# Introduction to Computer Networks

**Book** · December 2023

CITATIONS
0

READS
1,732

**1 author:**

Youcef Benabderrezak
University of Boumerdes
**152** PUBLICATIONS **20** CITATIONS

SEE PROFILE

**University M'hamed Bougara-Boumerdes**

**Faculty of Sciences**

**IT departement**


# Introduction to Computer Networks

## Course notes

***Directed By :***

**Benabderrezak Youcef**

*- Researcher in **Cyber security** -*

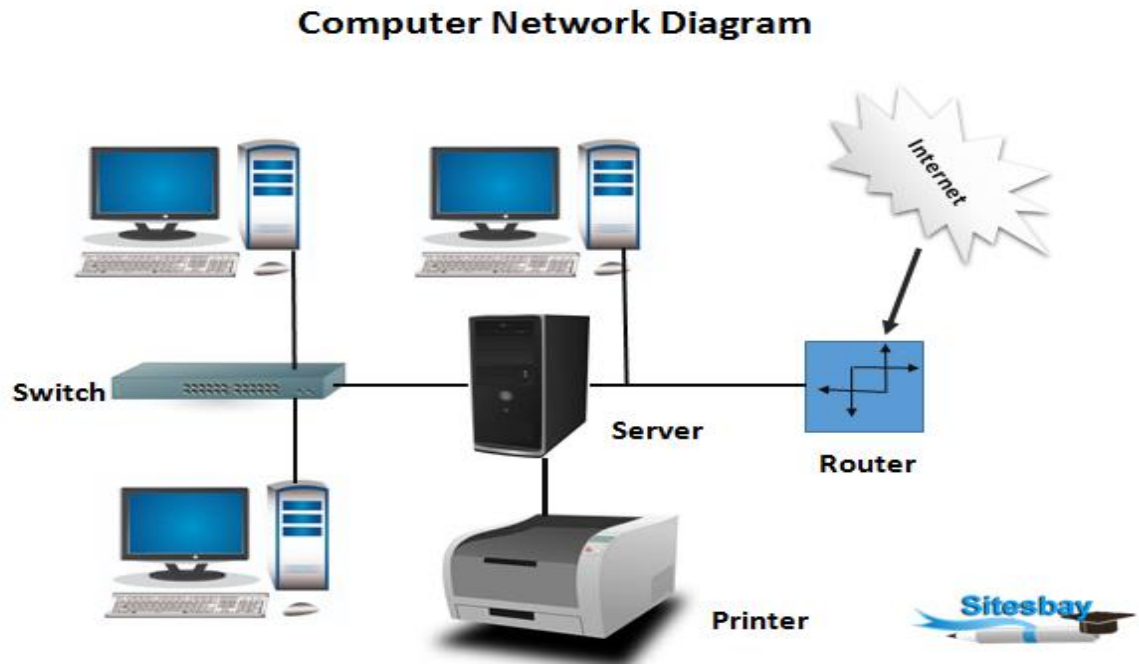
**y.brnabderrezak@univ-boumerdes.dz**

2023 / 2024

# Table of contents

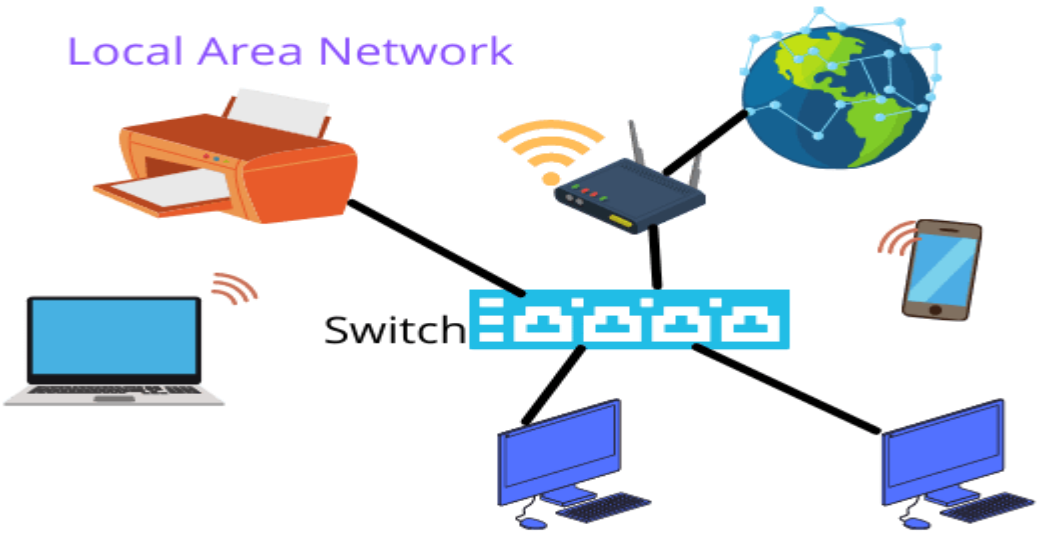
## 1. What is a computer network ?

⇨ A computer network is a **collection** of **interconnected computers**, **devices**, and other communication equipment that enables them to **share resources, exchange information,** and **communicate with each other**




## 2. Local networks

⇨ A local network, or LAN (Local Area Network), is a type of computer network that **covers a limited geographic area**, such as a home, office, school, or a small group of buildings in **close proximity**



## 2.1. Main characteristics of LAN

1. **Limited Geographic Area**
2. **High Data Transfer Rates** : megabits / seconde (Mbps) or gigabits /second (Gbps), ...
3. **Private Ownership :** LANs are usually privately owned and maintained by organizations or individuals.
4. **Topology Variability :** (star, bus, ring...)
5. **Local Services :** host local services, such as file servers, print servers, and email servers, to cater to the needs of the local users
6. **Resource Sharing** : sharing files, printers, internet connections, and other resources.
7. **Ease of Management**
8. **Security Measures** : LANs often employ firewalls, encryption, user authentication, access control lists, and other security mechanisms to enhance network security.
9. **Wired or Wireless Connectivity**

⇨ LANs can be established using wired connections (e.g., Ethernet cables) or wireless technologies (e.g., Wi-Fi).

10. **Scalability**

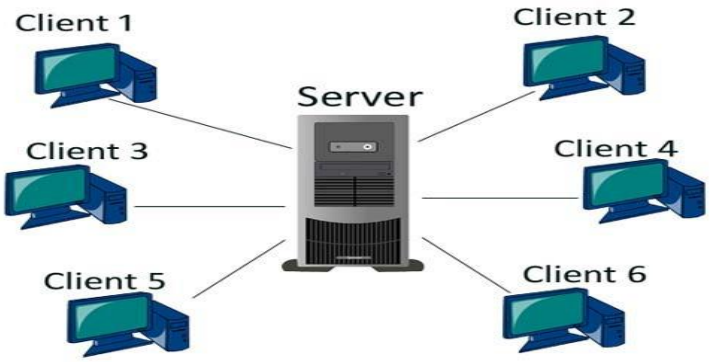
## 2.2. Types of LAN

LANs can be classified based on the **types of devices they connect**, the **design** of the underlying **architecture**, and the **medium** used :

1. **<u>Client-server LAN</u>**

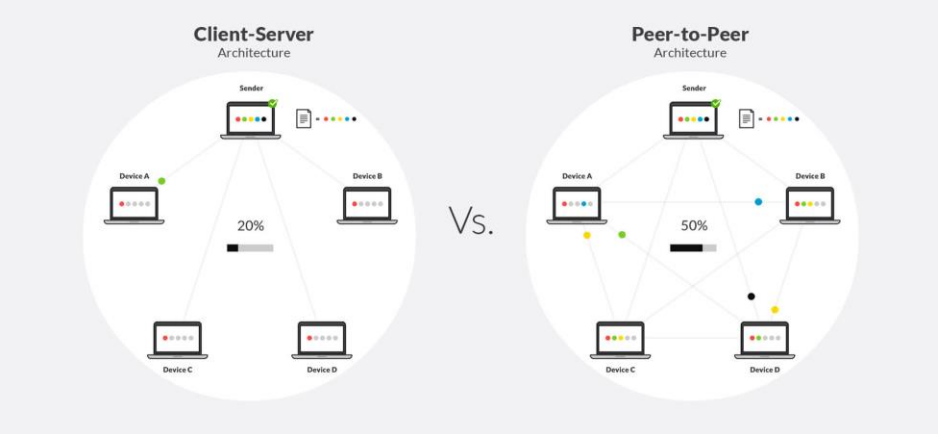
⇨ **Single server** connects to multiple devices known as **clients**.

⇨ Client devices cannot interact with each other and a centralized machine handles activities like network traffic management, network access control, etc.



## 2. Peer to peer LAN

⇨ There is **no centralized server**, and all connected devices have access to each other, regardless of whether they are servers or clients.

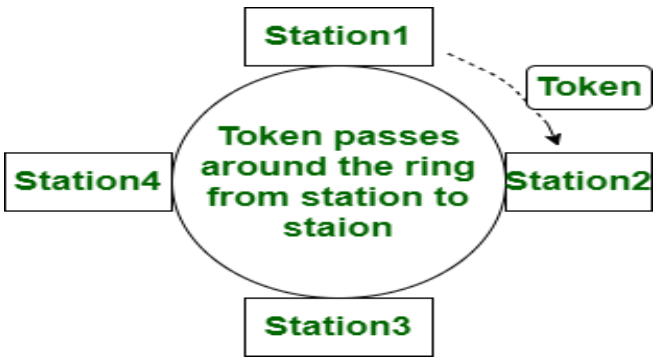



## 3. Token ring LAN

⇨ Based on the architecture design, you can classify LANs into a token ring or token bus categories.

⇨ In the former, all devices are arranged in a ring when they are connected.

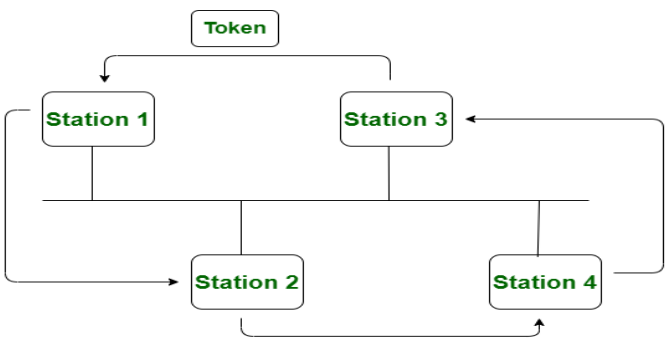
⇨ A token is assigned to every connected device based on its requirements




## 4. Token bus LAN

⇨ In a token bus LAN, connected nodes are arranged in a tree-like topology, and tokens are transferred either left or right.

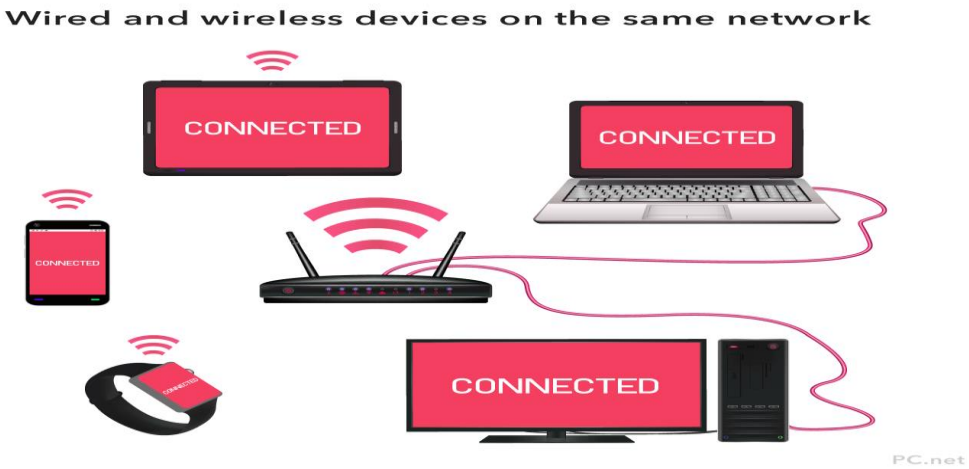
⇨ Typically, it provides better bandwidth capacities than a token ring LAN environment.



## 5. Wired LAN

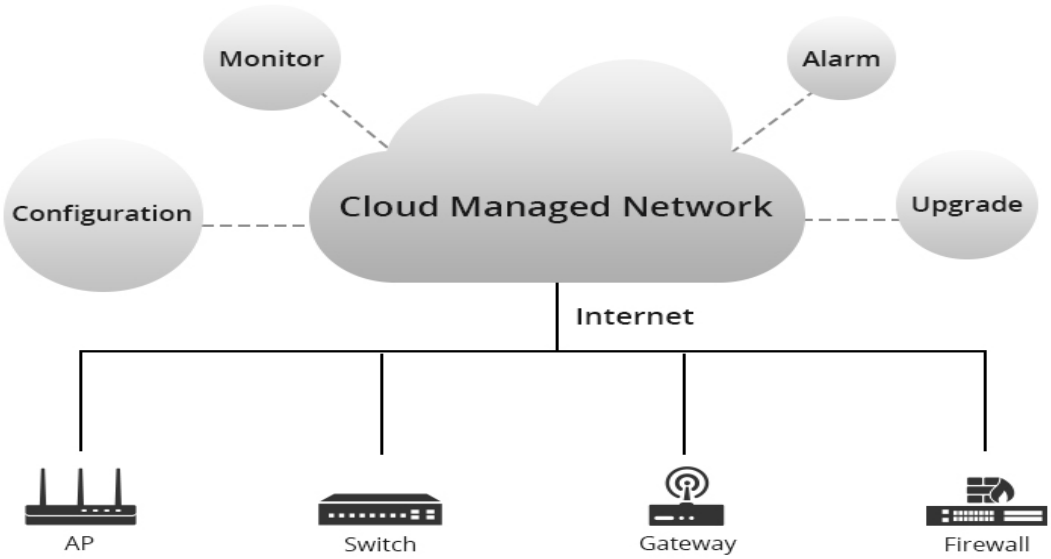
⇨ It uses **electronic waves** to transfer data across optical fiber (or cable variants) instead of tokens.

⇨ Wired LAN is extremely reliable and can be very fast, depending on the performance of the central server.




## 6. Cloud-managed LAN

⇨ Cloud-managed LAN is a specific type of wireless LAN where a centralized cloud platform is used to manage network provisioning, policy enforcement, access control, and other aspects of network performance and security.



