Introduction to Computer Networks

Networks

TCP/IP Protocol

Data and Signals

Digital Signals

Network Performance

IPv4 address

Wired LANs –Ethernet–

Wireless LANs –WiFi–

Chapter One

Introduction to Computer Networks

1.1 Introduction

This chapter provides an introduction to Computer networks and covers fundamental topics like data, information to the definition of communication and computer networks.

The **main objective** of data communication and networking is to enable seamless exchange of data between any two points in the world. This exchange of data takes place over a computer network.

1.2 Data & Information

Data refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.

Ex. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.

The word **data** refers to any information which is presented in a form that is agreed and accepted upon by is creators and users.

Networks and communication involve connecting different systems and devices to share data and information. This setup includes hardware like computers, routers, switches, and modems, as well as software protocols that manage how data flows between these devices.

Protocols such as TCP/IP and HTTP are essential for communication between devices. They set the rules for how data is exchanged, ensuring a common connection.

Advancements in technology have led to the creation of complex communication networks, like the Internet. The Internet has transformed how we communicate and access information. It has made it easier for people to connect, work more efficiently, and find information and resources quickly.

Data communications and networking enable to exchange data such as text, audio, and video from all points in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

1.3 Data Communication

Transferring data (In the form 0's and 1's) over a transmission medium (such as wire cable) between two or more devices, systems, or places is known as data communication. Nowadays, computing and telecommunications depend heavily on this data transmission, which makes a variety of applications conceivable, including email, video chatting, the Internet, and many more things.

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication (devices in the same building) usually occurs face to face, while remote communication takes place over distance.

The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

The effectiveness of a data communications system depends on four fundamental characteristics:

1. **Delivery**. The system must deliver data to the correct destination.

2. **Accuracy**. The system must deliver the data accurately, without errors.

3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, without significant delay (real-time transmission).

4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

1.4 Components of data communications system

There are mainly five components of a data communication system Figure 1.1.

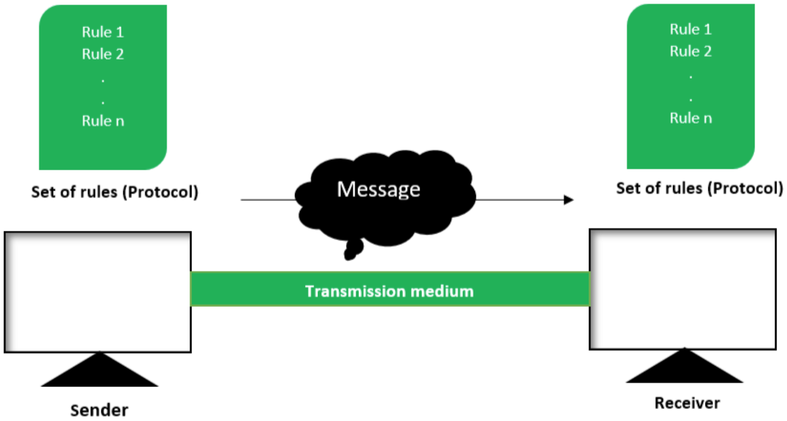


Figure (1-1): Five components of data communication system

1. **Message**. It is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender**. It is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. **Receiver**. It is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium**. It is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**. It is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

1.5 Data Representation

Information today comes in different forms such as:

Text in data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols, for example, the American Standard Code for Information Interchange (ASCII) which uses 32 bits to represent a symbol or character used in any language in the world. Each set is called a code, and the process of representing symbols is called coding.

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number.

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete.

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images.

All these information forms represent the material that may be sent and received in any data communication system.

1.6 Data Flow

Data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

Simplex communication: It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data. For example, the keyboard can only introduce input; the monitor can only accept output. Figure (1-2).

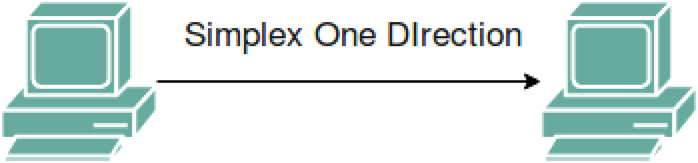


Figure (1-2): Simplex mode

Half-Duplex communication: It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, the Walkie-talkies devices. Figure (1-3).

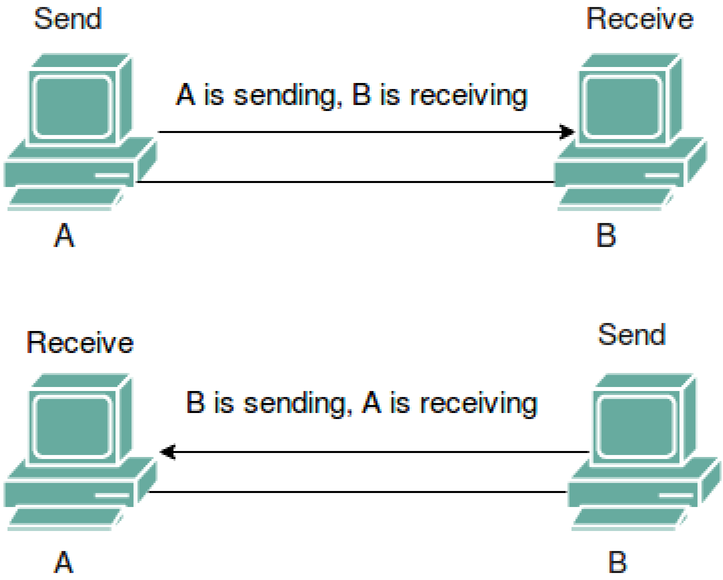


Figure (1-3): Half duplex mode

Full-Duplex communication: (also called duplex), It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones. Figure (1-4).

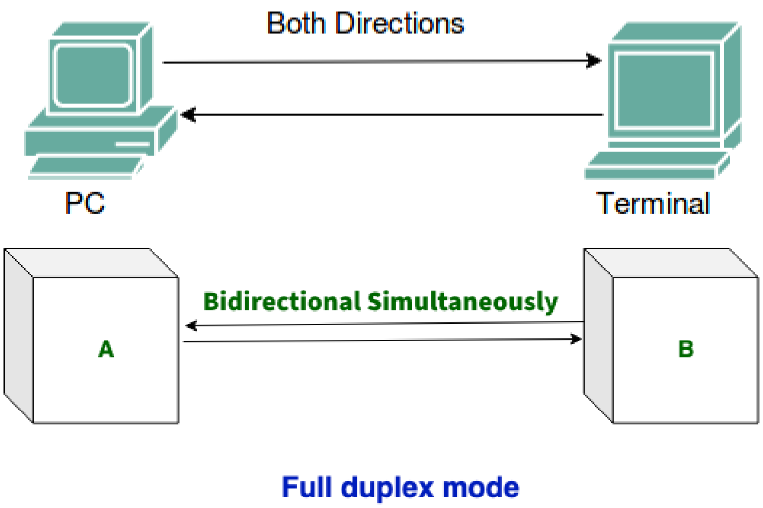


Figure (1-4): Full duplex mode

1.7 Computer Networks

A computer network can be defined as a collection of devices (nodes). A node can be any device (computer, printer) capable of transmitting or receiving data generated by other nodes on the network. The communicating nodes have to be connected by communication links.

1.7.1 Network Criteria

A network must meet the following network criteria:

Performance – It is measured by transit time and response time also depends on users, medium, hardware, and software.

Reliability – Reliability is measured by the frequency of failure.

Security – Security protects data from unauthorized access.

1.7.2 Distributed Processing

Distributed computing refers to a system where processing and data storage is distributed across multiple devices or systems, rather than being handled by a single central device. In a distributed system, each device or system has its own processing capabilities and may also store and manage its own data. These devices or systems work together to perform tasks and share resources, with no single device serving as the central hub.

Figure (1.5): Distributed data processing

One example of a distributed computing system is a cloud computing system Figure (1.5), where resources such as computing power, storage, and networking are delivered over the Internet and accessed on demand. In this type of system, users can access and use shared resources through a web browser or other client software.

There are several key **components** of a Distributed Computing System

Devices or Systems: The devices or systems in a distributed system have their own processing capabilities and may also store and manage their own data.

Network: The network connects the devices or systems in the distributed system, allowing them to communicate and exchange data.

Resource Management: Distributed systems often have some type of resource management system in place to allocate and manage shared resources such as computing power, storage, and networking.

1.7.3 Types of Network Connections

There are two possible types of connections:

Point-to-Point: This connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices, Figure 1.6. **For example:** establishing a point-to-point connection between the remote control and the television's control system.

Multipoint: In this connection, more than two specific devices share a single link Figure 1.6. The capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

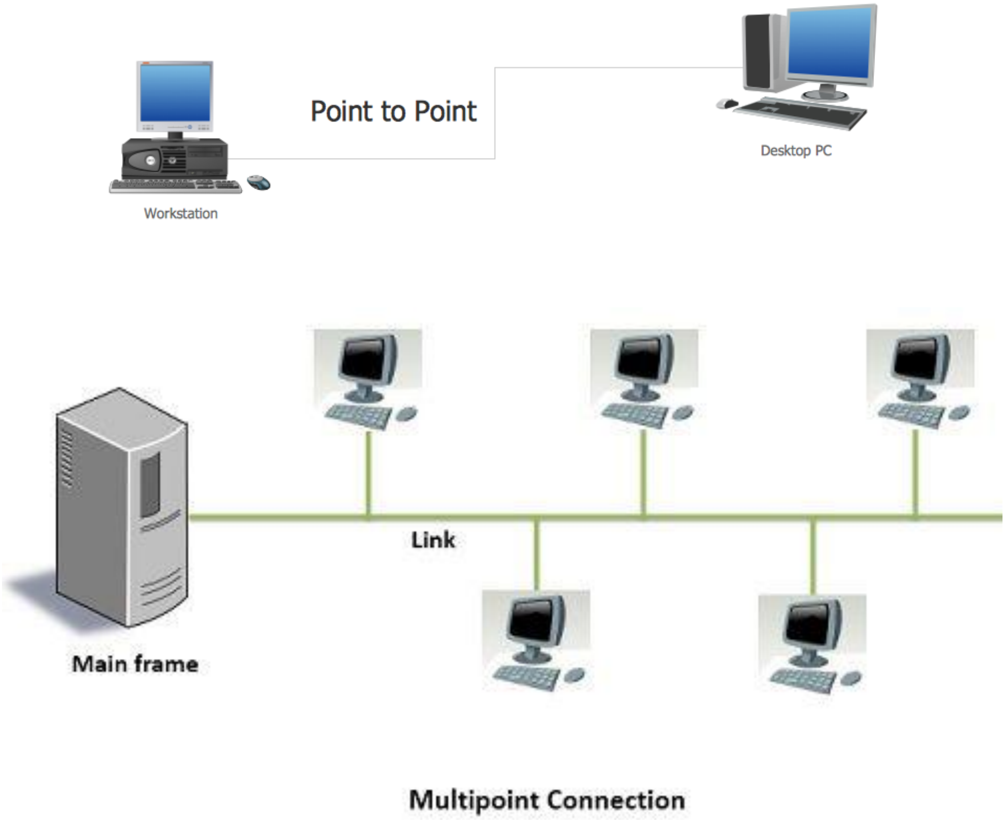


Figure (1-6): Point to point and multipoint connections

1.7.4 Physical Network Topology

A network topology is the arrangement of devices (nodes) and connections (links) in a computer network. It shows how computers, servers, and other devices are connected and how data flows between them. There are two main types of topology:

Physical Topology: The term physical topology refers to the way in which a network is arranged physically. The actual physical layout of cables and devices.

