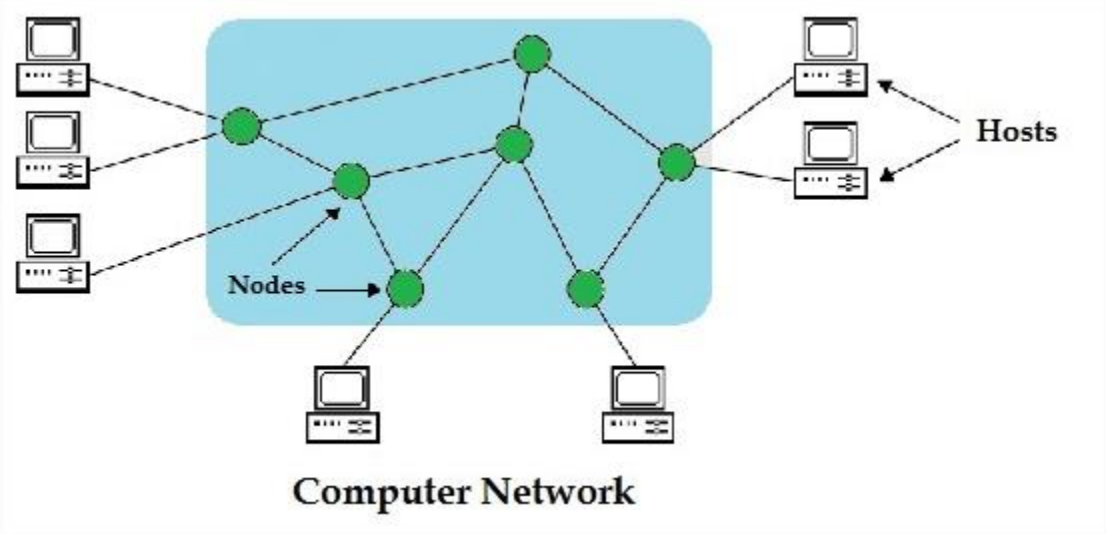
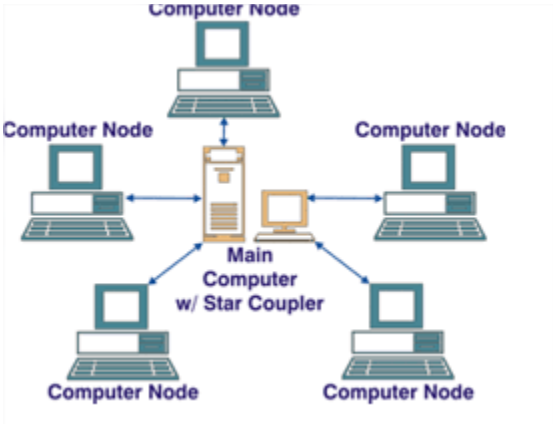
Network Simulation

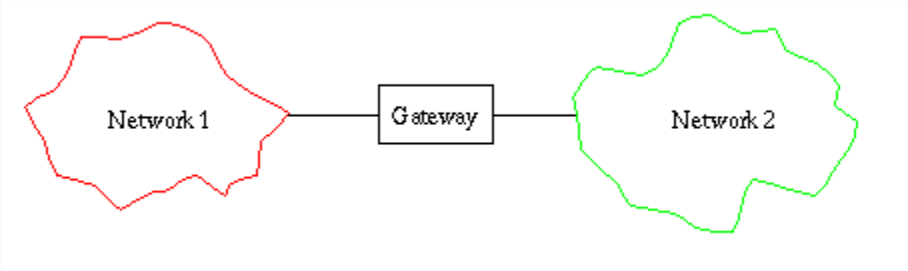
Network Terminology

- A ***node*** is a point of intersection/connection within a network. In an environment where all devices are accessible through the network, these devices are all considered as nodes. In data communication, a physical network node may either be data communication equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment(DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