## 2.3. LAN protocols

1. **Ethernet (IEEE 802.3)**

⇨ A widely used LAN protocol that defines how devices communicate over wired connections.

2. **Wi-Fi (IEEE 802.11)**

⇨ A set of wireless LAN protocols that enable devices to connect to a network without physical cables.

3. **TCP/IP (Transmission Control Protocol/Internet Protocol)**

⇨ A suite of protocols that underpins the internet and most LANs, governing how data is sent and received.

4. **ARP (Address Resolution Protocol)**

⇨ Used in LANs to map IP addresses to physical MAC addresses.

5. **ICMP (Internet Control Message Protocol)**

⇨ Provides error and control messages for network communication.

6. **IGMP (Internet Group Management Protocol)**

⇨ Manages multicast group memberships on a LAN.

7. **Spanning Tree Protocol (STP)**

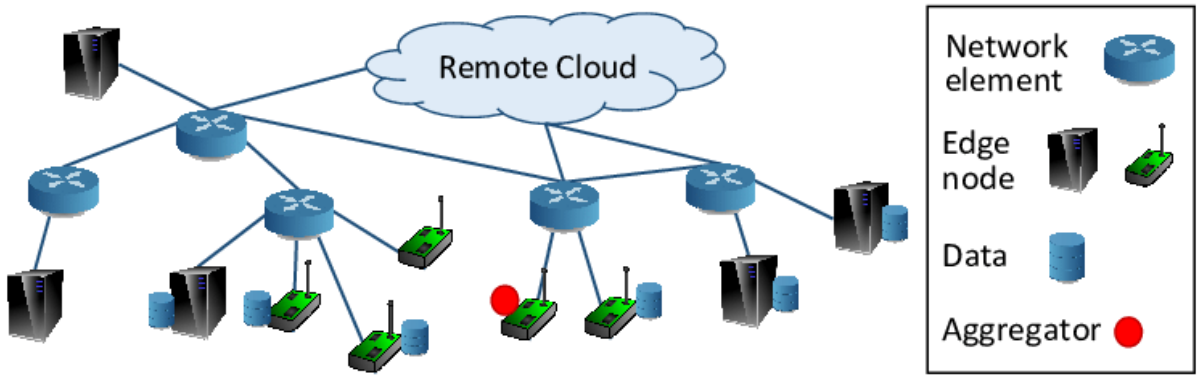
⇨ Prevents network loops in Ethernet LANs.

8. **LLDP (Link Layer Discovery Protocol)**

⇨ Discovers and advertises information about connected devices in a LAN.

## 2.4. Large-scale computer networks

These are computer networks that span large geographic areas and are often used to interconnect remote systems, sites or organizations. Large-scale networks can be private (for example, extended enterprise networks or campus networks) or public (for example, the Internet).

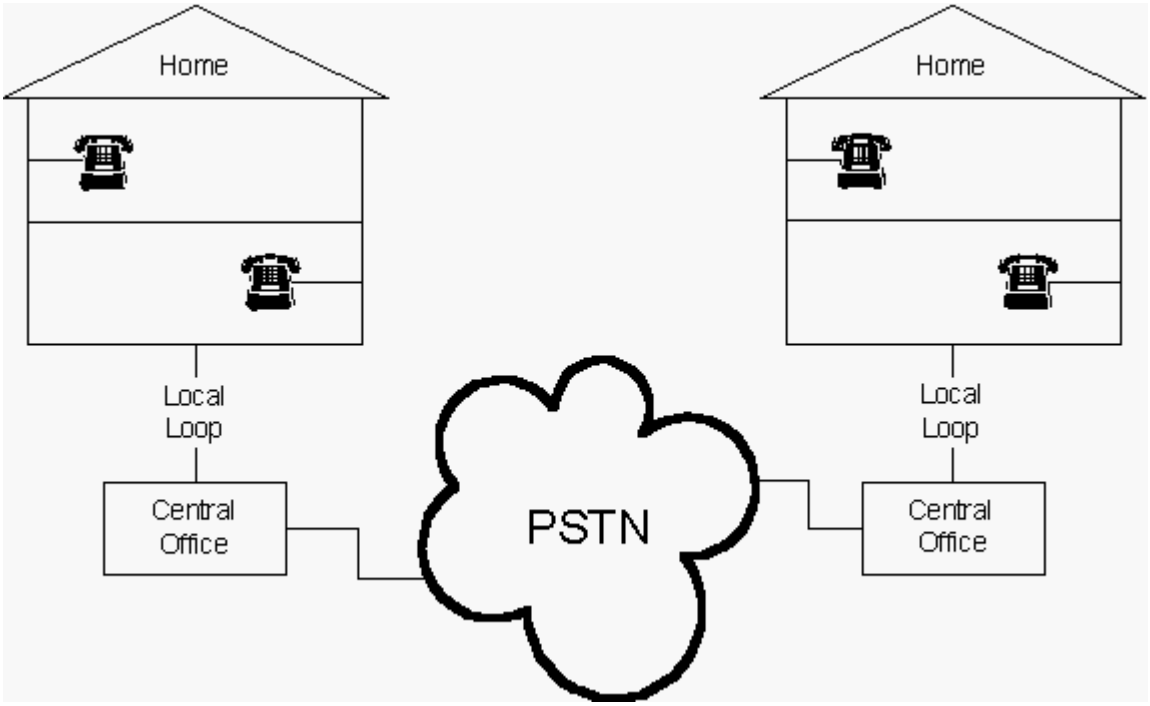


## 2.5. Public data networks

- ⇨ Public data networks refer to communication networks that are publicly accessible and used for transmitting data, information, and communications.
- ⇨ These networks are typically operated and maintained by government agencies, telecommunication companies, or other entities and are made available for public use.
- ⇨ Public data networks can take various forms, including:

1. **Public Switched Telephone Network (PSTN):**

PSTN is a traditional circuit-switched telephone network that has been used for voice and data communication for many years. It includes both landlines and mobile networks.

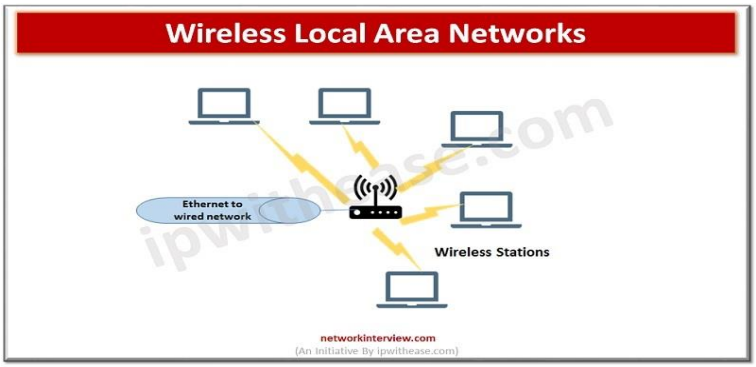



2. **Internet**

The **global public data network** that connects millions of computers and devices worldwide

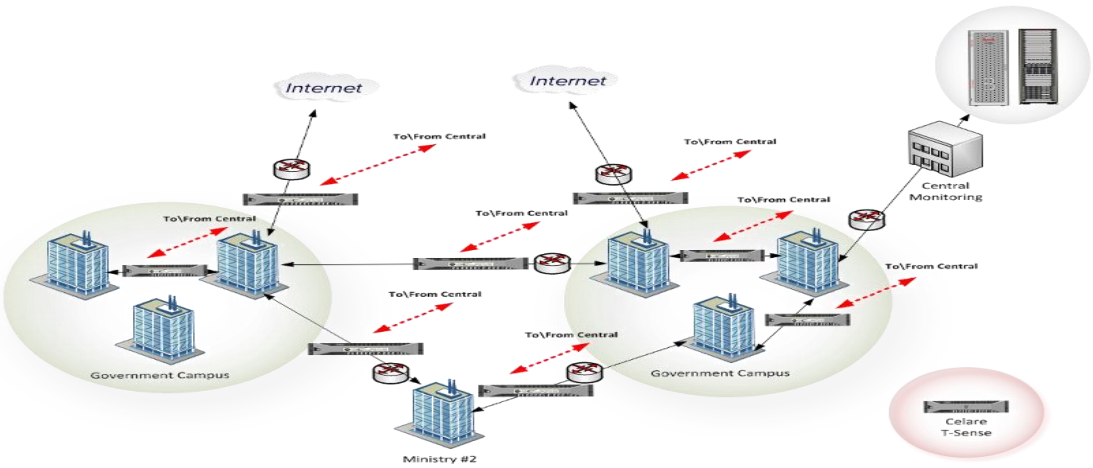
### 3. Public Wireless Networks

⇨ These include cellular networks (e.g., 3G, 4G, 5G), public Wi-Fi networks in cafes, airports, libraries, and other public places, as well as **satellite-based networks for remote or global connectivity.**



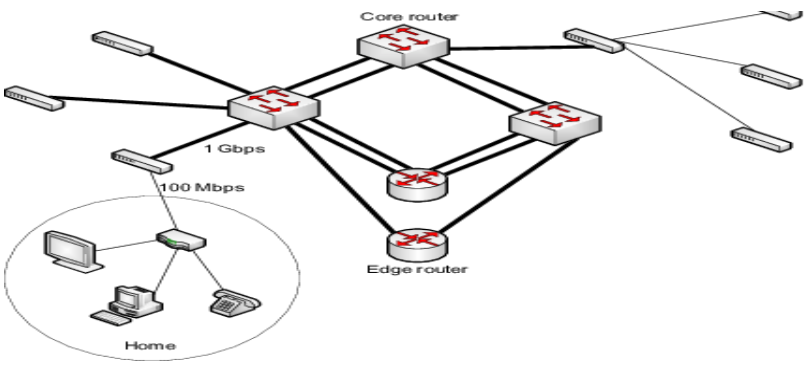

### 4. Government Data Networks

Many governments operate their own data networks for various purposes, including public safety, government communications, and public services.



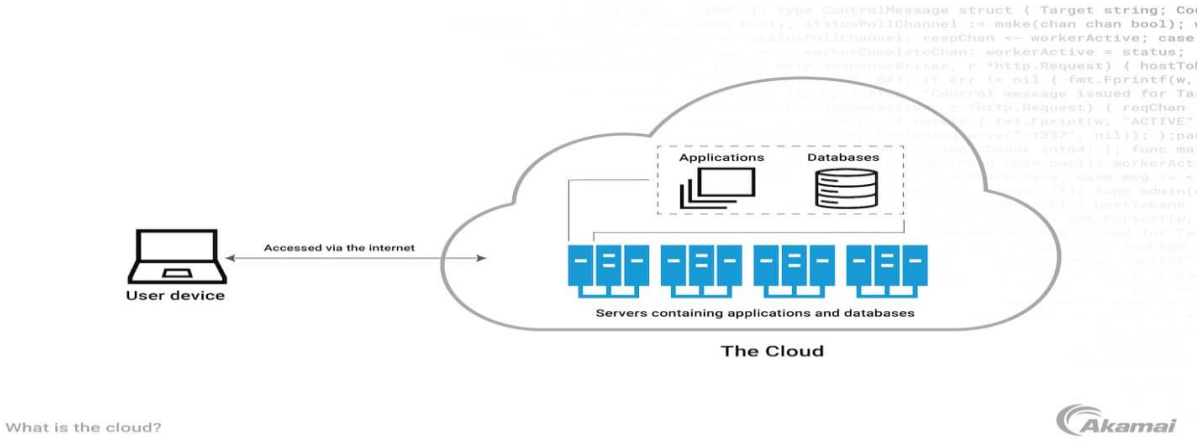

### 5. Municipal Networks

⇨ Some cities and municipalities deploy their own public data networks to provide internet access and other services to residents.



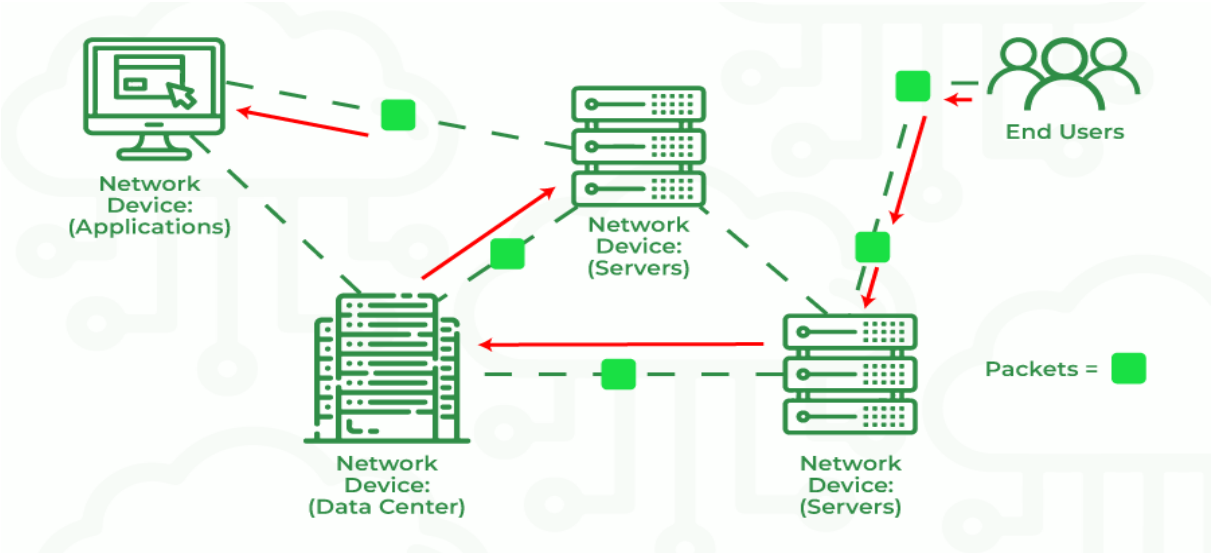
6. **Public Cloud Networks**

⇨ Cloud service providers offer public cloud networks, allowing organizations to access and use computing resources and services over the internet.




