NETWORK - A BASIC GUIDE

BY JITENDRA SINGH TOMAR

INDEX

INTRODUCTION

- The main purpose of network is to share the data and can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.
- The networking process also involves designing, implementing, upgrading, managing and working with networks and network technologies.

WHAT IS COMPUTER NETWORKING?

- A computer network is a system that connects numerous independent computers in order to share information (data) and resources.
- A computer network is a collection of two or more computer systems that are linked together.
- A network connection can be established using either cable or wireless media.
- Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network.

WHAT DO COMPUTER NETWORKS DO?

Computer Networks help in providing better connectivity that helps nowadays. Modern computer networks have the following functionality like

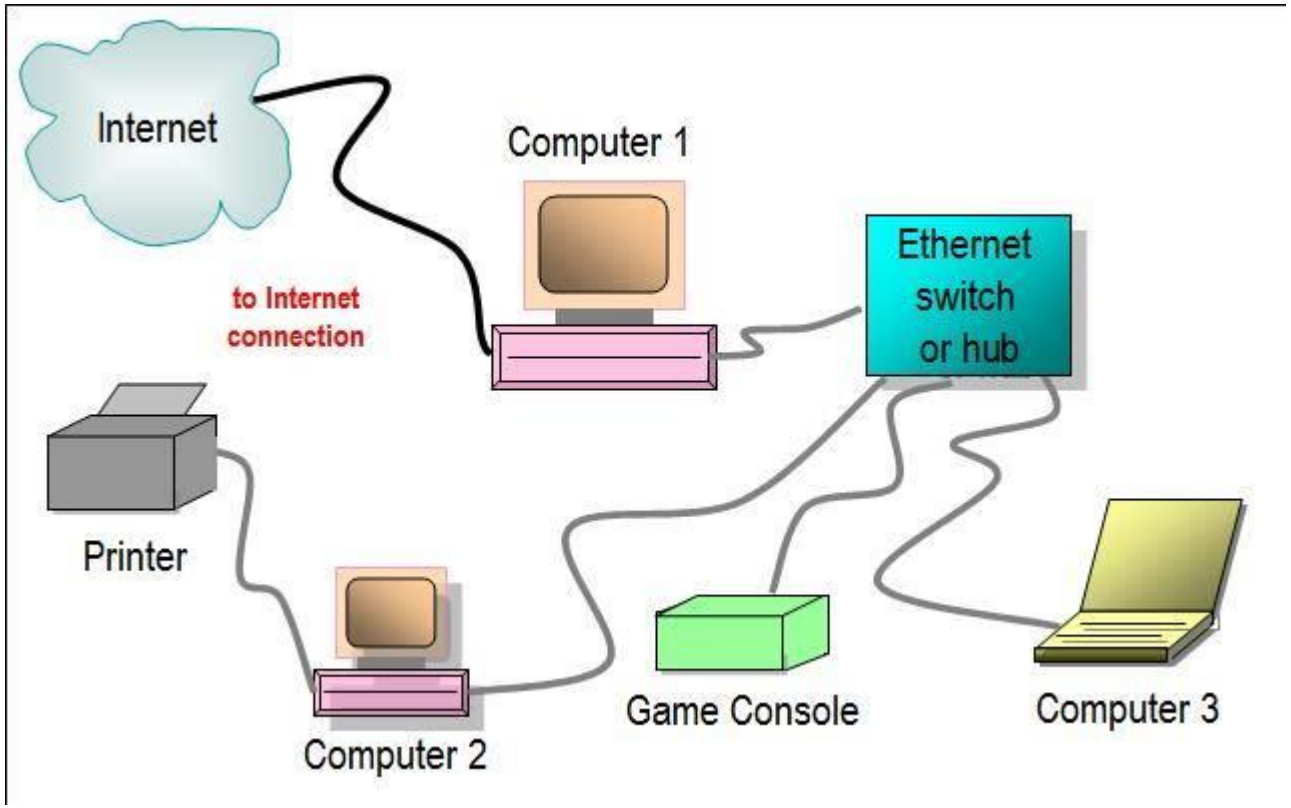
- Computer Networks help in operating virtually.
- Computer Networks integrate on a large scale.
- Computer Networks respond very quickly in case of conditions change.
- Computer Networks help in providing data security.

CRITERIA OF A GOOD NETWORK

- **Performance**: It can be measured in many ways, including transmit time and response time.
  - Transit time is the amount of time required for a message to travel from one device to another.
  - The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware
- **Reliability**: In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network's robustness in catastrophe.
- **Security**: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

PURPOSE OF NETWORK

Networking is the practice of associating two or more computing devices together physically or logically for the purpose of sharing data and resources.



GOALS OF COMPUTER NETWORKING

- Load sharing
- Reduced costs
- Reliability
- Scalability
- Communication and mail
- Information Access
- Entertainment
- Social Networking

TYPES OF NETWORK - BASED ON THE COMMUNICATION MEDIUM

- **Wired Network**
  - Communication done in a wired medium. Copper wire, twisted pair, or fiber optic cables are all options.
  - A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.
- **Wireless Network**
  - "Wireless" means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves.
  - Antennas or sensors will be present on all wireless devices.

TYPES OF NETWORK - BASED ON AREA COVERED

- **Local Area Network** (LAN)
  - A LAN is a network that covers an area of around 10 kilometers.
  - Depending upon the needs of the organization, a LAN can be a single office, building, or Campus.
- **Metropolitan Area Network** (MAN)
  - MAN refers to a network that covers an entire city.
  - For example: consider the cable television network.
- **Wide Area Network** (WAN)
  - WAN refers to a network that connects countries or continents.
  - For example, the Internet allows users to access a distributed system called www from anywhere around the globe.

TYPES OF NETWORK - BASED ON TYPE OF ARCHITECTURE

- **P2P Networks**
  - Computers with similar capabilities and configurations are referred to as peers.
  - The "peers" in a peer-to-peer network are computer systems that are connected to each other over the Internet.
- **Client-Server Networks**
  - Each computer or process on the network is either a client or a server in a client-server architecture (client/server). The client asks for services from the server, which the server provides.
  - Servers are high-performance computers or processes that manage disc drives (file servers), printers (print servers), or network traffic (network servers)
- **Hybrid Networks**
  - The hybrid model uses a combination of client-server and peer-to-peer architecture. Ex: Torrent.

NETWORK DEFINED BY ARCHITECTURE

Two most common network types are **peer-to-peer** and **client/server**.

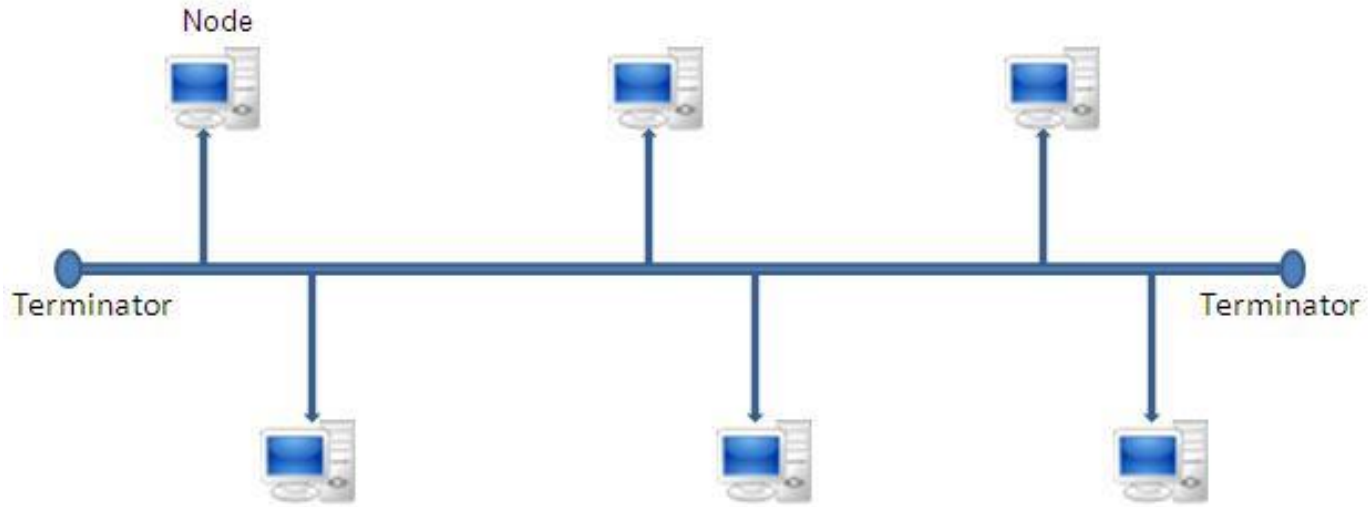
- **Peer–to– Peer-** Since there is no dedicated server, all workstations are considered equal and any one of them can act as the client or the server depending on the need and request. Cost effective network solution.
- **Client/Server Topology** – By accessing the server computer, the clients can also access the files and folders kept in the server. Main disadvantage of a client server model is, the server getting overloaded and slow when many clients trying to access the network at a same point of time.