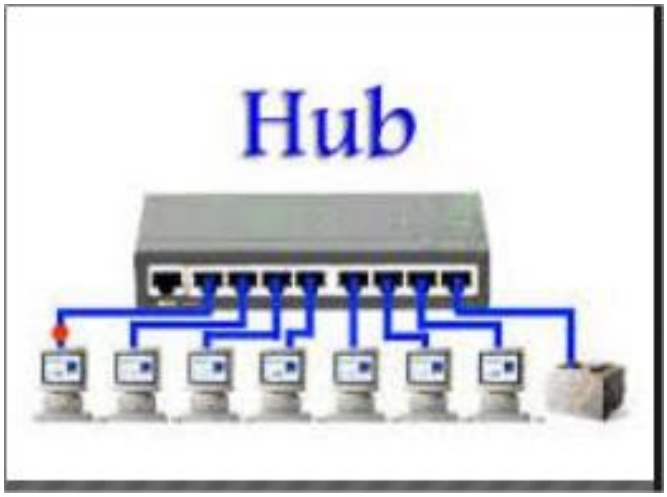




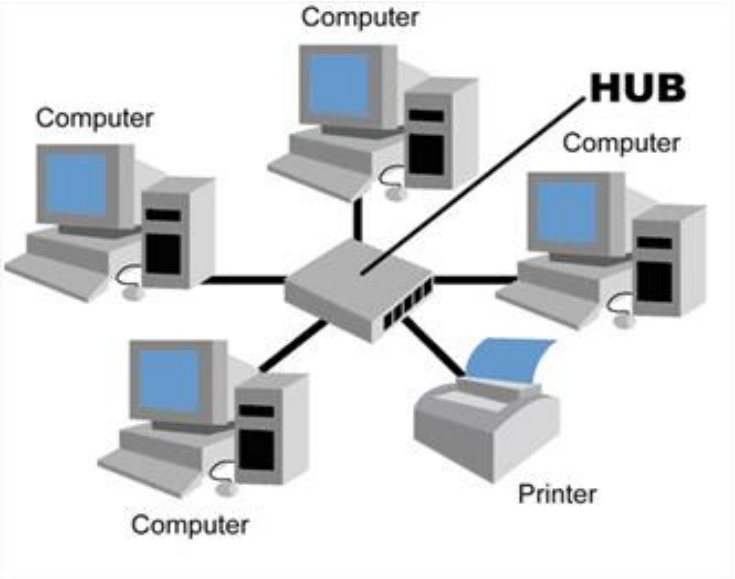
- ***Gateway:*** A gateway is a network point that acts as an entry point to another network, or a connecting point between two dissimilar networks. Gateway interfaces between two networks, normally a local area network and a wide area network. A gateway will have two IP addresses, one for the local network and one for the wide area.



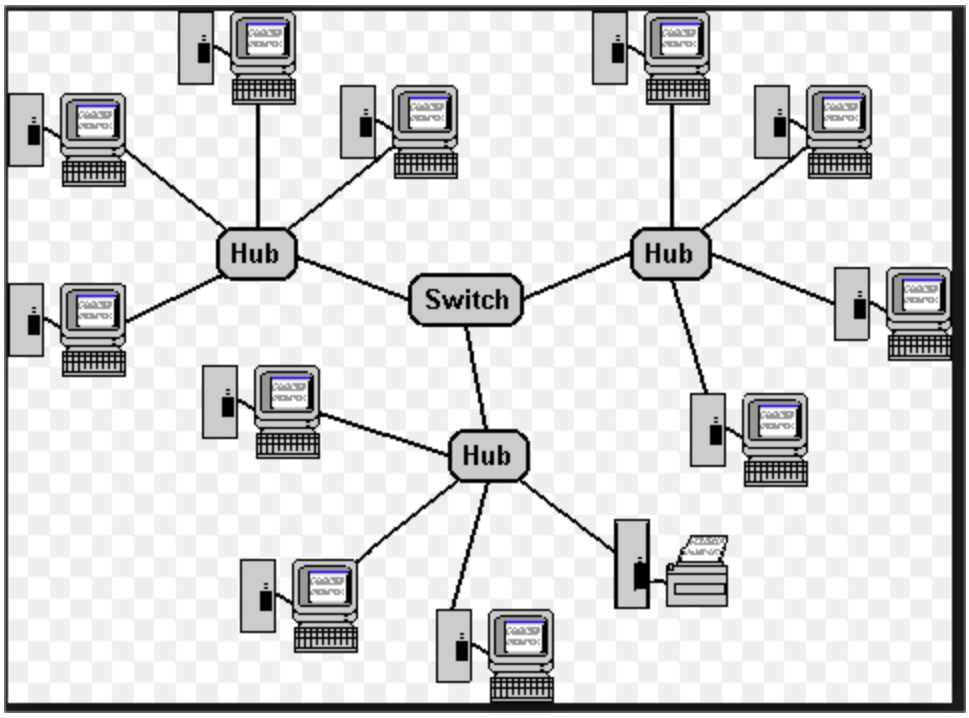
- ***Hub:*** A hardware device that serves as a central point for connecting devices over a local area network. Hubs broadcast frames to all network-enabled devices on the Ethernet network and therefore create more collisions than a switch.



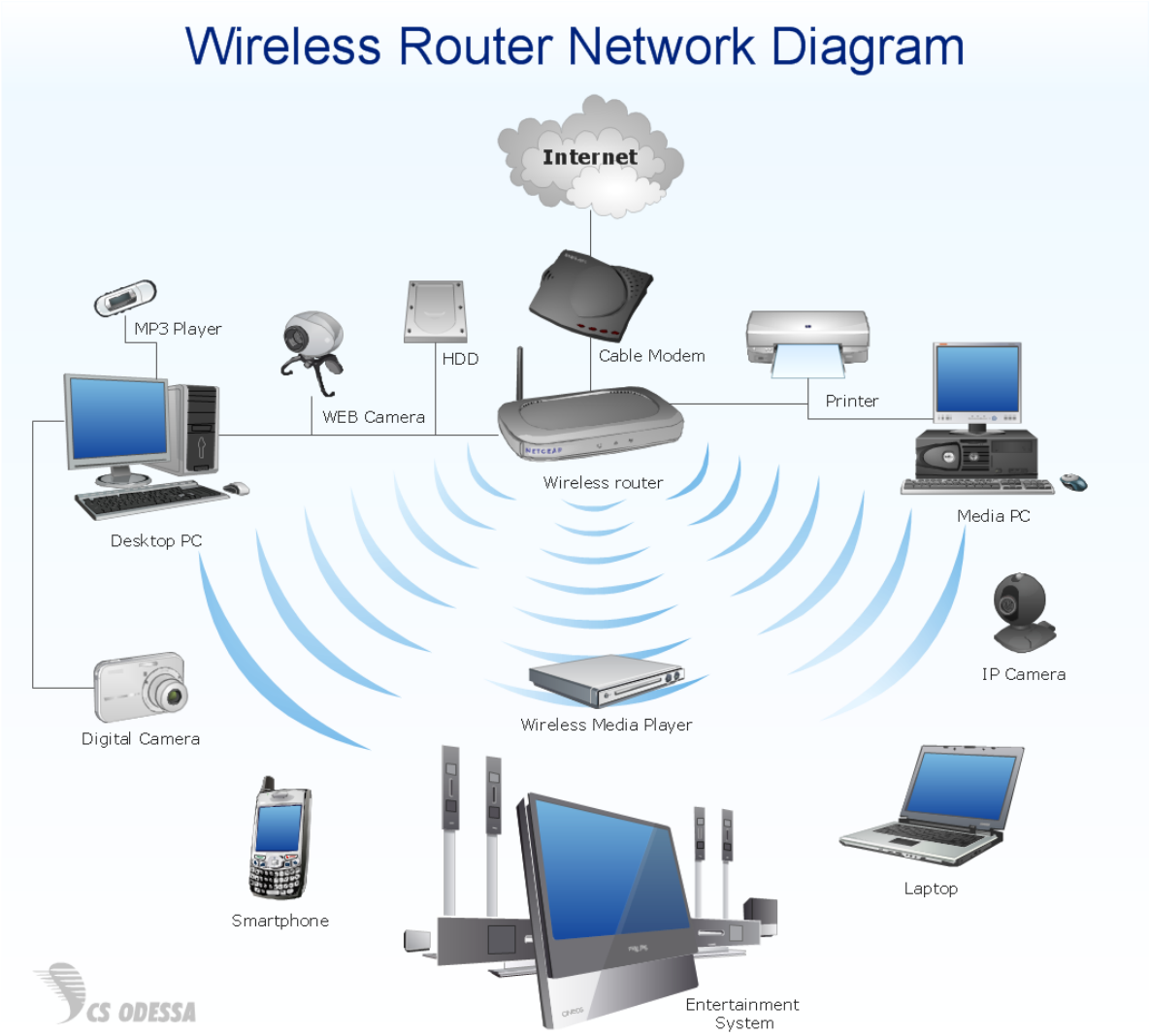
Ali Al-Safi
AliAl-Safi@mustaqbal-college.edu.iq