## 2.6. Packet-switched networks

Are a type of telecommunications network that transmit data in discrete packets or **chunks** of information

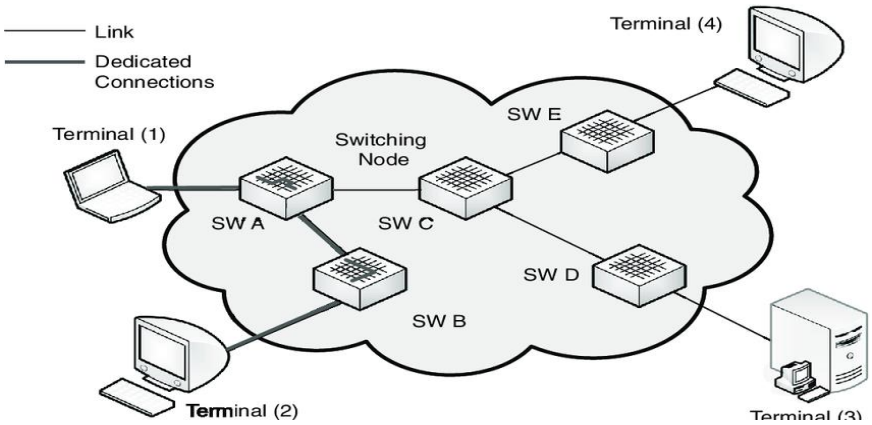



Here are their key characteristics and benefits in simple terms:

1. **Packetization**: Data is broken into small packets for efficient sending.
2. **Shared Resources**: Many packets share the same network, making it efficient.
3. **Reliability**: If one route is blocked, packets find a new path.
4. **Adaptability**: They can handle different types of data and grow as needed.
5. **Cost-Effective**: They use resources efficiently, saving money.
6. **Global Connection**: Like the internet, they connect the world.

## 2.7. Circuit-switched networks

⇨ Are like having a direct phone line from one person to another, where the connection is reserved exclusively for them as long as they're talking.




Key Characteristics and Benefits:

1. **Dedicated Connection:** You get a continuous, exclusive line for your call, like a private road.
2. **Constant Quality:** The quality of the call remains steady, like a clear radio station.
3. **Predictable:** You know exactly how much bandwidth you have, like a fixed water pipe.
4. **Simple:** Works well for voice calls but less efficient for data transfer.
5. **Less Efficient:** It can be wasteful when you're not actively talking, like a road with only one car.
6. **Limited Scalability:** Adding more connections can be expensive and challenging, like building more roads for each new car.

## 2.8. Integrated Digital Network Services

⇨ A telecommunications technology that was widely used in the past for digital voice and data transmission.

⇨ ISDN is like a digital Swiss Army knife for communication, offering various services like clear phone calls, fast data transfer, and even video conferencing over a single digital line.

**Key Characteristics and Benefits**

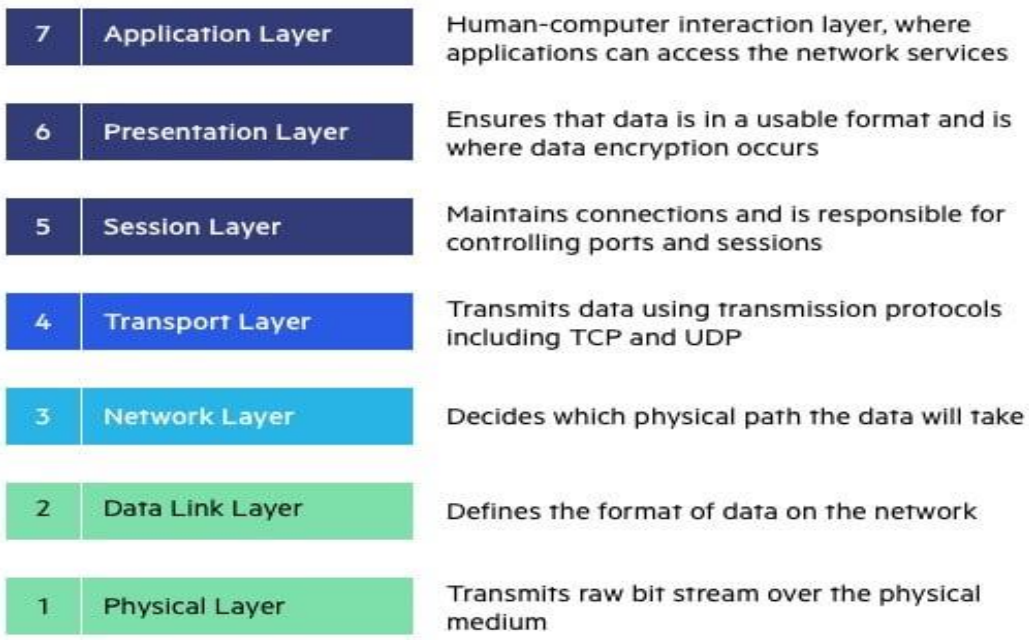
1. **Digital Communication:** It converts voice and data into digital format for high-quality transmission.
2. **Multiple Services:** ISDN can handle voice, data, and even video communication simultaneously on a single line.
3. **Reliable:** It offers stable and predictable connections for clear calls and fast data transfer.
4. **Fast Setup:** Connections are established quickly, reducing call setup time.
5. **Flexible:** ISDN lines can be adapted for different needs, from basic voice calls to high-speed internet access.
6. **Widespread Use:** It was commonly used for business communications before broadband internet became prevalent.
7. **Dial-up and BRI:** ISDN comes in two flavors: Basic Rate Interface (BRI) for small setups and Primary Rate Interface (PRI) for larger ones.

# 3. Network Layer

## 3.1. OSI model

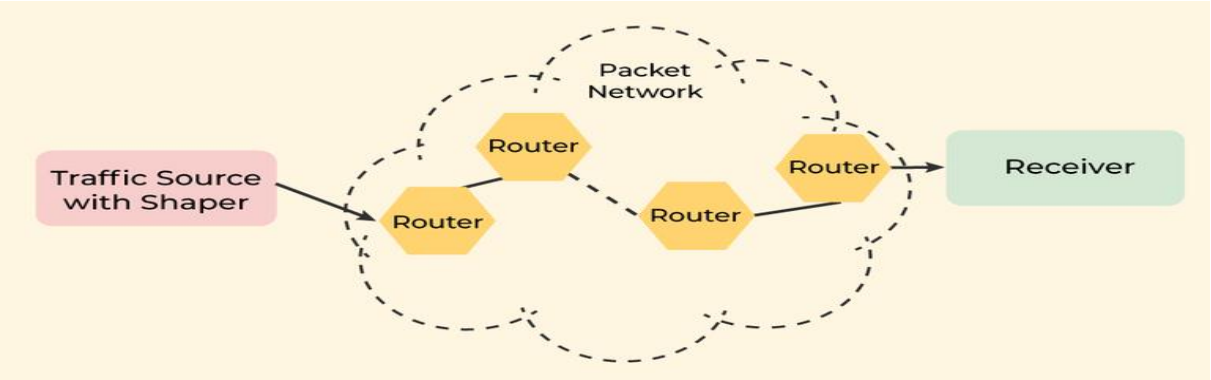
⇨ The OSI (Open Systems Interconnection) model is like a blueprint for how computers and devices should communicate with each other.

⇨ It breaks down this communication into seven easy-to-understand layers, each with its own job.



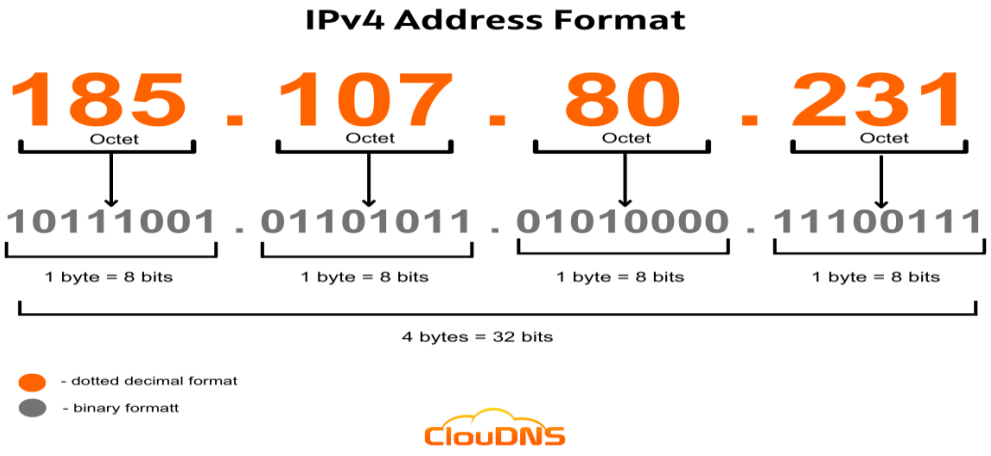
## 3.2. Introduction to network layer

- The network layer, often referred to as **Layer 3** in the OSI model, plays a crucial role in the process of computer network communication
- The network layer **helps** your **data navigate the complex network** infrastructure, making sure it reaches the right destination, even if that means hopping through multiple routers and networks along the way.



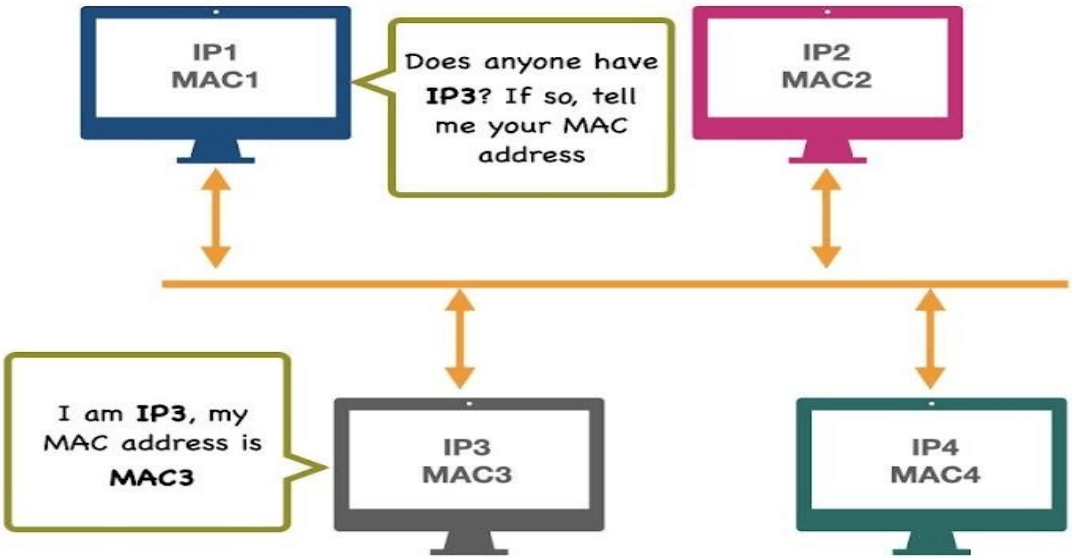

## 3.3. IPv4

- IPv4, or Internet Protocol version 4, is a foundational and widely used protocol for identifying and routing data packets on computer networks, including the global Internet.
- IP (version 4) addresses are **32-bit integers** that can be expressed in hexadecimal notation.
- The more common format, known as dotted quad or dotted decimal, is x.x.x.x, where each x can be any value between 0 and 255.
- For example, 192.0.2.146 is a valid IPv4 address.



### 3.4. ARP

⇨ ARP **(Address Resolution Protocol)** is a network protocol used to find out the hardware (MAC) address of a device from an IP address.




**1. ARP Request:**

⇨ When a device on a local network wants to communicate with another device and knows its IP address but not its MAC address, it initiates an ARP request.

⇨ The sender creates an ARP request packet containing its own IP address, its own MAC address, the target IP address it wants to reach, and a placeholder (all zeros) for the target MAC address.

**2. Broadcast**

⇨ The sender broadcasts the ARP request packet onto the local network

⇨ This broadcast is sent to all devices within the network segment, and it contains a broadcast MAC address (FF:FF:FF:FF:FF:FF)

**3. Reception**

⇨ All devices on the local network receive the ARP request packet.

**4. ARP Table Check**

⇨ Each device that receives the ARP request packet checks if the target IP address in the ARP request packet matches its own IP address.

⇨ If it does, that device is the one being sought in the ARP request.

**5. ARP Reply**

⇨ The device with the matching IP address sends an ARP reply packet back to the sender.

⇨ This ARP reply packet contains its own IP address and MAC address.

### 6. Cache Update

⇨ The sender, upon receiving the ARP reply, updates its ARP cache (also known as the ARP table) with the newly learned MAC address for the target IP address.

### 7. Data Transmission:

⇨ With the MAC address of the target device now known, the sender encapsulates its data packets with the destination MAC address and can send them directly to the target device on the local network.

## 3.5. Networking with / without classes

⇨ Networking with and without classes typically refers to the way IP addresses are managed and assigned within a network.

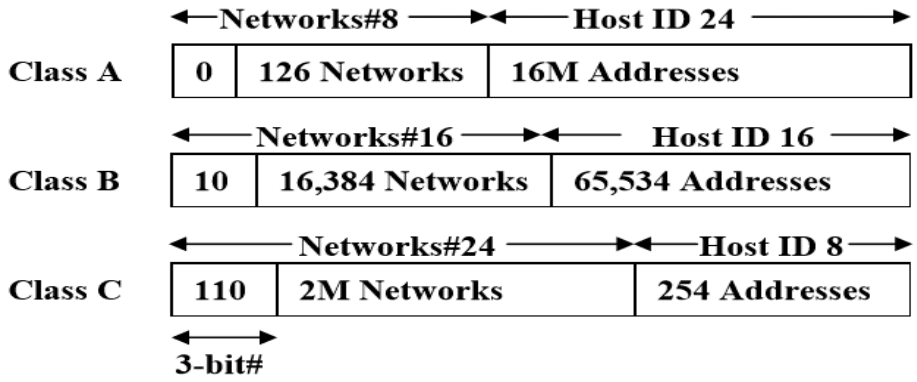
⇨ This distinction is more relevant in the context of IPv4 (Internet Protocol version 4) addressing

### A. Networking with Classes (Classful Networking)

⇨ IPv4 addresses **were divided** into classes to determine the network and host portions of an IP address.

⇨ This classful system **was rigid and inefficient for address allocation**, leading to IP address exhaustion and inefficient use of address space.