Logical Topology: How data moves across the network, regardless of physical layout.

There are **five** possible basic topologies:

1- **Mesh**: In a mesh topology, every device has a dedicated point-to-point link (channel) to every other device as shown in Fig. (1-7).

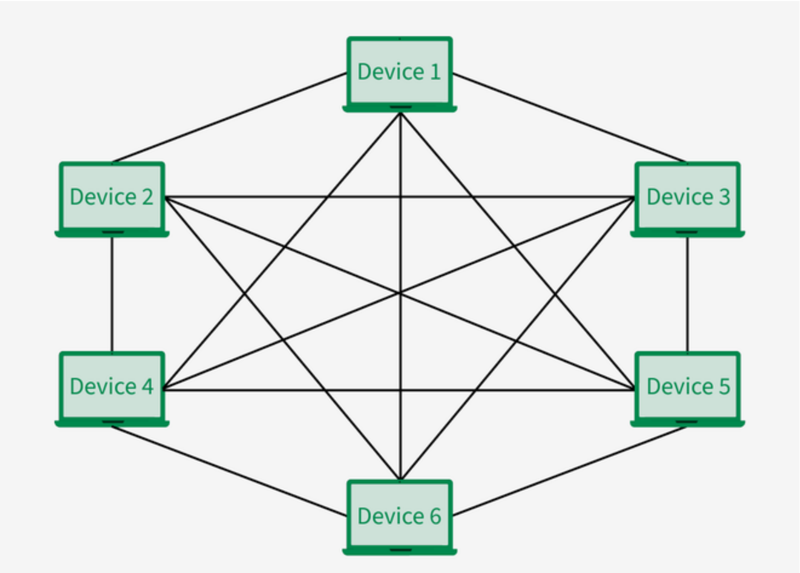


Figure (1-7): Mesh topology

Advantages:

1) Eliminating the traffic problems.
2) If one link becomes unusable, it does not fall the entire system.
3) High privacy or security.
4) Communication is very fast between the nodes.
5) Mesh Topology is robust.
6) The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

Disadvantages:

1) Amount of cabling is required.
2) Installation and configuration are difficult.
3) The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
4) The cost of maintenance is high.
5) Number of I/O ports (e.g., LAN Cards) is required.

Suppose, the **N** number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is **N−1**. In Figure (1-7), there are 6 devices connected to each other, hence the total number of ports required by each device is 5. The total number of ports required **= N * (N-1)**

Suppose, **N** number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is: **N * (N-1)/2**. In Figure (1-7), there are 6 devices connected to each other, hence the total number of links required is: 6 * 5/2 = 15.

2. Star Topology: In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Figure (1-8).

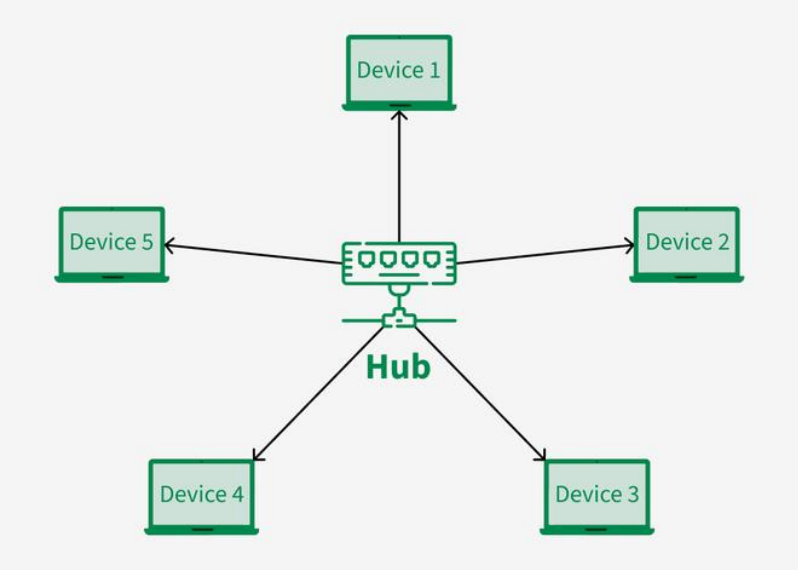


Figure (1-8): Star topology

Advantages:

1) Each device needs only one link and one I/O port to connect it.
2) Easy to install and reconfigure.

Disadvantages:

1) Single point dependency. If the hub goes down, the whole network is dead.
2) The cost of installation is high.

3. Bus Topology: This topology is multipoint. It is bi-directional. One long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps Figure (1-9).

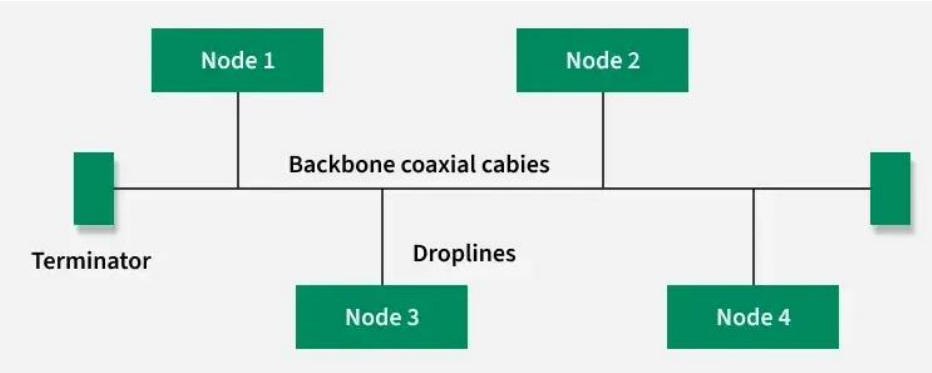


Figure (1-9): Bus topology

Advantages:

1) Ease of installation.
2) Less cabling than mesh or star topologies.

Disadvantages:

1) Difficult reconnection and fault isolation.
2) A bus topology is quite simpler, but still, it requires a lot of cabling.
3) If the common cable fails, then the whole system will crash down.
4) If the network traffic is heavy, it increases collisions in the network.
5) Adding new devices to the network would slow down networks.
6) Security is very low.

4. <u>Ring Topology</u>: Each device has a dedicated point-to-point connection with exactly two neighboring devices. A signal is passed along the ring in one direction, from device to device, until it reaches its destination (if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node). Figure (1-10) explain how to arrange the network with the ring topology.

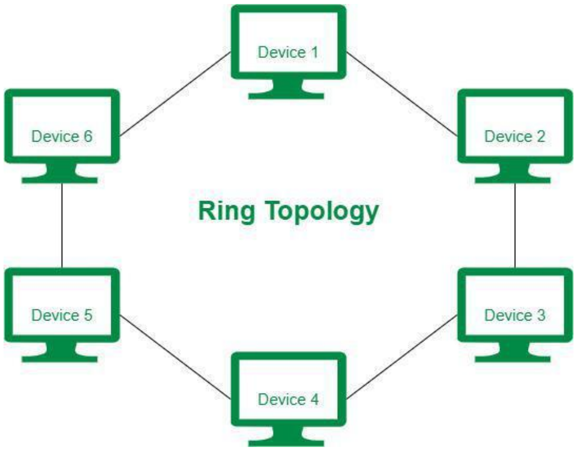


Figure (1-10): Ring topology

Advantages:

1) Easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).

2) Cheap to install and expand.

Disadvantages:

Unidirectional traffic i.e., a break in the ring (such as a disabled station) can disable the entire network.

5. Hybrid Topology: Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. For **example**, we can have a main star topology with each branch connecting several stations in bus and ring topology as shown in Figure (1-11).

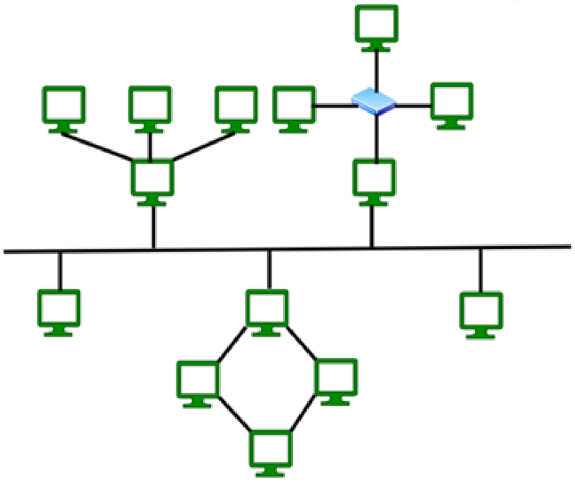


Figure (1-11): Hybrid network

Advantages:

1) This topology is very flexible.
2) The size of the network can be easily expanded by adding new devices.

Disadvantages:

1) It is challenging to design the architecture of the Hybrid Network.
2) Hubs used in this topology are very expensive.
3) The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices.

1.7.5 Categories of networks

The category of networks is determined by its **size** and **connection type**. Figure (1-12) classifies the networks by their rough physical size.

Inter-processor distance	Processor Location	Example
0.1 m	Circuit Board	Data flow machine
1m	System	Multi Computer
10m	Room	LAN
100m	Building	
1km	Campus	
10km	City	WAN
100km	Country	
1000km	Continent	
10000km	Planet	Internet

Figure (1-12): Classification of networks by size

1. Personal Area Networks (PANs) is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 10 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. In the simplest form, Figure (1-13). Examples of PAN are Bluetooth connection between a phone and wireless earbuds, Infrared communication between TV and remote.

