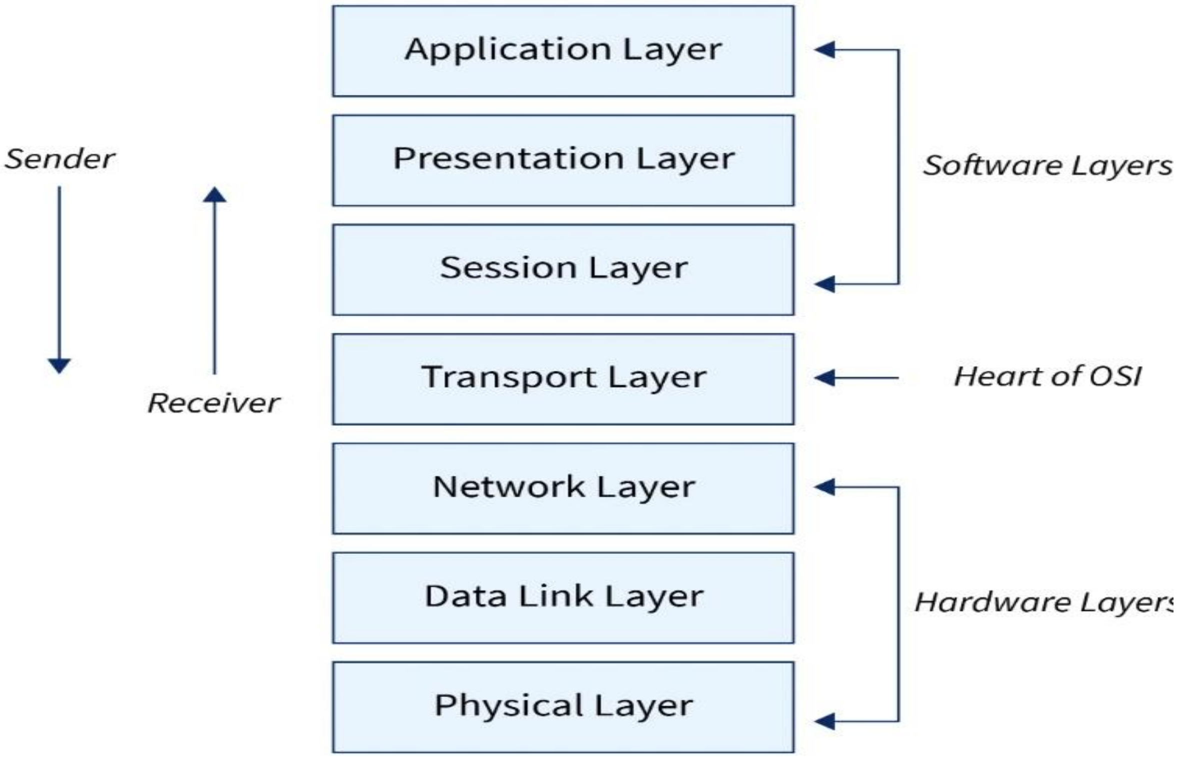
- Introduced in 1983
- Published by ISO in 1984

ISO(International Standards Organisation).

7 Types of the OSI Model



1. Application Layer
2. Presentation Layer Software Layer
3. Session Layer
4. Transport Layer → Heart of the Model
5. Network Layer
6. Data Link Layer Hardware Layer
7. Physical Layer

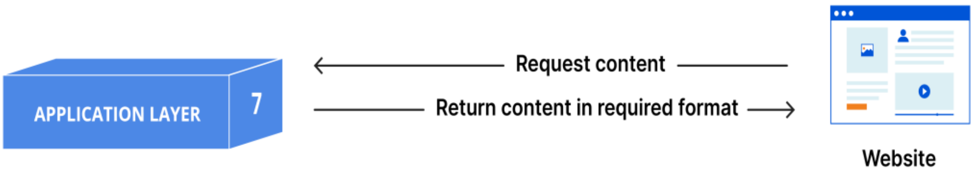


1. Application Layer

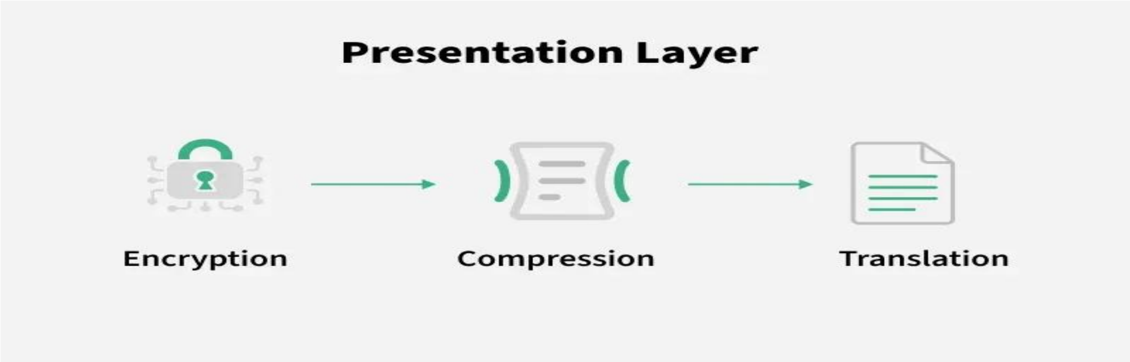
- ❖ Provide user interface
- ❖ provide different protocols HTTP, FTP, SMTP

Ex- Chrome, Microsoft Edge, Opera Mini Browser

Application Layer



2. Presentation Layer



(i) Data Encryption.

ABC → plane Tent

Xom COVEYpy JKJ0 0C693 KBgA – Ciphertext

(ii) Data Reformating

11-10-2025

↓

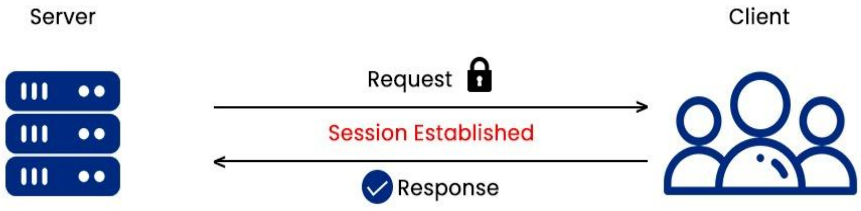
11/10/2025

(iii) Data compression.

Just like Images, videos compress

3. Session Layer

(i) Create and manage a session



(ii) Session maintenance

- Keeps the session active as long as communication continues.
- Maintains the correct order of data.
- Ensures that no data is duplicated or lost during transmission.

(iii)Add Check paints

(iv)**Dialog control**

- simplex - Tr broadcast, Radio transmission
- Half-Duplex - Walkie-talkies.
- Full-Duplex- Telephone calls, Zoom/Google Meet calls.

(v)**Session Termination**

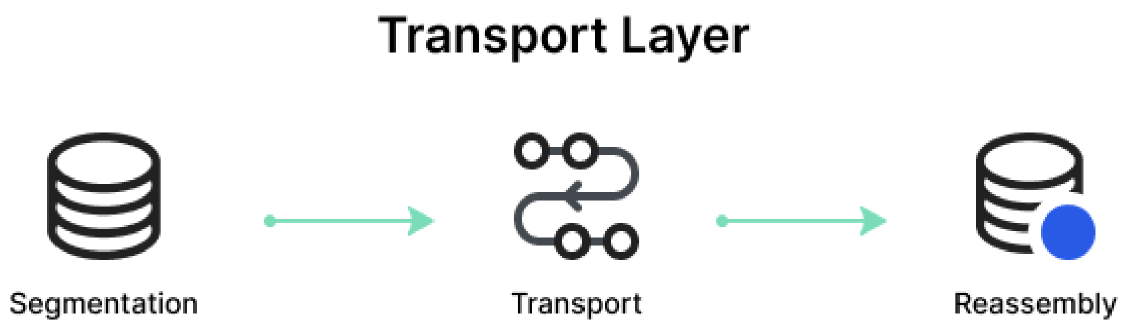
⇒ Safely closes the session when communication ends.

⇒ Faces up system resources Clive memory and ports).

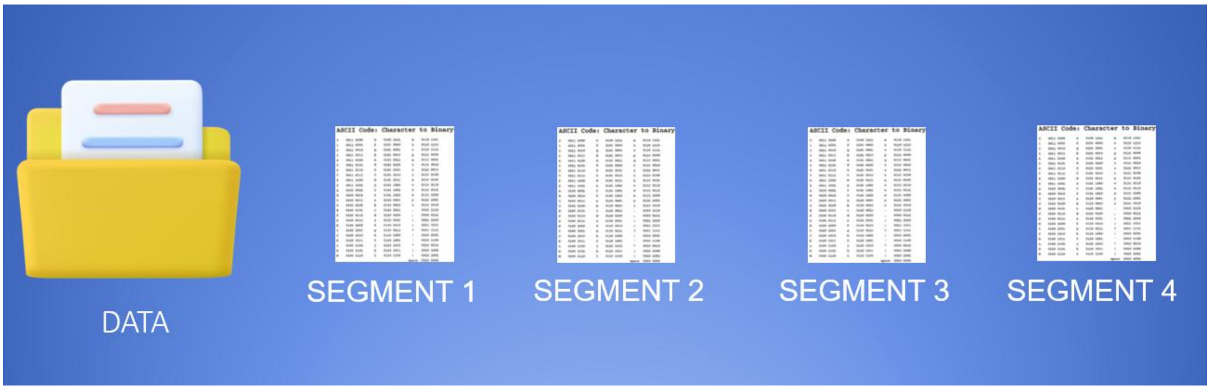
4. Transport layers

(i) Service to service layer

Direct communication with the program



(ii)**Convert data to segments**

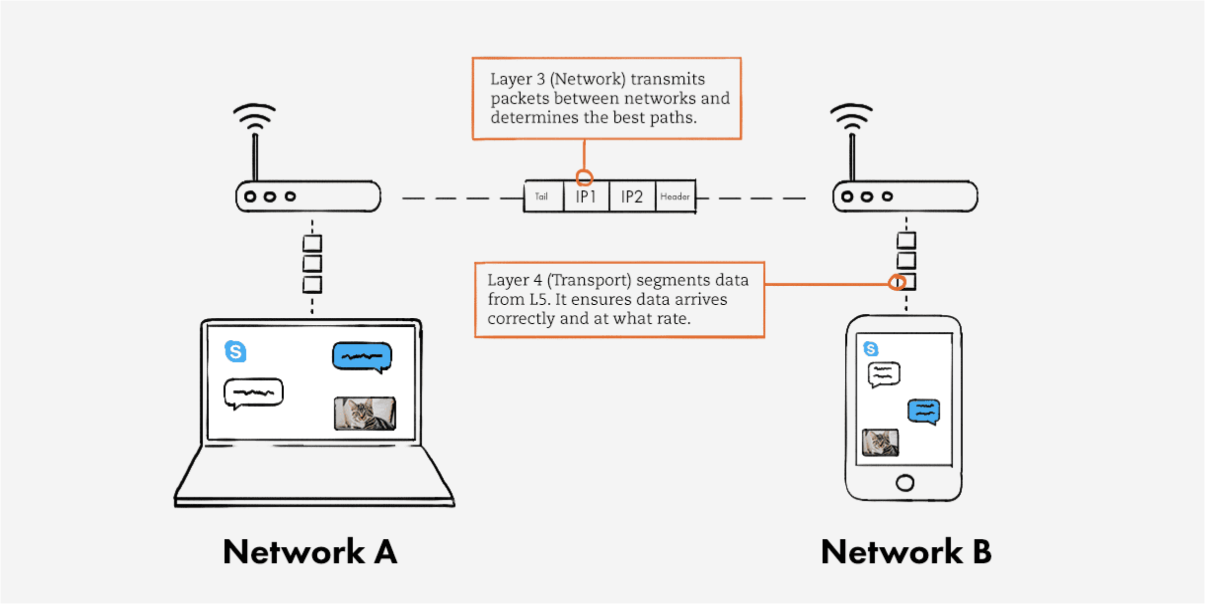


(iii)Controlling data Transportation

(iv)Data Flow control

5. Network Layer

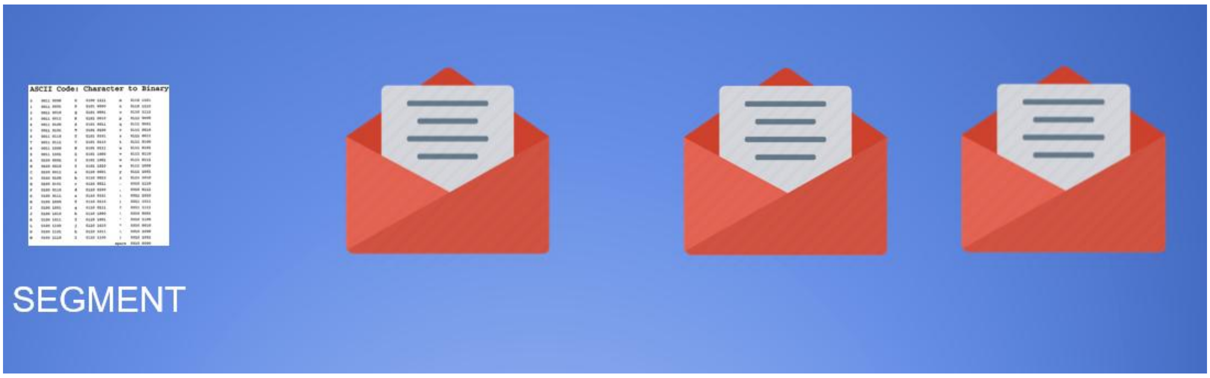
- Convert segment to packet
- Select the most quickest path add a header