NETWORK TOPOLOGIES

- Physical Topology
  - Bus Topology
  - Star Topology
  - Mesh Topology
  - Ring Topology
  - Dual-ring topology
  - Hybrid Topology
  - The Hub and Spoke Topology

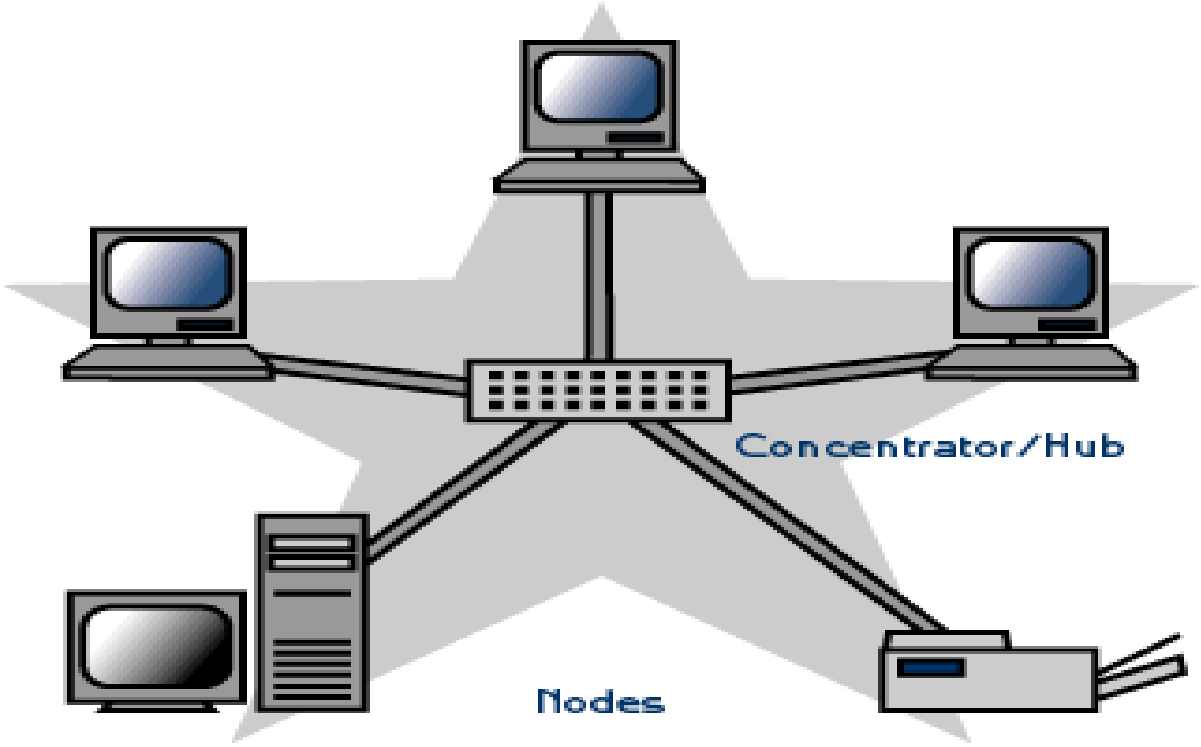
BUS TOPOLOGY

- Uses one single cable as a core line to connect all the systems and devices on a network together.



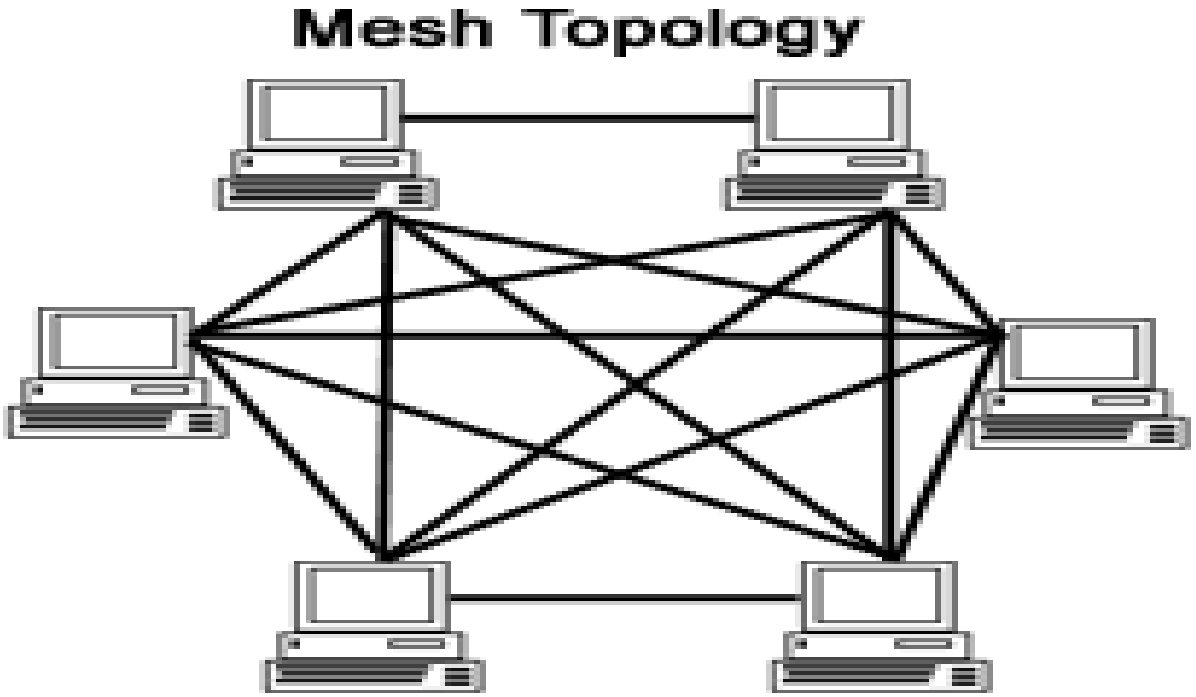
STAR TOPOLOGY

- They are connected through one central device called a hub or a switch or a concentrator.