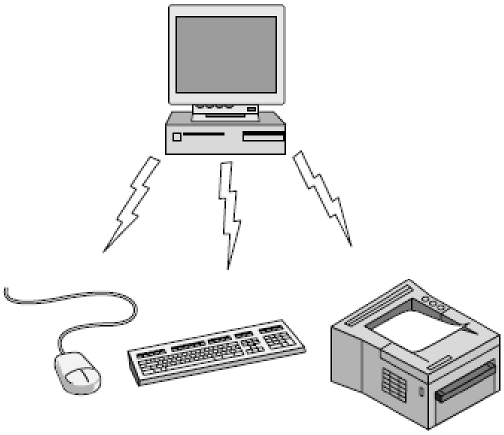


Figure (1-13): Bluetooth PAN configuration

2. Local area networks (LANs) link the devices in a single office, building, or campus Figure (1-14). LANs can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company, they are called enterprise networks.

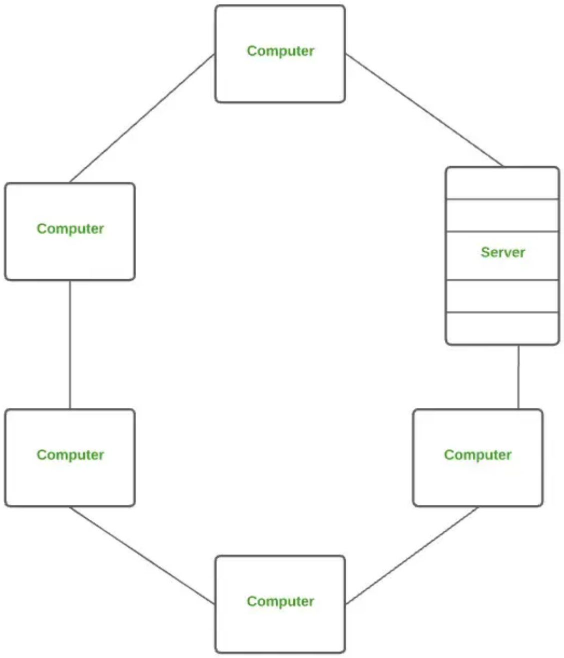


Figure (1-14): LAN

Wireless LANs are very popular these days in which every computer has a radio modem (e.g., wireless LAN card) to communicate with other computers. Each computer talks to an Access Point or wireless router Figure (1-15) to relay data packets between the wireless computers and also with the Internet. There is a standard for wireless LANs called IEEE 802.11, popularly known as WiFi. It runs at speeds from 11 to hundreds of Mbps1.

Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber. Typically, wired LANs run at speeds of 100 Mbps to 1 Gbps, have low delay (microseconds or nanoseconds), and make very few errors. Compared to wireless networks, wired LANs exceed them in all dimensions of performance. IEEE 802.3, popularly called Ethernet, is the most common type of wired LAN. Figure (1-15).

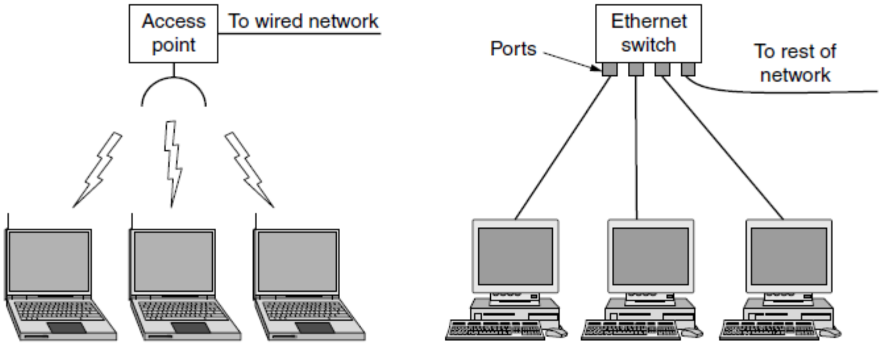


Figure (1-15): Wire and wireless LANs

3. Metropolitan Area Network (MAN) covers a city. The best-known examples of MANs are the cable television networks available in many cities.

In Figure (1-16) we see both television signals and Internet being fed into the centralized cable head-end for subsequent distribution to people's homes.

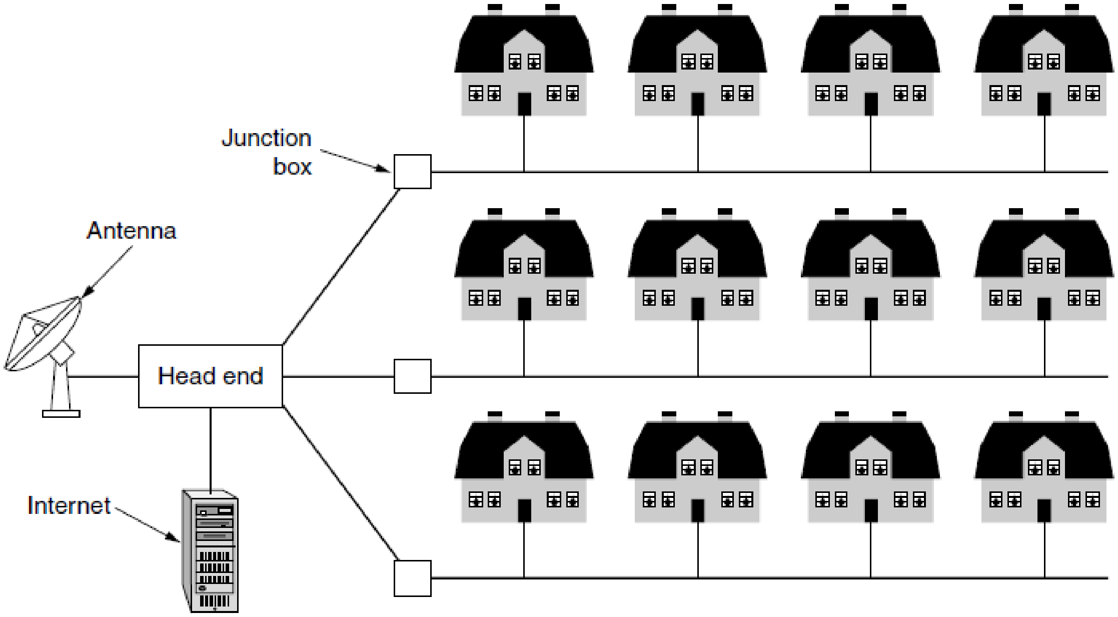


Figure (1-16): A metropolitan area network based on cable TV.

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. **Examples** of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.

4. A wide area network (WAN) provides long-distance transmission of data over large geographic areas that may comprise a country, a continent, or even the whole world.

The WAN in Figure (1-17) is a network in Australia that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computer machines intended for running user (i.e., application) programs. Each of these machines are called **host**. The rest of the network that connects these hosts is then called the communication **subnet**, or just subnet2 for short.

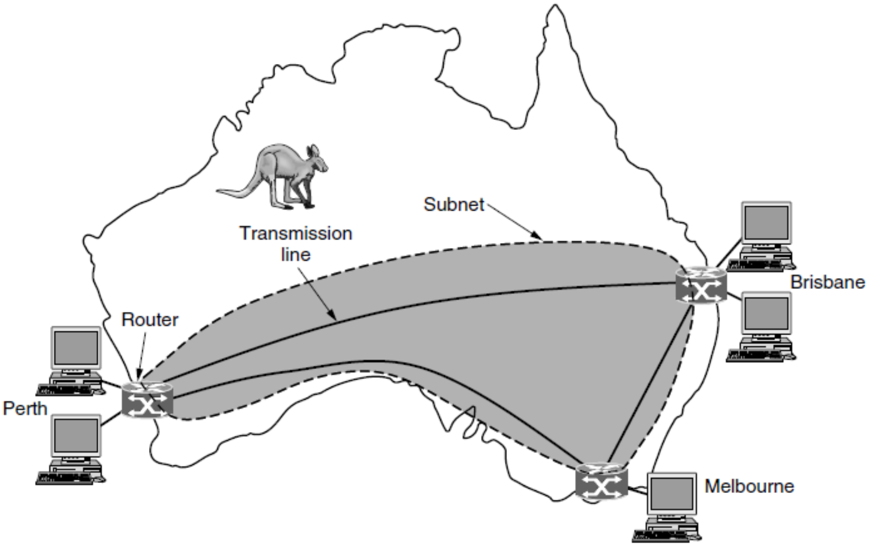


Figure (1-17): WAN that connects three branch offices in Australia.

5. Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a WAN in isolation; they are connected to one another. When two or more networks with different hardware and software are connected, they become an internetwork, or internet. (i.e., it is a collection of interconnected networks). These terms are used in a generic sense, in contrast to the worldwide Internet (which is one specific internet), which we will always capitalize.

6. Internet

The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting lines and switching devices Figure (1-18).

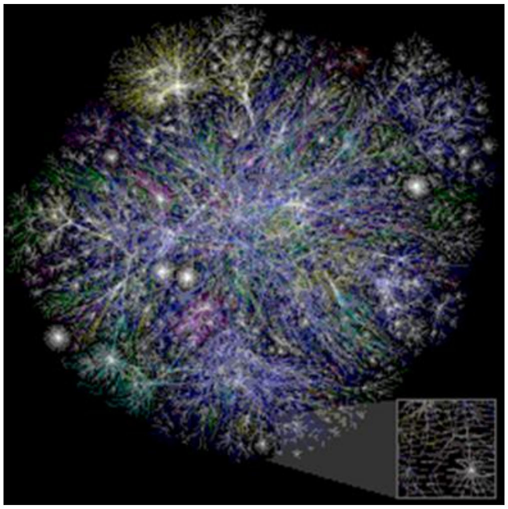


Figure (1-18): Internet Map

Chapter Two

Networks

2.1 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1. Performance

It can be measured in many ways, including transit time (the amount of time required for a message to travel from one device to another) and response time (is the time between an inquiry and a response).

The performance of a network depends on a number of factors:

- Number of users.
- Type of transmission medium.
- Capabilities of the connected hardware.
- Efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay.

2. Reliability network reliability is measured by the:

- Accuracy of delivery.
- Frequency of failure.
- The time it takes a link to recover from a failure.
- Network's robustness in a catastrophe.

3. Security network security issues include:

- Protecting data from unauthorized access
- Protecting data from damage and change.
- Implementing policies for recovery from data losses.