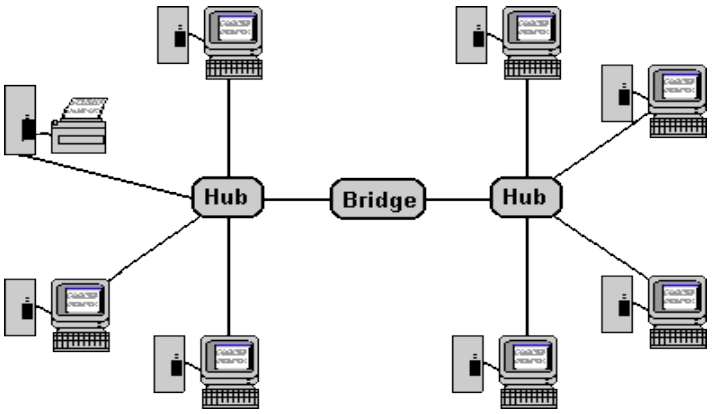
- ***Switch:*** A hardware device that serves as an efficient central point for connecting network-enabled devices over a local area network. A Switch has several advantages over hubs. For example, switches allow the division of a network into multiple segments to reduce the number of data collisions. Further, a switch only forwards frames to the network enabled device that connects to the intended destination of the data.



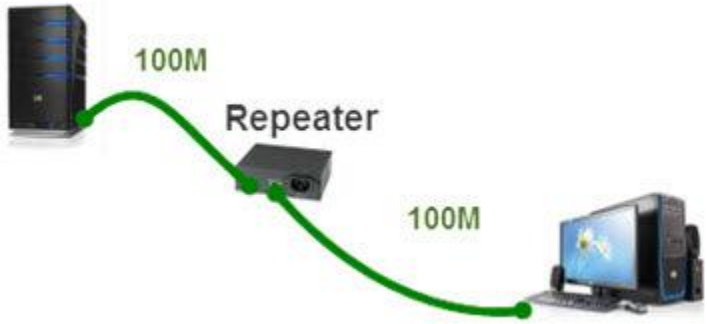
- ***Router:*** A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and determine how to forward it. The destination address in the packet governs the line (interface) to which the router directs an outgoing packet.

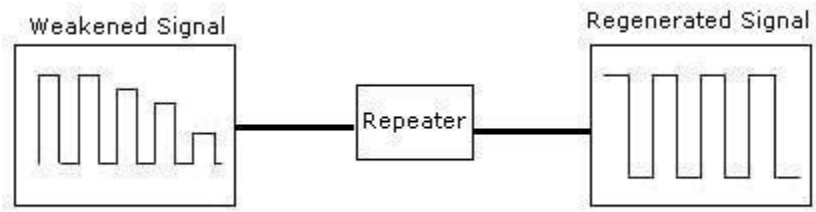


- ***Bridge:*** a device that connects multiple network segments along the data link layer. It works on OSI layer 2.

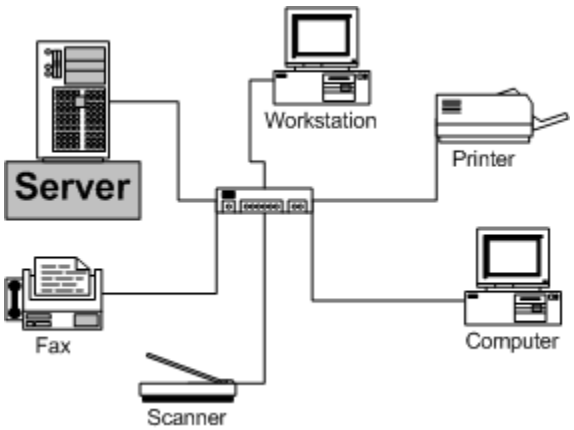


- ***Repeater:*** a device which amplifies or regenerates digital signals received while sending them from one part of a network into another. It works on OSI layer 1.