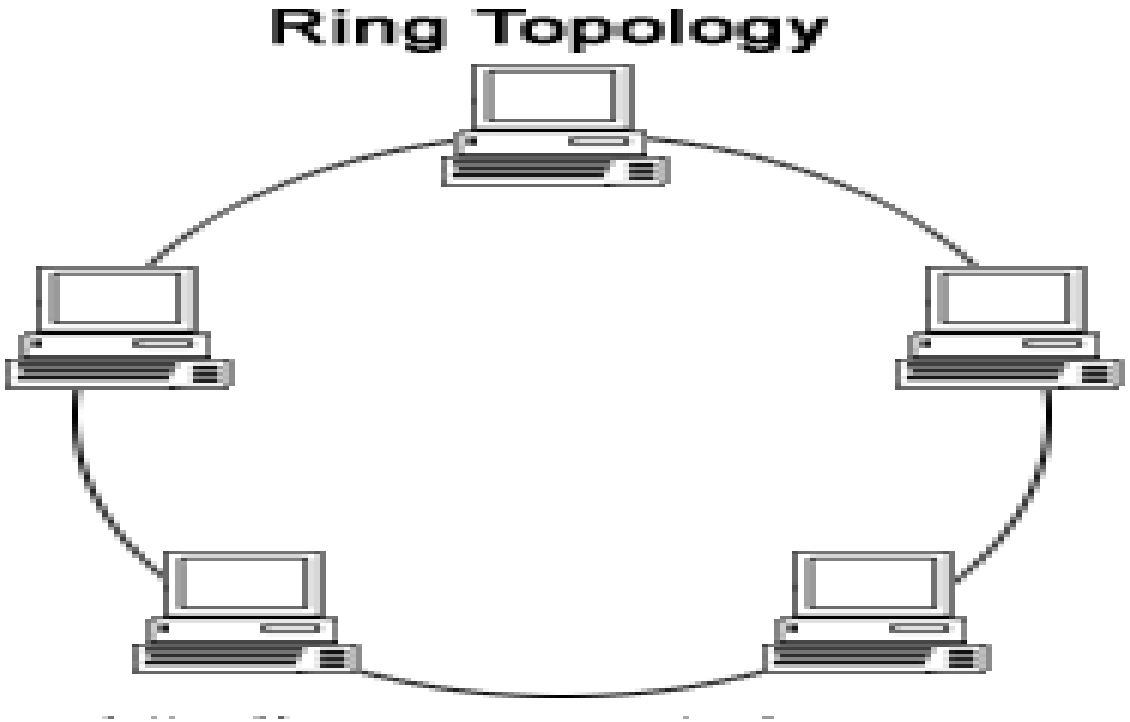
MESH TOPOLOGY

- Even if one of the connections goes down, by using other connections a node can be alive on a network



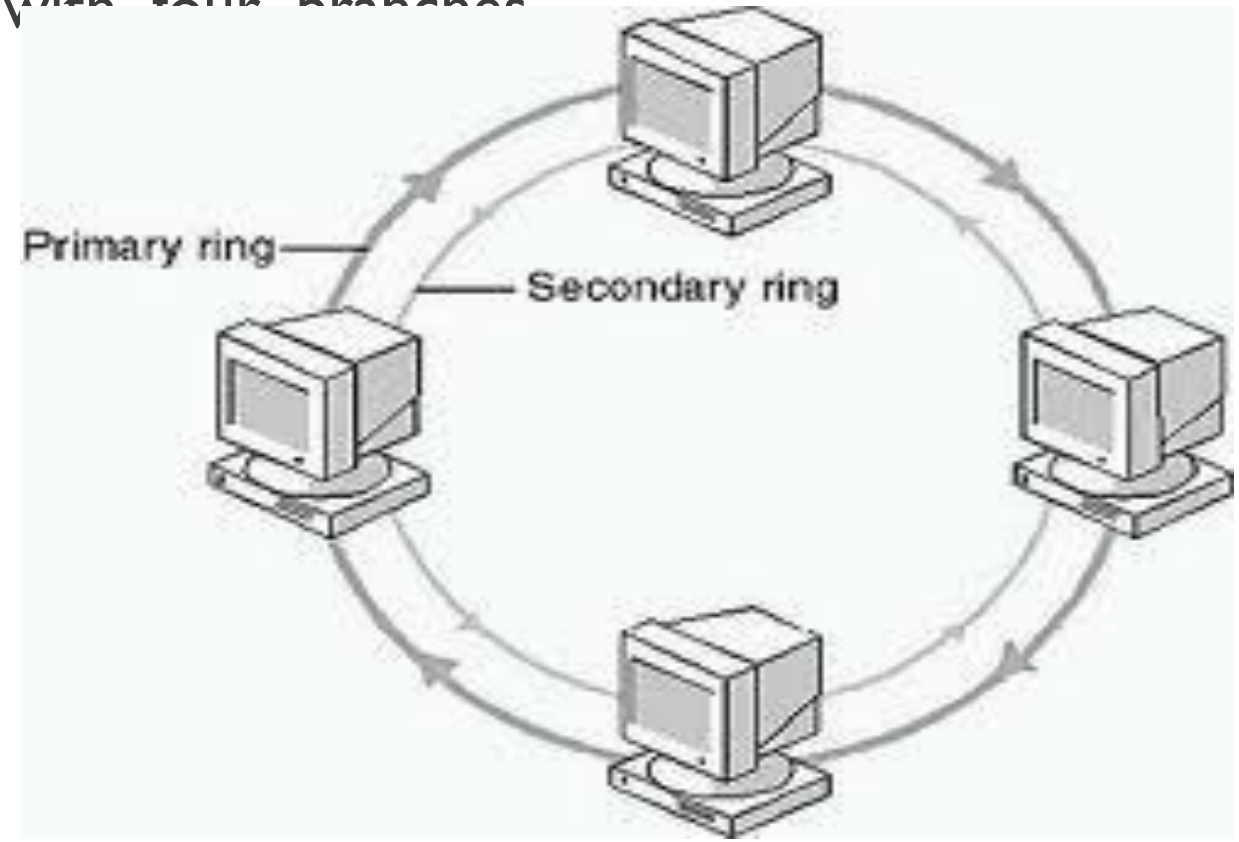
RING TOPOLOGY

- A ring topology is where each node or device on the network connects to two other nodes.



DUAL-RING TOPOLOGY

- Network redundant topology where nodes are connected using two concentric rings with four branches



NETWORKING PROTOCOL

- A network protocol is a set of rules that govern data communication between different devices in the network.
- It determines
  - what is being communicated,
  - how it is being communicated, and
  - when it is being communicated.
- It permits connected devices to communicate with each other, irrespective of internal and structural differences.

NETWORKING PROTOCOL

The protocols can be broadly classified into three major categories:

1. Network Communication
2. Network Management
3. Network Security

NETWORKING PROTOCOL - NETWORK COMMUNICATION

- Hypertext Transfer Protocol (HTTP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Border Gateway Protocol (BGP)
- Address Resolution Protocol (ARP)
- Internet Protocol (IP)
- Dynamic Host Configuration Protocol (DHCP)

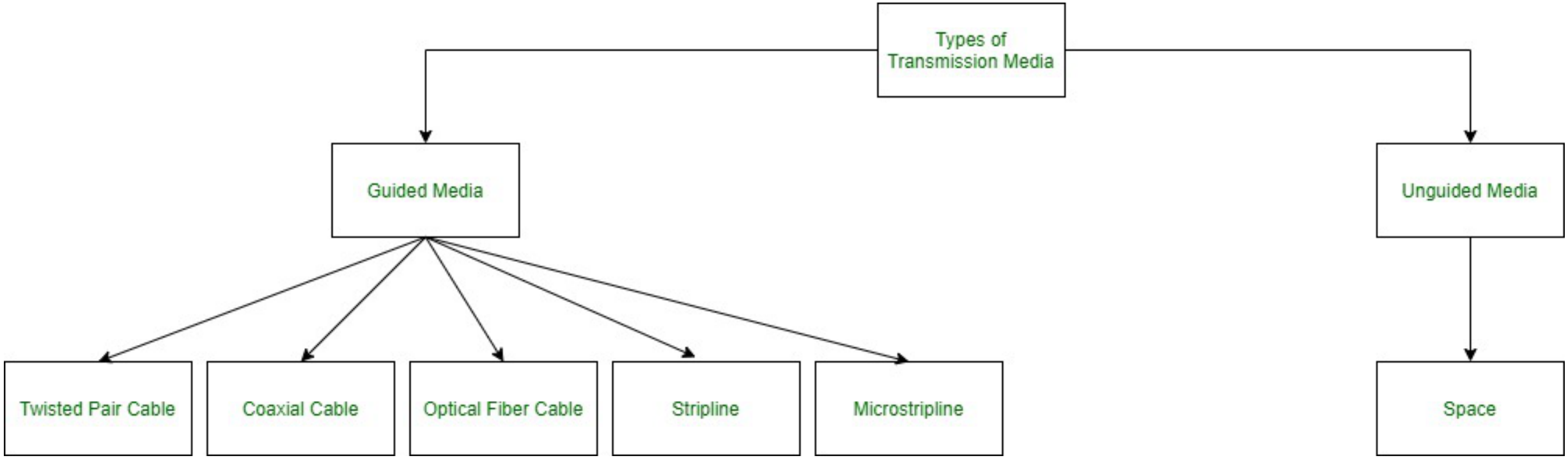
NETWORKING PROTOCOL - NETWORK MANAGEMENT