⇨ There were three primary classes:




**Network Address Range**
**A=1.0.0.0 → 126.0.0.0**
**B=128.0.0.0 → 191.255.0.0**
**C=192.0.0.0 → 233.255.255.0**

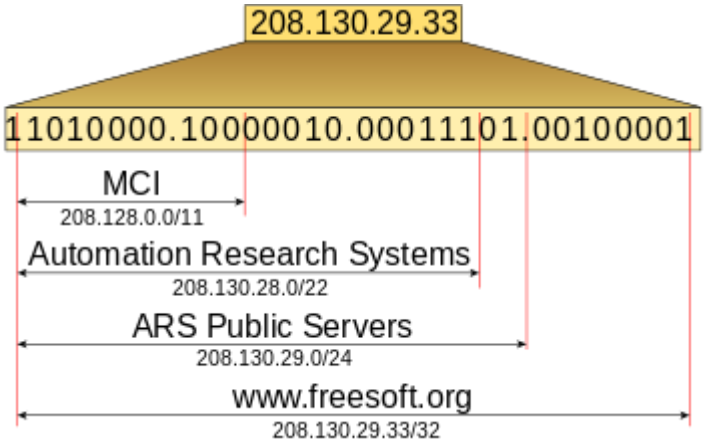
**IP Address Range**
**A=1.0.0.1 → 126.255.255.254**
**B=128.0.0.1 → 191.255.255.254**
**C=192.0.0.1 → 233.255.255.254**

### B. Networking without Classes (Classless Networking or CIDR)

⇨ CIDR was introduced to provide a more flexible and efficient way of managing IP addresses.

⇨ With CIDR, IP addresses are no longer strictly bound by class boundaries.

- ⇨ Instead, CIDR allows for variable-length subnet masks, which means that networks can be divided into subnets of different sizes.
- ⇨ CIDR notation is used to express IP address ranges and subnet masks more precisely.
- ⇨ For example, instead of reserving entire Class A, B, or C networks, CIDR allows for more granular allocation.
- ⇨ An IP address range might be represented as follows: "192.168.1.0/24," where "/24" indicates a subnet mask of 24 bits.




### 3.6. Sub-networking

- ⇨ Is a networking practice that involves dividing a single larger network into smaller, more manageable subnetworks or subnets

1. **Determine IP Address and Subnet Mask**

- ⇨ Start with the IP address block you have been allocated. This could be a Class A, B, or C address or a CIDR notation (e.g., 192.168.1.0/24).
- ⇨ Also, determine the subnet mask you intend to use.

2. **Divide the Network**

- ⇨ Decide how many subnets you want to create and how many hosts you need in each subnet. This will determine the subnet mask length.

3. **Calculate Subnet Masks**

- ⇨ Calculate the new subnet masks for each subnet based on the desired number of subnets and hosts per subnet.

4. **Allocate Addresses**

- ⇨ Allocate IP addresses to each subnet, ensuring that there is no overlap, and each subnet has a unique range of addresses.

5. **Implement Routing**

- ⇨ Configure routers or layer 3 switches to route traffic between the subnets, ensuring that devices in different subnets can communicate when necessary.

**Example 1**:

- ⇨ Suppose you have the IP address range 192.168.1.0/24 (Class C)
- ⇨ We want to create four subnets, each capable of accommodating 30 hosts. Here's how you might subnet it:

**Original Network: 192.168.1.0/24**

Subnet 1: 192.168.1.0/27 (30 hosts)

Subnet 2: 192.168.1.32/27 (30 hosts)

Subnet 3: 192.168.1.64/27 (30 hosts)

Subnet 4: 192.168.1.96/27 (30 hosts)

Subnet 5: 192.168.1.128/27 (30 hosts)

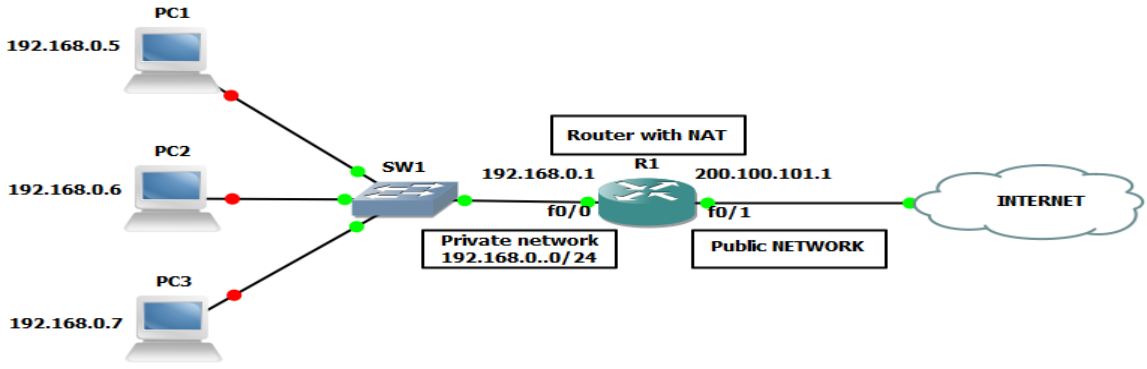
Subnet 6: 192.168.1.160/27 (30 hosts)

Subnet 7: 192.168.1.192/27 (30 hosts)

Subnet 8: 192.168.1.224/27 (30 hosts)

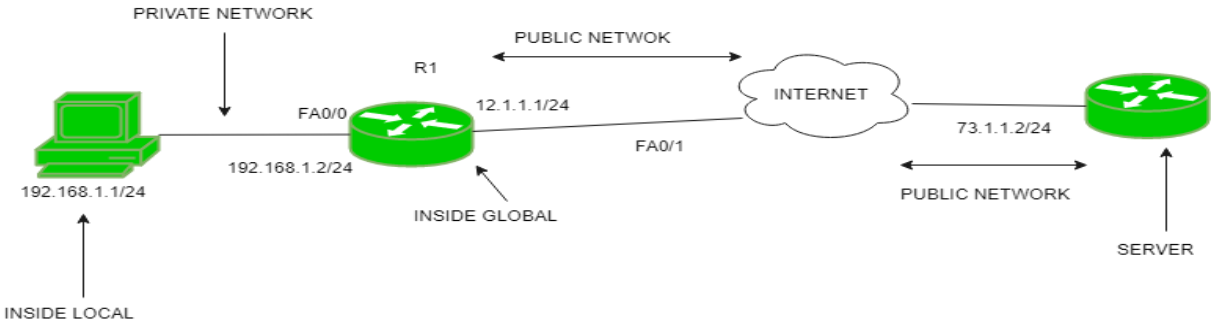
### 3.7. NAT

- ⇨ NAT stands for network address translation.
- ⇨ It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.



### 1. Static NAT

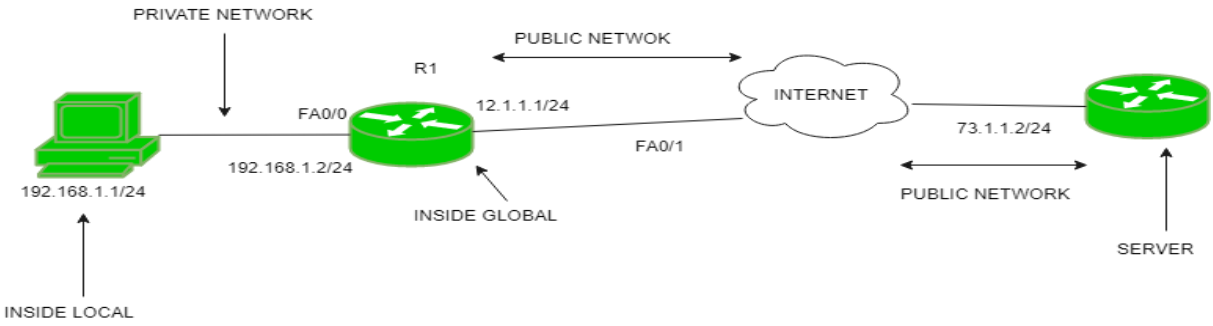
⇨ When the local address (private address) is converted to a public one, this NAT chooses the same one.




### 2. Dynamic NAT

⇨ Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses.

⇨ This results in the router or NAT device getting a different address each time the router translates the local address to a public address.



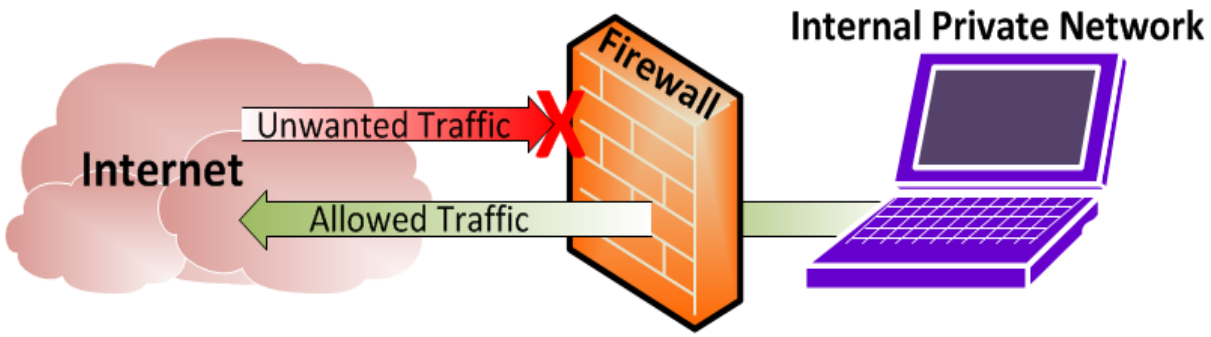

### 3. PAT

⇨ PAT stands for port address translation.

⇨ It's a type of dynamic NAT, but it bands several local IP addresses to a singular public one.

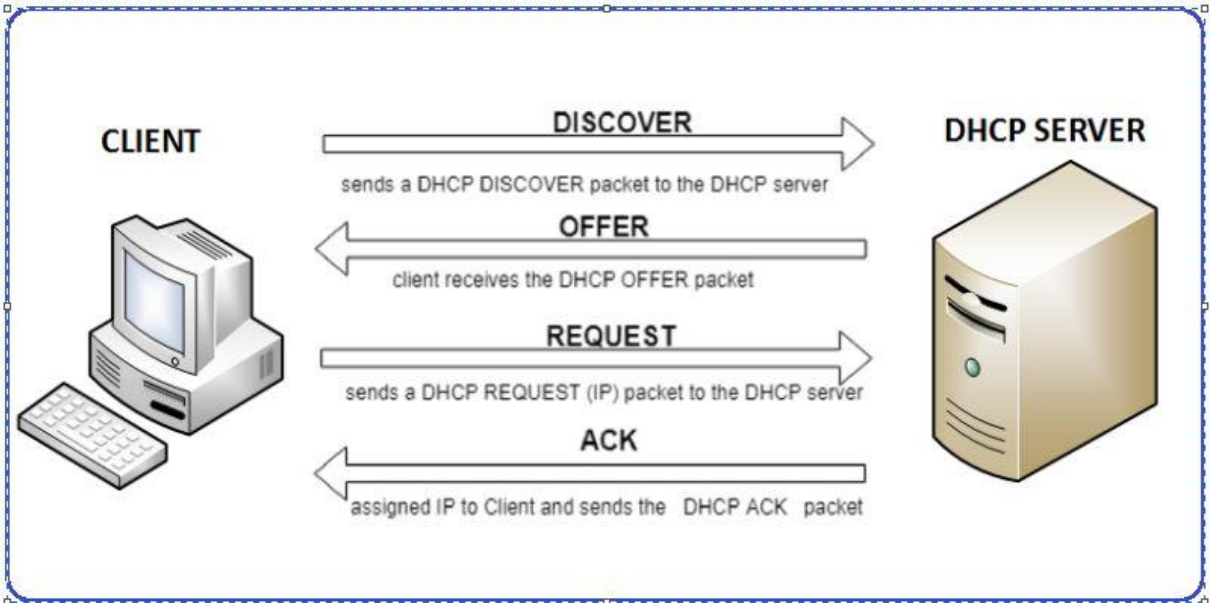
## 3.8. Firewall

A firewall is a network security device that monitors traffic to or from your network



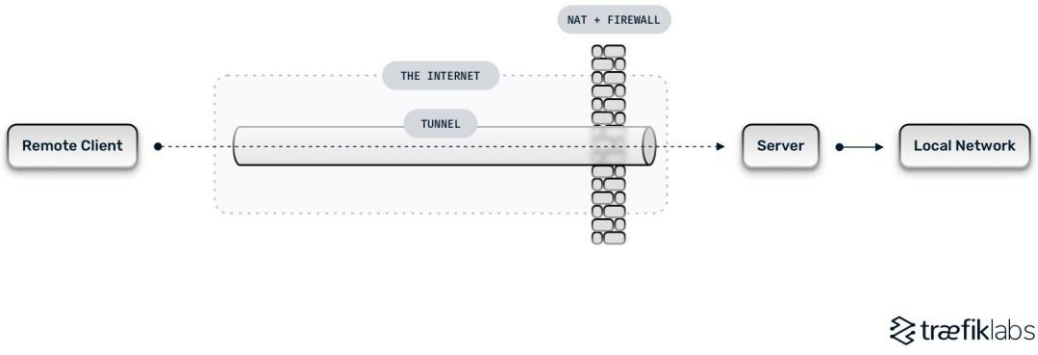
### 3.9. DHCP

- ⇨ The DHCP (Dynamic Host Configuration Protocol) process is a network protocol used to dynamically assign IP addresses and other network configuration parameters to devices (hosts) on a local network.
- ⇨ DHCP simplifies the process of IP address assignment and configuration, especially in larger networks.




### 3.10. Tunneling

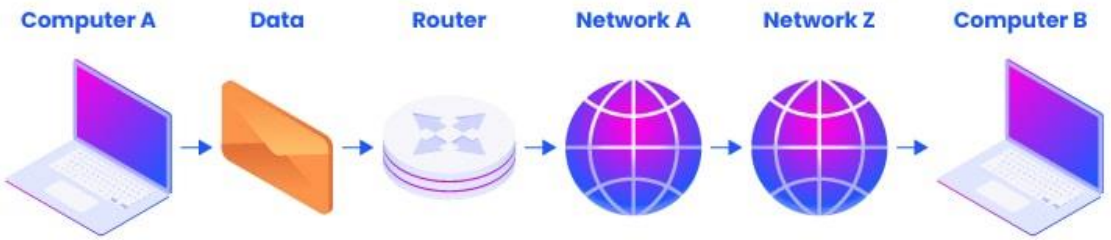
- ⇨ Tunneling is a method of discretely transmitting data across an otherwise public network.
- ⇨ The transmission takes place using a public network; however, the data are intended for use only within a private network.
- ⇨ Network tunnels provide a direct connection between a remote server and the local network, and the transmission of data is undetectable by the public network.