- ***Server:*** A network-enabled device that provides a specific kind of service to client software running on other computers on a network.



- ***Internet Protocol (IP):*** A protocol by which data is sent from one network-enabled device to another on the Internet. Each network-enabled device has at least one IP address that identifies it from all other devices on the network. An

address may be either a public address or a private address. Public Addresses are generally unique. Private Addresses are only unique within the context of the local network.

- ***Packet:*** A packet is the most basic data unit that is transferred over a network. When communicating over a network, packets are the envelopes that carry your data (in pieces) from one end point to the other.Packets have a header portion that contains information about the packet including the source and destination, timestamps, network hops, etc. The main portion of a packet contains the actual data being transferred. It is sometimes called the body or the payload.

- ***Link or cable:*** Networking cables are used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables like Coaxial cable, Optical fiber cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).While wireless networks are much easier deployed when total throughput is not an issue, most permanent larger computer networks use cables to transfer signals from one point to another. There are number of cable, these are:

    1. **Twisted pair cabling:** is a form of wiring in which pairs of wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from other wire pairs and from external sources. This type of cable is used for home and corporate Ethernet networks. There are two major types of twisted pair cables: shielded, unshielded.
    2. **Coaxial lines:**Two conductors separated by insulation. Maximum length of 185 to 500 meters.

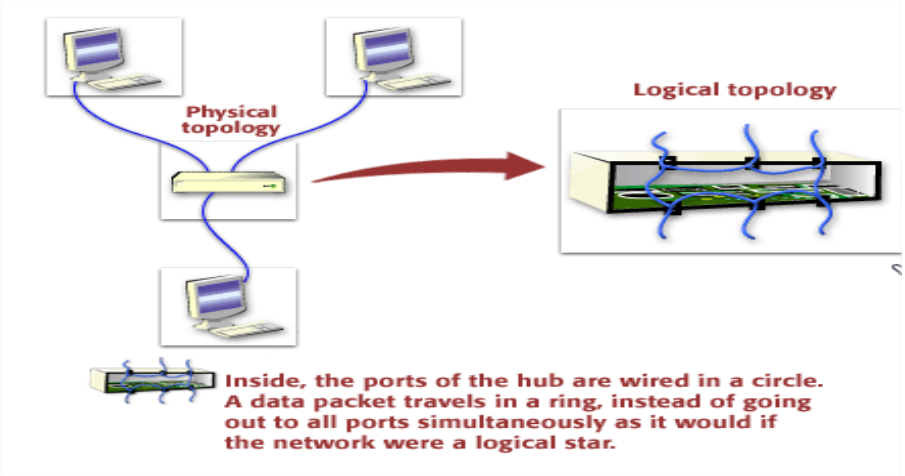
3. **Fiber-optic** - Data is transmitted using light rather than electrons. Usually there are two fibers, one for each direction. Cable length of 2 Kilometers. Speed from 100Mbps to 2Gbps. This is the most expensive and most difficult to install, but is not subject to interference.

2.2. Network Topologies

A topology describes the configuration of a communication network. The way in which the elements of a network are mapped or arranged is known as a network topology. A topology describes the physical and the logical interconnection between the different nodes of a network. Network topologies are classified as physical, logical and signal topologies.

1. A **physical topology** describes the placement of network nodes and the physical connections between them. This includes the arrangement and location of network nodes and they are connected.

2. The **logical topology**, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.Logical topologies are bound to the network protocols that direct how the data moves across a network. Mapping of the paths taken by data packets as they travel over the network is known as a logical topology.



Types of Physical Topology

1. **Bus Topology**: In this type of network topology, all the nodes of a network are connected to a common transmission medium having two endpoints. All the data that travels over the network is transmitted through a common transmission medium known as the bus or the backbone of the network. When the transmission medium has exactly two endpoints, the network topology is known by the name, 'linear bus topology'. In case the transmission medium, has more than two endpoints, the network is said to have a distributed bus topology. Bus topology is easy to handle and implement and is best suited for small networks. But the downside of this topology is that the limited cable length limits the number of stations, thus limiting the performance to a less number of nodes.

The advantages of using bus topology are:

- It is easy to handle and implement.
- It is best suited for small networks.

The disadvantages of using bus topology are:

- The cable length is limited. This limits the number of stations that can be connected.
- This network topology can perform well only for a limited number of nodes.

2. **Ring Topology:** In a ring topology, every node in the network is connected to two other nodes and the first and the last nodes are connected to each other. The data transmitted over the network pass through each of the nodes in the ring until they reach the destination node. In a ring network, the data and the signals that pass over the network travel in a ***single direction***. The ring topology does not require a central server to manage connectivity between the nodes and facilitates an orderly network operation. But, the failure of a single station in the network can render the entire network inoperable. Changes and moves in the stations forming the network affect the network operation.

   The advantages of using Ring topology are:

   - The data being transmitted between two nodes passes through all the intermediate nodes.
   - A central server is not required for the management of this topology.

   The disadvantages of using Ring topology are:

   - The failure of a single node of the network can cause the entire network to fail.
   - The movement or changes made to network nodes affects the performance of the entire network.