- Internet Control Message Protocol (ICMP)
- Simple Network Management Protocol (SNMP)
- Gopher
- File Transfer Protocol (FTP)
- Post Office Protocol (POP3)
- Telnet

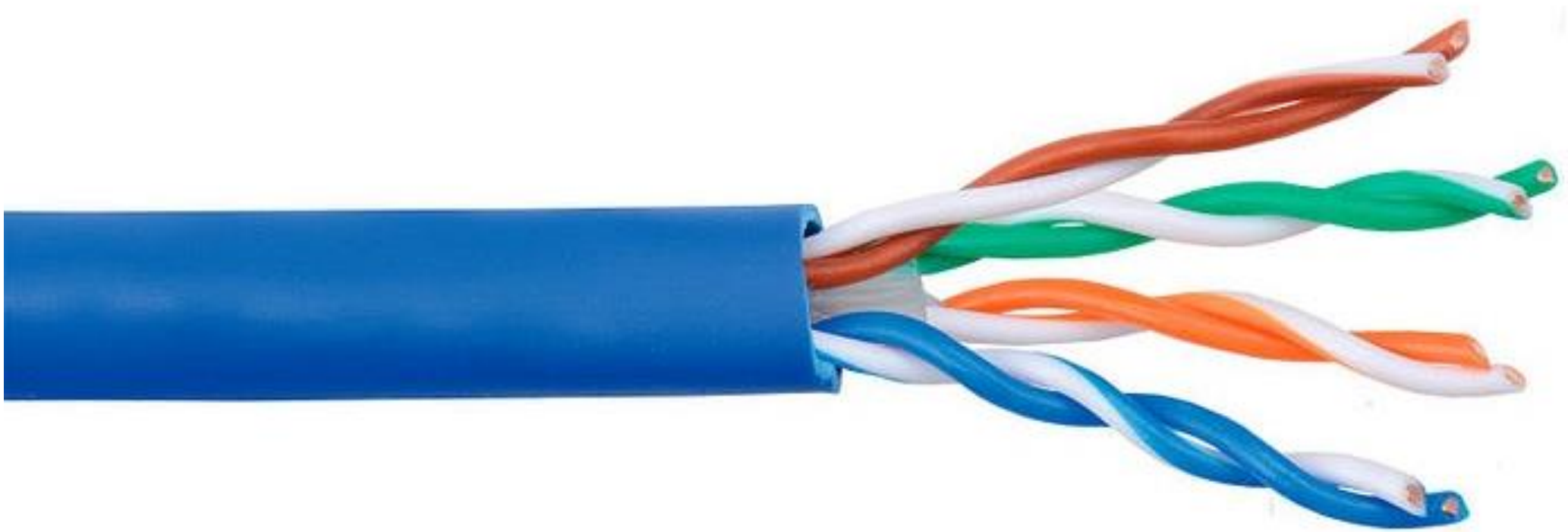
NETWORKING PROTOCOL - NETWORK SECURITY

- Secure Socket Layer (SSL)
- Hypertext Transfer Protocol (HTTPS)
- Transport Layer Security (TLS)
  - TLS 1.0 (deprecated)
  - TLS 1.5 (old applications)
  - TLS 2.0 (latest)