Layer 3 (Network) transmits packets between networks and determines the best paths.
Tail
IP1
IP2
Header
Layer 4 (Transport) segments data from L5. It ensures data arrives correctly and at what rate.
Network A
Network B

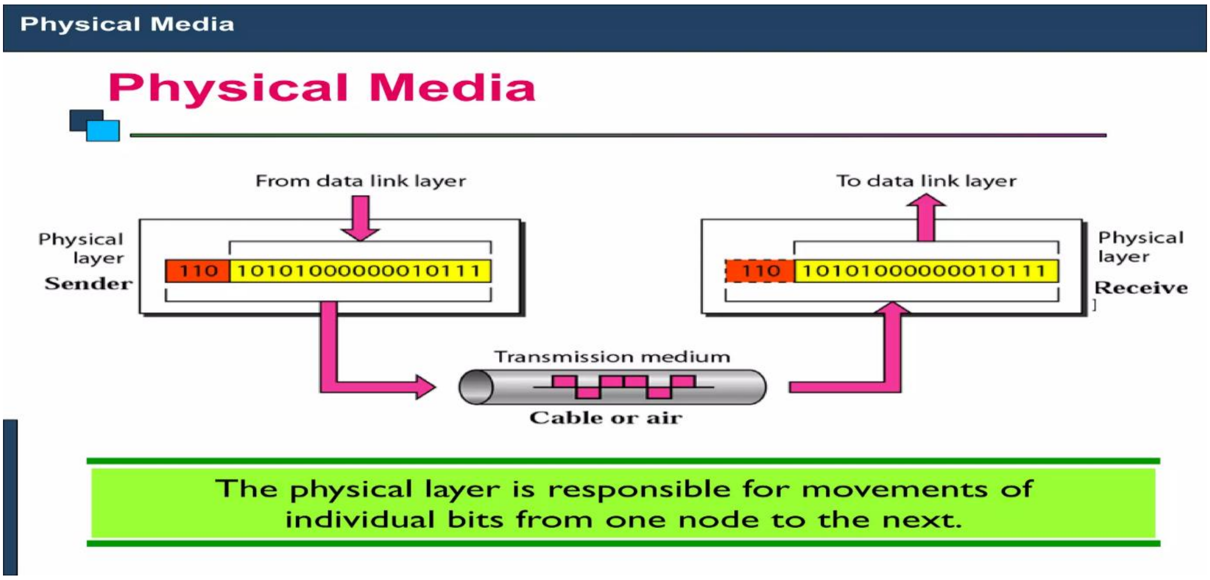
6. Data Link Layer

Convert packet to frame

Frame size 100 to 1000 bites



7. Physical Layer



Physical Media

Physical Media

The physical layer is responsible for movements of individual bits from one node to the next.

(i) **Bit Transmission**

converts data into bits (Os and 1s) and sends them.

Example: 101010 - Electrical pulses/Light pulses / Radio waves

(ii)**Physical Topology definition**

Determines the layout of physical connections between network devices.

Example:- Bus, star, Ring, mesh topology

(iii)**Transmission mode**

- ❖ Simplex Data flows in only one direction
- ❖ Half-Duplex: Data can flow in both directions. but only one direction at a time.
- ❖ Full-Duplex: Data can flow in both directions simultaneously

(iv)**Data Rate (Bit Rate) Definition**

specifies how many bits per second (bps) will be transmitted.

Example: 10 Mbps, 100 Mbps, 1 Gbps

(v)**Physical medium selection**

Chooses the medium for data transmission

Examples: -

- Copper Cable (Twisted pair, Coaxial)
- Fiber optic cable
- wireless (Radio waves, Infrared, microwaves)

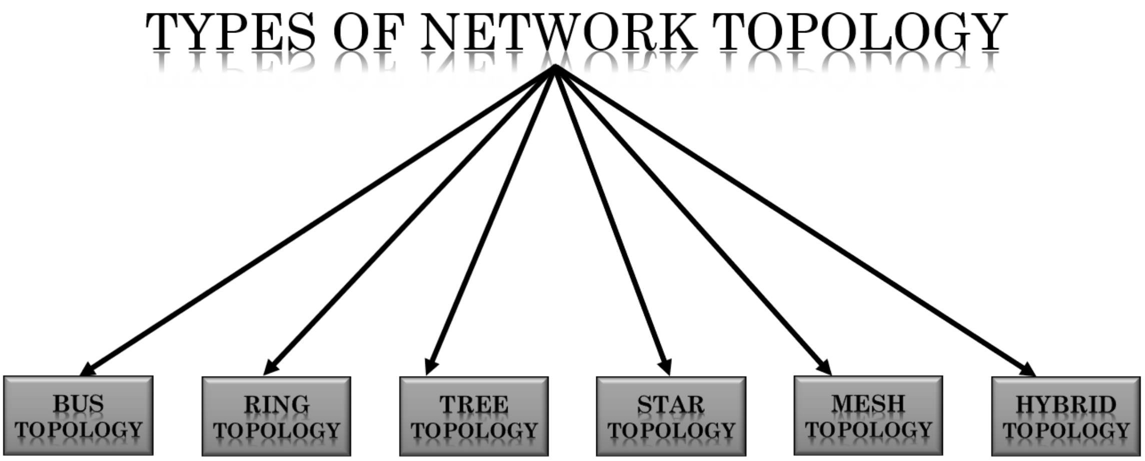
(vi)**Synchronisation of Bits**

- Ensures the sender and receiver clocks are synchronised
- so that 0s and 1s are correctly interpreted.

Network Topology

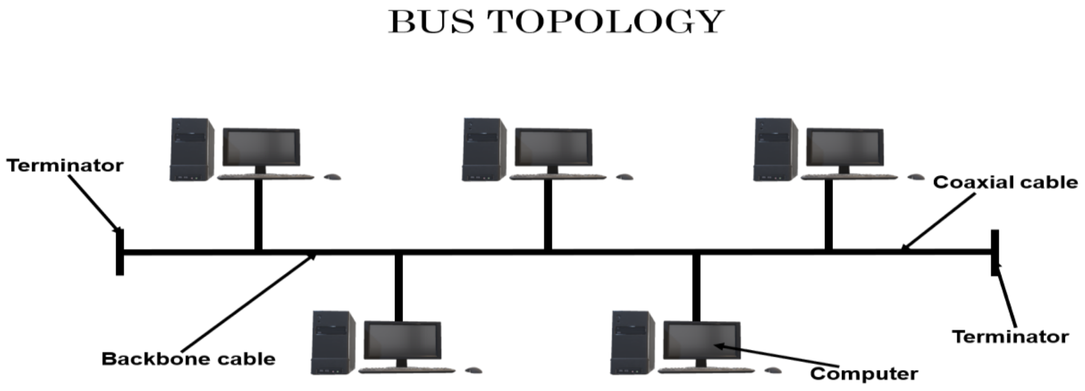
Network topology is the **arrangement or layout of computers, cables, and other devices** in a computer network. It describes how the different nodes (like computers, switches, and routers) are **connected** and how **data travels** between them.

Types of Network Topology



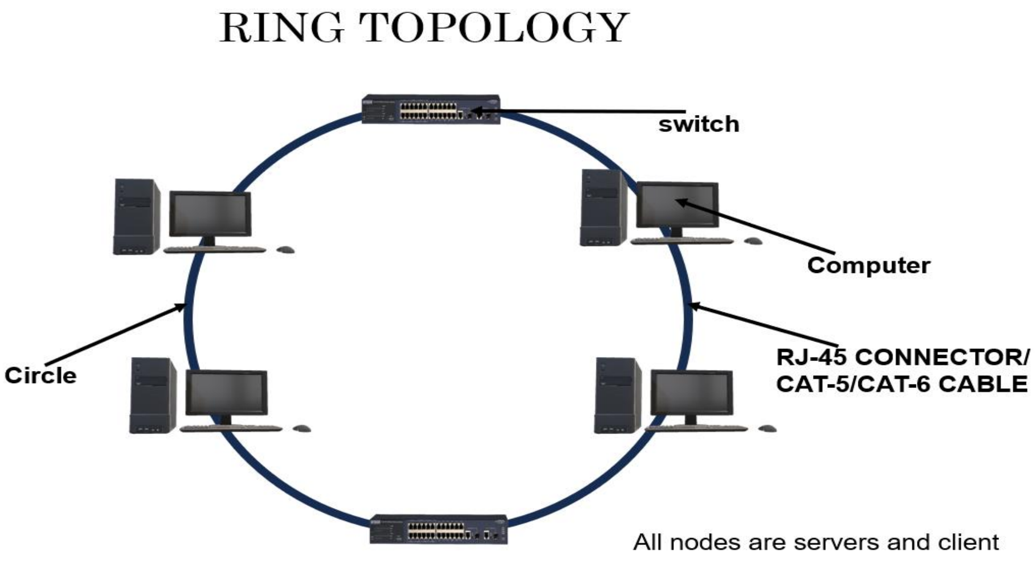
1. Bus Topology

- All devices are connected to a single central cable (called a bus or backbone).
- **Advantages:** Easy to install, requires less cable.
- **Disadvantages:** If the main cable fails, the entire network goes down.
- **Example:** Early LANs.



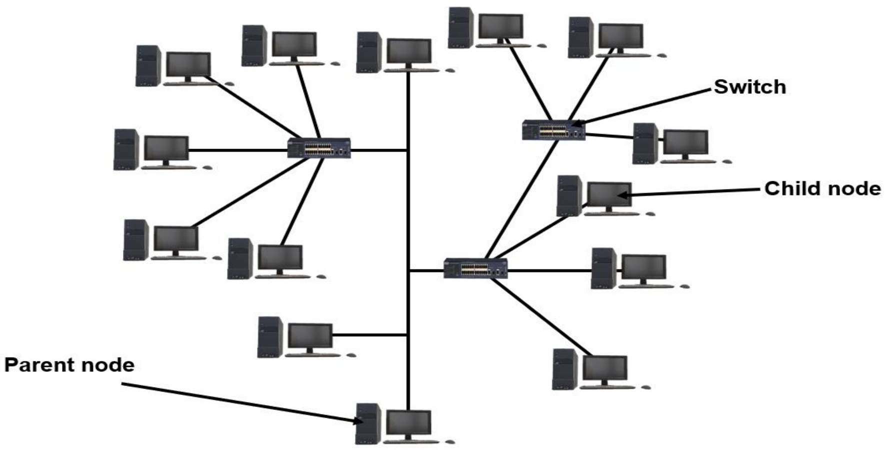
2. Ring Topology

- Each device is connected to two others, forming a circular path.
- **Advantages:** Data flows in one direction, reducing chances of collision.
- **Disadvantages:** Failure of one device affects the whole network.
- **Example:** Token Ring networks.



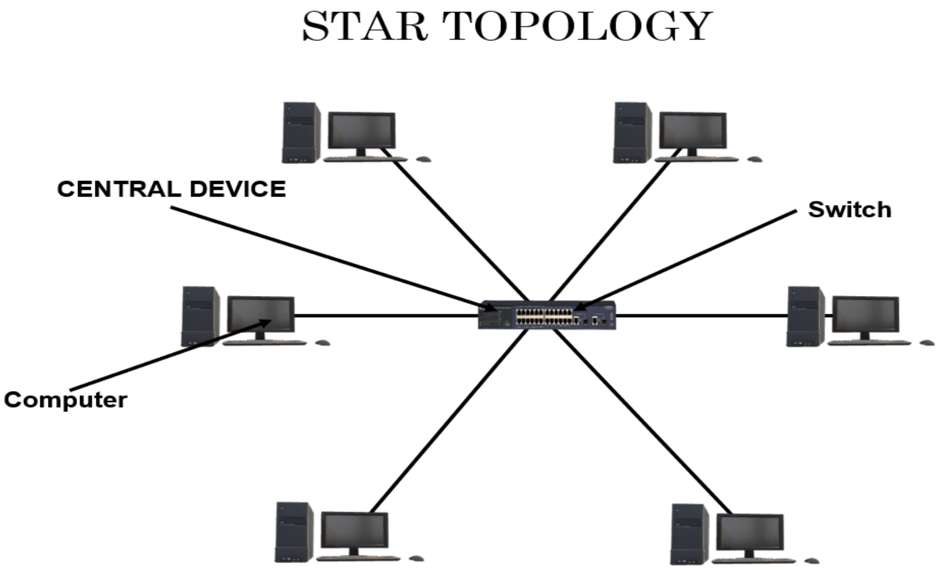
3. Tree (Hierarchical) Topology

- Combination of star topologies arranged in a hierarchy.
- **Advantages:** Easy to expand and manage.
- **Disadvantages:** If the root node fails, the entire segment is affected.
- **Example:** Used in large organisations.