2.2. Protocols and Standards

A) Protocol

A protocol defines *what* is communicated, *how* it is communicated, and *when* it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax It refers to the structure or format of the data, meaning the order in which they are presented.

For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics It refers to the meaning of each section of bits. *How* is a particular pattern to be interpreted, and *what* action is to be taken based on that interpretation?

For example, does an address identify the route to be taken or the final destination of the message?

Timing Refers to the synchronization and coordination between devices while transferring the data. It refers to two characteristics: *when* data should be sent and *how* fast they can be sent.

For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost. Timing ensures preventing of data loss, collisions, and other timing-related issues.

B) Standards

Standards are the set of rules for data communication that are needed for the exchange of information among devices. It is important to follow Standards which are created by various Standard Organizations like IEEE, ISO, ANSI, etc.

Standard Organizations for Data Communication Committees

- International Organization for Standardization (ISO). It creates set of rules and standards for graphics, document exchange, data communication etc.

- American National Standards Institute (ANSI). The ANSI is a completely private in USA. It provides various set of rules and standard for Data Communication.

- Institute of Electrical and Electronics Engineers (IEEE). It is US based professional organization of electronic, computer and communication engineering. It provides various set of rules and standard in communication and networking field.

- Electronic Industries Association (EIA). In the field of information technology (IT), the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

2.3 Network Models

The OSI model failed to become the ultimate standard because the TCP/IP suite gained dominance through its widespread implementation and testing on the early Internet, a practical advantage over the OSI model, which was never fully implemented in commercial systems. The OSI model was a theoretical seven-layer architecture intended to standardize network communication, but its development was complicated by competing interests, and it was published after TCP/IP was already being used. Figure 2.1 shows the layers included in the TCP/IP and OSI models and also the main protocols and services provided by each layer.

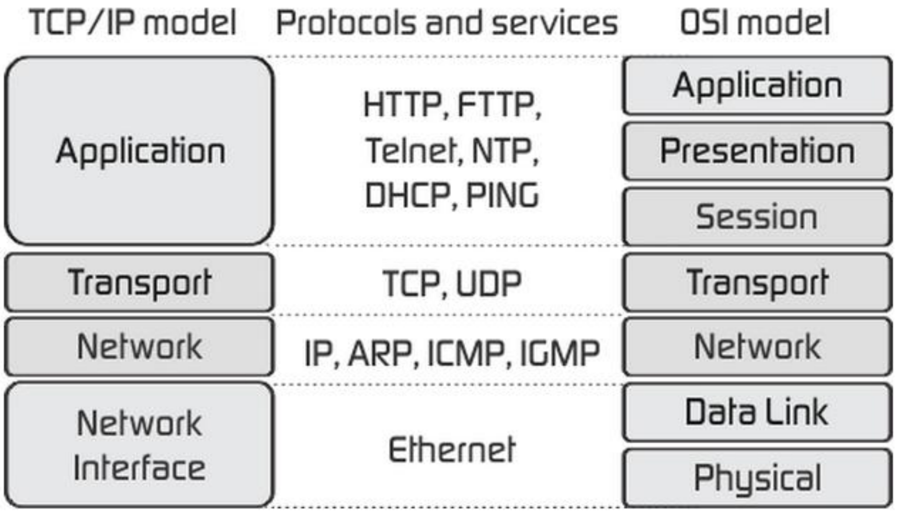


Figure (2-1): The TCP/IP and OSI models for data communications and networking

2.3.1 Layered Task

We use the concept of layers in our daily life. As an example, two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure 2.2 shows the steps in this task.

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

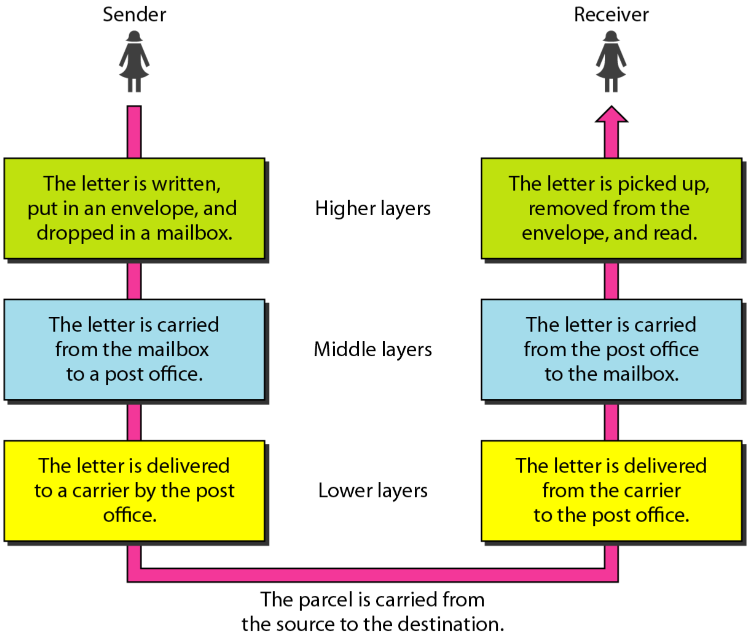

Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

Figure (2-2): Tasks involved in sending a letter

2.3.2 The OSI Model

The Open Systems Interconnection (OSI) model is introduced in the late 1970s by the International Standards Organization (ISO).

The **OSI model** is a layered model for the design and understands of network systems that allows communication between all types of computer systems.

The **OSI model** is **not** a protocol; it is a model for understanding and designing a network architecture that is flexible and robust.

OSI consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. See figure (2-3).

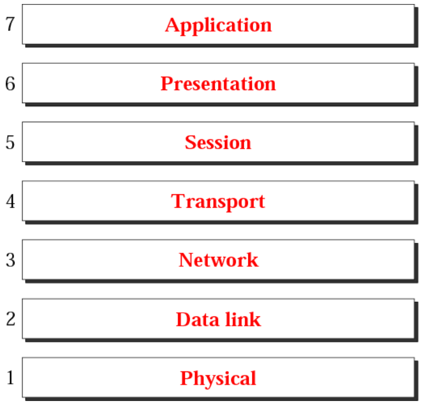


Figure (2-3): The OSI model

Figure 2.4 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes, called **routers**. These intermediate nodes usually involve only the first three layers of the OSI model.

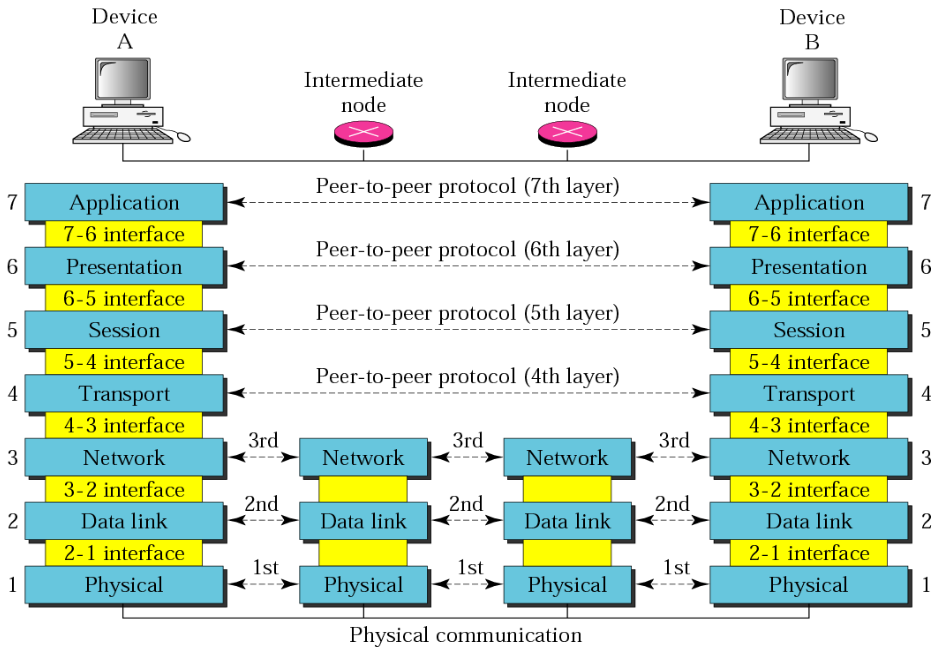


Figure (2-4): The interaction between layers in the OSI model

Each layer defines a family of functions distinct from those of the other layers. **Layer 3**, for ***example***, uses the services provided by layer 2 and provides services for layer 4.

The processes on each machine that communicate at a given layer are called **peer-to-peer processes**. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

The **interfaces between layers** are to define the information and services that each layer must provide for the layer above it.

The seven layers are belonging to ***three subgroups***. Layers 1, 2, and 3 are *the network support layers*; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, and physical addressing). Layers 5, 6, and 7 are the *user support layers*; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups. Figure (2-5) explains exchange using the OSI model.

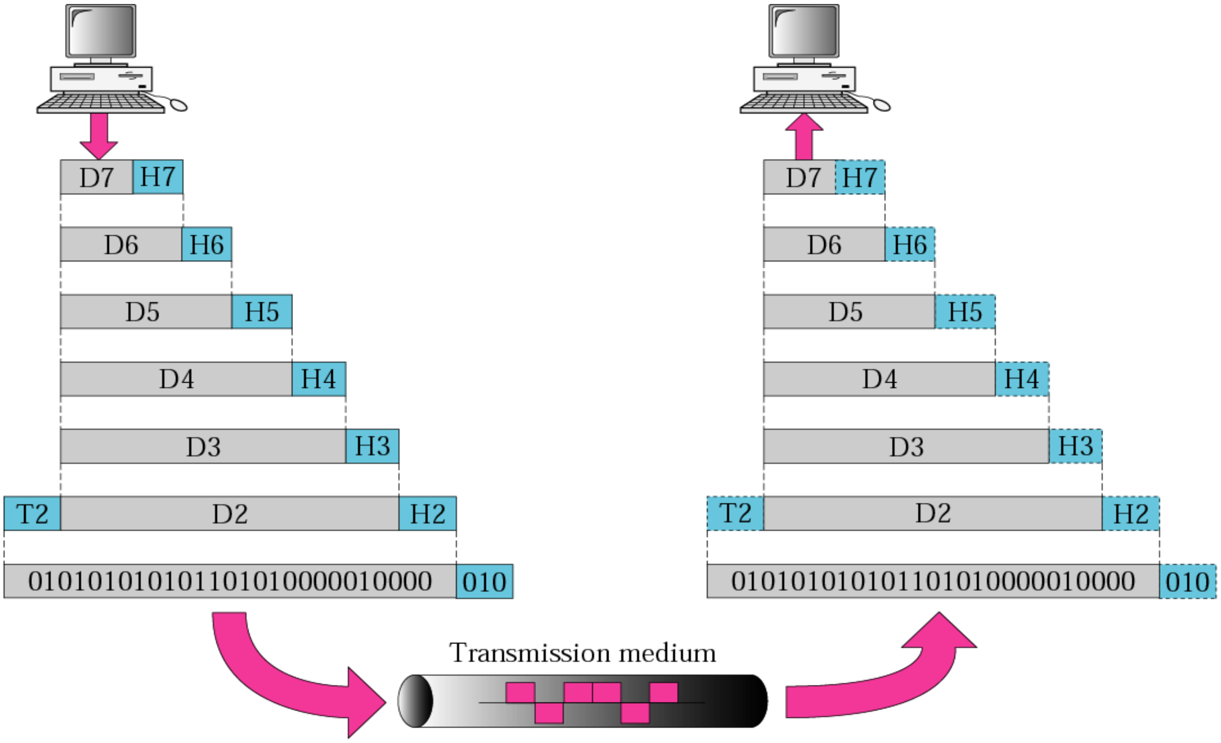


Figure (2-5): An exchange using the OSI model

2.3.3 Layers in the OSI Model

The following describes the functions of each layer in the OSI model.

1. Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium (see Figure 2.6).

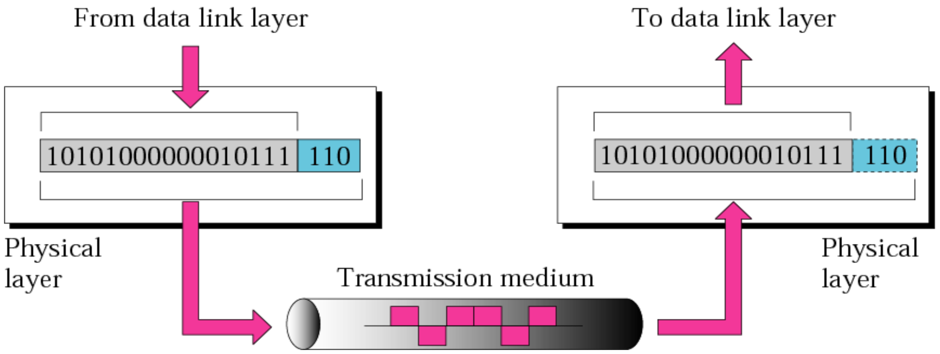


Figure (2-6): Physical layer

The **physical layer** is responsible for the **movement of individual bits** from one hop (node) to the next. The physical layer is concerned with the following:

- Physical characteristics of interfaces and medium.
- Representation of bits (sequence of 0s or 1s) with defining the type of encoding (how 0s and 1s are changed to signals).
- Data rate or the transmission rate (the number of bits sent each second).
- Synchronization of bits, the sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
- Line configuration (point-to-point or multipoint configuration).
- Physical topology (mesh, star, bus, etc.).
- Transmission mode (simplex, half-duplex, or full-duplex).

2. Data Link Layer

The **data link** layer makes the physical layer appear **error-free to the upper layer** (network layer). Figure 2.7 shows the relationship of the data link layer to the network and physical layers.

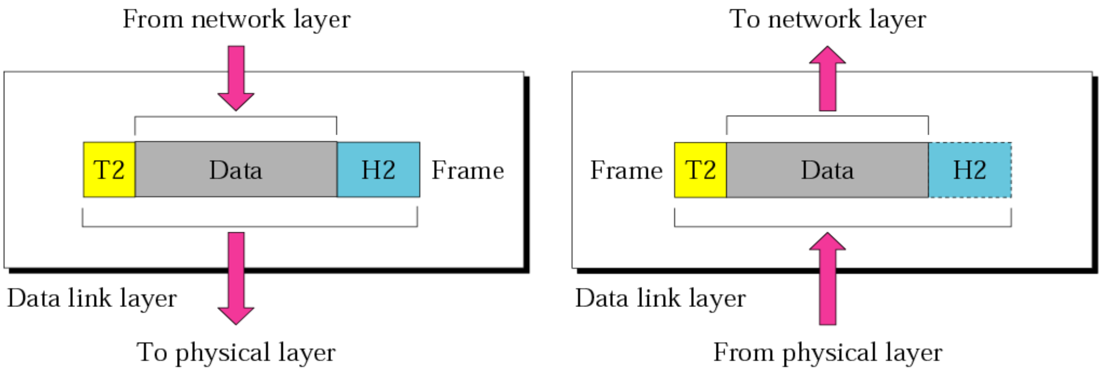


Figure (2-7): Data link layer

The data link layer is responsible for **moving frames** from one hop (node) to the next figure (2-8). Other responsibilities of the data link layer include the following:

- **Framing**. The data link layer **divides** the stream of bits received from the network layer into manageable data units called **frames** (see Figure 2.7).
- **Physical addressing**. The data link layer **adds** a *header to the frame* to define the sender and/or receiver devices of the frame. The devises are defined by the physical address (or MAC address).
- **Flow control**. The data link layer **ensures** the rate at which data are produced in the sender and arrived in the receiver.
- **Error control**. The data link layer **adds mechanisms to detect** and retransmit damaged or lost frames. *Error control* is normally achieved through a *trailer* added to the end of the frame (see the T2 in Figure 2.7).
- **Access control**. The data link layer controls the access to the link when two or more devices are connected to the same link.

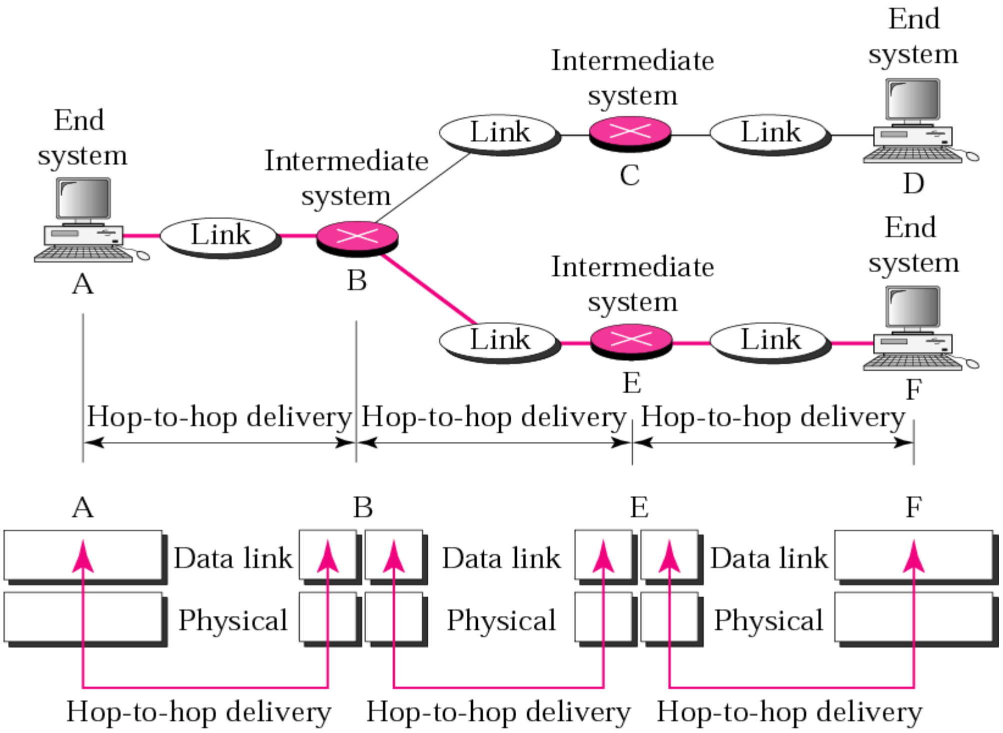


Figure (2-8): Hop-to-Hop delivery

3. Network Layer

The network layer is responsible for the **source-to-destination delivery** of a packet (from one source host to another destination host (host-to-host)) (see Figures 2.9 and 2.10), possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links).

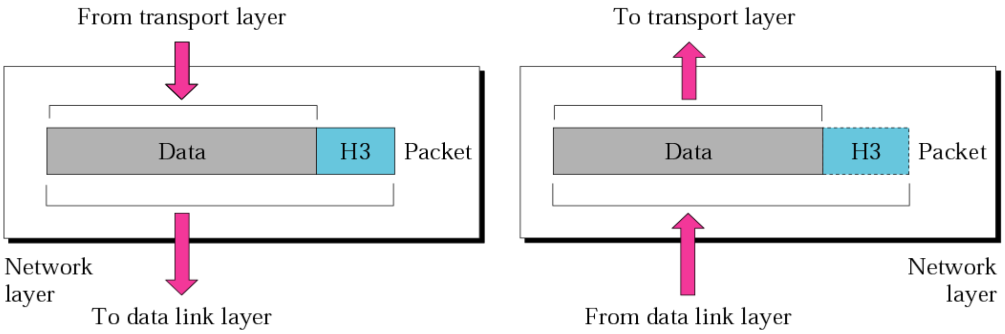


Figure (2-9): Network layer

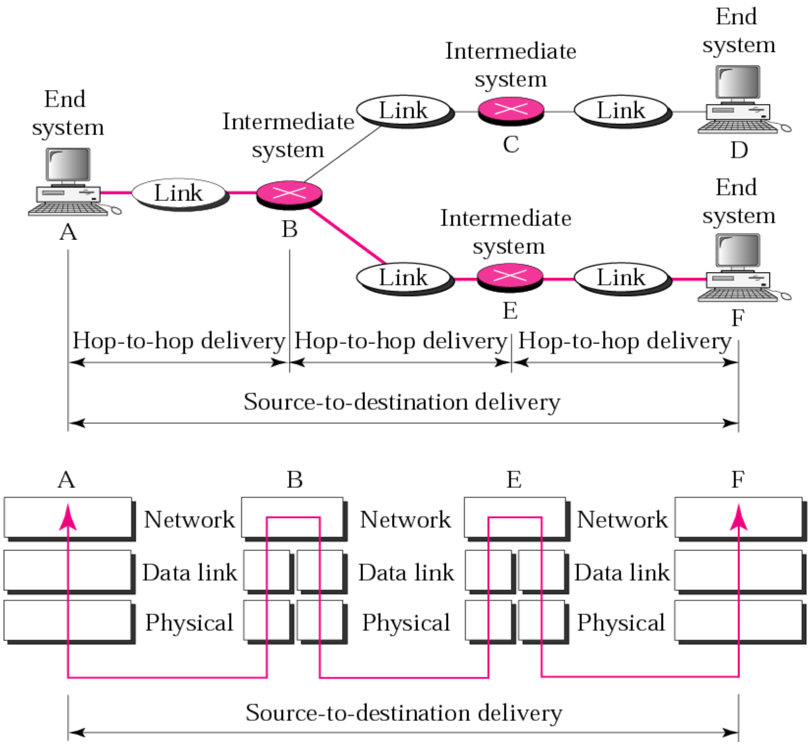


Figure (2-10): Source to destination delivery

Other responsibilities of the network layer include the following:

- **Logical addressing**. The network layer **adds a header to the packet** coming from the upper layer that, among other things, includes the logical addresses (IP address) of the sender and receiver. We discuss logical addresses in a next lecture.
- **Routing**. When independent networks or links are connected to create internetworks, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4. Transport Layer

The transport layer is responsible for **process-to-process delivery** of the **entire message**. A ***process*** is an application program running on a host (deliver the data). Whereas the network layer oversees source-to-destination delivery of individual packets. Figure (2-11 and 2-12).