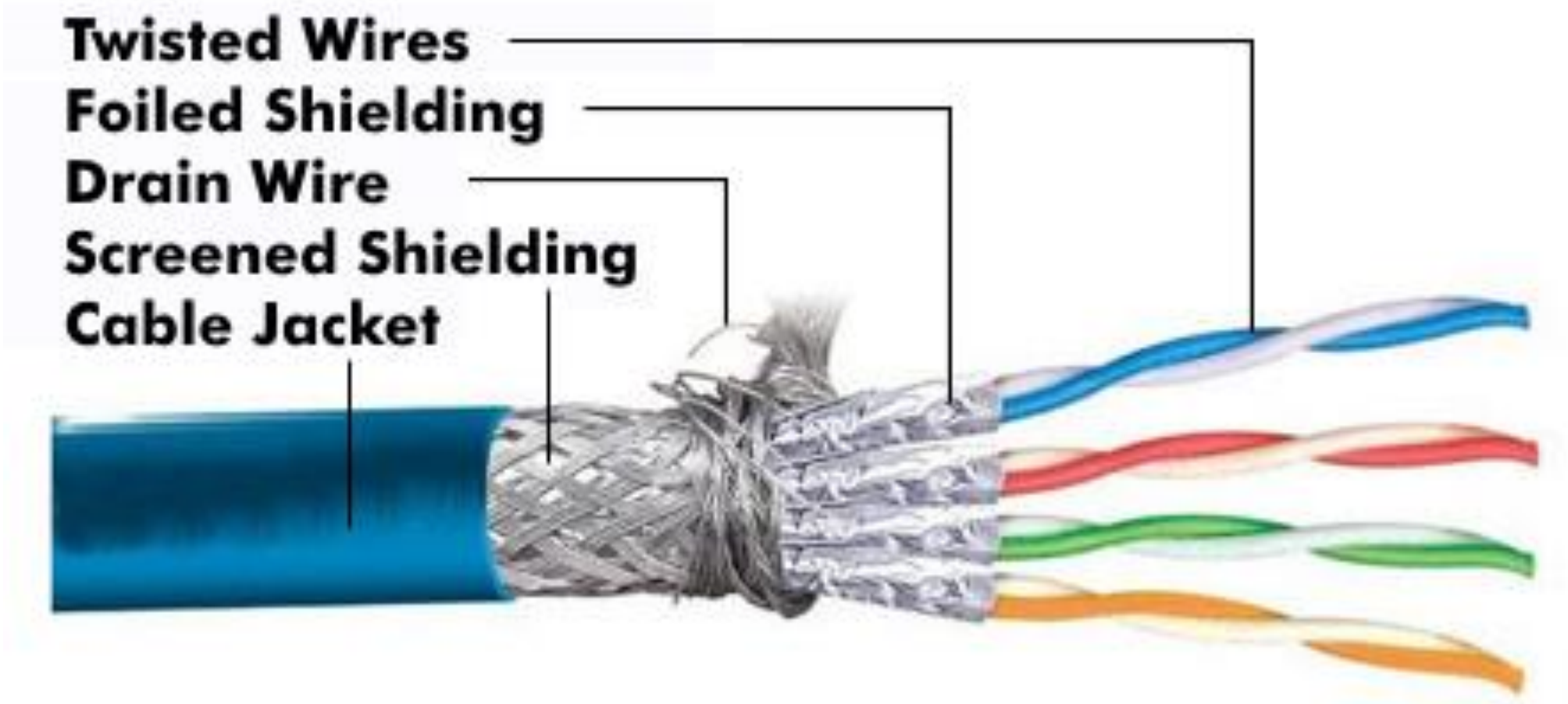
NETWORK MEDIA / TRANSMISSION MEDIA



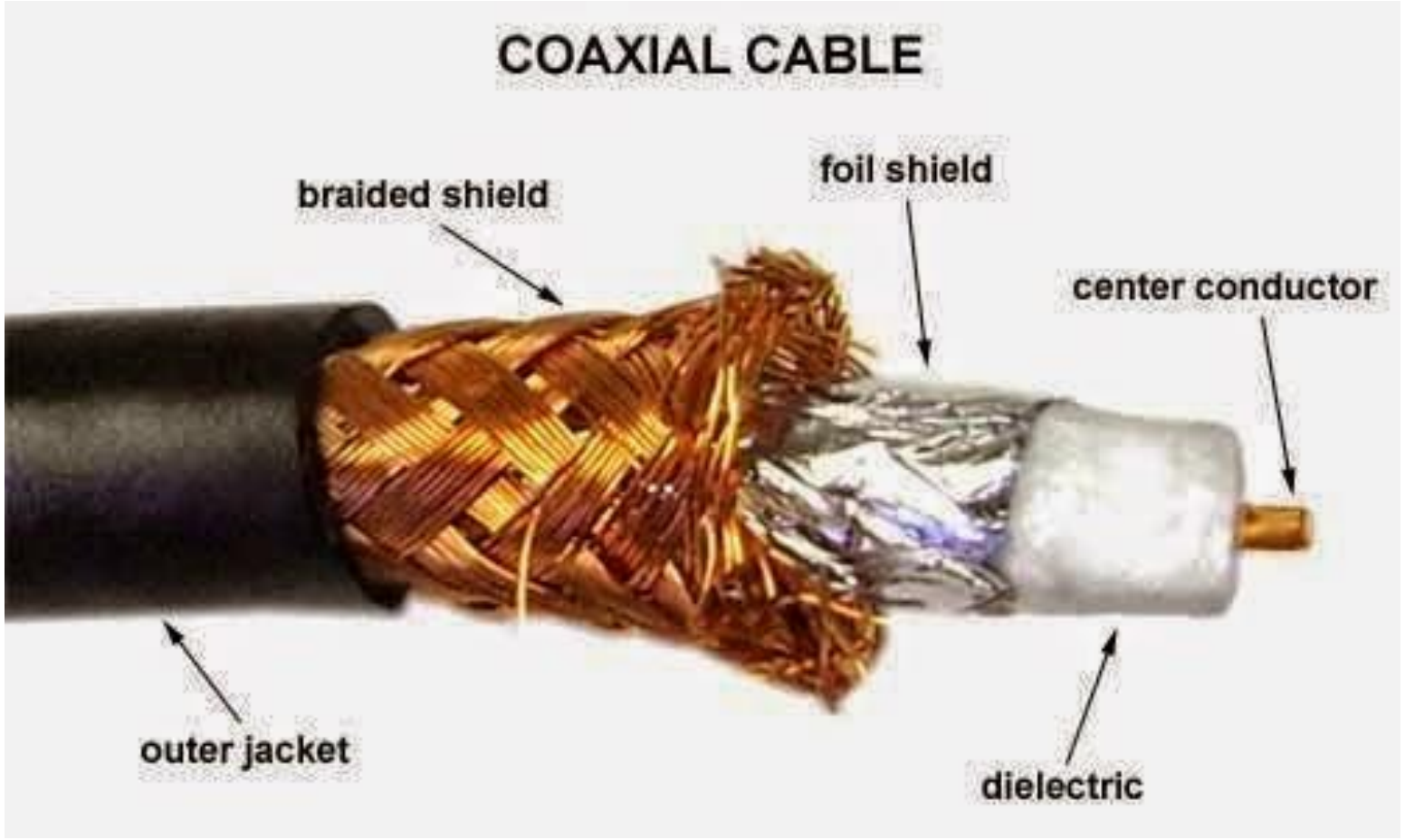
UNSHIELDED TWISTED PAIR (UTP)



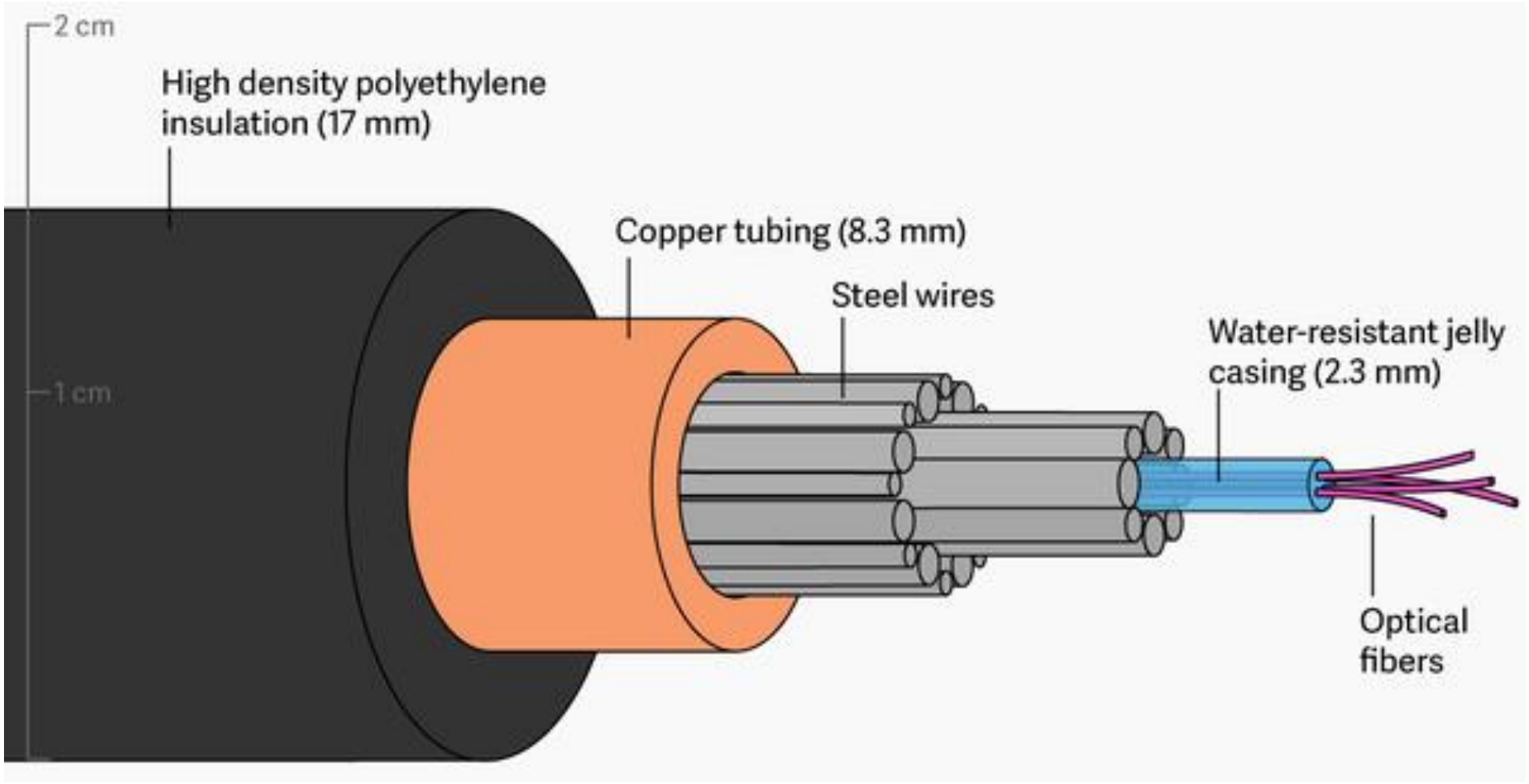
SHIELDED TWISTED PAIR (STP)