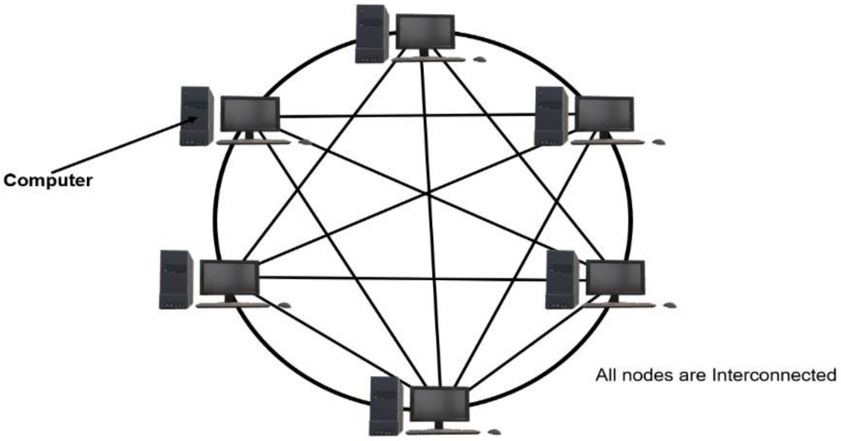
4. Star Topology

- All devices are connected to a central hub or switch.
- **Advantages:** Easy to manage, failure of one device doesn't affect others.
- **Disadvantages:** If the hub fails, the network fails.
- **Example:** Modern LANs.



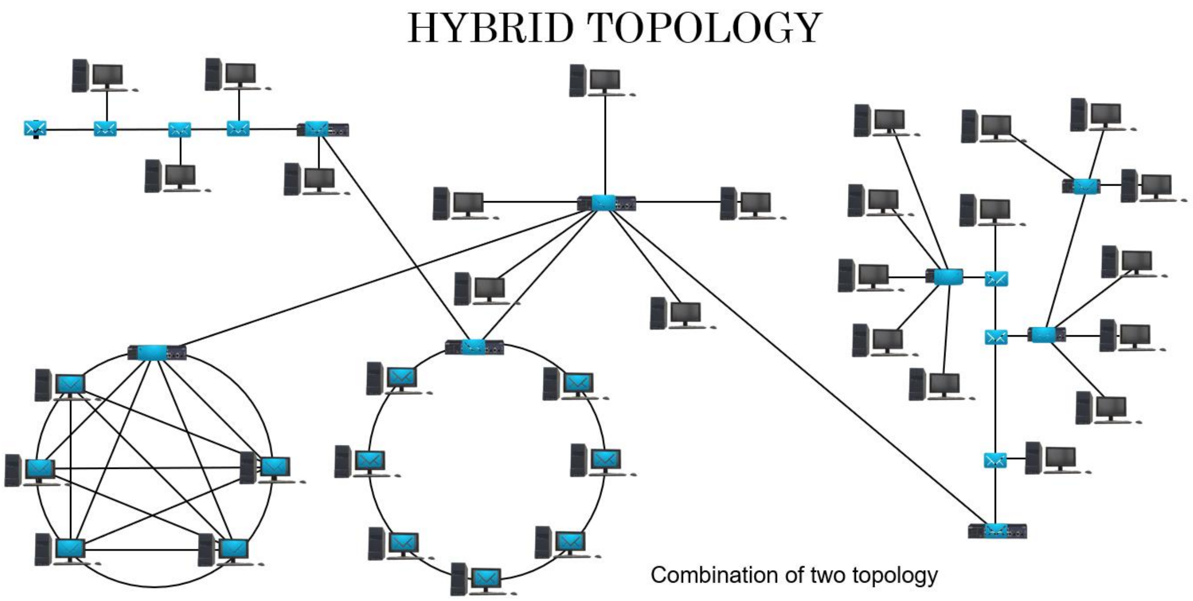
5. Mesh Topology

- Every device is connected to every other device.
- **Advantages:** Very reliable, no single point of failure.
- **Disadvantages:** Expensive due to high cabling cost.
- **Example:** Used in critical network setups (military, banking).



6. Hybrid Topology

- Combination of two or more topologies (**e.g**. star + ring).
- **Advantages:** Flexible and scalable.
- **Disadvantages:** Complex design and costly.



Network Topology - Practical

Cisco Packet Tracer

⇩

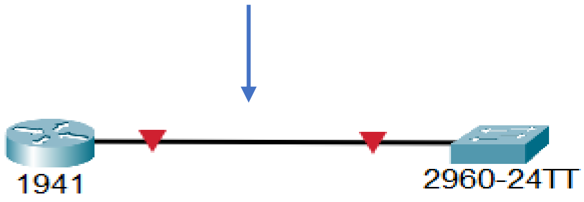
Download and install

⇩

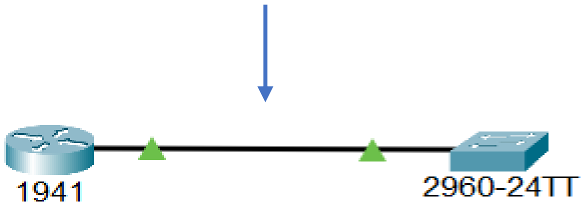
Testing for network Topology.

EX- Bus, star, ring, Tree, mesh, Hybrid Topology

→ Red Arrow रहने पर communication नहीं होगा।



→ Green Arrow रहने पर communication होगा।



IP Address Range

Class A = 1 – 126 → WAN

Class B = 128-191 → MAN

Class C = 192-223 → LAN

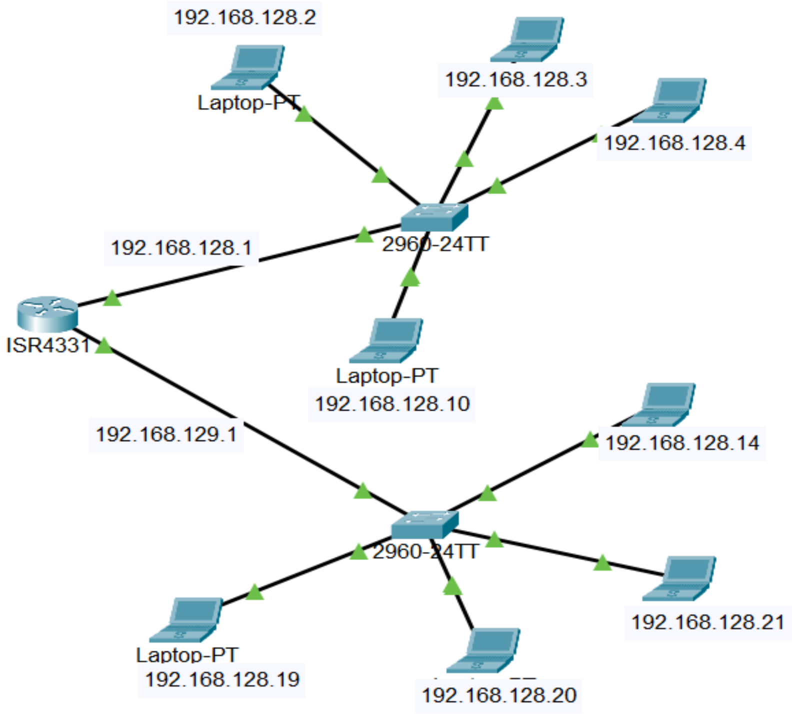
127 Loop back IP कहा जाता है।

IP address Assign करने के लिए follow steps

① select PC 🖥/Desktop / IP config / IPV4 Address

② Router/config/Gigabit Ethernet 0/0/0 / IP configuration/ON ✓

Note:- जब दो या दो से अधिक Router हो तब Static/RIP Routing किया जाता है ताकि मेसेज एक Router से दुसरे Router में आसानी से Send हो सके|



Switch CLI Practical

```
Switch> enable

Switch# configure terminal


Switch(config)# vlan 10

Switch(config-vlan)# name Accounts

Switch(config-vlan)# exit


Switch(config)# vlan 20

Switch(config-vlan)# name HR

Switch(config-vlan)# exit

Switch(config)# interface range fa0/1 - 5

Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

Switch(config)# interface range fa0/6 - 10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
```

For saving settings

```
Switch# write memory
```

Or

```
Switch# copy running-config startup-config
```

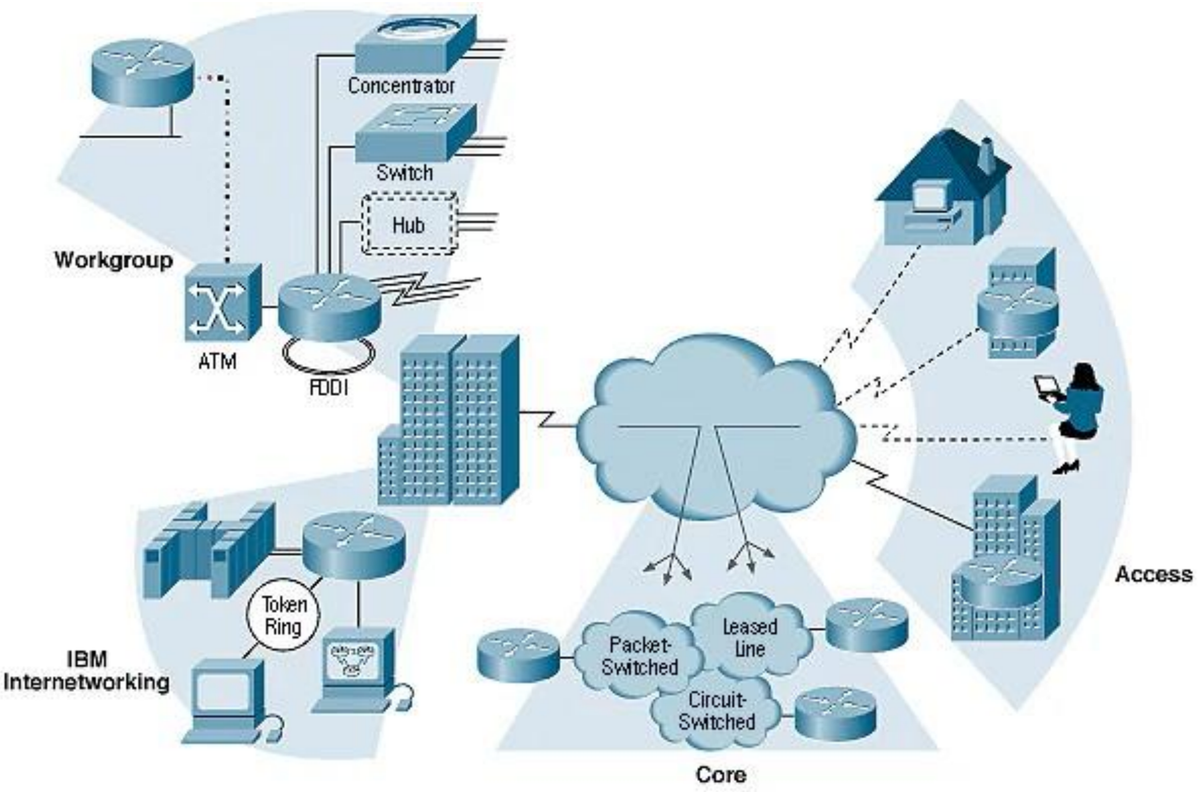
For details

```
Switch# show running-config
```

Delete CLI Data

```
Switch# erase startup-config
Switch# reload
```

Internetworking



Connecting multiple computer networks (LANs, MANs, WANs) to work as a single large network. Is called internetworking

Devices:-

- **Router –** Connects different networks.
- **Switch –** Connects devices within the same LAN.
- **Bridge –** Connects two LAN segments.
- **Gateway –** Connects networks using different protocols.

Router

- A Router is a networking device that connects two or more different networks and forwards data packets between them based on their IP addresses.
- It works at Layer 3 (Network Layer) of the OSI Model.

Switch

- A Switch is a networking device that connects multiple computers or devices within the same network (LAN) and forwards data to the correct device using MAC addresses.
- It works at Layer 2 (Data Link Layer) of the OSI Model.

Bridge

- A Bridge is a networking device that connects two or more LAN segments (Local Area Network segments) together to make them work as a single network.
- It works at Layer 2 (Data Link Layer) of the OSI Model, just like a switch.

Getway

- A Gateway is a networking device that connects two different networks that may use different communication protocols.
- It works at the OSI Model Layer 3 and above (Network Layer to Application Layer).
- If two networks use different communication protocols, the Gateway converts data from one format to another.
- Like-Email gateway converts emails between Internet (SMTP) and local mail system.
- Voice gateway converts VoIP packets into telephone signals.

IP (Internet Protocol)

- The main protocol for communication across the internet.
- Work at Layer: Network Layer (Layer 3).
- Version-

  IPv4: 32-bit address (e.g., 192.168.1.1).

  IPv6: 128-bit address (e.g., 2001:db8::1).

- ➢ Function –

  Logical addressing.

  Packet routing.

  Fragmentation and reassembly.

Addressing

- ➢ Addressing means giving an identity (address) to each device or node in a network, so that data can be sent and received correctly .

just like you need a home address to receive a letter.

Types

- **Physical Address (MAC address**) – Assigned to the NIC card, used at the Data Link Layer.
- **Logical Address (IP address)** – Used at the Network Layer for identifying hosts globally.
- **Port Address** – Identifies processes/services (e.g., HTTP → port 80).
- **Application Address (URL, email ID)** – Used at Application Layer.

Routing

- ➢ The process of selecting the best path for data to travel from source to destination across networks.
- ➢ Device used: Router.