Other responsibilities of the transport layer include the following:

- **Service-point addressing**. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery **not only** from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The **transport layer header** must therefore include a type of address called a **service-point address** (or port address). The *network layer* gets each packet to the correct computer; the *transport layer* gets the entire message to the correct process on that computer.

- **Segmentation and reassembly**. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly at the destination (see Figure 2.11).

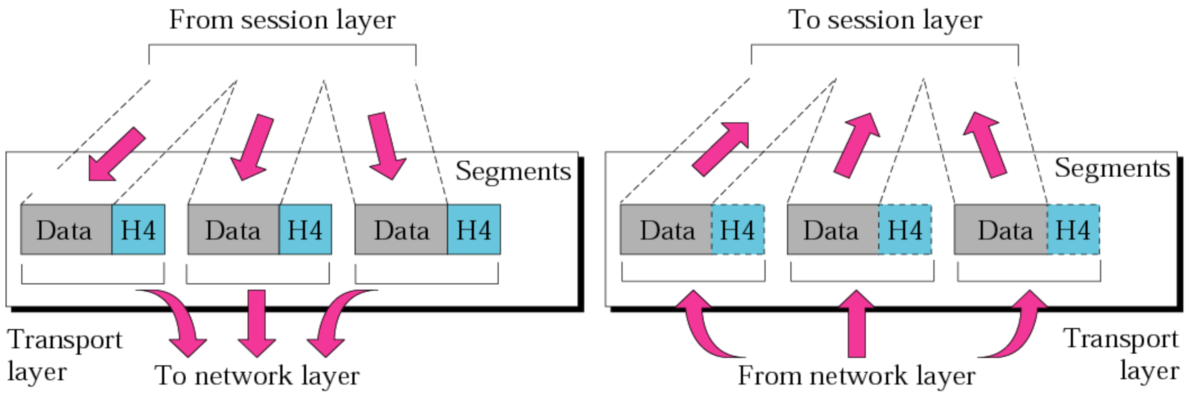


Figure (2-11): Transport layer

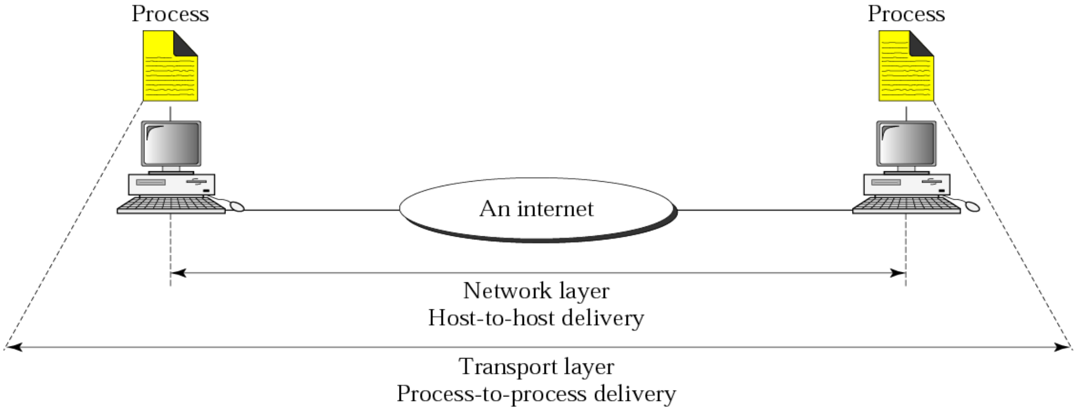


Figure (2-12): Reliable process-to-process delivery of a message

- **Flow control**. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed *end to end* rather than across a single link.

- **Error control**. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed *process-to-process* rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).

5. Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is responsible for **dialog control and synchronization**. Figure 2.13.

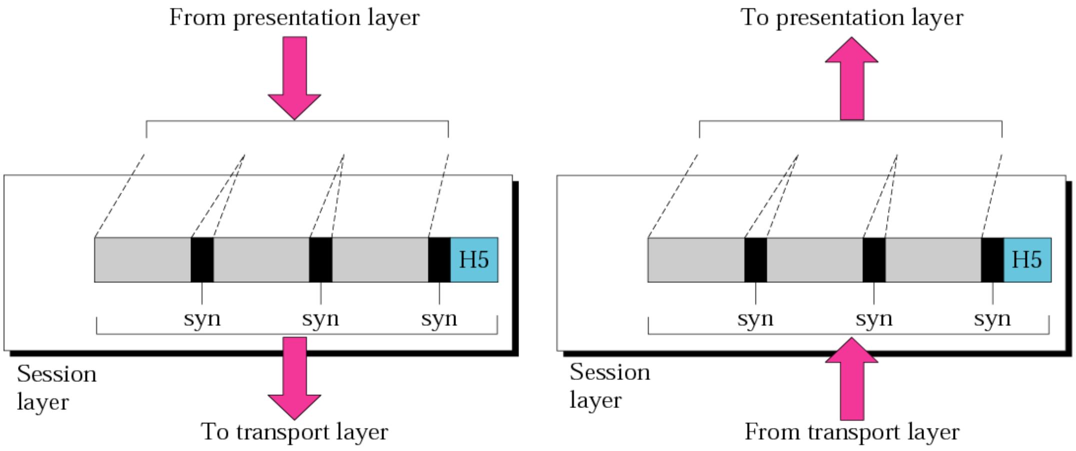


Figure (2-13): Session layer

Specific responsibilities of the session layer include the following:

- **Dialog control**. The session layer allows the communication between two processes to take place in either half-duplex (one way at a time) or full duplex (two ways at a time) mode.
- **Synchronization**. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data (see Figure 2.13). For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages.

6. Presentation Layer

The **presentation layer** is concerned with the **syntax and semantics** of the information exchanged between two systems (see Figure 2.14).

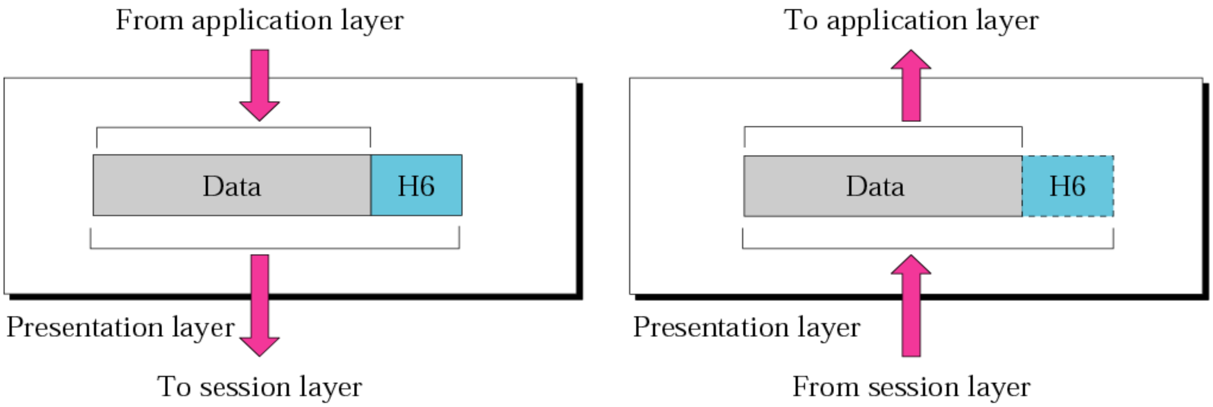


Figure (2-14): Session layer

Specific responsibilities of the presentation layer include the following:

- **Translation**. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these **different** encoding methods.

- **Encryption**. To carry sensitive information, a system must be able to ensure privacy.

- **Compression**. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the data transmission.

7. Application Layer

The **application layer** is responsible for **providing services to the user**. It enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, and other types of distributed information services.

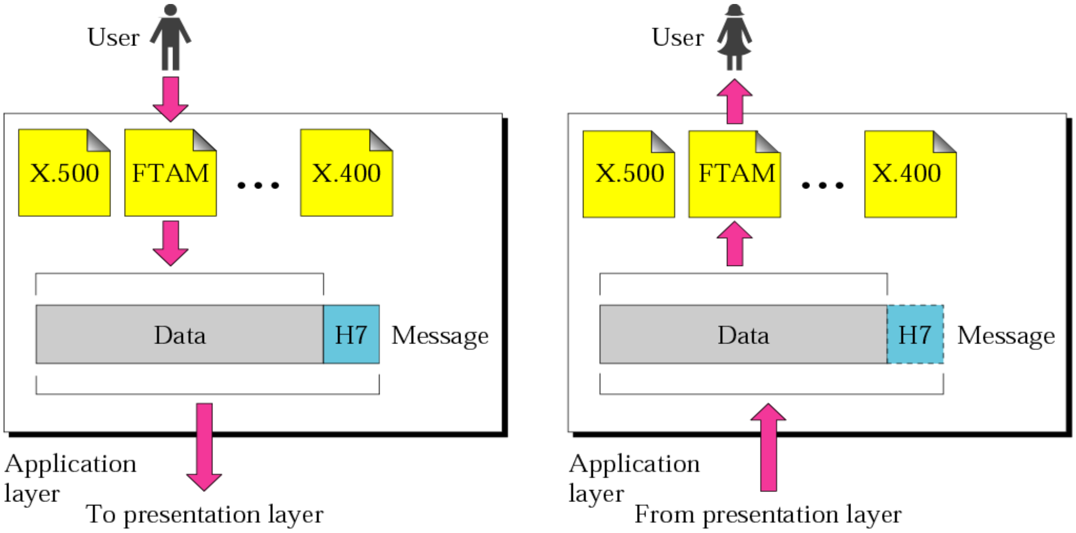


Figure (2-15): Application layer

Figure 2.15 shows only three application services available on a user computer:

XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.