COAXIAL CABLE



OPTICAL FIBRE CABLE



CRIMPING OF TWISTED PAIR CABLE

RJ45 Crimping Tool

Cable Stripper

RJ45 Connectors

https://docs.seattlecommunitynetwork.org/learn/cable-crimping.html

NETWORKING DEVICES

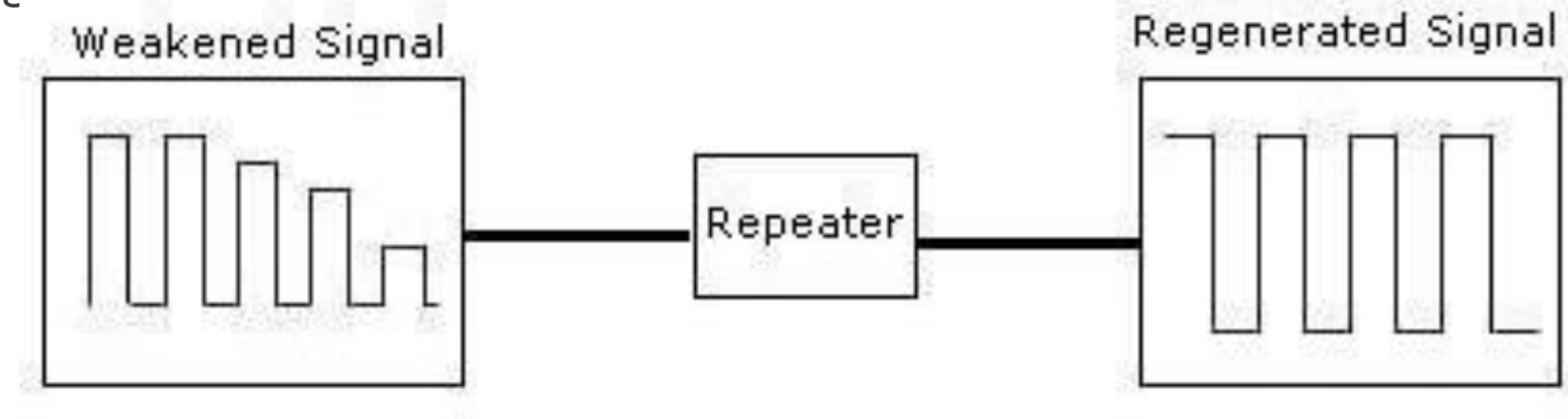
- NIC (Network Interface Card)
- Repeater
- Hub
- Bridges
- Switches
- Routers
- Gateways

NETWORKING DEVICES - NIC

- A network card, often known as a network adapter or NIC (network interface card), is computer hardware that enables computers to communicate via a network.
- It offers physical access to networking media and, in many cases, MAC addresses serve as a low-level addressing scheme.
- Each network interface card has a distinct identifier. This is stored on a chip that is attached to the card.

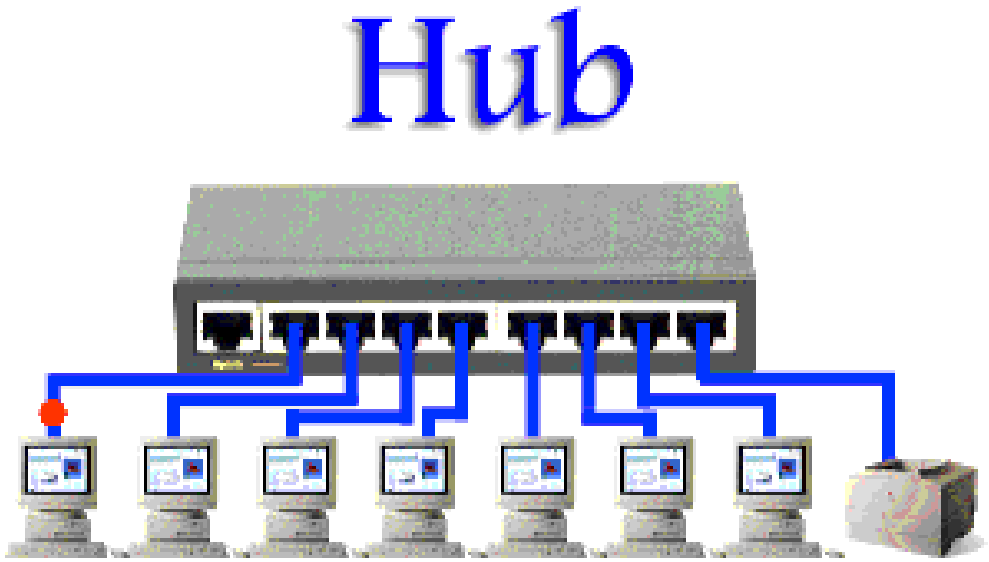
NETWORKING DEVICES - REPEATER

- A repeater is an electrical device that receives a signal, cleans it of unwanted noise, regenerates it, and retransmits it at a higher power level or to the opposite side of an obstruction, allowing the signal to travel greater distances without degradation.
- In the majority of twisted pair Ethernet networks, Repeaters are necessary for cable lengths longer than 100 meters in some systems. Repeaters are based on physics.



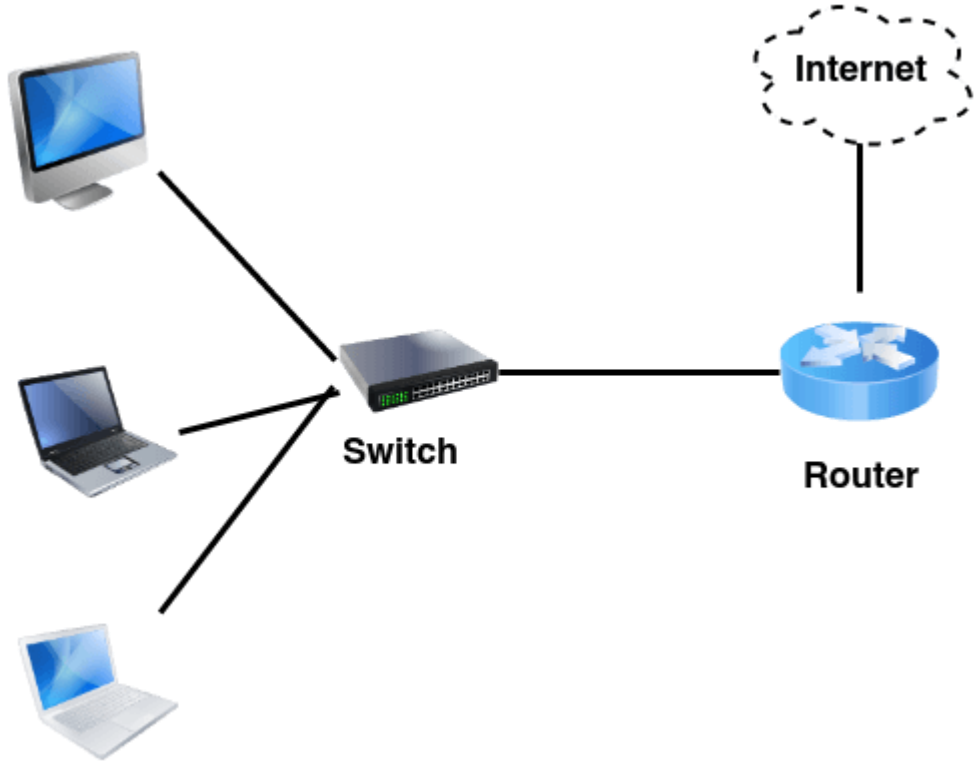
NETWORKING DEVICES - HUB

- A hub is a device that joins together many twisted pairs or fiber optic Ethernet devices to give the illusion of a formation of a single network segment.
- A network hub is a relatively simple broadcast device.
- Any packet entering any port is regenerated and broadcast out on all other ports, and hubs do not control any of the traffic that passes through them.
- Packet collisions occur as a result of every packet being sent out through all other ports, substantially impeding the smooth flow of communication.