# 4. Ethernet routing and architecture

## 4.1. What is Routing ?

⇨ Routing is a fundamental concept in networking that involves **determining** the **optimal path** for data packets to travel from a source to a destination within a computer network.




IPXO

## 4.2. Routing basic algorithms

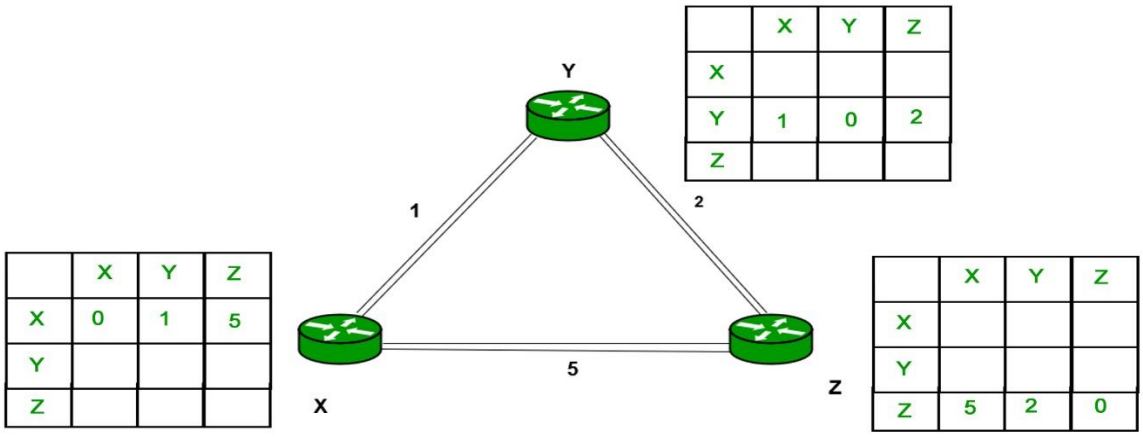
⇨ Routing algorithms are used to determine the best path for data to travel from a source to a destination in a computer network.

⇨ Two fundamental categories of routing algorithms are distance-vector and link-state routing algorithms

### 1. Distance-Vector Routing:

⇨ Distance-vector routing algorithms, also known as **Bellman-Ford algorithms**, operate by sharing routing information among neighboring routers.

⇨ They calculate the distance (or cost) to reach all possible destinations in the network and select the path with the shortest distance.



⇨ Key characteristics of distance-vector routing include:

**1. Distance Metric**

⇨ Each router maintains a routing table that contains the distance (metric) to reach various destinations.

⇨ The metric can represent factors like hop count, bandwidth, or latency.

**2. Periodic Updates**

⇨ Routers periodically exchange routing information with their neighboring routers.

⇨ They share their routing tables, allowing neighboring routers to update their own tables.

**3. Routing Loops**

⇨ Distance-vector routing algorithms are susceptible to routing loops, where routers continuously exchange outdated information, causing incorrect routing decisions.

⇨ To mitigate this, techniques like split horizon and route poisoning are used.

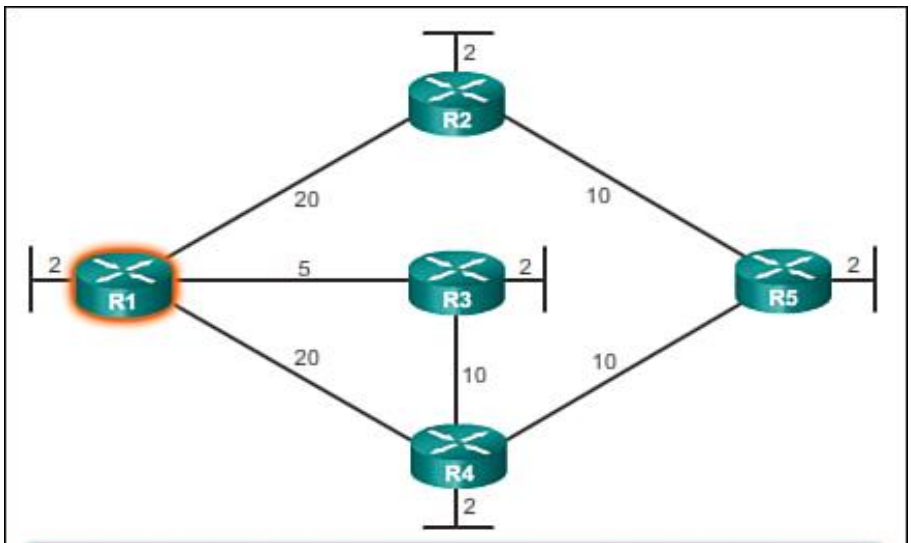
**4. Convergence Time**

⇨ Convergence (the process of routers reaching a consistent view of the network) can be slow in distance-vector algorithms, especially in large networks, as routers wait for periodic updates to propagate.

**2. Link-State Routing**

⇨ Link-state routing algorithms, also known as Dijkstra's algorithms, operate by building a detailed map of the entire network.

⇨ They calculate the shortest path to reach a destination based on this map.




| Destination | Shortest Path | Cost |
|---|---|---|
| R2 LAN | R1 to R2 | 22 |
| R3 LAN | R1 to R3 | 7 |
| R4 LAN | R1 to R3 to R4 | 17 |
| R5 LAN | R1 to R3 to R4 to R5 | 27 |

⇨ Key characteristics of link-state routing include:

**1. Link-State Database :** Each router maintains a link-state database, which contains information about the network's topology, link costs, and the state of each link (up or down).

**2. Flooding**

⇨ Routers periodically send link-state advertisements (LSAs) to all routers in the network.

⇨ These LSAs contain information about the router's local links and their states. LSAs are flooded throughout the network.

**3. Dijkstra's Algorithm**

⇨ Routers use Dijkstra's algorithm to calculate the shortest path to all destinations based on the link-state database.

⇨ This results in a routing table that contains the best path to each destination.

**4. Fast Convergence**

⇨ Link-state routing algorithms typically converge more quickly than distance-vector algorithms because routers have a complete view of the network and can make decisions based on up-to-date information.

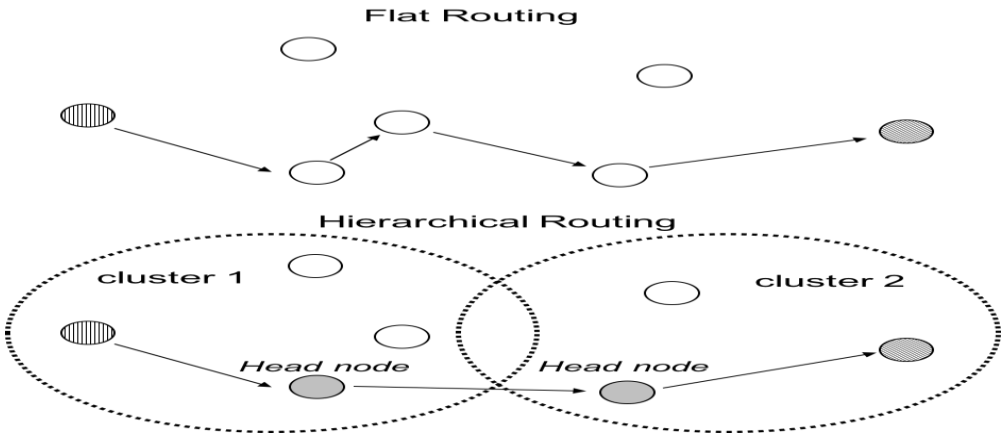
### 4.3. Hierarchical routing, autonomous systems

⇨ Hierarchical routing and autonomous systems are concepts and practices used in large-scale computer networks, particularly in the context of the Internet, to manage and organize network routing efficiently.

**1. Hierarchical Routing**

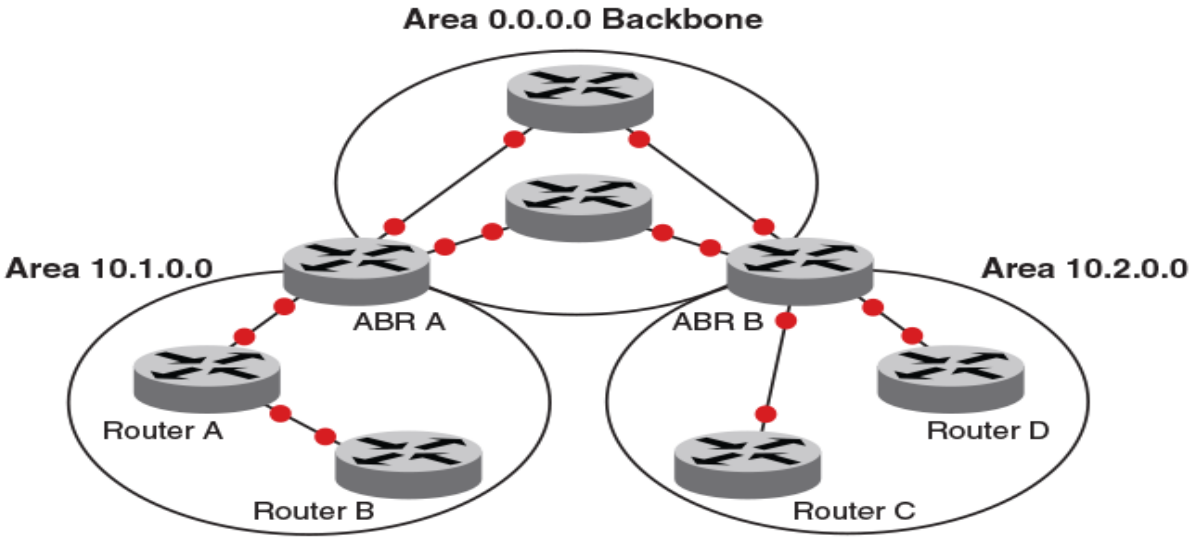
⇨ Hierarchical (routing or addressing or network design, is an approach used to simplify and optimize network routing in large networks, such as the global Internet.

⇨ It involves dividing the network into multiple levels or tiers, with each level responsible for a specific portion of the routing process.



## 2. Autonomous Systems (AS)

- An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization or entity that follows a common routing policy.
- ASes are a fundamental concept in the Internet's Border Gateway Protocol (BGP), which is used for routing between different ASes




### 4.4. Internal routing

- Internal routing refers to the process of forwarding data packets within a single network or autonomous system (AS).
- It involves the routing of data between devices, subnets, or segments within the same network, rather than routing data between different networks or autonomous systems.
- Internal routing is typically used within an organization's private network or within a single Internet Service Provider's (ISP) network.

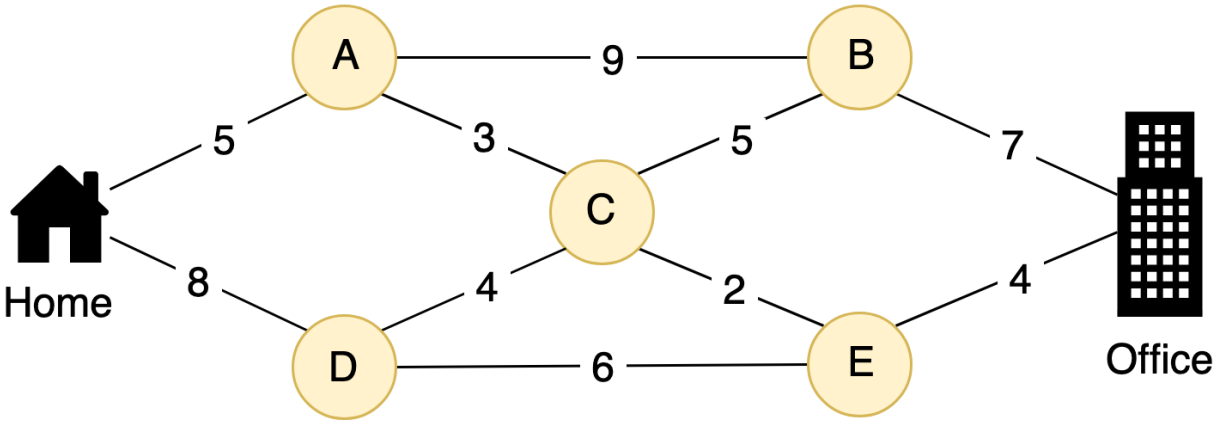
## Open Shortest Path First (OSPF) protocol

- Open Shortest Path First (OSPF) is a routing protocol commonly used in IP networks, especially in large enterprise networks and the Internet.
- OSPF is designed to efficiently determine the best paths for data packets to travel within a network, based on various factors, while also being adaptable to changes in network topology.
- Here are the key features and aspects of OSPF:

### 1. Link-State Protocol

- OSPF is a link-state routing protocol, which means that it maintains a detailed and up-to-date map of the entire network's topology.

⇨ Each router in an OSPF network knows about all the other routers and the links connecting them.




⇨ This information is stored in the router's Link-State Database (LSDB).

### 2. Hierarchical Structure

⇨ OSPF networks are often organized hierarchically.

⇨ The network can be divided into areas, each with its own routing information.

⇨ This hierarchical design helps manage large networks more efficiently.

### 3. Area Types

⇨ OSPF defines several area types, including backbone areas (Area 0) and non-backbone areas (Area 1, Area 2, etc.).

⇨ The backbone area connects all the other areas and plays a central role in OSPF routing.

### 4. Shortest Path First (SPF) Algorithm

⇨ OSPF uses the SPF algorithm (Dijkstra's algorithm) to calculate the shortest path to reach all destinations within the network based on the link-state database.

⇨ This ensures that OSPF routers choose the most efficient paths.

### 5. Hello Protocol

⇨ OSPF routers use the Hello protocol to establish and maintain neighbor relationships.

⇨ Routers send Hello packets to discover neighbors and ensure they are still reachable.

⇨ Neighbor relationships are essential for OSPF routing updates.

### 6. Cost-Based Routing

- ⇨ OSPF uses a cost metric known as the "cost" or "metric" associated with each link.
- ⇨ By default, the cost is inversely proportional to the link's bandwidth.
- ⇨ Routers choose paths with the lowest total cost when making routing decisions.

### 7. Dynamic Updates

- ⇨ OSPF routers exchange routing updates when network topology changes occur.
- ⇨ These updates are sent only to routers affected by the change, minimizing network traffic.

### 8. Load Balancing

- ⇨ OSPF supports load balancing by allowing multiple paths to reach the same destination.
- ⇨ This is particularly useful for distributing traffic and improving network performance.

### 9. Authentication

- ⇨ OSPF provides authentication mechanisms to secure routing updates and ensure that only authorized routers can participate in OSPF routing.