Summary of OSI Layers

Figure 2.16 shows a summary of duties for each layer in the OSI model.

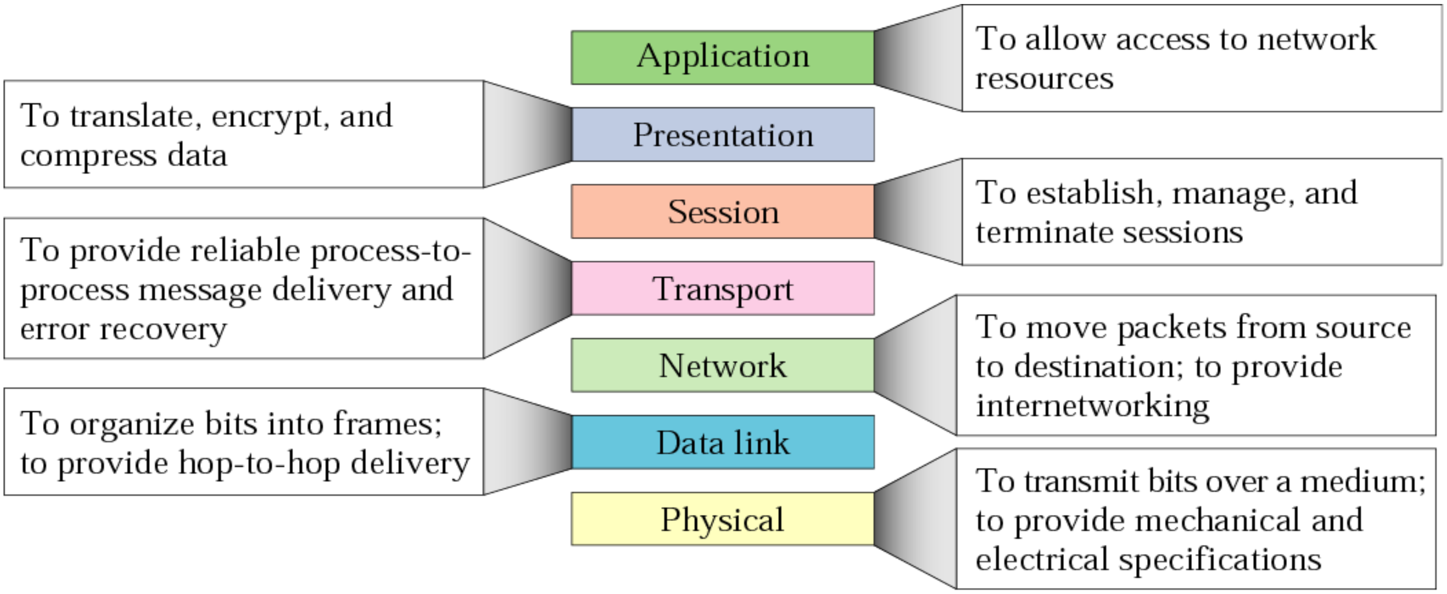

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

Figure (2-16): Summary of OSI model layers

Chapter Three
TCP/IP Protocol

3.1 TCP/IP Protocol Suite

The TCP/IP protocol suite is made of **five** layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model (see Figure 3.1). The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the *application layer*.

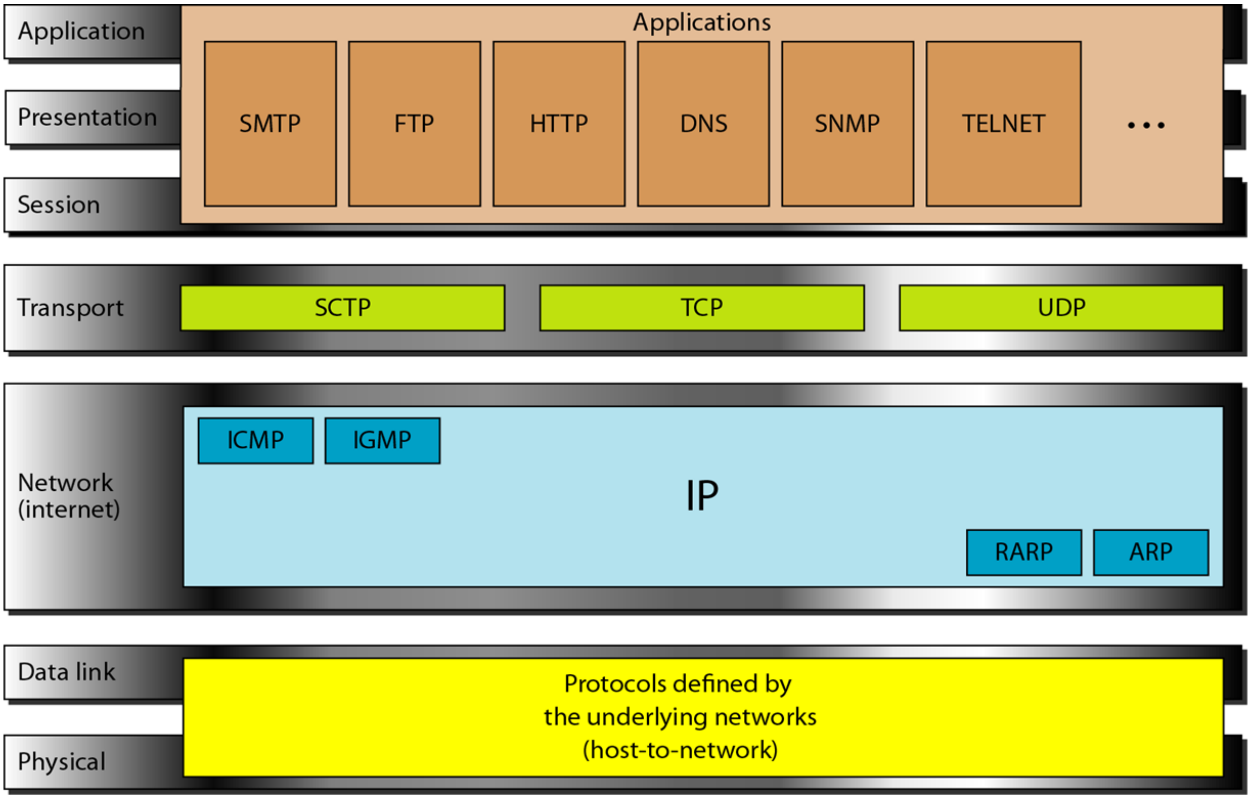


Figure (3-1): TCP/IP and OSI Model

1. Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2. Network Layer

At the network layer (or the internetwork layer), TCP/IP supports the Internetworking Protocol (IP). IP uses four supporting protocols: ARP, RARP, ICMP, and IGMP as described in the following:

The Internetworking Protocol (IP): is the transmission mechanism used by the TCP/IP protocols. IP transports data in packets called ***datagrams***, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated.

The Address Resolution Protocol (ARP): is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known. https://www.youtube.com/watch?v=cn8Zxh9bPio

https://www.youtube.com/watch?v=yGVEd4CqmTM

The Reverse Address Resolution Protocol (RARP): allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time.

The Internet Control Message Protocol (ICMP): is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

https://www.youtube.com/watch?v=xdUqXYkIA-8

https://www.youtube.com/watch?v=xTqtm7-k25o

The Internet Group Message Protocol (IGMP): is used to facilitate the simultaneous transmission of a message to a group of recipients.

https://www.youtube.com/watch?v=aHcnT7dfst0

3. Transport Layer

The main protocols in transport layer are the TCP and UDP. IP protocol in network layer is a source-to-destination protocol, meaning that it can deliver a packet from one physical device to another. Weather, UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process (process-to-process protocols).

The User Datagram Protocol (UDP): is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

The Transmission Control Protocol (TCP): is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

The Stream Control Transmission Protocol (SCTP): provides support for newer applications such as voice over the Internet.

4. Application Layer

The application layer in TCP/IP is equivalent to the combined **session**, **presentation,** and **application layers** in the OSI model. Many protocols are defined at this layer.

3.2 Addressing

Four levels of addresses are used in an internet employing the TCP/IP protocols: **physical (link) addresses**, **logical (IP) addresses**, **port addresses**, and **specific addresses** (Figure 3.2).

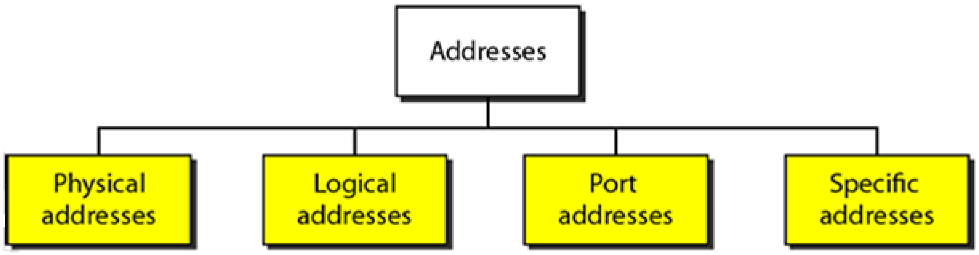


Figure (3-2): Addressing in TCP/IP

Each address is related to a specific layer in the TCP/IP architecture, as shown in Figure (3-3).