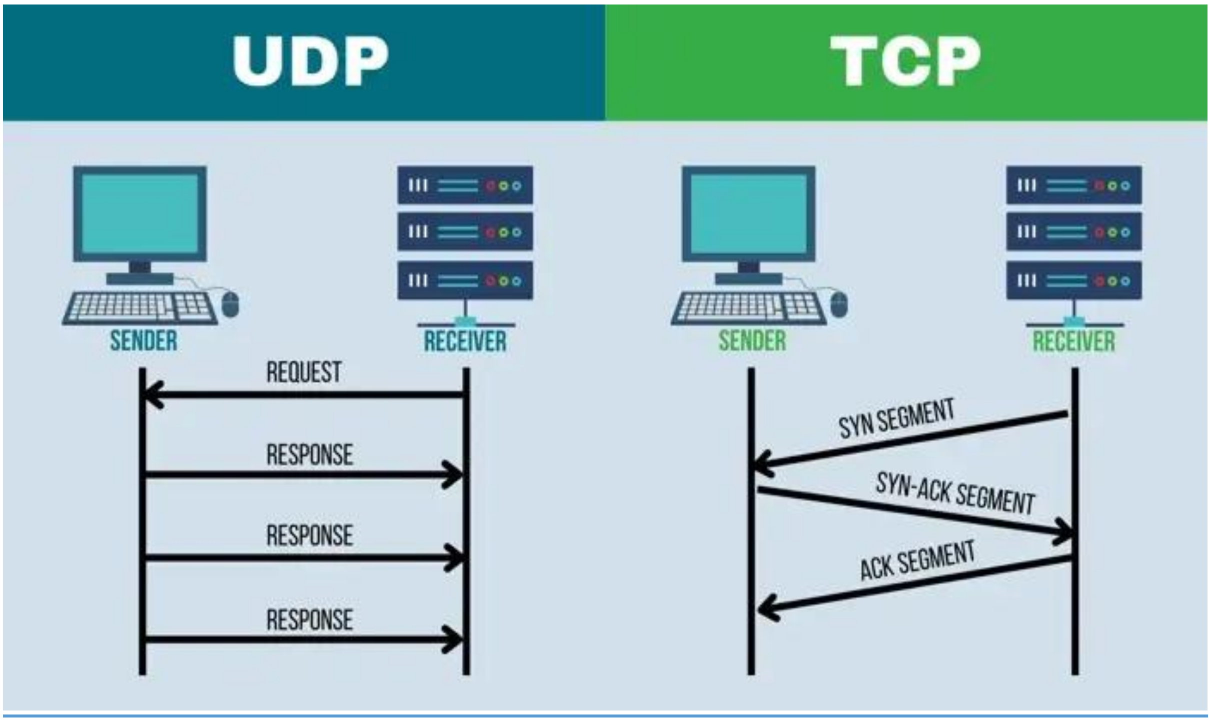
Types of Routing

- Static Routing – Manually configured by admin.
- Dynamic Routing – Routers exchange info automatically.
- Default Routing – All unknown traffic sent to a default route.

Routing Protocol

- These are algorithms used by routers to exchange routing information.
- Distance Vector Protocols (based on hop count):
    - RIP (Routing Information Protocol)
    - IGRP (Interior Gateway Routing Protocol)
- Link State Protocols (based on network topology):
    - OSPF (Open Shortest Path First)
    - IS-IS (Intermediate System to Intermediate System)
- Hybrid Protocols (mix of both):
    - EIGRP (Enhanced Interior Gateway Routing Protocol)
- Path Vector Protocol (used the Internet):
    - BGP (Border Gateway Protocol)

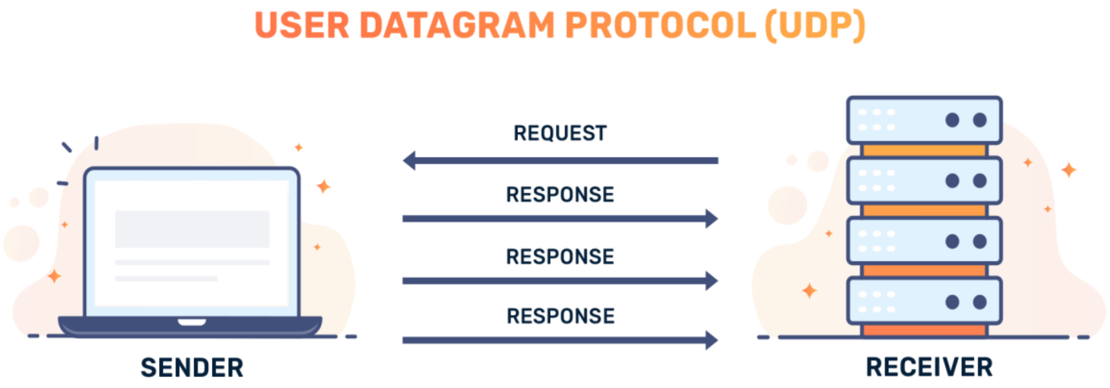
UDP and TCP



UDP (User Datagram Protocol)

Works at the **Transport Layer** of the OSI Model.

- It is a Connectionless Protocol.
- It has no Error Control, Flow Control, or Congestion Control.
- Simply sends data without checking whether it has reached the destination.
- It is fast but unreliable.



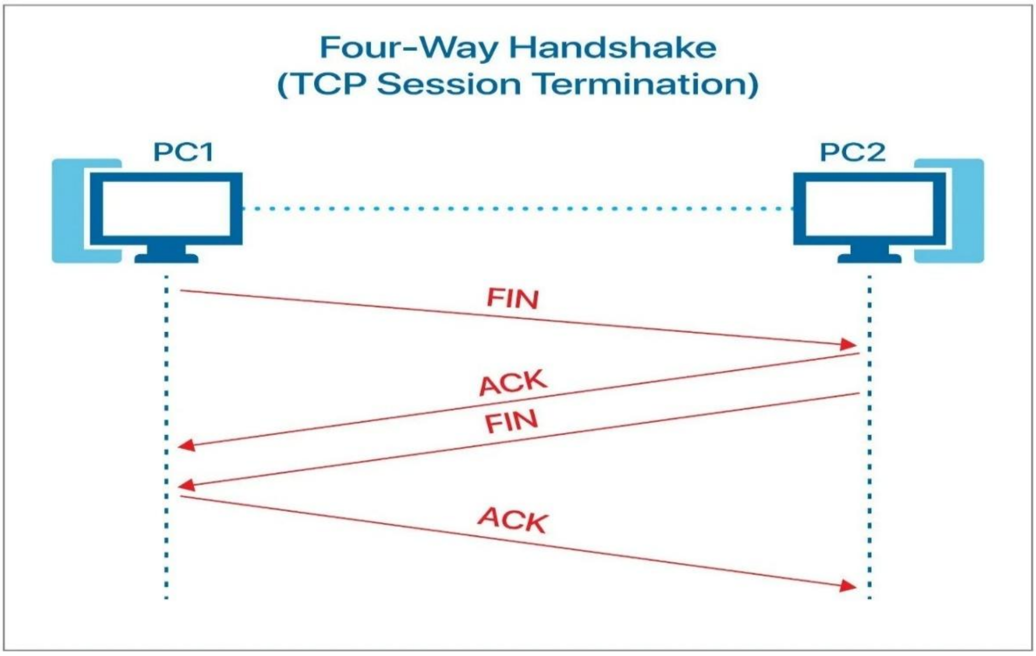
Examples:

- DNS Query
- VoIP (Voice over IP)
- Video Streaming
- Online Gaming

TCP (Transmission Control Protocol)

Works at the Transport Layer of the OSI Model.

- It is a Connection-Oriented Protocol.
- Provides Error Control, Flow Control, and Congestion Control.
- Breaks data into smaller units called segments.
- Uses Acknowledgement (ACK) to ensure data is received correctly.



Examples:

- HTTP / HTTPS
- Email (SMTP, POP3)
- File Transfer (FTP)

Congestion Control

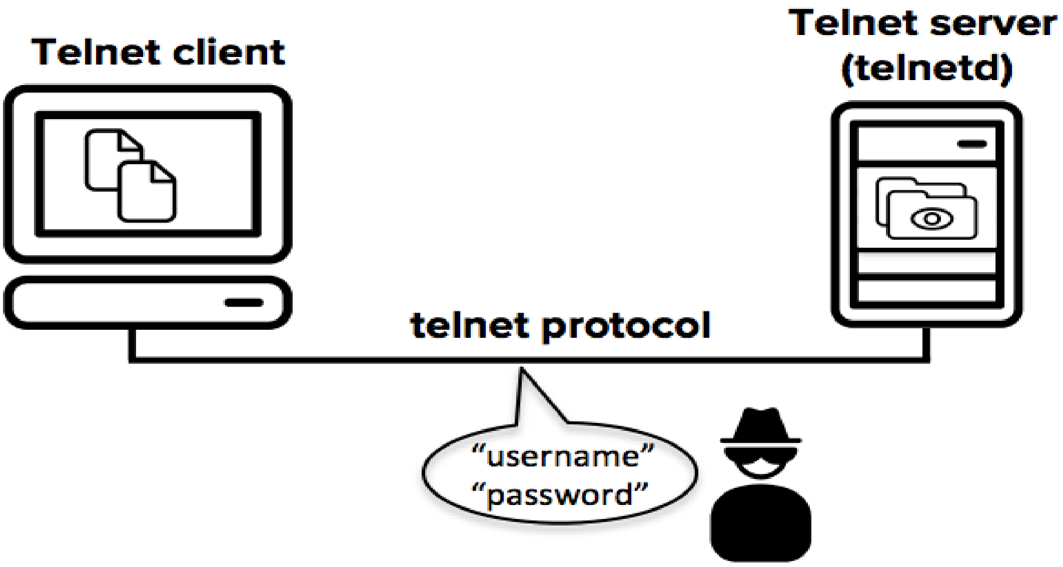
- When too many packets are transmitted simultaneously and exceed the router or link capacity, network congestion occurs.
- To control network traffic and reduce packet loss and delay.

Presentation Aspects

Converts data into a format that the Application Layer can understand.

- Data Translation – Converts between different data formats (e.g., ASCII ↔ EBCDIC).
- Data Encryption/Decryption – Secures data for transmission.
- Data Compression/Decompression – Reduces data size for faster transmission.

TELNET



TELNET (short for **Telecommunication Network**) is a **network protocol** used to provide a command-line interface for communication with a **remote device (router, switch) or server.**

How TELNET Works

1. The Telnet client connects to the Telnet server on port 23.
2. The user provides username and password for authentication.
3. After login, the user can run commands on the remote device as if they were using it locally**.**

Uses of TELNET

- To remotely configure network devices (like routers and switches).
- To test connectivity to specific ports.
- To access servers or mainframes remotely.

Features of TELNET

1. **Text-Based Protocol**
   - Communication happens using plain text commands through a command-line interface (CLI).
   - Makes it simple to send and receive text-based data.
2. **Remote Access**
   - Allows users to log in and control remote computers or network devices over a network.
   - Useful for configuring routers, switches, and servers from anywhere.
3. **TCP/IP Protocol**
   - Works using the TCP/IP protocol suite.
   - Uses TCP port 23 by default for reliable connection-oriented communication.
4. **Client-Server Model**
   - A Telnet client connects to a Telnet server to start a remote session.
5. **Interactive Command Session**
   - Users can run commands in real-time on the remote device.
6. **Platform Independent**
   - Works on various operating systems (Windows, Linux, macOS, Cisco devices, etc.).

Steps for TELNET Complete Communication

1. **Connection Establishment**
   The Telnet client connects to the Telnet server using TCP port 23**.**
2. **Command Execution**
   The user logs in and enters commands through the virtual terminal**.**

3. **Data Exchange**
   Commands and responses are sent and received as plain text between client and server.

TELNET Commands Example (Cisco Router)

```
Router>en

Router#config t

Router(config)# line vty 0 4

Router(config-line)# password cisco

Router(config-line)# login

Router(config-line)# transport input telnet

Router(config-line)# exit

Router(config)# enable password admin
```

After configuration, you can connect using

```
telnet <IP address>
```

Advantages:

- Simple and easy to use.
- Allows remote device management.

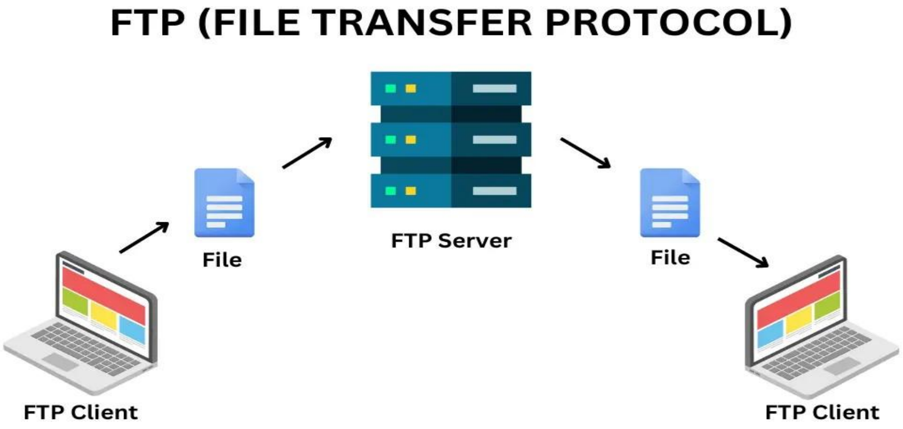
Disadvantages:

- **Not secure** — data (including passwords) is sent in **plain text**.
- Can be easily intercepted by attackers.
- **Replaced by SSH (Secure Shell)** for secure remote access.

FTP – FILE TRANSFER PROTOCOL

FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files from one host to another over a TCP-based network, such as the Internet.