### 10. Scalability

- ⇨ OSPF is designed to scale efficiently, making it suitable for both small and large networks.
- ⇨ Its hierarchical structure and efficient SPF algorithm contribute to its scalability.

### 11. IPv6 Support

- ⇨ OSPFv3 is the version of OSPF designed for IPv6 networks, providing routing capabilities for the next generation of Internet Protocol

## 4.5. External Routing

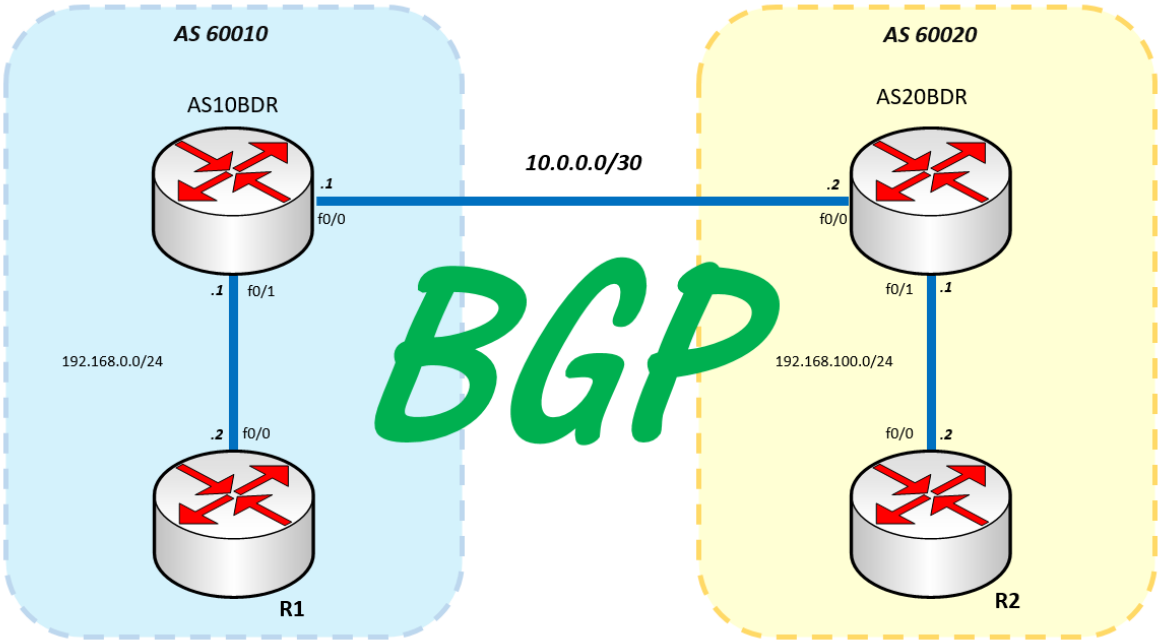
- ⇨ External routing, also known as **interdomain routing** or **exterior routing**
- ⇨ refers to the process of determining the best path for data packets to travel between different autonomous systems (ASes) or networks on the Internet

⇨ It is responsible for routing data between networks that are not part of the same administrative domain

### a. BGP protocol

⇨ BGP (Border Gateway Protocol) is the protocol that enables the global routing system of the internet.

⇨ It manages how packets get routed from network to network by exchanging routing and reachability information among edge routers (is a specialized router located at a network boundary that enables an internal network to connect to external networks.)




⇨ BGP helps provide redundancy by enabling routers to quickly adapt and send packets through another connection if one internet path goes down.

⇨ It is often used in large networks, such as internet service provider networks, wide area networks and infrastructure-as-a-service environments.

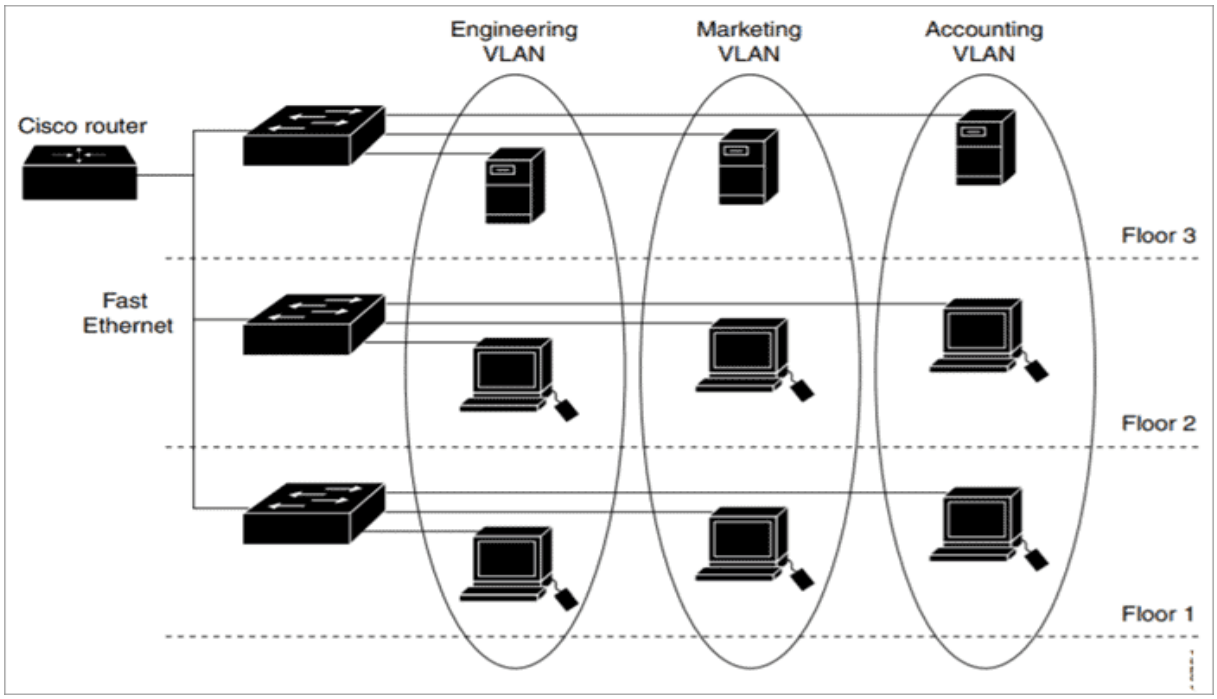
**How does BGP work?**

- ⇨ Each router maintains a routing table that controls how packets are directed.
- ⇨ The BGP process on the router generates routing table information, which is based on the following factors:

1. Incoming information from other routers.
2. Information in the BGP routing information base (RIB), which is a data table stored on a server on the BGP router.
3. The RIB contains information both from directly connected external peers and internal peers.
4. The RIB contains policies for what routes should be used and what information should be published, and it continually updates the routing table as changes occur.

## 4.6. VLAN (virtual local area network)

- ⇨ Is a network technology that allows you to logically segment a physical network into multiple isolated virtual networks.
- ⇨ Each VLAN operates as if it were a separate physical network, even though devices within the same VLAN can be located physically dispersed across a network.

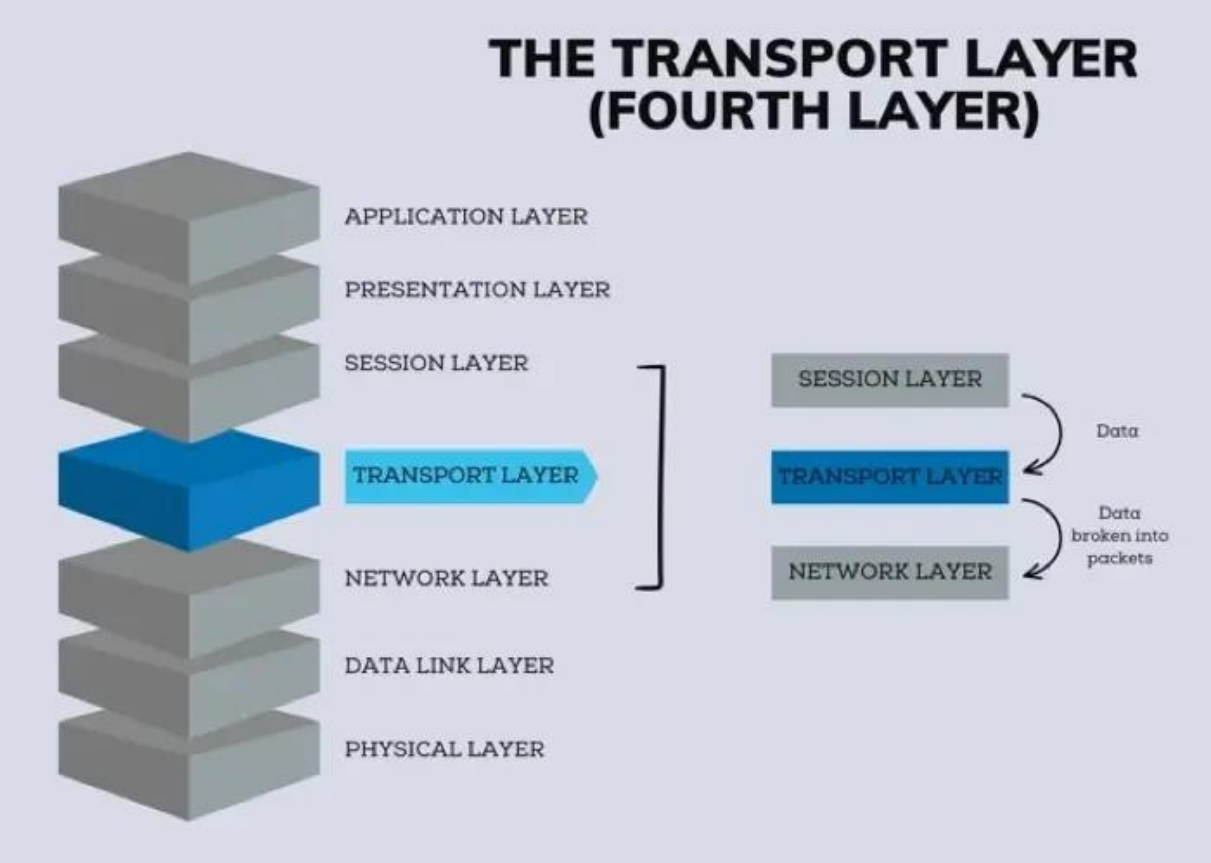


# 5. Transport Layer

## 5.1. Definition

⇨ The transport layer is Layer 4 of OSI model.

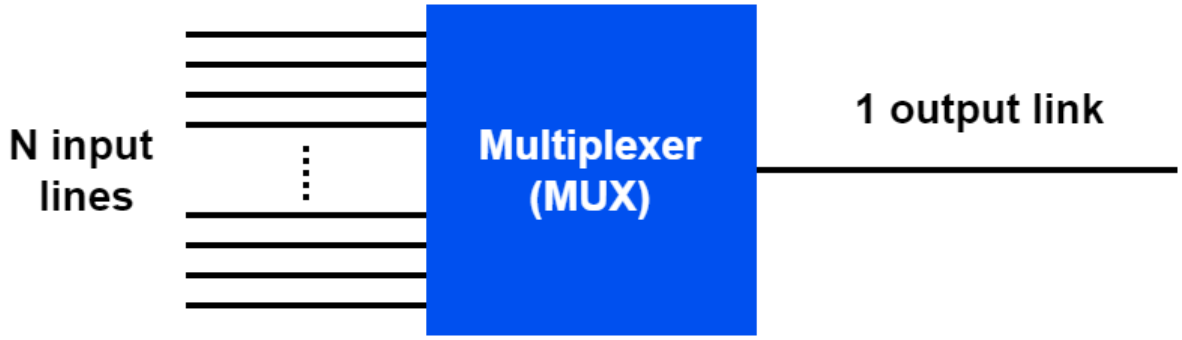
⇨ It is responsible for **ensuring that the data packets arrive accurately and reliably between sender and receiver.**




- To illustrate the transport layer, imagine a computer is a big company with many departments.
- The data packets are letters.
- The network layer is like the Postal Service that gets the letters to the correct address of the company.
- The transport layer is like the company mailroom. It receives the letters and does an initial inspection.

## 5.2. Multiplexing

⇨ Multiplexing involves combining multiple data streams into a single transmission channel




⇨ The primary purpose of multiplexing is to increase the capacity of the transmission medium, which could be a physical wire, a fiber optic cable, or even a wireless channel.

⇨ Instead of dedicating separate channels to each signal, multiplexing allows several signals to share a single channel.

⇨ In this way, it makes more efficient use of the available bandwidth.

### b. Types

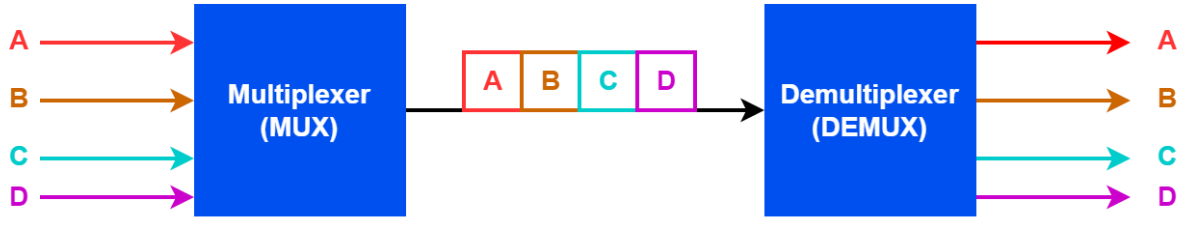
⇨ these techniques are used to improve the effectiveness and scalability of communication networks by enabling the transmission of numerous signals over a single channel.

**1. <u>Time-division multiplexing (TDM)</u>**

⇨ In TDM, we first divide the **available bandwidth** of the communication channel into time slots.

⇨ Furthermore, we assign each input signal to a specific time slot.

⇨ Therefore, the input signals are then transmitted sequentially, one after the other, in their assigned time slots:

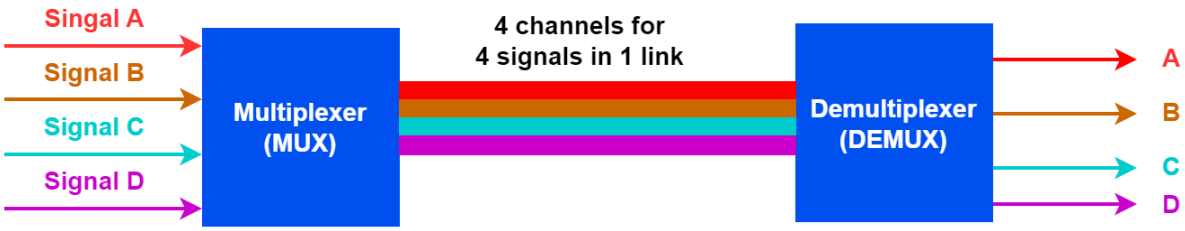


2. **frequency-division multiplexing (FDM)**

⇨ In FDM, we divide the available bandwidth of the communication channel into multiple frequency bands.