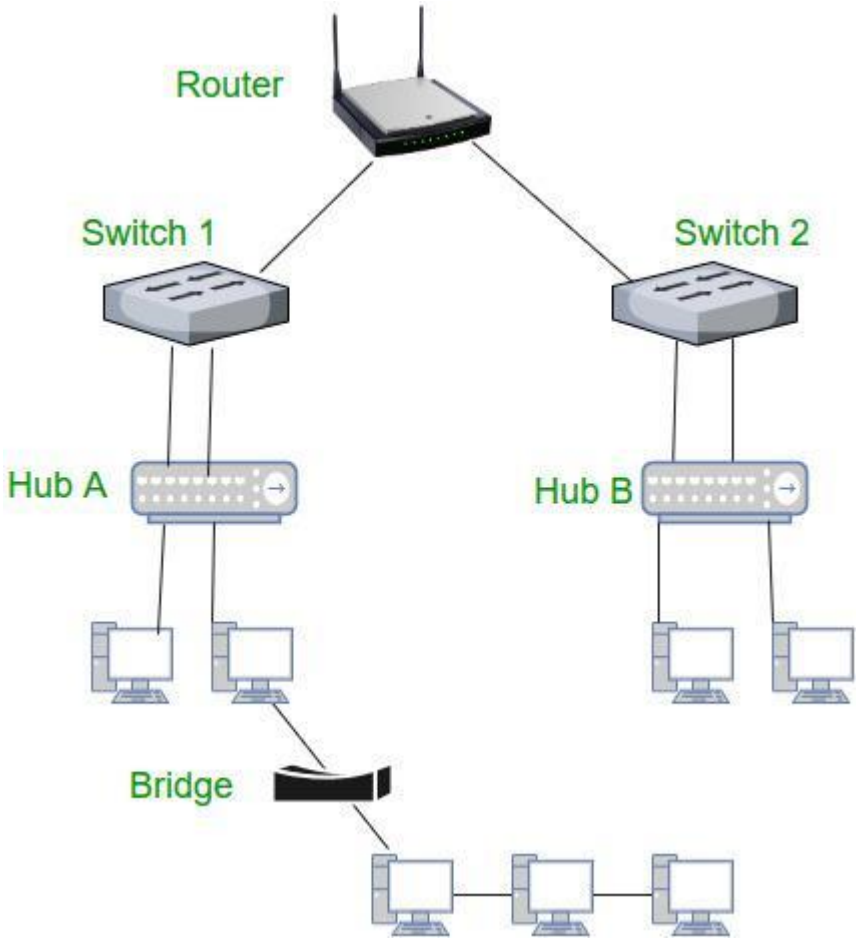
NETWORKING DEVICES - SWITCHES

- A switch differs from a hub in that it only forwards frames to the ports that are participating in the communication, rather than all of the ports that are connected.
- The collision domain is broken by a switch, yet the switch depicts itself as a broadcast domain. Frame-forwarding decisions are made by switches based on MAC addresses.



NETWORKING DEVICES - ROUTERS

- Routers are networking devices that use headers and forwarding tables to find the optimal way to forward data packets between networks.
- A router is a computer networking device that links two or more computer networks and selectively exchanges data packets between them.
- A router can use address information in each data packet to determine if the source and destination are on the same network or if the data packet has to be transported between networks.
- When numerous routers are deployed in a wide collection of interconnected networks, the routers share target system addresses so that each router can develop a table displaying the preferred pathways between any two systems on the associated networks.



IP ADDRESSING

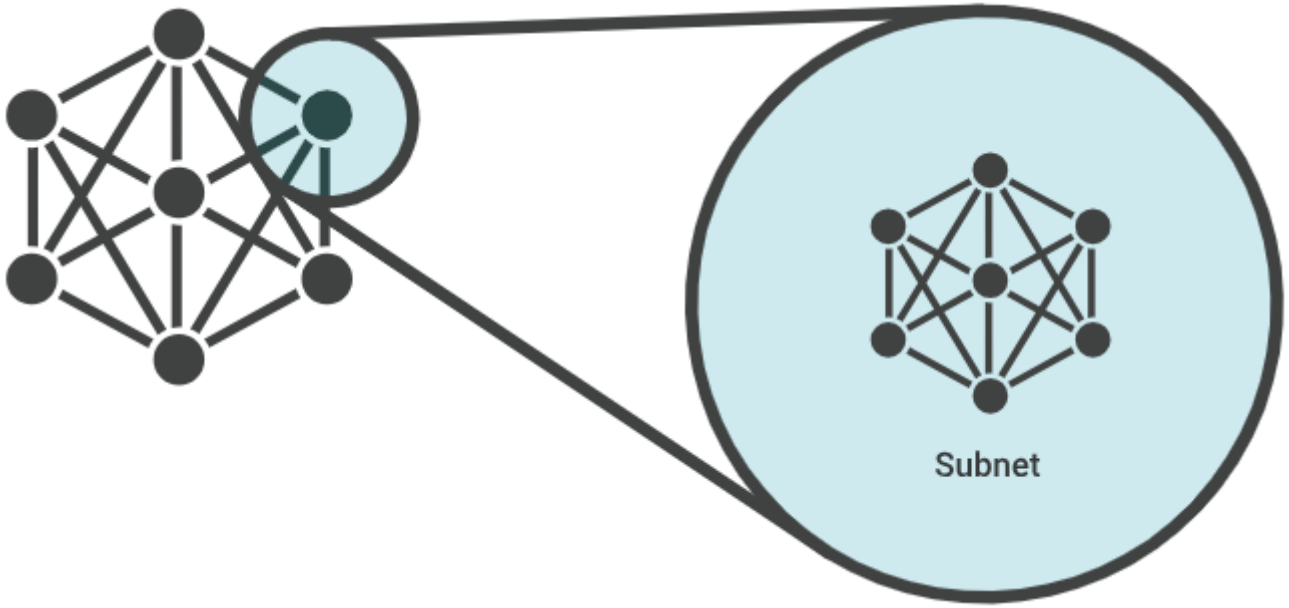
- Each device that uses a network receives an IP address, which is a special identifier number.
- IP addresses are necessary for routing packets of data between devices and for enabling Internet communication between devices.
- There are two primary forms of IP addresses
  - IPv4 and
  - IPv6

IPV4 & IPV6

Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

SUBNETTING

- A network is divided into smaller subnetworks, or subnetworks, through the process known as a subnetwork.
- The sub-network enables network managers to create more controllable and segmented networks for performance or security needs.
  - For example, a large enterprise could segment its network into subnetworks for multiple divisions or locations.



IP ADDRESSING AND SUBNETTING

Parameters	IP Addressing	Subnetting
Purpose	Assign unique identifiers to devices on a network.	Divide a network into smaller subnetworks for better management and performance.
Process	Assigns unique IP addresses to devices on a network.	Divides a network into smaller subnets by borrowing bits from the host portion of the IP address to create a network portion.
Result	Each device on the network has a unique IP address.	The network is broken down into smaller subnets, each with its own unique network ID and range of IP addresses.
Benefits	Enables devices to communicate with each other over the Internet.	Improves network performance and security by reducing network congestion, isolating network traffic, and making it easier to manage IP address assignments and security.
Types	IPv4 and IPv6	CIDR (Classless Inter-Domain Routing)
Notation	Dotted decimal notation (e.g., 192.168.0.1)	Subnet mask (e.g., 255.255.255.0) or CIDR notation (e.g., /24)
Length	32 bits (IPv4) or 128 bits (IPv6)	Variable (depends on the number of bits borrowed for the network portion of the IP address).
Example	192.168.0.1	192.168.0.0/24

IPV4 ADDRESS CLASSES

- Class A (0-127)
- Class B (128-191)
- Class C (192-223)
- Class D (224-239)
- Class E (240-255)

- Class A has 24 Host ID Bits
- Class B has 16 Host ID Bits
- Class C has 8 Host ID Bits

THE NUMBER OF USABLE IP ADDRESSES THAT CAN BE CREATED IS

The total number of IP Addresses creatable = $2^{\text{The total number of Host ID Bits}} - 2$.

Class A Network can have $2^{24} - 2$

Class B Network can have $2^{16} - 2$

Class C Network can have $2^{8} - 2$

Class D and Class E do not contribute for IP Address creation.