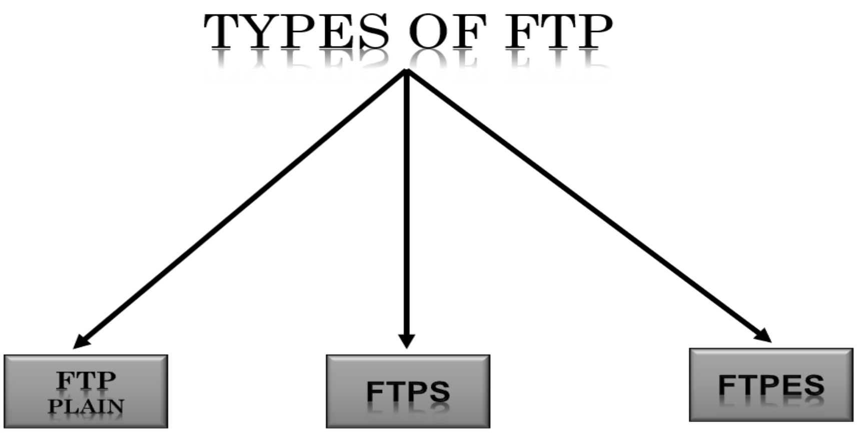
FTP works by opening two connections that link the computers trying to communicate with each other. One connection is designated for the commands and replies that get sent between the two clients, and the other channel handles the transfer of data. During an FTP transmission, there are four commands used by the computers, servers, or proxy servers that are communicating. These are “send,” “get,” “change directory,” and “transfer.”



FTP Useful for

One of the main reasons why modern businesses and individuals need FTP is its ability to perform large file size transfers. When sending a relatively small file, like a Word document, most methods will do, but with FTP, you can send hundreds of gigabytes at once and still get a smooth transmission.

Types Of FTP



FTP Plain

FTP Plain refers to the standard **FTP** protocol without encryption. By default, it uses port 21 and is supported by most web browsers.”

FTPS

FTPS refers to FTP Secure or FTP Secure Sockets Layer (SSL) because this kind of FTP server uses SSL encryption, which is slightly different from traditional FTP. The primary difference is the security that comes with FTPS, which was the first type of encrypted FTP invented.

FTPES

The “E” in FTPES means “explicit,” making the acronym stand for File Transfer Protocol over explicit transport layer security (TLS)/SSL. This type of FTP begins like regular FTP, using port 21, but then special commands upgrade it to a TLS/SSL-encrypted transmission. Because it tends to work well with firewalls, some prefer to use FTPES over FTPS.

Email

Electronic mail, commonly shortened to “email,” is a communication method that uses electronic devices to deliver messages across computer networks. "Email" refers to both the delivery system and individual messages that are sent and received.

Email has existed in some form since the 1970s, when programmer Ray Tomlinson created a way to transmit messages between computer systems on the Advanced Research Projects Agency Network (ARPANET). Modern forms of email became available for widespread public use with the development of email client software (e.g. Outlook) and web browsers, the latter of which enables users to send and receive messages over the Internet using web-based email clients (e.g. Gmail).

Once an email message has been sent, it follows several steps to its final destination:

- The sender’s mail server, also called a Mail Transfer Agent (MTA), initiates a Simple Mail Transfer Protocol (SMTP) connection.
- The SMTP checks the email envelope data — the text that tells the server where to send a message — for the recipient’s email address, then uses the Domain Name System (DNS) to translate the domain name into an IP address.

- The SMTP looks for a mail exchange (MX) server associated with the recipient’s domain name. If one exists, the email is forwarded to the recipient’s mail server.
- The email is stored on the recipient’s mail server and may be accessed via the Post Office Protocol (POP)* or Internet Message Access Protocol (IMAP). These two protocols function slightly differently: POP downloads the email to the recipient’s device and deletes it from the mail server, while IMAP stores the email within the email client, allowing the recipient to access it from any connected device.
- Using port 587

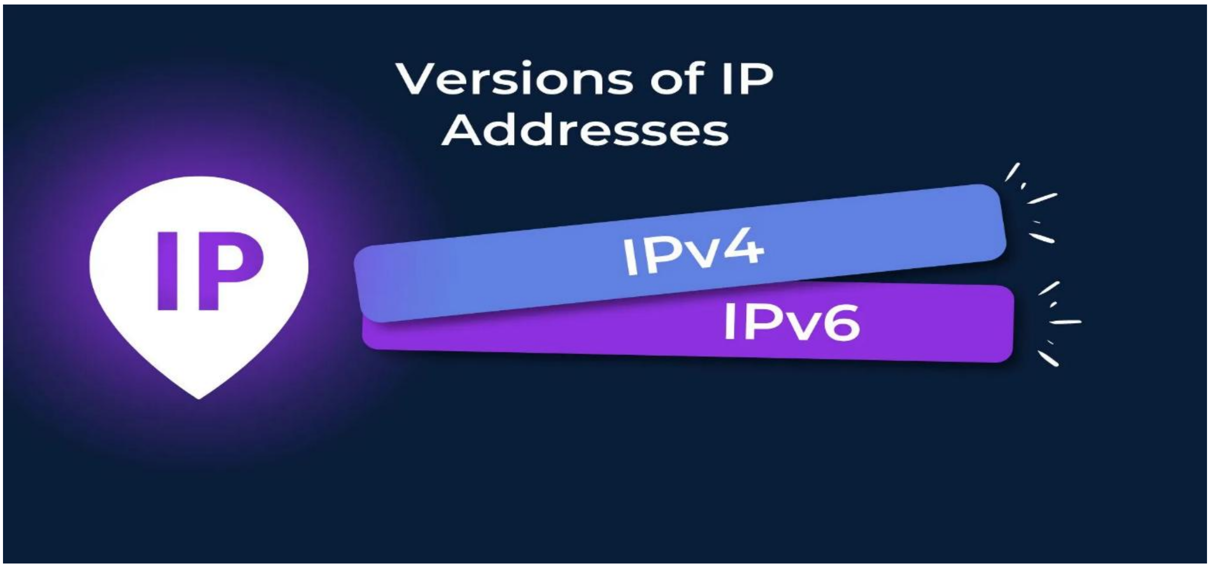
IP Address (Internet Protocol)

An IP address is a source or destination address for connecting with network.

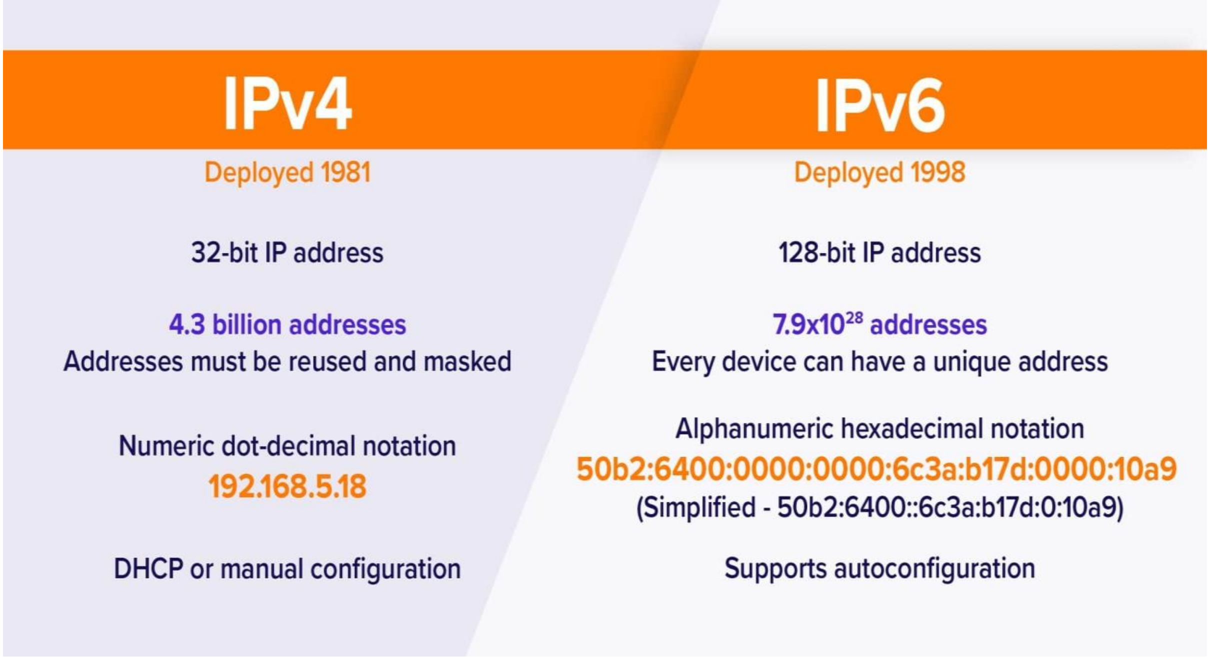
It’s allowing devices to send or receive information within a network

IP addresses are not random. They are mathematically produced and allocated by the (IANA) INTERNET ASSIGNED NUMBERS AUTHORITY, a division of the (ICANN) INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS . ICANN is a non-profit organization that was established in the united States in 1998 to help maintain the security of the internet.

IP Version



IP Version



IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	$7.9x10^{28}$ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

IPV4

192.168.128.1

TYPES OF IPV4

CLASS A	**1 - 126**	**N.H.H.H**
CLASS B	**128-191**	**N.N.H.H**
CLASS C	**192-223**	**N.N.N.H**
CLASS D	**224-239**	RESERVE FOR FUTURE AND SCIENTIFIC RESEARCHERS
CLASS E	**240-255**	MULTICASTING

127 ip is a loopback ip

PRIVATE IP IN IPV4

CLASS A	10.0.0.0	to	10.255.255.255.
CLASS B	172.16.0.0	to	172.31.255.255
CLASS C	192.168.0.0	to	192.168.255.255

IPV4 SUBNETTING

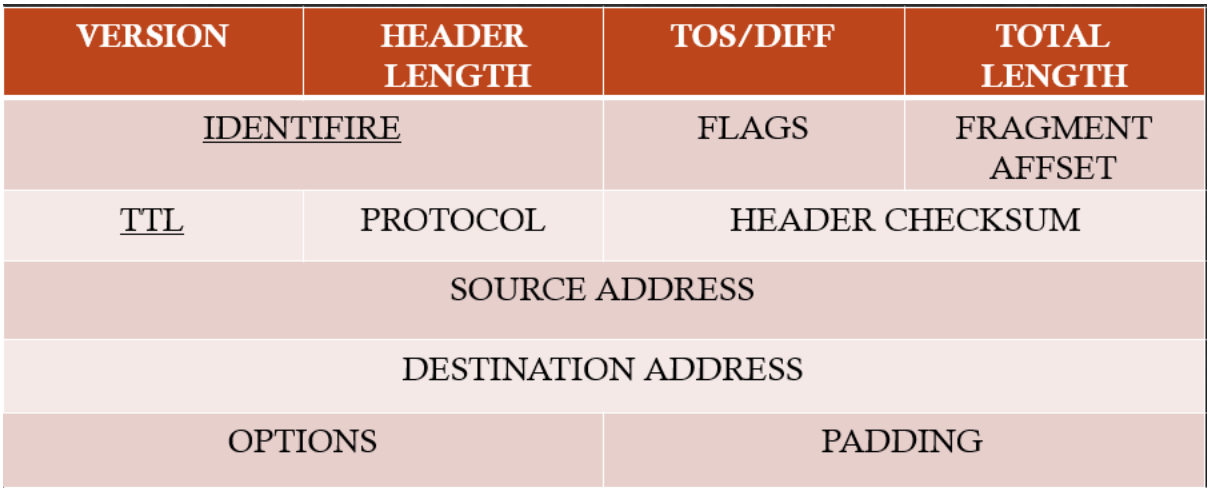
192.168.128.10

00000000.00000000.00000000.00000000

11111111.11111111.11111111.00000000

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

IPV4 HEADER



VERSION	HEADER LENGTH	TOS/DIFF	TOTAL LENGTH
IDENTIFIRE		FLAGS	FRAGMENT AFFSET
TTL	PROTOCOL	HEADER CHECKSUM	
SOURCE ADDRESS			
DESTINATION ADDRESS			
OPTIONS		PADDING	

IPV4 HEADING

VERSION	HEADER LENGTH	TOS/DIFF	TOTAL LENGTH
IDENTIFIRE		FLAGS	FRAGMENT AFFSET
TTL	PROTOCOL	HEADER CHECKSUM	
SOURCE ADDRESS			
DESTINATION ADDRESS			
OPTION		PADDING	

- **VERSION**: 4 bits
- **HEADER LENGTH**: 4 bits
- **TOS/DIFF**: 8 bits
- **TOTAL LENGTH**: 16 bits
- **IDENTIFIER**: 16 bits
- **FLAGS**: 3 bits
- **FRAGMENT OFFSET**: 13 bits
- **TTL**: 8 bits
- **PROTOCOL**: 8 bits
- **HEADER CHECKSUM**: 16 bits
- **SOURCE ADDRESS**: 32 bits
- **DESTINATION ADDRESS**: 32 bits
- **OPTIONS**: Variable length
- **PADDING**: Variable length