3. **Mesh Topology:** In a full mesh network, each network node is connected to every other node in the network. Due to this arrangement of nodes, it becomes possible for a simultaneous transmission of signals from one node to several other nodes. In a partially connected mesh network, only some of the network nodes are connected to more than one node. This is beneficial over a fully connected mesh in terms of

redundancy caused by the point-to-point links between all the nodes. The nodes of a mesh network require possessing some kind of routing logic so that the signals and the data traveling over the network take the shortest path during each of the transmissions.

The advantages of using Mesh topology are:

- The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.

The disadvantages of using Mesh topology are:

- The arrangement wherein every network node is connected to every other node of the network, many of the connections serve no major purpose. This leads to the redundancy of many of the network connections.

4. **Star Topology**: In this type of network topology, each node of the network is connected to a central node, which is known as a hub. The data that is transmitted between the network nodes passes across the central hub. A distributed star is formed by the interconnection of two or more individual star networks. The centralized nature of a star network provides a certain amount of simplicity while also achieving isolation of each device in the network. However, the disadvantage of a star topology is that the network transmission is largely dependent on the central hub. The failure of the central hub results renders the entire network inoperable.

The advantages of using Star topology are:

- Due to its centralized nature, the topology offers simplicity of operation.
- It also achieves an isolation of each device in the network.

The disadvantages of using Star topology are:

- The network operation depends on the functioning of the central hub. Hence, the failure of the central hub leads to the failure of the entire network.

5. **Tree Topology:** It is also known as a hierarchical topology and has a central root node that is connected to one or more nodes of a lower hierarchy. In a symmetrical hierarchy, each node in the network has a specific fixed number of nodes connected to those at a lower level.

6. **Hybrid Topology:** Apart from these basic types, there are hybrid network topologies, which have a combination of two or more basic topologies. As a hybrid topology results from a combination of two or more topologies, it has the advantages as well as the disadvantages of both. The main advantage of hybrid topology is that two dissimilar topologies can be combined without disturbing the existing architecture of a network. Use of hybrid technologies makes a network easily expandable.

2.3. Networking Architectures

A computer network is the infrastructure that allows two or more computers (called hosts) to communicate with each other.

2.3.1. Network Components

Figure 1 shows an abstract view of a network and its hosts. The network is made up of two types of components: **nodes** and communication **lines**. The nodes typically handle the network operation. A node is usually itself a computer (general or special) which runs specific network software. The communication lines may take many different shapes and forms, even in the same network.

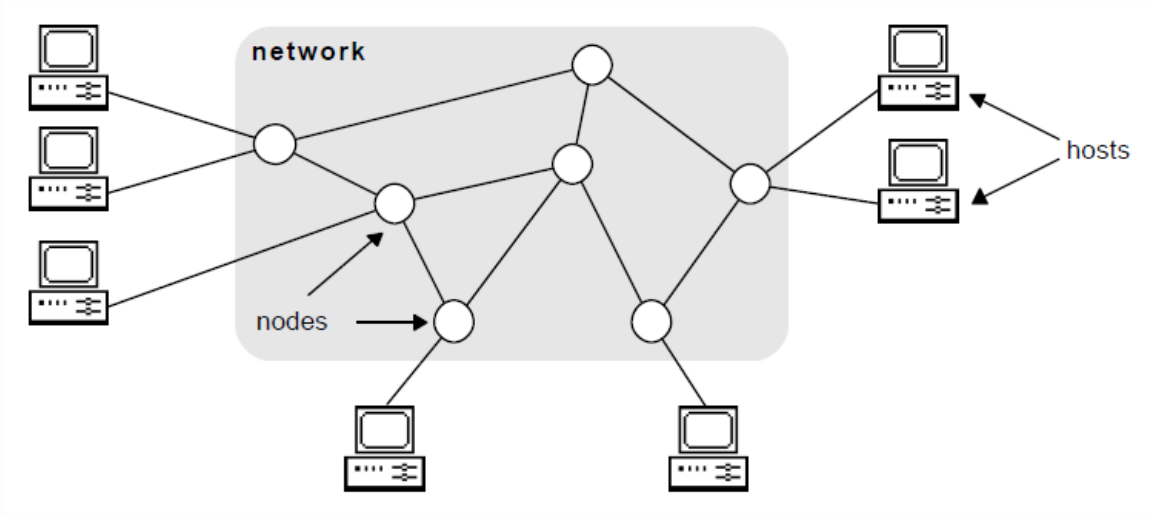


Figure 1: An Abstract Network

2.3.2. Types of Network Technologies

The technologies which can be used to construct any network can be classified into three broad categories based on the underlining network architecture and how the network is constructed. These are:

1. Wired Networking.
2. Infrastructure Wireless Networking.
3. Infrastructure less Wireless Networking (Ad hoc Network).

2.4. Network Classification

Many types of networks exist, and can be categorized in various ways set out in the following subsections depending on the criteria chosen for their classification.

2.4.1. By Network Formation and Architecture

Wireless networks can be divided into two broad categories based on how the network is constructed and the underlining network architecture:

1. **Infrastructure-based network.** A network with preconstructed infrastructure that is made of fixed and wired network nodes and gateways, with, typically, network services delivered via these preconfigured infrastructures. For example, cellular networks.

2. **Infrastructureless (ad hoc) network.** In this case a network is formed dynamically through the cooperation of an arbitrary set of independent nodes. There is no prearrangement regarding the specific role each node should assume. Instead, each node makes its decision independently, based on the network situation, without using a preexisting network infrastructure. For example, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another.