Class D is used for multicasting purpose

Class E is used for Address Range Calculator

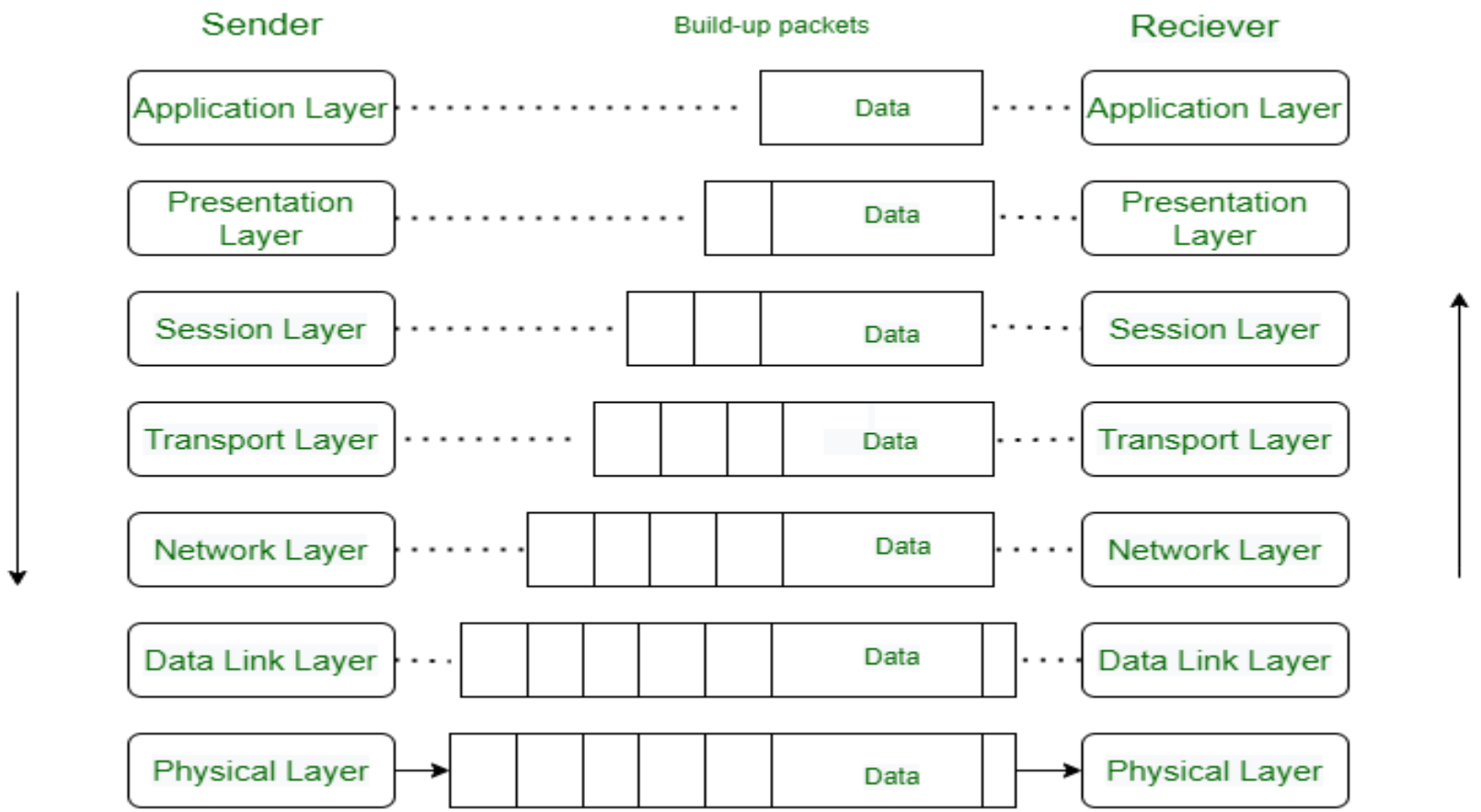
TOTAL IP ADDRESSES WITHIN A NETWORK

Class Network	Total Number of IP Addresses
Class A	1, 67, 77, 214
Class B	65, 534
Class C	254

THE OSI REFERENCE MODEL

- OSI stands for Open Systems Interconnection.
- It is a 7-layer architecture with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe. OSI model was developed by ISO – 'International Organization for Standardization', in the year 1984.
- The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.

OSI MODEL


Sender
Build-up packets
Reciever
Application Layer
Data
Application Layer
Presentation Layer
Data
Presentation Layer
Session Layer
Data
Session Layer
Transport Layer
Data
Transport Layer
Network Layer
Data
Network Layer
Data Link Layer
Data
Data Link Layer
Physical Layer
Data
Physical Layer

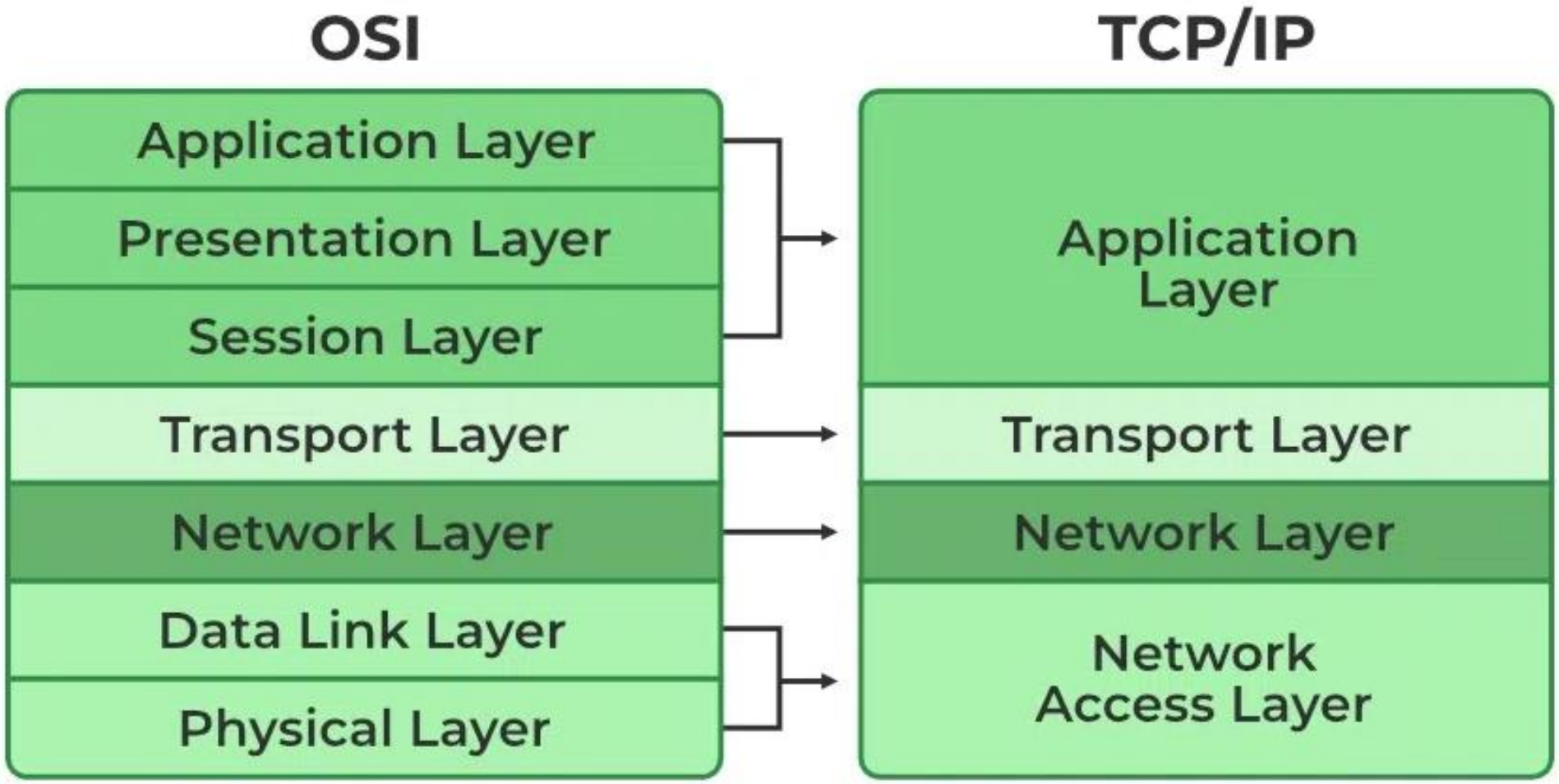
LAYERS OF THE OSI MODEL

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

TCP/IP MODEL

- TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.
- The TCP/IP model is a concise version of the OSI model.
- It contains four layers, unlike the seven layers in the OSI model.

TCP/IP MODEL


OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

LAYERS OF TCP/IP MODEL

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Data Link Layer (MAC)
- Physical Layer