CLASS

000 DEFAULT :- Standard emails or non-urgent web browsing.

001 PRIORITY :- Business-critical emails or high-priority application traffic.

010 IMMEDIATE :- Financial transactions or real-time gaming.

011 FLASH :- Emergency notifications or critical VoIP calls.

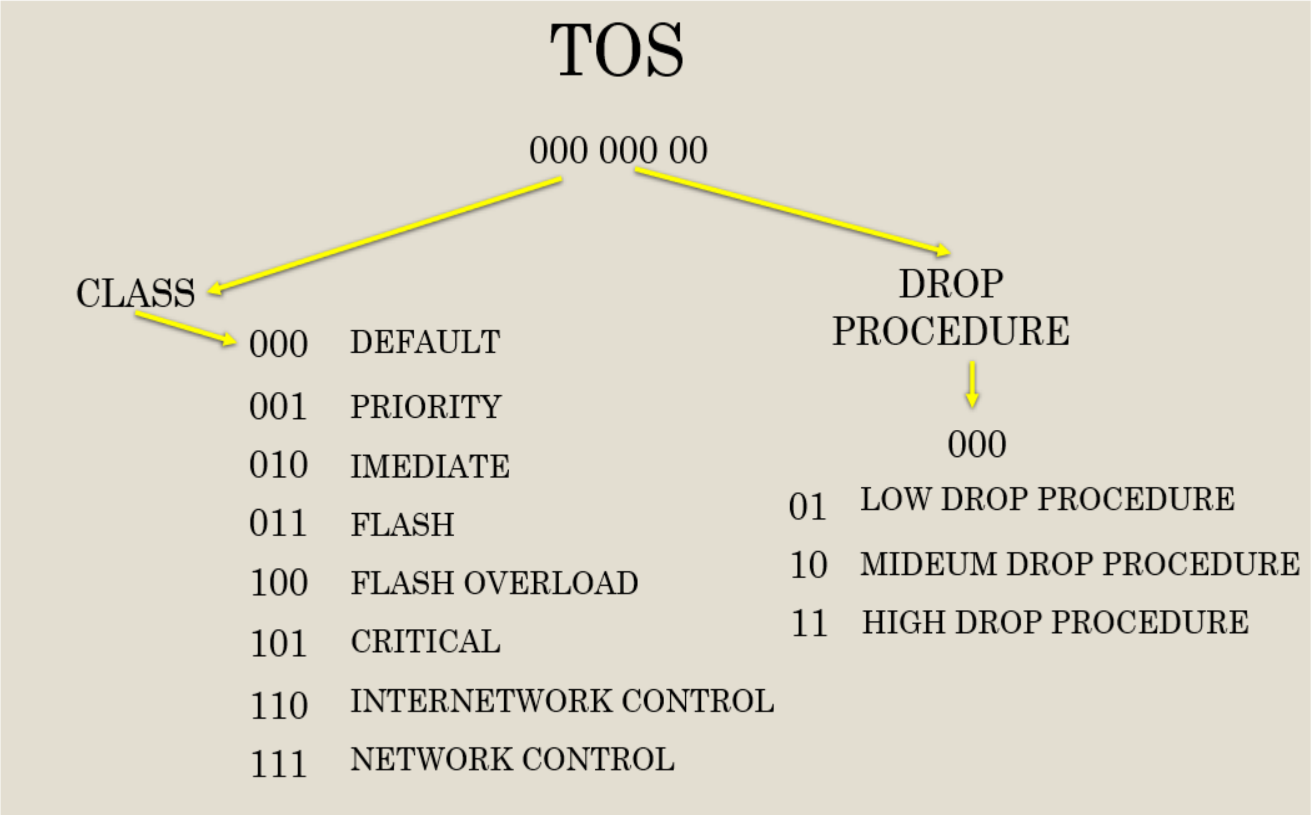
100 FLASH OVERLOAD :-
Police or fire department communications during emergencies.

101 CRITICAL :-
Government or military communications in crisis situations.

110 INTERNETWORK CONTROL :-
Routing updates or BGP messages between routers.

111 NETWORK CONTROL :-
Messages related to network stability and control protocols.

TOS



TOS

000 000 00

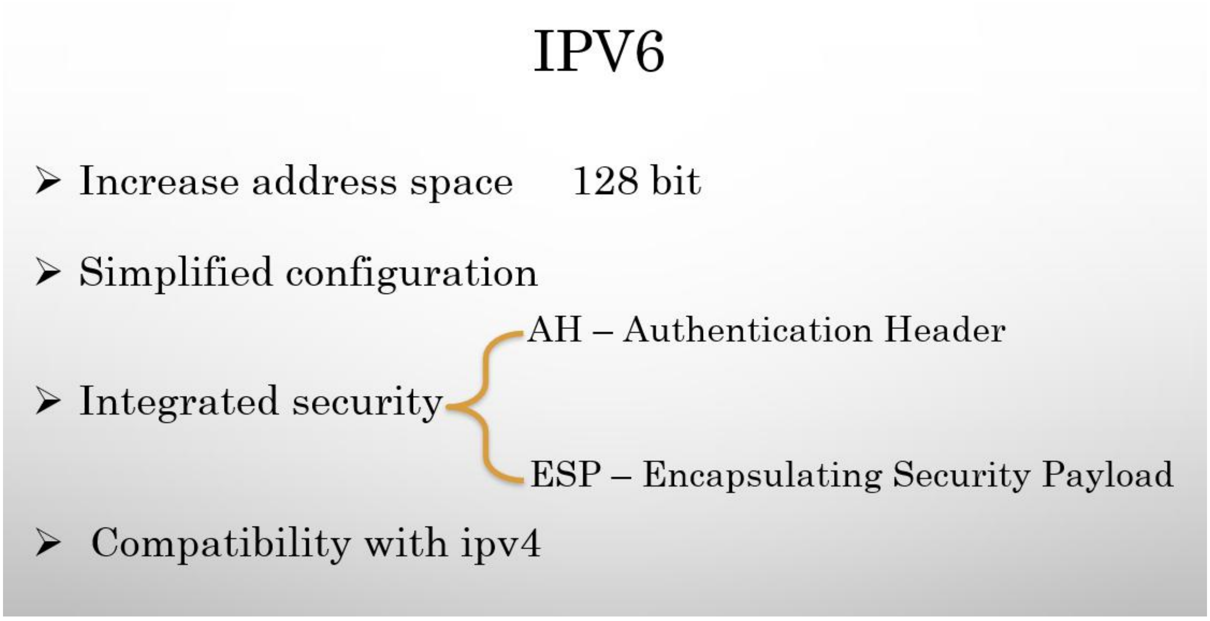
CLASS

000 DEFAULT
001 PRIORITY
010 IMEDIATE
011 FLASH
100 FLASH OVERLOAD
101 CRITICAL
110 INTERNETWORK CONTROL
111 NETWORK CONTROL

DROP PROCEDURE

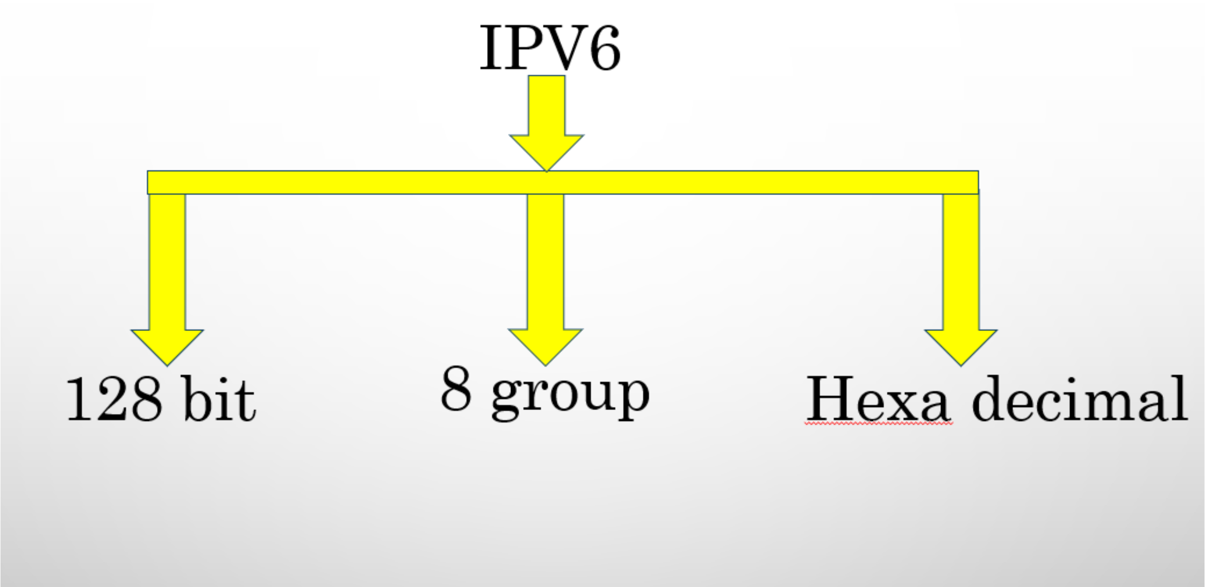
000
01 LOW DROP PROCEDURE
10 MIDEUM DROP PROCEDURE
11 HIGH DROP PROCEDURE

IPV6



IPV6

- Increase address space 128 bit
- Simplified configuration
- Integrated security
  - AH – Authentication Header
  - ESP – Encapsulating Security Payload
- Compatibility with ipv4



IPV6

128 bit

8 group

Hexa decimal

IPV6

16 . 16 . 16 . 16 . 16 . 16 . 16 . 16

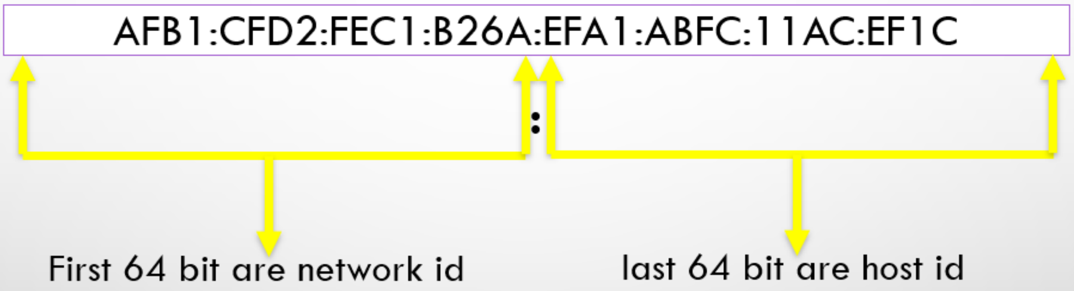
AFB1:CFD2:FEC1:B26A:EFA1:ABFC:11AC:EF1C

0FB1:0000:0000:006A:0000:0000:00AC:0F1C

AFB1:0:0:B26A::11AC:EF1C

IPV6

Network prefix



AFB1:CFD2:FEC1:B26A:EFA1:ABFC:11AC:EF1C

:

First 64 bit are network id

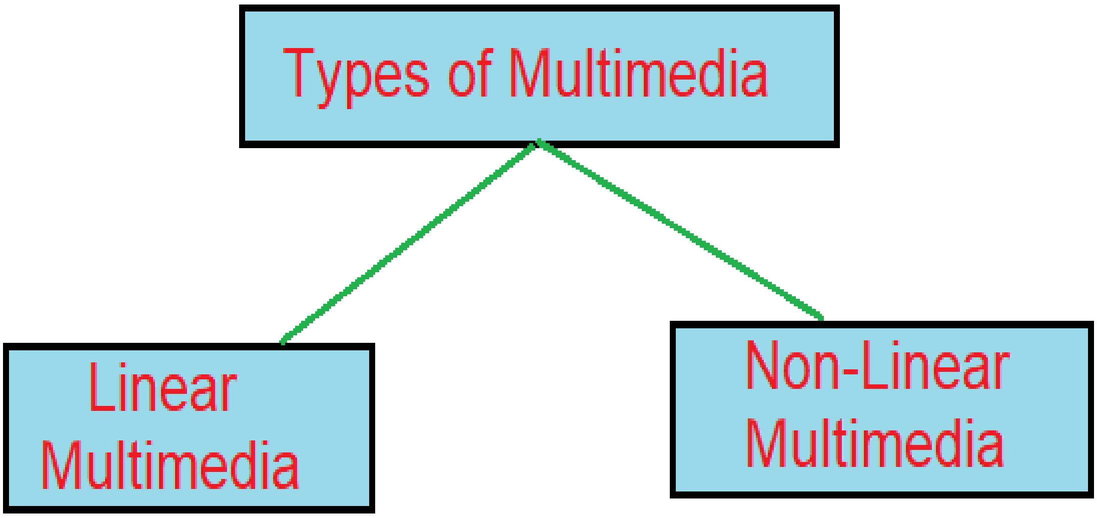
last 64 bit are host id

MULTIMEDIA

Multimedia is a technology where two or more media components are used together to present information. It includes **Text**, **Audio**, **Images**, **Animation**, and **Video**.

Types of Multimedia

1. **Linear Multimedia**
2. **Non-Linear Multimedia**



Linear Multimedia

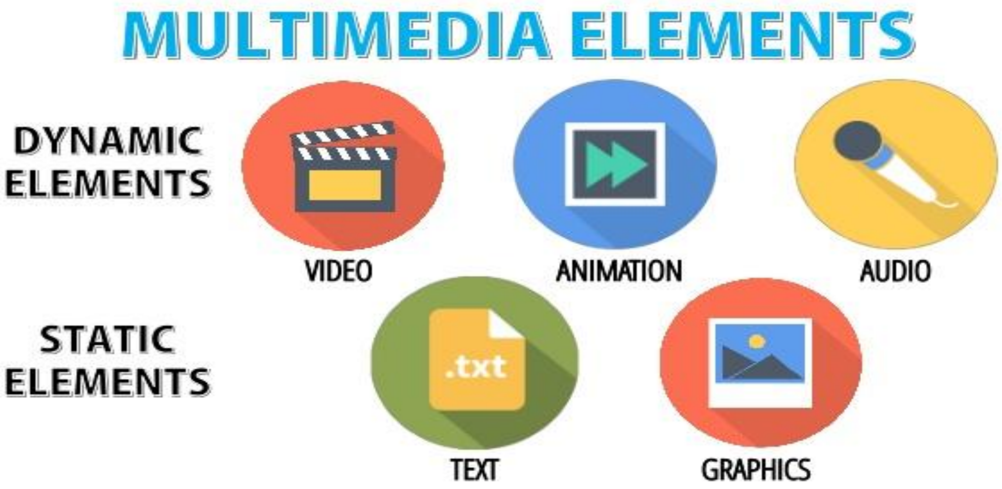
The user only watches/listens, with no control over the content.
Example: TV shows, Movies

Non-Linear Multimedia

The user can interact with the content.
Example: Websites, Games, E-learning

Elements of Multimedia

1. Text
2. Audio
3. Image
4. Animation
5. Video



Text

The most common and basic form of information.
Used in headings, paragraphs, buttons, links, etc.