2.4.2. By Communication Coverage Area

Networks can be classified into different types based on the distances over which data is transmitted as shown in figure 2:

1. **Wireless Wide Area Networks (Wireless WANs)**. Wireless WANs are infrastructure-based networks that rely on networking infrastructures like tower and base stations to enable mobile users to establish wireless connections over remote public or private networks. These connections can be made over large geographical areas, across cities or even countries, through the use of multiple antenna sites or satellite systems maintained by wireless service providers. Cellular networks and satellite networks are good examples of wireless WAN networks.

2. **Wireless Metropolitan Area Networks (Wireless MANs).** Wireless MAN networks are sometimes referred to as fixed wireless. These are also infrastructure-based networks that enable users to establish broadband wireless connections among

multiple locations within a metropolitan area, for example, among multiple office buildings in a city or on a university campus, without the high cost of laying fiber or copper cabling and leasing lines.

3. **Wireless Local Area Network (Wireless LANs).**Wireless local area networks enable users to establish wireless connections within a local area, typically within a corporate or campus building, or in a public space, such as an airport, usually within a 100 m range. Wireless LANs can operate in infrastructure-based or in ad hoc mode.

4. **Wireless Personal Area Networks (Wireless PANs).**Wireless PAN Technologies enable users to establish ad hoc, wireless communication among personal wireless devices such as PDAs, cellular phones, or laptops that are used within a personal operating space, typically up to a 10 meter range. Two key Wireless PAN Technologies are Bluetooth and infrared light.

2.5. Communication Model Employed By the Nodes

The communication between the nodes is either based on a **point-to-point** model or a **Broadcast** model (see Figure 3). In the point-to-point model, a message follows a specific route across the network in order to get from one node to another. In the broadcast model, on the other hand, all nodes share the same communication medium and, as a result, a message transmitted by any node can be received by all other nodes. A part of the message (an address) indicates for which node the message is intended. All nodes look at this address and ignore the message if it does not match their own address.

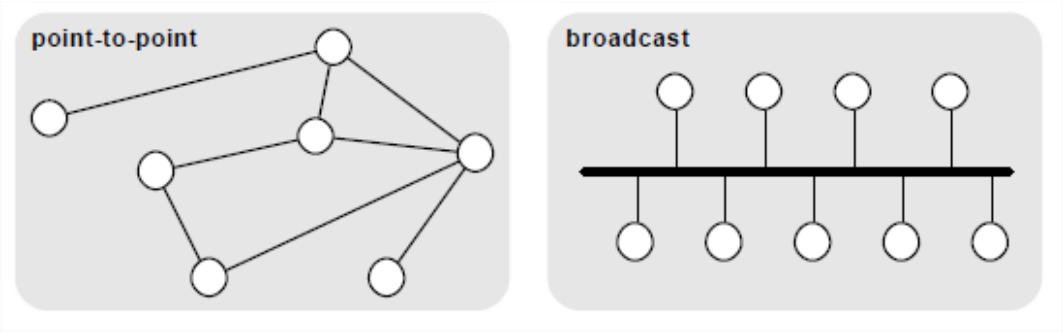


Figure 3: Communication Models

2.6. Network Protocol

A protocol is a **set of rules** that governs (manage) the communications between computers on a network. In order for two computers to talk to each other, they must be speaking the same language. Many different types of network protocols and standards are required to ensure that your computer can communicate with another computer located on the next desk or half-way around the world. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

Network protocols incorporate all the processes, requirements and constraints of initiating and accomplishing communication between computers, servers, routers and other network enabled devices. Network protocols must be confirmed and installed by the ***sender and receiver*** to ensure network/data communication and apply to software and hardware nodes that communicate on a network. There are several broad types of networking protocols, including:

- **Application Layer Protocol** such as ***Telnet*** (Remote login to hosts), ***FTP*** (File Transfer Protocol), ***SMTP*** (Simple Mail Transfer Protocol), ***DNS*** (Domain Name System).

- **Transport layer protocol** such as Transmission Control Protocol (**TCP**), User Datagram Protocol (**UDP**), Datagram Congestion Control Protocol (**DCCP**), Stream Control Transmission Protocol (**SCTP**).

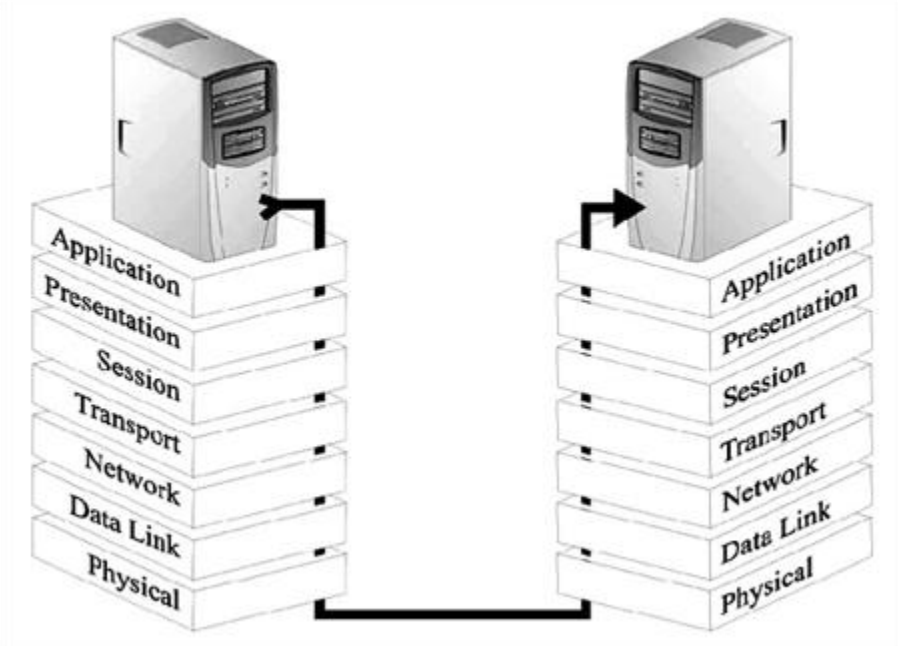
- **Network Layer Protocol** such as Connectionless Networking Protocol **(CLNP),** Exterior Gateway Protocol (EGP), Enhanced Interior Gateway Routing Protocol (**EIGRP**), Internet Control Message Protocol(**ICMP**), Internet Group Management Protocol**(IGMP),** Interior Gateway Routing Protocol(**IGRP**), Internet Protocol version 4(**IPv4**), Internet Protocol version 6(**IPv6**).