⇨ Additionally, we assign each input signal to a specific frequency band.

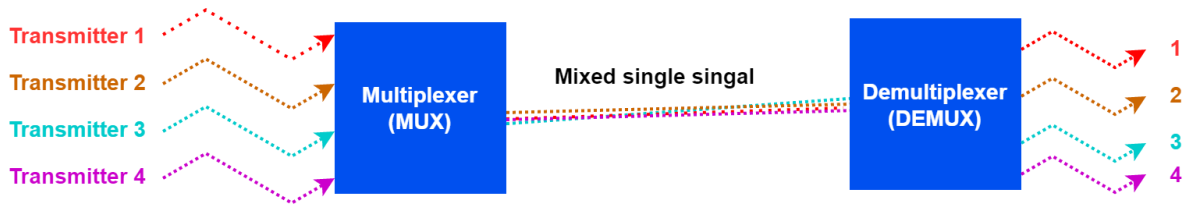
⇨ Moreover, the input signals are then transmitted simultaneously, each in their assigned frequency band:




3. **Wavelength-division multiplexing (WDM)**

⇨ Is similar to FDM but used in optical communication systems.

⇨ In WDM, in order to allocate each input signal to a wavelength band, we split the possible bandwidth of an optical fiber into a number of **wavelength** bands:




### c. Advantages and Disadvantages

| Advantages | Disadvantages |
|---|---|
| Allows multiple data streams to be transmitted over a single channel | Can be complex. Hence, require specialized equipment and expertise to implement |
| Reduces the cost of transmitting data | Can limit the flexibility of a system. Therefore, as all data streams must be compatible with the same channel |
| Reduces the amount of time required to transmit data | If the multiplexing system fails, all data streams transmitted over the channel will be affected |
| Allows more data to be transmitted over a given bandwidth | Can increase latency, as data streams may have to wait to be transmitted over the channel |

## 5.3. Connected / No-connected Mode

### a. Connected mode

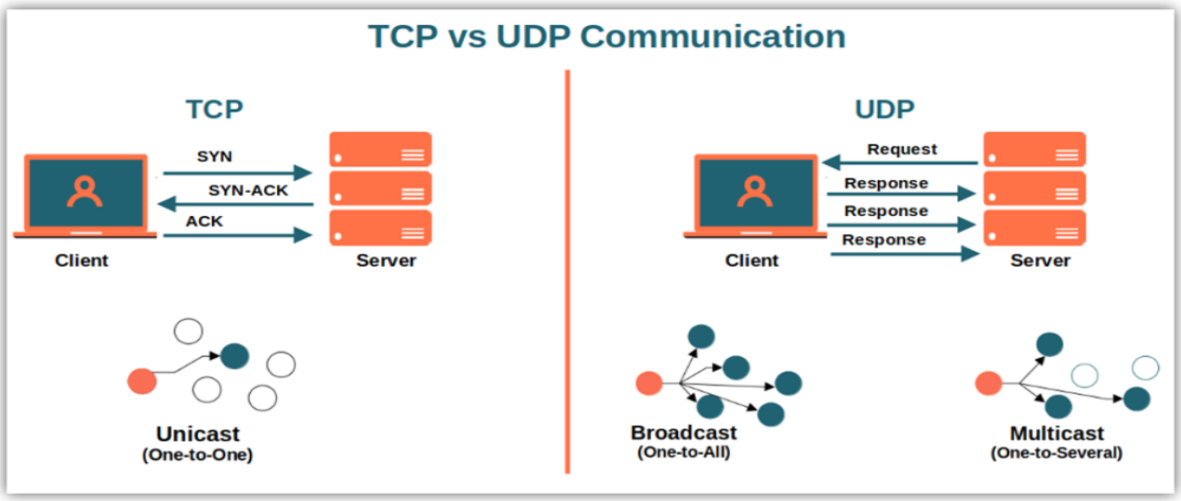
- ⇨ This refers to protocols like TCP that establish a virtual circuit between two devices before data transfer begins.
- ⇨ Data is sent in a reliable, ordered, and error-checked manner.
- ⇨ Examples include file transfer protocols (FTP) and web browsing.

### b. Non-connected mode

- ⇨ This refers to protocols like UDP that send data packets without establishing a prior connection.
- ⇨ Packets are independent and may arrive out of order or not at all.
- ⇨ Examples include video streaming and online gaming.

## 5.4. TCP vs UDP

- ⇨ both of them in Transport layer (layer 4 in OSI model)
- ⇨ TCP (Transmission Control Protocol) ensures reliable, ordered data transfer with connection setup.
- ⇨ UDP (User Datagram Protocol) provides faster, connectionless data transmission, prioritizing speed over guaranteed delivery and ordering.



⇨ Here some differences between TCP and UDP

| Feature | TCP | UDP |
|---|---|---|
| Connection Type | Connection-oriented | Connectionless |
| Reliability | Reliable: Guarantees in-order delivery and error checking with retransmissions. | Unreliable: No guarantees; packets may arrive out of order or be lost. |
| Speed | Slower due to overhead of connection establishment and error checking. | Faster due to simpler structure and lack of error checking. |
| Data Order | Ordered: Packets delivered in the same order they were sent. | Unordered: Packets may arrive in any order or not at all. |
| Error Handling | Handles errors with retransmissions and checksums. | No error handling; lost packets are not recovered. |
| Congestion Control | Implements congestion control mechanisms to adjust data flow and avoid network overload. | No congestion control; all packets treated equally. |
| Overhead | Higher overhead due to header information and control flags. | Lower overhead due to simpler header structure. |
| Suitable for: | Reliable data transfer, file transfer, email, web browsing, secure communication. | Streaming media, online gaming, VoIP, real-time applications. |

# 6. Network Layer

## 6.1.Remote connection

⇨ A remote connection is a connection between two computers that are physically separated.

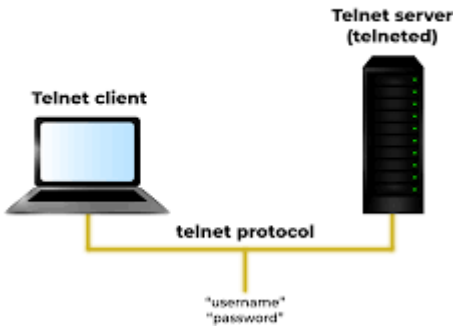
⇨ It allows a computer user to access and interact with another computer as if he were sitting in front of him.

⇨ Remote connections can be established in various ways, including:

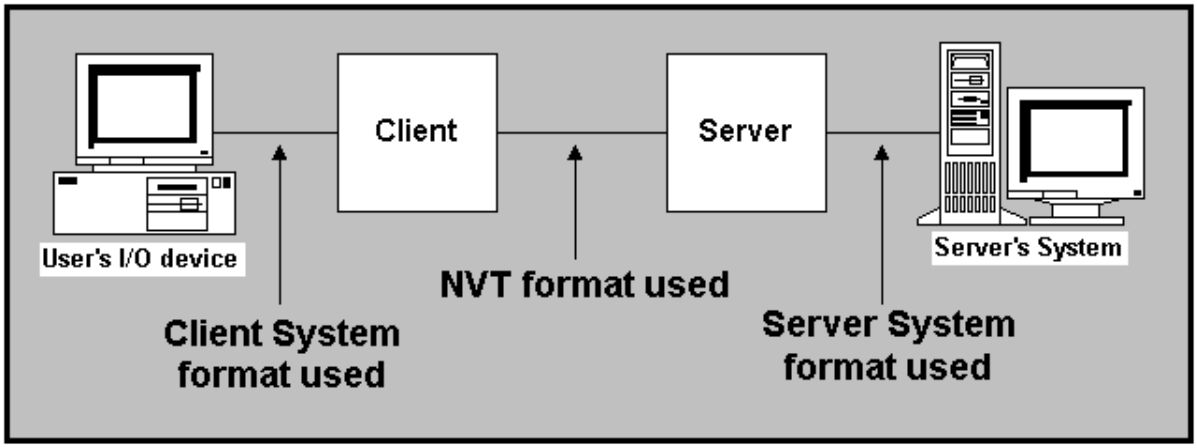
1. **Modem connection**: A modem connection uses a telephone line to establish a physical connection between two computers.
2. **Network connection**: A network connection uses a local area network (LAN) or a wide area network (WAN) to establish a connection between two computers.
3. **Satellite connection**: A satellite connection uses a satellite to establish a connection between two computers that are located at remote distances.

### a. Telnet Protocol

⇨ is a protocol that allows a client to communicate with a remote server by exchanging lines of text and receiving responses also as text.



- The **NVT representation** is a set of conventions used by the Telnet protocol to represent data exchanged between two computers.
- The NVT representation defines the formats of text, binary, and other data types. It also defines the control codes used to control the data flow.

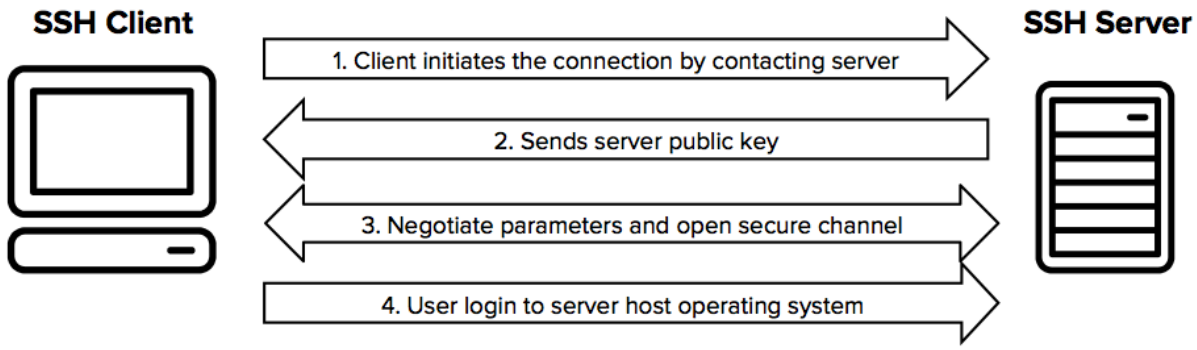



### b. rlogin

- rlogin is a program that allows a computer user to access and interact with another computer as if he were sitting in front of him.
- rlogin is **similar to the Telnet protocol**, but it is **more secure**.
- rlogin uses encryption protocol to protect data exchanged between the two computers.

### d. SSH

- SSH is a security protocol that allows a user of one computer to access and interact with another computer securely.



⇨ SSH provides a variety of security features, including:

1. **Authentication**: SSH uses strong authentication methods, such as public key authentication, to authenticate users.
2. **Encryption**: SSH uses encryption to protect the data exchanged between the two computers.
3. **Access Control**: SSH allows administrators to control access to remote resources.

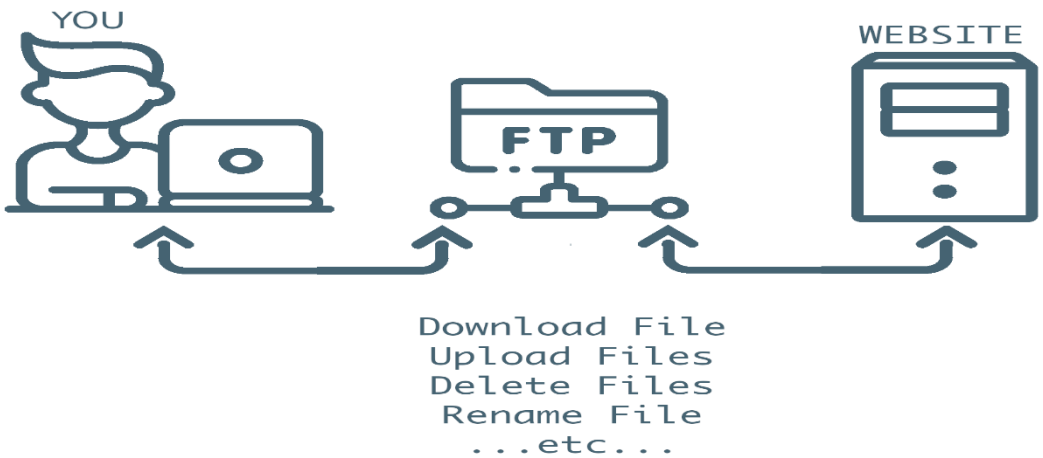
## 6.2. File transfer

⇨ File transfer refers to the process of moving files between different computer systems across a network or other data storage medium.

⇨ This common operation allows for sharing data, backups, remote access, and other essential tasks.

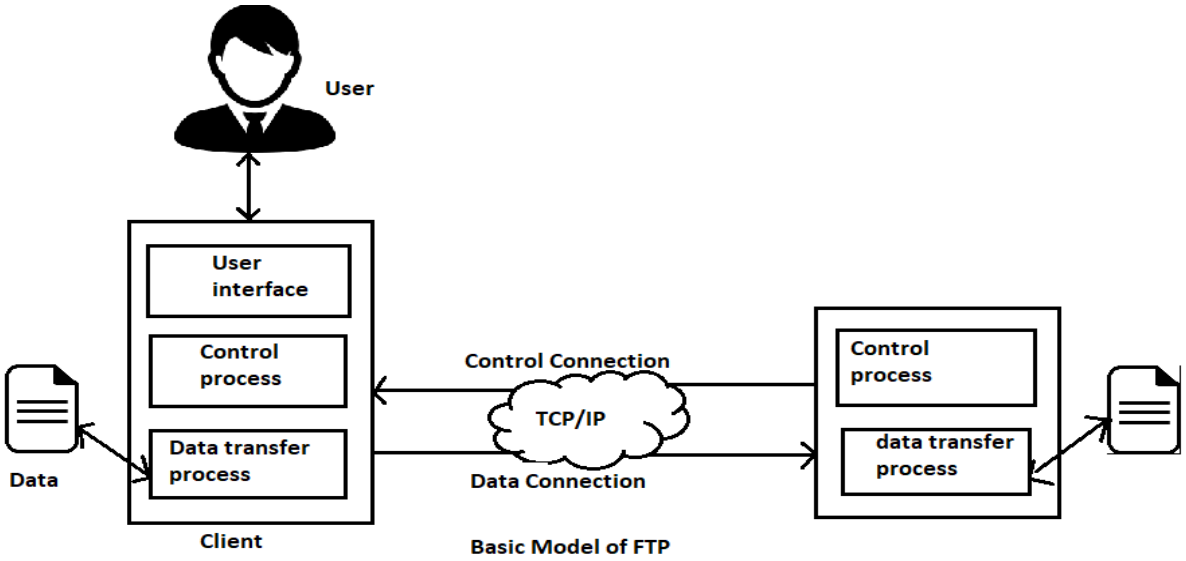

### a. FTP Protocol (File Transfer Protocol)

⇨ FTP is a well-established protocol for transferring files over a network.