Image

A visual medium to convey information.
Formats: JPEG, PNG, BMP, etc.
Examples: Diagrams, Photos, Charts.

Animation

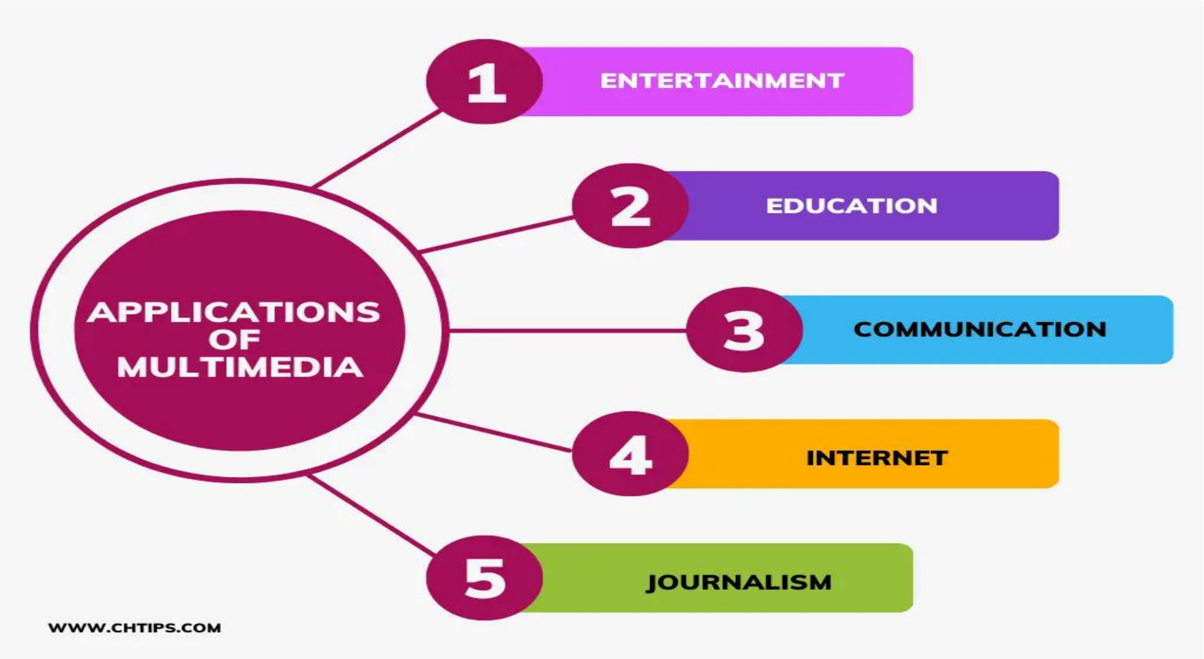
A Series of changing images that create an illusion of motion.
Usage: Cartoons, Scientific Experiments, Simulations.

Video

A combination of moving images and sound.
One of the most impactful mediums.
Formats: MP4, AVI, MOV

APPLICATION OF MULTIMEDIA

1. Education
2. Entertainment
3. Healthcare



Education

Helps to easily understand complex topics through animation and video.
Forms the basis of e-learning and virtual classes.

Entertainment

Entertainment is a form of activity that holds the attention and interest of an audience or gives pleasure and delight. It can be an idea or a task,

Ex- Movies, games, music, social media content. CC

Healthcare

Multimedia plays a pivotal role in medical imaging, such as MRI, CT scans, and ultrasounds, by producing high-resolution visual data for accurate diagnoses.

Surgical simulations, medical training and health guide videos.

Advantages and limitations

Advantage	Limitation
1. Makes education interesting 2. User engagement through interactivity 3. Available in multiple languages and formats 4. A powerful medium for communication	1. High development cost 2. Requires large storage 3. Needs fast processors and better hardware 4. Issues with slow internet connectivity

SECURITY, MONITORING & CONTROL

Security, monitoring, and control in computer networks are crucial for protecting data and ensuring smooth operations.

Security

- Network security involves implementing measures to protect th e network and its data from unauthorised access, misuse, or th eft.
- Firewalls: Monitor and control incoming and outgoing network t raffic based on predetermined security rules
- Intrusion Detection Systems (IDS): Monitor network traffic for suspicious activity and alert administrators to potential threats
- Encryption: Encode data to prevent unauthorized access, ensuring confidentiality and integrity.

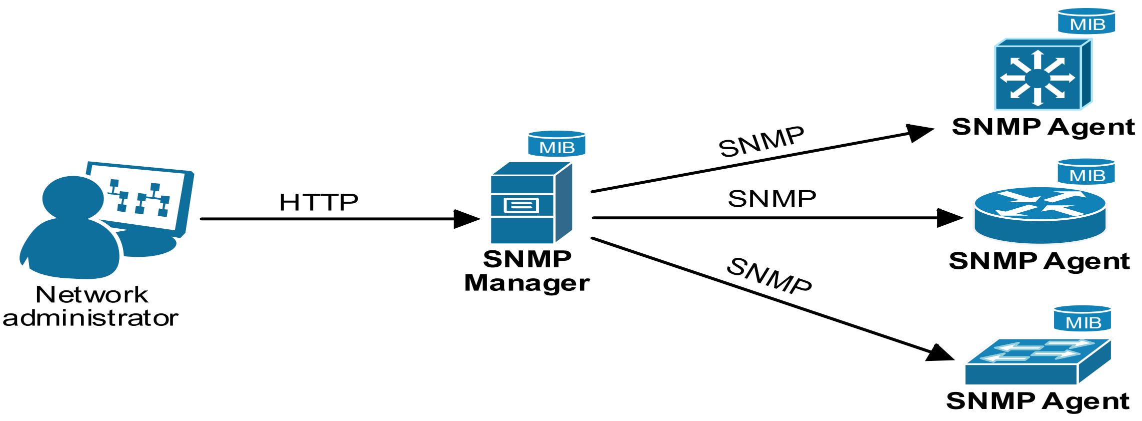
Monitoring

Network monitoring involves using software to keep an tracking on the network's health and reliability.

Control

Network control involves managing and regulating the network to ensure optimal performance and security.

SNMP



- SNMP (Simple Network Management Protocol) is indeed an available tool for security, monitoring, and control in computer networks
- Used for monitoring, management and troubleshooting in live network
- Designed by: IETF (Internet Engineering Task Force

It is an application-layer protocol

Uses UDP port no. 161 and 162

There are 3 versions used in SNMP

It works of server-client based model

Its main 4 components

- SNMP MANAGER
- SNMP AGENT
- MANAGEMENT DEVICE
- MIB (Management Information Base)

SNMP Manager

- Is a computer system that monitors network traffic

through the SNMP manager, the manager sends queries

and receives answers from the agent, and controls them

- It is hardware server on which monitoring software is

running

- Like : Solarwind Orian, PRTG, Zabbix and etc.

- Server collects on the details from SNMP client and display it in GUI
- Network Administrator managed all the client from server

SNMP AGENT

- It is a software program, which is stored in the network element (network device), it collects real-time information from the device, and provides SNMP manager and stores and retrieves the information.

SNMP MANAGER

There are 3 messages used by SNMP

- Get message: Sent by manager to agent
- Set message: Sent by manager to agent
- Trap/Inform message: Sent by agent to server

SNMP MANAGER

There are 3 messages used by SNMP

- Get message: Send by manager to collect the info of agent like : uptime, interface,status & etc
- Set message: Send by manager to agent to apply some configuration on agent/.client.
- Trap/Inform message: from agent to server to updates the alert like high CPU, high Bandwidth and etc

MANAGEMENT DEVICE

- All types of network devices come inside it.

Like – Router, Switch, Hub, Etc.

MIB

Its full name is (Management Information Base)

It is a circular information storage that stores management information.

There are 3 versions available

- V1 less secure, less complex
- V2 update from v1
- V3 is more secure and more complex like authentication and encryption like MD5, SHA

VPN (Virtual Private Network)

A **Virtual Private Network (VPN)** is a technology that enables secure and private communication over the internet or any untrusted network. It creates a virtualised, encrypted connection between a user's device and a private network, allowing data to be transmitted as if the devices were physically connected to the same local network.

Tunnelling Protocol

VPNs use tunnelling protocols to encapsulate and protect data during transmission. Common protocols include PPTP, L2TP/IPsec, SSTP, and OpenVPN.

Encryption

Data transmitted through the VPN is encrypted to ensure confidentiality. Encryption protocols like AES are commonly used to secure the data.

Authentication

VPNs use authentication methods to verify the identity of users and devices accessing the network. This can involve passwords, digital certificates, or multi-factor authentication.

Access Control

VPNs often include access control mechanisms to restrict network access based on user credentials and the security posture of the connecting device.

Type of VPN

- Remote Access VPN
- Site-to-Site VPN

Remote Access VPN

Allows individual users to connect to a private network securely from a remote location.

Site-to-Site VPN

Connects entire networks, such as branch offices, securely over the internet.

DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that automates the process of assigning IP addresses and other configuration information to devices on a network. It eliminates the need for manual IP address configuration, making network administration more efficient.

Network security

Network security is a broad field that involves implementing measures to protect the integrity, confidentiality, and availability of computer networks and the data transmitted over them.

Security Attacks

1. Malware Attacks
2. Phishing Attacks
3. Denial of service (DOS) Attacks
4. Man in the Middle (MitM) Attacks
5. SQL Injection Attacks

Malware Attacks

Malicious software designed to harm or exploit systems.

Phishing Attacks

Deceptive attempts to obtain sensitive information by posing as a trustworthy entity.

Denial of service (DOS) Attacks

Overloading a system's resources to make it unavailable.

Man in the Middle (MitM) Attacks

Intercepting and possibly altering communication between two parties.

SQL Injection Attacks

Exploiting vulnerabilities in database queries to manipulate or access data.

Security Mechanisms

- Firewalls
- Encryption
- Access Control lists (ACLs)
- Security Protocols (SSL/TLS)

Firewalls

Monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Encryption

Transforming data into a secure form that can only be accessed with the correct decryption key.

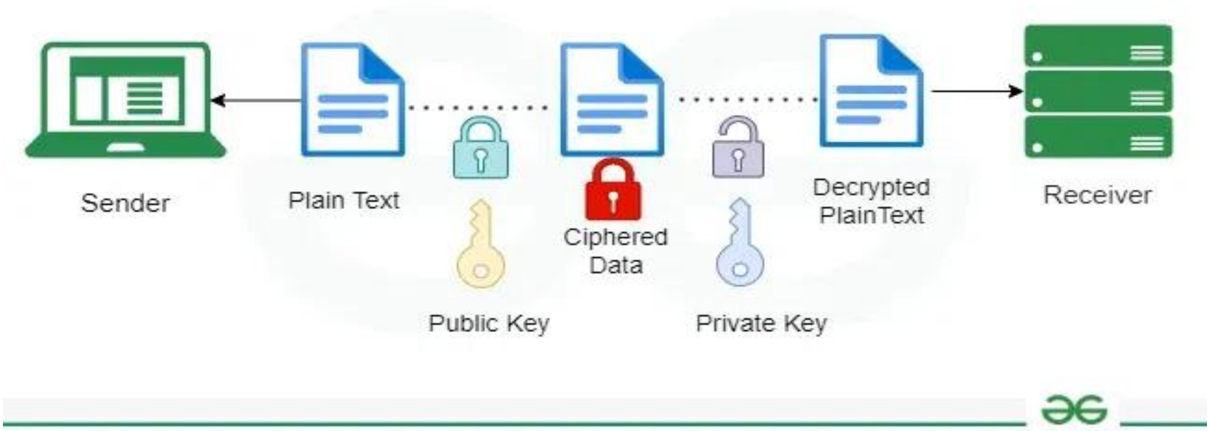
Access Control lists (ACLs)

Defining permissions to control access to resources.

Security Protocols (SSL/TLS)

Establishing secure communication channels over networks.

Cryptography



Cryptography is the science and art of secure communication in the presence of adversaries. It involves the use of mathematical techniques and algorithms to transform information into a secure and unreadable format, ensuring confidentiality, integrity, and authenticity of the data. Here are key concepts in cryptography:

Encryption and Decryption

The process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a key.

The reverse process of converting ciphertext back into plaintext using a decryption algorithm and the correct key.

Key

A key is a piece of information used by an algorithm to transform plaintext into ciphertext during encryption and vice versa during decryption. Keys can be symmetric (same key for both encryption and decryption) or asymmetric (different keys for encryption and decryption).

Symmetric Cryptography

In symmetric-key cryptography, the same key is used for both encryption and decryption. Examples include DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

Asymmetric Cryptography

Asymmetric-key cryptography involves a pair of public and private keys. Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. Examples include RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography).