- **Data Link Layer Protocol** such as **HDLC** (High-level Data Link Control), **SLIP** (Serial Line Interface Protocol), **PPP** (Point-to-Point Protocol), **LAP** (Link Access Procedure).

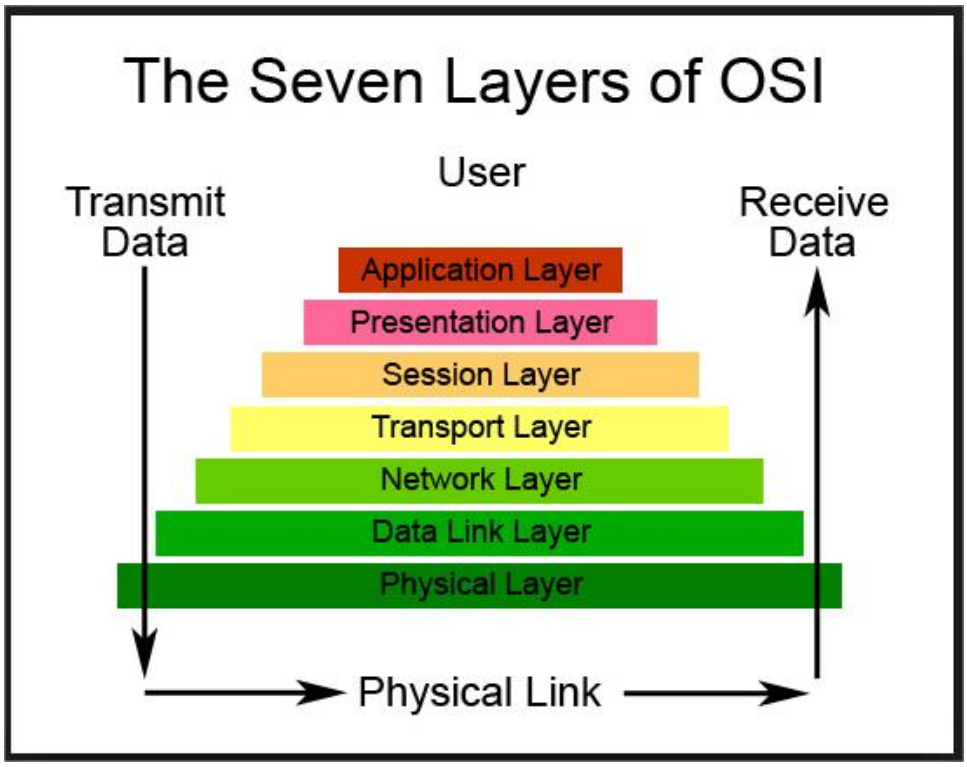
- **Physical Layer Protocol** such as **Ethernet** (IEEE 802.3), **Token Ring**, **RS-232**, **FDDI**, and others.

2.7. Open Systems Interconnection (OSI) Model

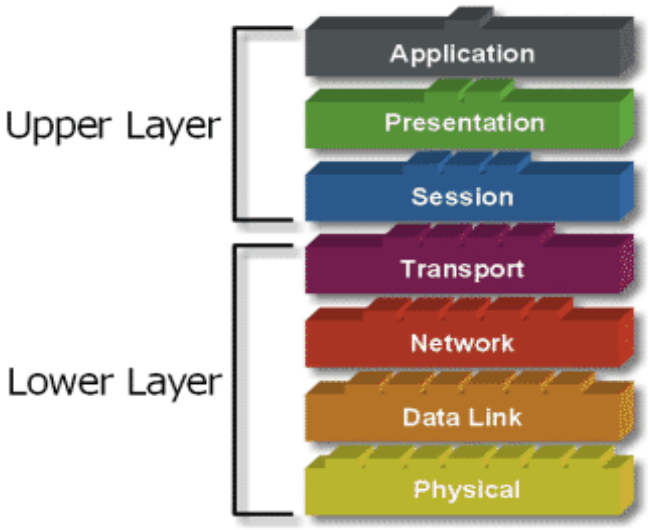
The Open System Interconnection (OSI) model defines a networking framework to implement protocols in the seven layers. Control is passed from one layer to the next, starting at the ***application layer*** in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy as shown in the figure below:



Ali Al-Safi
AliAl-Safi@mustaqbal-college.edu.iq



The Open Systems Interconnection (OSI) model can be considered as a reference tool for understanding data communications between any two networked systems. It divides the communications processes into ***seven layers***. Each layer both performs specific functions to support the layers above it and offers services to the layers below it. The four lowest layers focus on passing traffic through the network to an end system. The top three layers come into play in the end system to complete the process.