⇨ It establishes a dedicated connection between client and server and employs two channels:

1. **Control Channel**: Handles commands for file manipulation, directory listing, etc.
2. **Data Channel**: Transfers the actual file data itself.



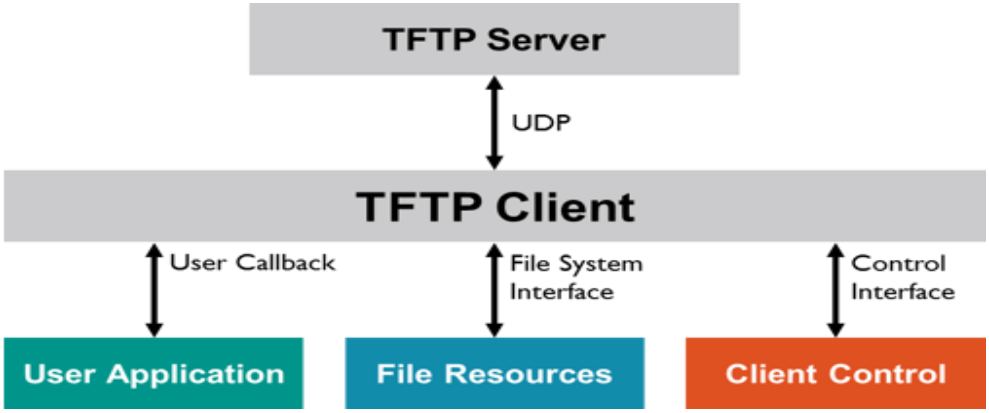
Basic Model of FTP

⇨ While offering features like username/password authentication and directory navigation, FTP has limitations:

1. **Unsecured Transmission:** Data channels are unencrypted, exposing them to potential interception and eavesdropping.
2. **Passive Mode:** Requires configuration for firewalls, making it less versatile.

### b. TFTP Protocol (Trivial File Transfer Protocol)

⇨ TFTP is a simple and lightweight protocol designed for transferring small files efficiently.



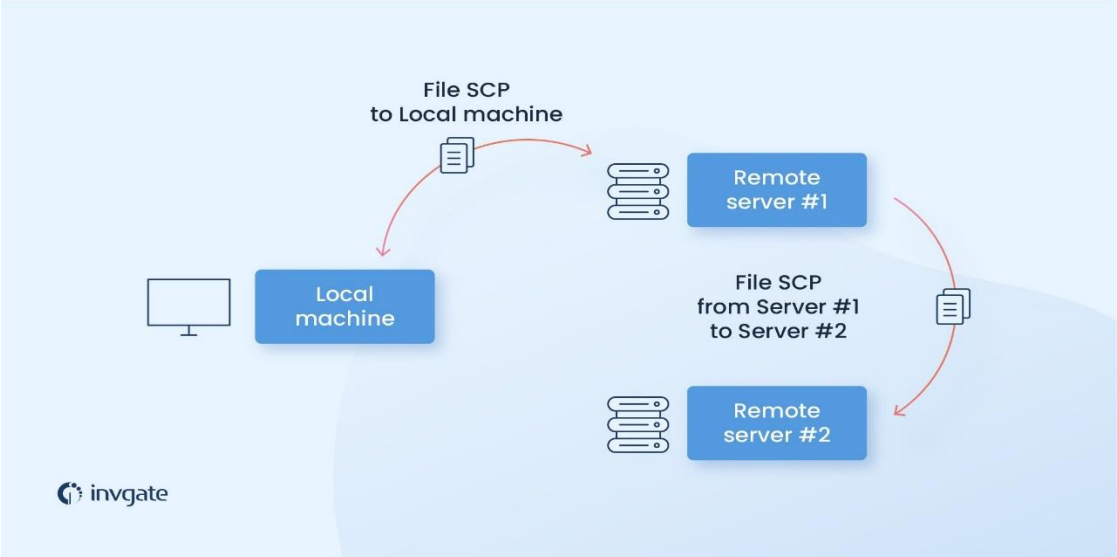
⇨ It **uses UDP** for faster transmission and avoids establishing dedicated connections, making it well-suited for:

1. Booting network devices
2. Transferring configuration files
3. Firmware updates

⇨ However, TFTP lacks security features like authentication and encryption, limiting its usage to trusted networks.

### c. rcp Protocol (remote copy protocol)

⇨ rcp is a command-line tool and protocol primarily used in Unix-like systems for transferring files between local and remote machines.



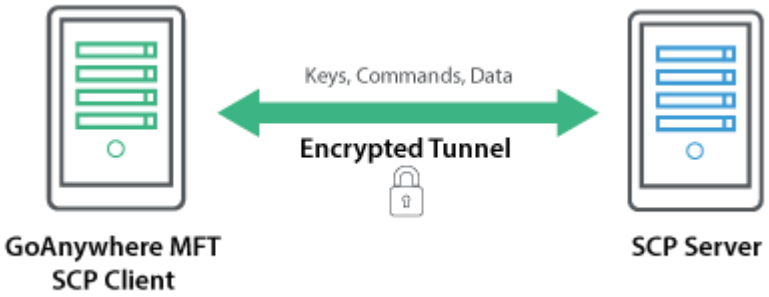

⇨ It utilizes TCP for reliable data transfer but requires separate authentication with commands like **rlogin**.

⇨ While efficient for basic file transfers within trusted environments, rcp lacks encryption and modern security features, making it less secure than newer protocols.

### e. scp Protocol (secure copy protocol)

⇨ scp is a secure version of **rcp** built on top of SSH (Secure Shell).

⇨ **It leverages SSH capabilities for secure authenticated connections and encrypts all data channels, protecting against unauthorized access and data eavesdropping.**




- scp offers a convenient and secure way to transfer files between remote machines and is widely used for system administration, software deployment, and remote collaboration.

### 6.3. Messaging architecture

- Messagin architecture refers to the overall structure and framework for how messages are exchanged between entities in a network.
- In email, the architecture involves different components like user agents (mail clients), mail servers (SMTP server, POP/IMAP server), and communication protocols.
- Message structure defines the format and organization of an email message itself. It includes **various components** like headers containing sender/recipient information, subject line, and timestamps, followed by the message body and potentially attachments.

#### a. MIME Format (Multipurpose Internet Mail Extensions)

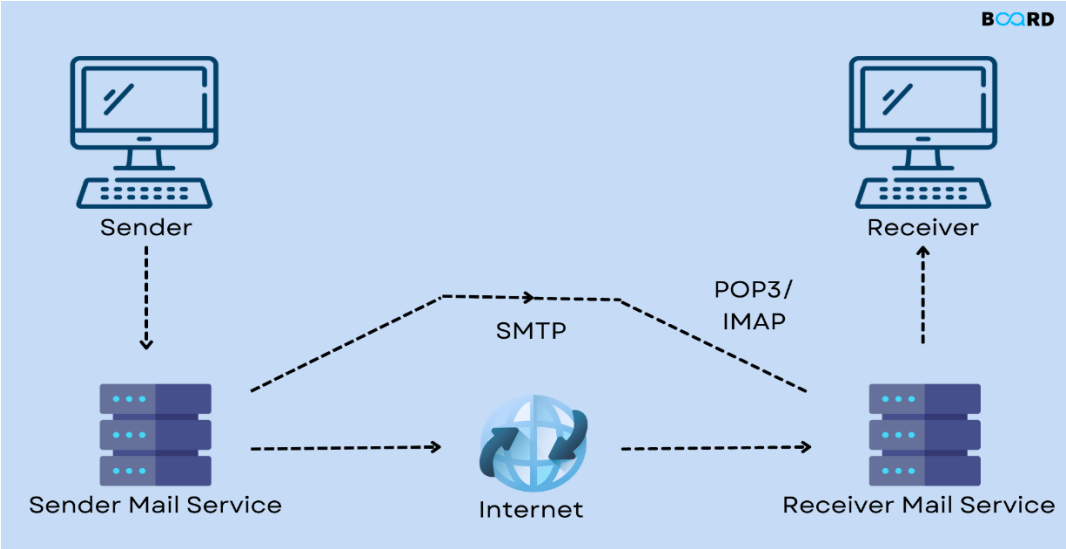
- This standard allows emails to **contain more than just plain text**.
- It enables the inclusion of **attachments like images, documents, multimedia files,** etc., by defining how to encode and represent different data types within the message body.
- MIME headers identify the type of content for each part of the message.

### b. SMTP Protocol (Simple Mail Transfer Protocol)

⇨ This is the protocol used for sending emails between mail servers. (port 25)

⇨ It defines the rules and commands for transmitting messages from a sending server to a receiving server.

⇨ SMTP doesn't store messages; it simply relays them.




### c. POP (Post Office Protocol)

⇨ This protocol allows email clients to retrieve messages from a mail server.

⇨ POP users download messages to their local device and then delete them from the server (unless configured otherwise).

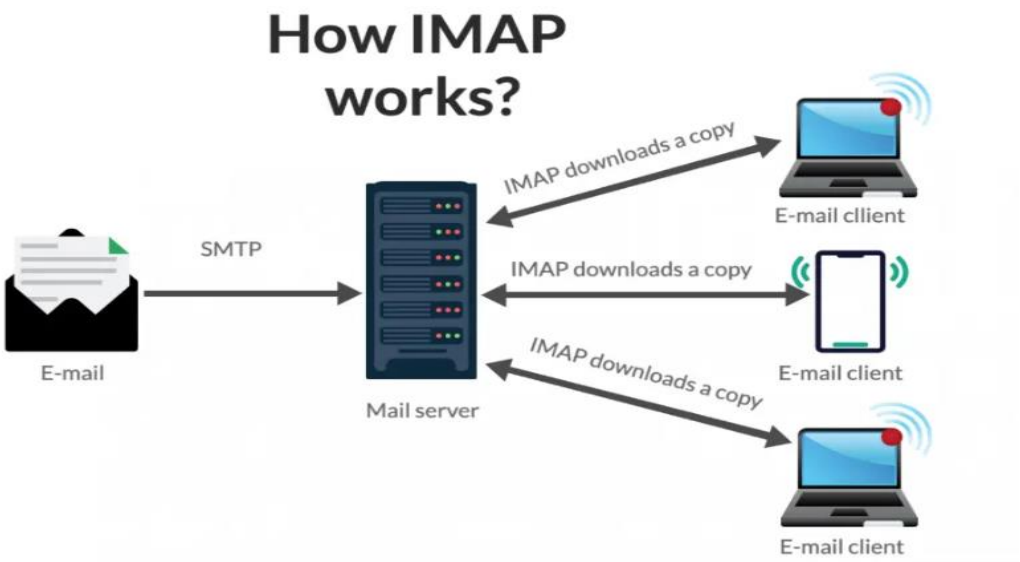
⇨ It's a simple protocol good for occasional email access.

### d. IMAP (Internet Message Access Protocol)

⇨ This protocol provides more sophisticated access to emails stored on a mail server.

⇨ Users can browse messages, download specific ones, and leave them on the server for later access from different devices.

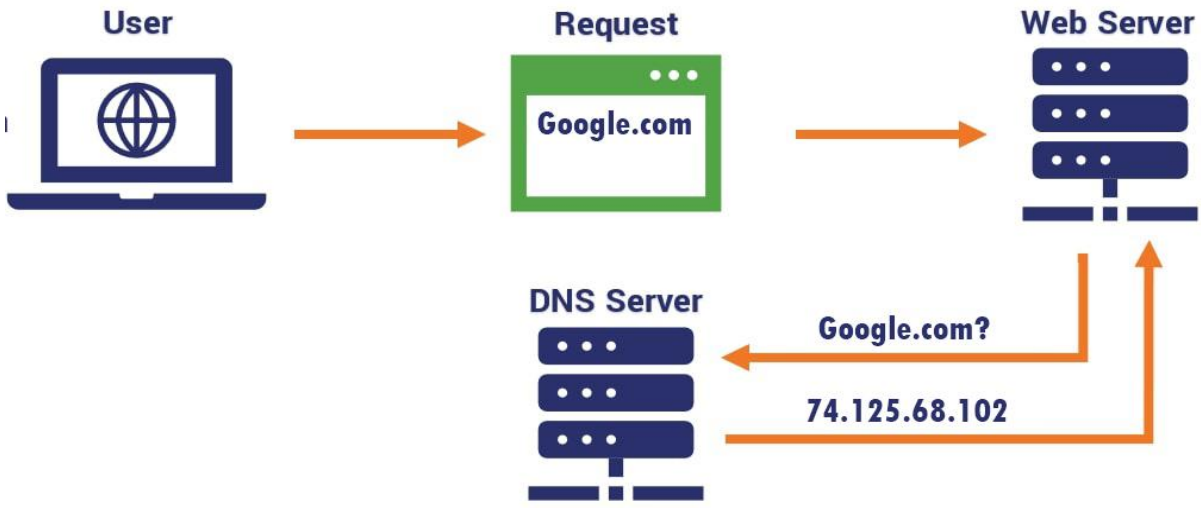
⇨ IMAP offers greater flexibility and convenience compared to POP.




## 6.4. DNS (domain name server)

⇨ The Internet DNS system works like a **telephone directory** by managing the mapping between **names and numbers**.

⇨ DNS servers **translate requests from names to IP addresses**, controlling which server an end user will connect to when they type a domain name into their browser.



## 7. References


1. https://www.geeksforgeeks.org/computer-network-tutorials/
2. https://bard.google.com/
3. https://en.wikipedia.org/wiki/Computer_network
4. https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/
5. https://chat.openai.com/
6. https://www.cloudflare.com/fr-fr/learning/email-security/what-is-smtp/