Hash functions

Hash functions take input data (of any size) and produce a fixed-size string of characters, which is typically a digest or hash value. They are used for data integrity verification. Common hash functions include SHA-256 (Secure Hash Algorithm 256-bit) and MD5 (Message Digest Algorithm 5).

Digital Signatures

Digital signatures provide a way to verify the authenticity and integrity of a message or document. They involve the use of asymmetric cryptography, where the sender signs the message with their private key, and the recipient can verify the signature using the sender's public key.

Intrusions

An intrusion refers to any unauthorized access, use, disclosure, or disruption of computer systems, networks, or data. It can be intentional or accidental.

Types of Intrusion

External Intrusion - Unauthorized access from outside the network

Internal Intrusion-Unauthorized access or actions from within the network.

Physical Intrusion- Unauthorized access to physical devices or facilities.

Viruses

A virus is a type of malicious software that attaches itself to legitimate programs or files, spreading from one host to another and potentially causing damage.

Characteristics

Self-Replication

Viruses can replicate and spread independently to other files or systems.

Payload

Viruses may carry a payload, such as destroying or corrupting data, stealing information, or enabling remote control of the infected system.

Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Functions/types of firewalls

Packet filtering

Examining packets of data and deciding whether to allow or block them based on defined rules.

Stateful inspection

Keeping track of the state of active connections and making decisions based on the context of the traffic.

Proxy services

Acting as an intermediary between internal and external networks, forwarding requests on behalf of clients.

Cyber Laws

Cyber laws, also known as internet laws or digital laws, are legal frameworks and regulations that govern and address issues related to the use of the internet, digital technologies, and electronic communication. These laws are essential for maintaining order, protecting individuals and organizations, and ensuring accountability in the digital space.

Data Protection and privacy laws

Protect the privacy and personal data of individuals, regulate the collection and processing of data by organizations.

Cybercrime Laws

Criminalize unauthorized access, hacking, and other malicious activities conducted on computer systems

Intellectual property laws

Protect intellectual property rights, including copyrights, trademarks, and patents, in the digital realm.

Electronic transactions Laws

Legally recognize and facilitate electronic transactions and contracts.

Cybersecurity standard ant compliance

Provide guidelines and best practices for organizations to implement effective cybersecurity measures and achieve compliance.

Incident Response and Reporting Laws

Mandate organizations to report data breaches and incidents promptly and implement measures to mitigate and prevent future occurrences.

National and International Cybersecurity strategies

Outline the government's approach to cybersecurity, including collaboration, threat mitigation, and infrastructure protection.

DHCP

DHCP (Dynamic Host Configuration protocol) configuration commands-

Enter Configuration Mode-

```
Router> enable
```

```
Router# configure terminal
```

Exclude IP Addresses-

```
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Create a DHCP Pool-

```
Router(config)# ip dhcp pool LAN_POOL
```

Define the Network and Subnet-

```
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
```

Specify the Default Gateway (Router)-

```
Router(dhcp-config)# default-router 192.168.10.1
```

Define the DNS Server-

```
Router(dhcp-config)# dns-server 8.8.8.8 1.1.1.1
```

Router CLI

```
Router>enable

Router# config t

Router(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.5

Router(config)# ip dhcp pool JITENDRA

Router(dhcp-config)# network 192.168.10.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.10.1

Router(dhcp-config)# dns-server 8.8.8.8 1.1.1.1
```

Wireless Connection

Open Cisco Packet Tracer

⬇

Select

⬇

Network Devices/Wireless Devices/Home Router

⬇

Double Click Router/Wireless/Save

⬇

Wireless Section में आप Network का नाम दे सकते है और किसी भी नेटवर्क को Enable/Disable कर सकते है|

⬇

Wireless/Wireless Security/Enable/Web/Key1

⬇

Wireless Security - इस Section में आप Password सेट कर सकते हैं|

⬇

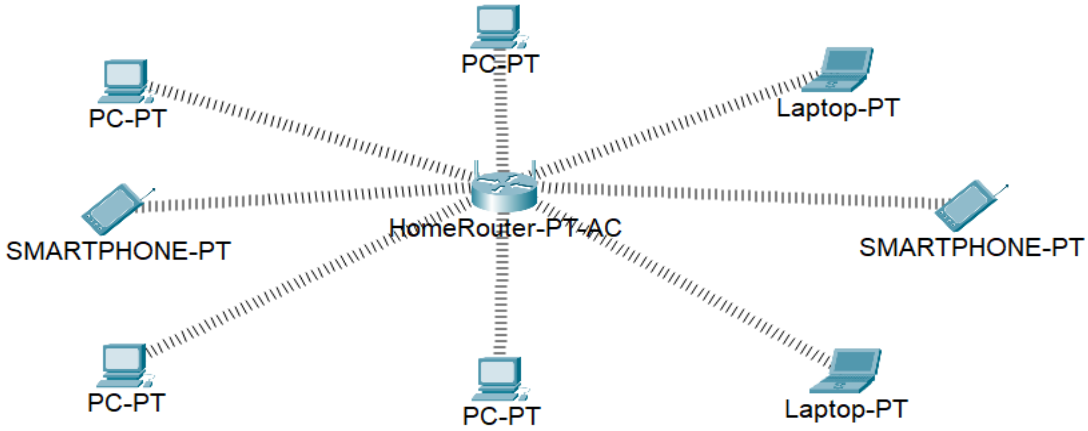
Select

⬇

End Devices/Select Pc, Laptop, Phone

⬇

Double Click On **Pc**/Physical/Pc Off/Select VMP300N(Wireless Port)/Connect/Pc ON/Desktop/Pc Wireless/Connect/Wireless Mode/Select Network

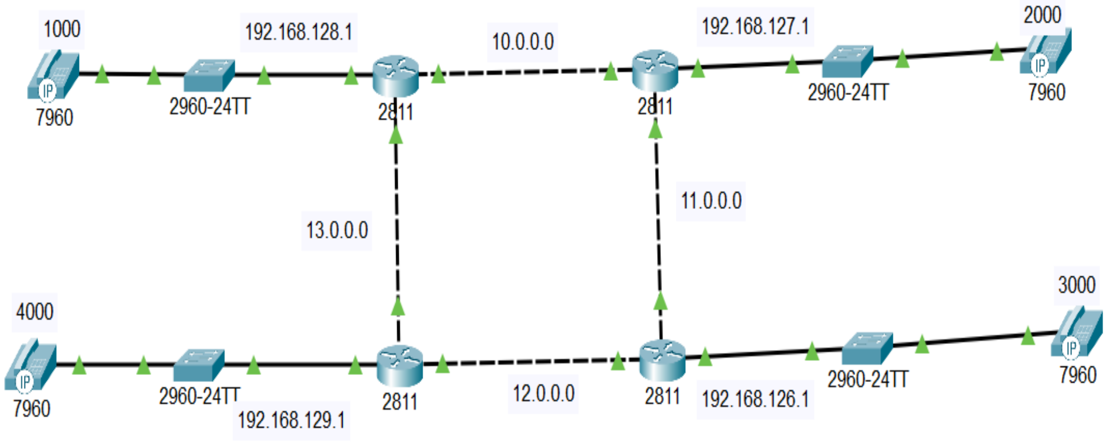


VOIP

Router - Select Router 2811

```
Router(config)#ip dhcp pool hello

Router(dhcp-config)#net 192.168.128.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.128.1

Router(dhcp-config)#option 150 ip 192.168.128.1

Router(dhcp-config)#exit

Router(config)#telephony-service

Router(config-telephony)#max-ephones 20

Router(config-telephony)#max-dn 5

Router(config-telephony)#ip source-address 192.168.128.1 port 2000

Router(config-telephony)#auto assign 1 to 5

Router(config-telephony)#ephone-dn 1

Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#number 11225

Router(config-ephone-dn)#ephone-dn 2

Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config-ephone-dn)#number 11226

Router(config)# do write

Router(config)# dial-peer voice 1 voip

Router(config-dia-peer)# destination-pattern 2....

Router(config-dia-peer)# session target ipv4:next hope ip address
```

Ex.- Fig



Note:- जब दो या दो से अधिक Router हो तब Static/RIP Routing किया जाता है ताकि मेसेज या कॉल एक Router से दुसरे Router में आसानी से पास हो सके|

Dial-peer for delete

# no dial-peer voice 1

# no dial-peer voice 2

Config delete

# erase startup-config

Config for show

# show running-config

Save for config

# do write/do wr

Switch

```
Switch(config)#int range f0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
Switch(config-if-range)# ex
Switch(config)#do wr
```

Cyber Security

Cyber Attack

A **Cyber Attack** is a malicious attempt by hackers or cyber criminals to damage your files, steal, or disrupt computer systems, networks, or digital devices. These attacks can lead to data breaches, financial losses, and even national security threats.

Types of CYBER ATTACKS

Types of
CYBER ATTACKS
Malware Attacks
Phishing Attacks
Man in the Middle (MitM) Attacks
DDoS Attacks
Denial of service (DOS) Attacks

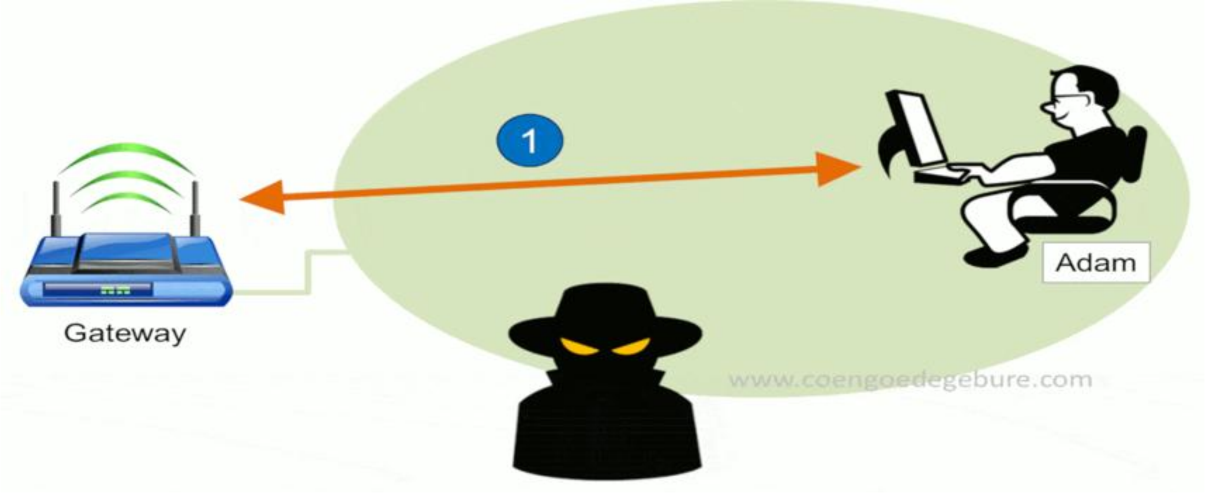
Malware Attacks

Harmful software like viruses, ransomware, or spyware infects a system.

Phishing Attacks

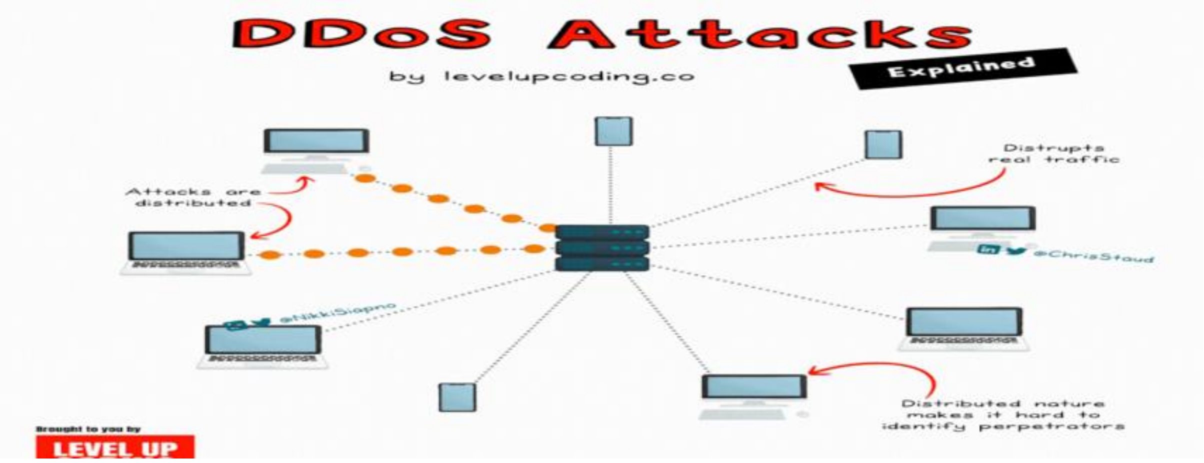
A phishing attack is a carefully crafted deception where cyber criminals first gain your trust, then manipulate you into giving away sensitive information, ultimately causing harm.

Man in the Middle (MitM) Attacks



Hackers intercept communication between two parties.

Denial of service (DOS) Attacks



Overloading a server or website with traffic to crash it.

CYBER SECURITY

Cyber Security is the refers to the technologies processes of protecting computers, networks, servers, mobile devices, and data from malicious attacks by hackers, malware, and other cyber threats. It involves implementing measures to prevent unauthorized access, data breaches, and damage to digital systems and information.

Types of Cyber Security

Firewalls

Monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Encryption

Transforming data into a secure form that can only be accessed with the correct decryption key.

Like – hello=1f2g@36

Access Control lists (ACLs)

Defining permissions to control access to resources.

Security Protocols (SSL/TLS)

Establishing secure communication channels over networks.