The seven layers of OSI model are:

Physical (Layer 1)

The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements. Electrical, mechanical, functional, and procedural specifications are provided for sending a bit stream on a computer network.This layer conveys the bit stream to electrical impulse, light or radio signal — through the network at the electrical and mechanical level. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Components of the physical layer include:

- Cabling system components
- Adapters that connect media to physical interfaces
- Connector design and pin assignments
- Hub, repeater, and patch panel specifications
- Wireless system components
- Parallel SCSI (Small Computer System Interface)
- Network Interface Card (NIC)

Data Link (Layer 2)

At this layer, data packets are encoded and decoded into bits. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.Layer 2 of the OSI model provides the following functions:

- Allows a device to access the network to send and receive messages
- Offers a physical address so a device’s data can be sent on the network

- Works with a device's networking software when sending and receiving messages
- Provides error-detection capability

Common networking components that function at layer 2 include:

- Network interface cards
- Ethernet and Token Ring switches
- Bridges

Network (Layer 3)

Layer 3, the network layer of the OSI model, provides an ***end-to-end*** logical addressing system so that a packetof data can be routed across several layer 2 networks (Ethernet, Token Ring, Frame Relay, etc.). Note that, networklayer addresses can also be referred to as logical addresses.

Routers communicate with one another using ***routing protocols***, such as Routing Information Protocol (RIP)and Open Shortest Path First (OSPF) protocol, to learn of other networks that are present and to calculate thebest way to reach each network based on a variety of criteria (such as the path with the fewest routers).Routers and other networked systems make these routing decisions at the network layer.

When passing packets between different networks, it may become necessary to adjust their outbound size toone that is compatible with the layer 2 protocol that is being used. The network layer accomplishes this via aprocess known as fragmentation. A router's network layer is usually responsible for doing the fragmentation.All reassembly of fragmented packets happens at the network layer of the final destination system.

Transport (Layer 4)

Layer 4, the transport layer of the OSI model, offers end-to-end communication between end devices through anetwork. Depending on the application, the transport layer

either offers reliable, connection-oriented or connectionless,best-effort communications.Some of the functions offered by the transport layer include:

- Application identification
- Confirmation that the entire message arrived intact
- Segmentation of data for network transport
- Control of data flow to prevent memory overruns
- Establishment and maintenance of both ends of virtual circuits
- Transmission-error detection

The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol(TCP) and the connectionless UDP User Datagram Protocol (UDP).

Session (Layer 5)

Layer 5, the session layer, provides various services, including tracking the number of bytes that each end ofthe session has acknowledged receiving from the other end of the session. This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end.

Presentation (Layer 6)

Layer 6, the presentation layer, is responsible for how an application formats the data to be sent out onto thenetwork. The presentation layer basically allows an application to read (or understand) the message.Examples of presentation layer functionality include:

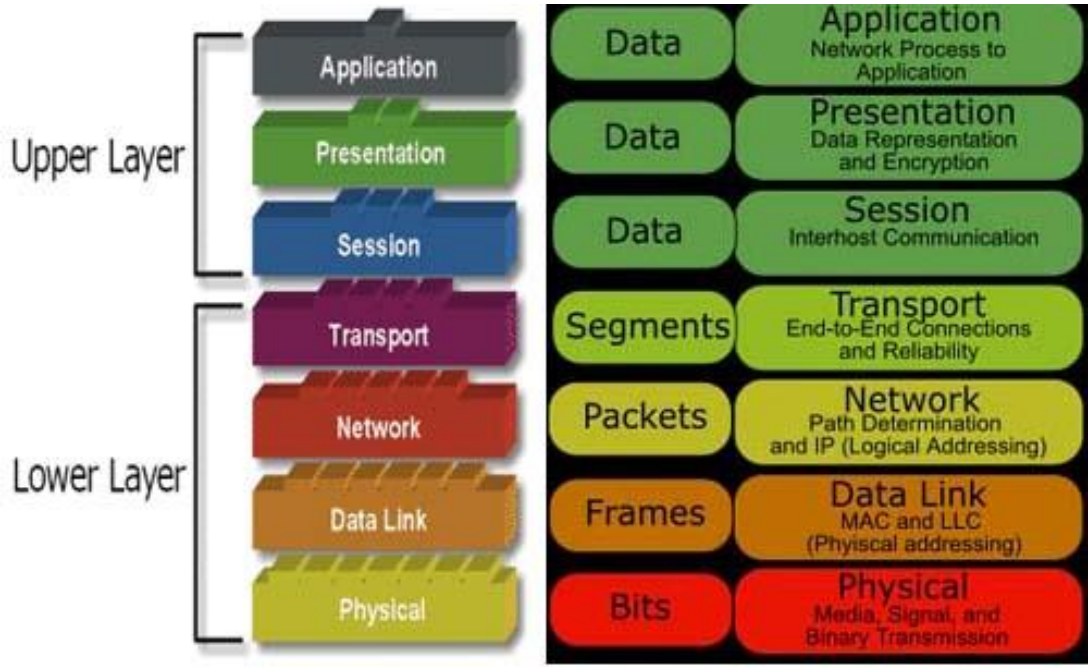
- Encryption and decryption of a message for security
- Compression and expansion of a message so that it travels efficiently
- Graphics formatting

- Content translation
- System-specific translation

Application (Layer 7)

Layer 7, the application layer, provides an interface for the end user operating a device connected to a network.This layer is what the user sees, in terms of loading an application (such as Web browser or e-mail); thatis, this application layer is the data the user views while using these applications.Examples of application layer functionality include:

- Support for file transfers
- Ability to print on a network
- Electronic mail
- Electronic messaging
- Browsing the World Wide Web



Ali Al-Safi
AliAl-Safi@mustaqbal-college.edu.iq