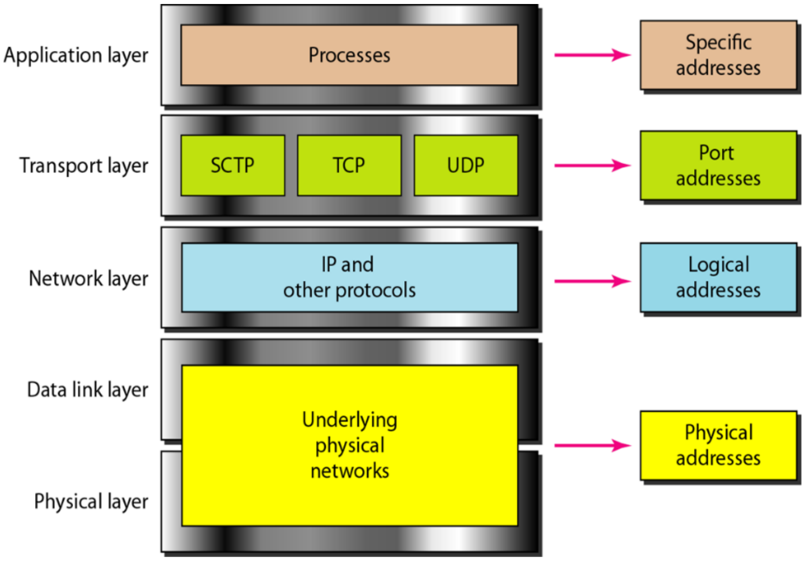


Figure (3-3): Relationship of layers and addresses in TCP/IP

3.2.1 Physical Addresses

The ***physical address***, also known as the *link address*, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address.

Example 1

In Figure (3.4 a) node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). At the *data link layer*, this frame contains physical (link) addresses in the header. These are the only addresses needed. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The trailer usually contains extra bits needed for error detection.

Encapsulation means that a packet (header, data and maybe trailer) at a specific level is encapsulated in one whole packet.

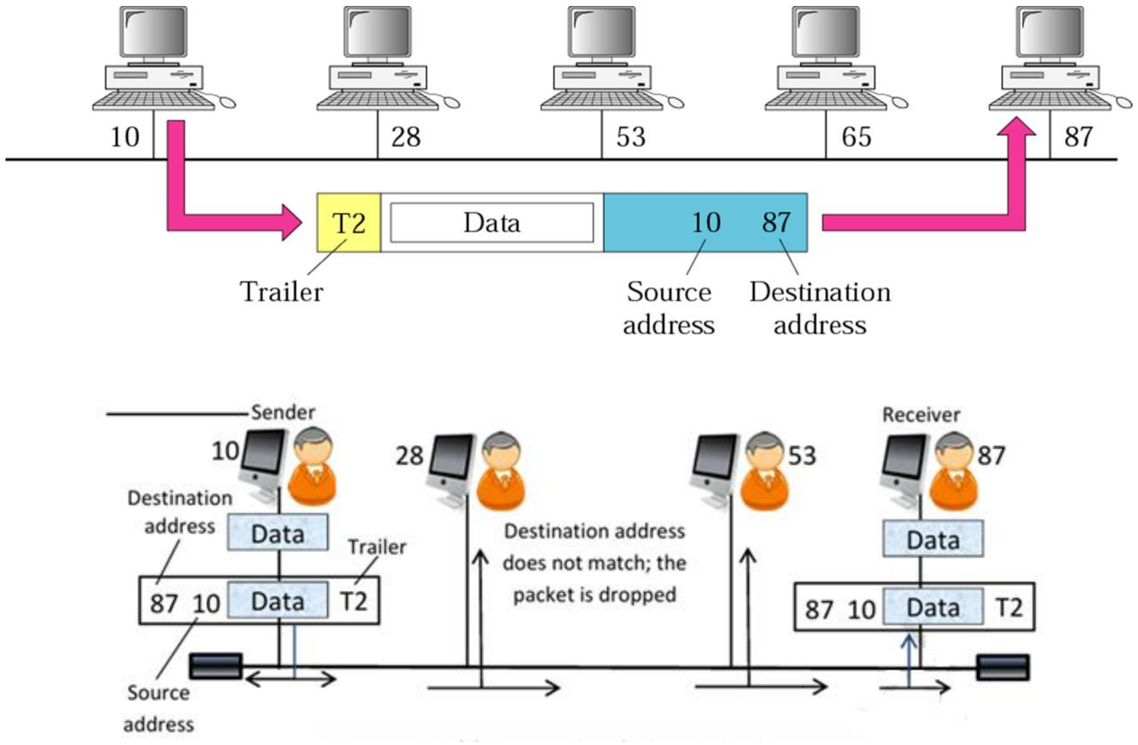


Figure (3-4 a): Example of physical address

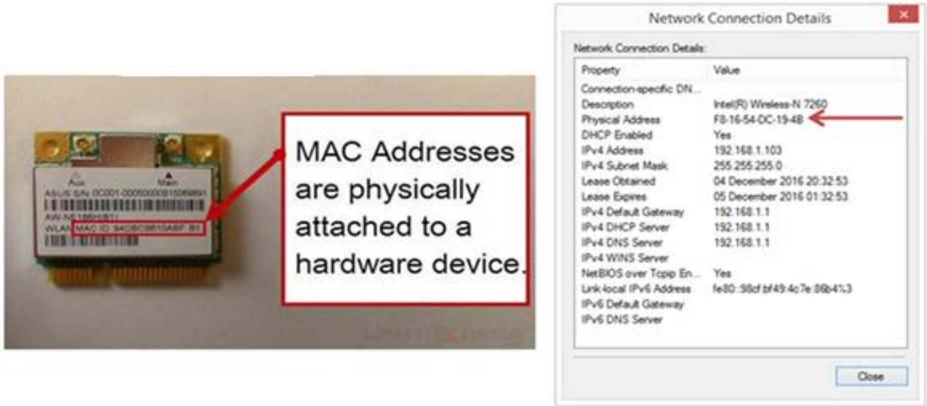
Example 2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every 2 bytes (hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

The **physical address** is imprinted on the network interface card (NIC) as shown in the left of Figure 3.4(b) and can be displayed on any computer as shown in the right.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Wireless-N 7260
Physical Address	F8-16-54-DC-19-4B
DHCP Enabled	Yes
IPv4 Address	192.168.1.103
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 December 2016 20:32:53
Lease Expires	05 December 2016 01:32:53
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::98cf:bf49:4c7e:86b4%3
IPv6 Default Gateway	
IPv6 DNS Server	

A screenshot that shows a physical address and other connection details

Figure (3-4b): Network interface card(NIC)

3.2.2 Logical Addresses

Physical addresses are not enough in an internetwork environment. A universal (or logical) addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.

A **logical address** in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed hosts on the Internet can have the same IP address.

192.168.1.100

IP (or logical) address, Version 4, Class C

Example 3

Figure 3.5 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical).

The computer with logical address **A** and **physical address 10** needs to send a packet to the computer with **logical address P** and **physical address 95**.

The sender encapsulates its data in a packet at the *network layer* and adds two logical addresses (A and P). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its **routing table** and finds the logical address of the next hop (router 1) to be F. The **ARP** finds the physical address of router 1 that corresponds to the logical address of 20. Now the network layer passes this address to the data link layer, which in turn encapsulates the packet with physical destination address 20 and physical source address 10.

Since the logical destination address does not match the router's logical address, the router 1 knows that the packet needs to be forwarded to router 2. When the frame reaches the destination, the packet is de-capsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer.

Note: Although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination (but there are some exceptions to this rule).

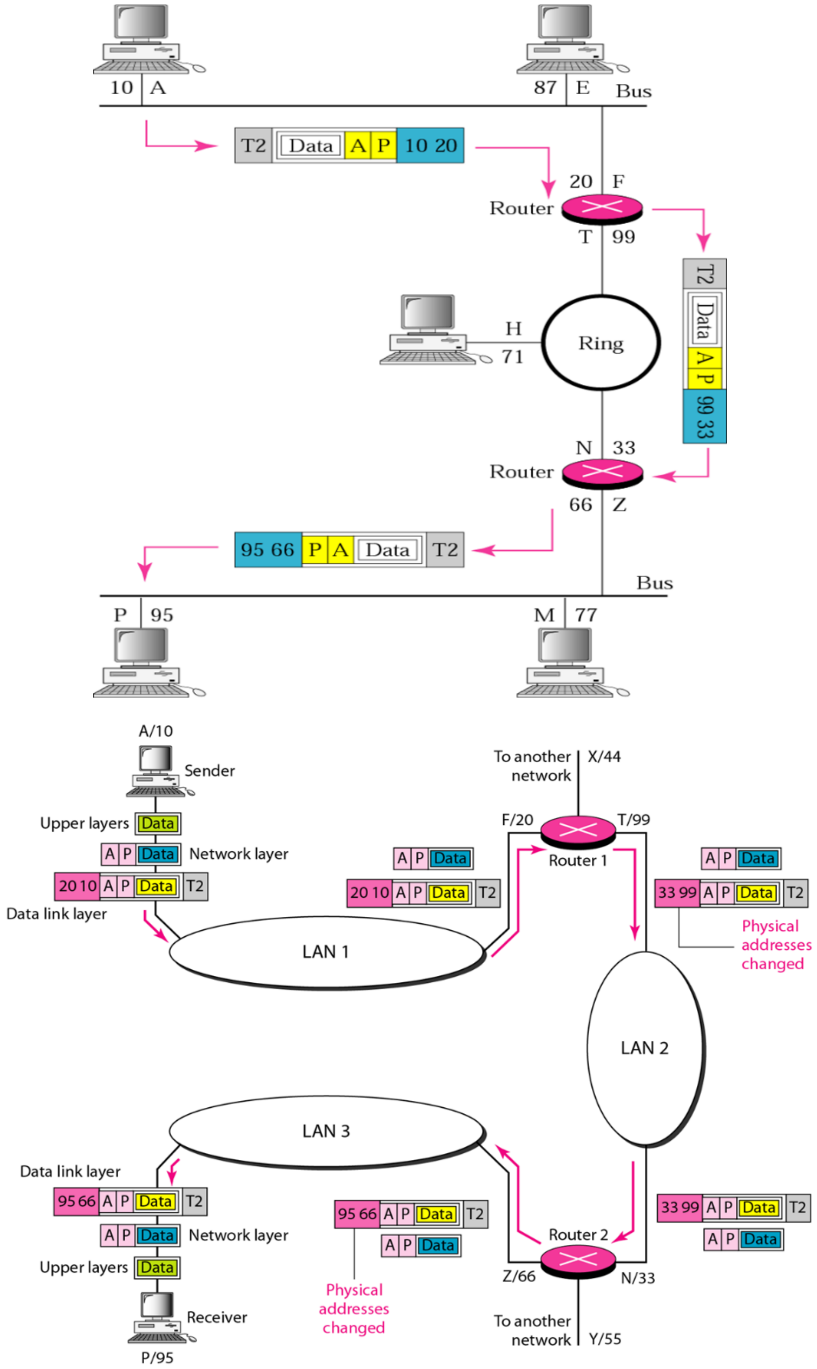


Figure (3-5): Logical IP address

3.2.3 Port Addresses

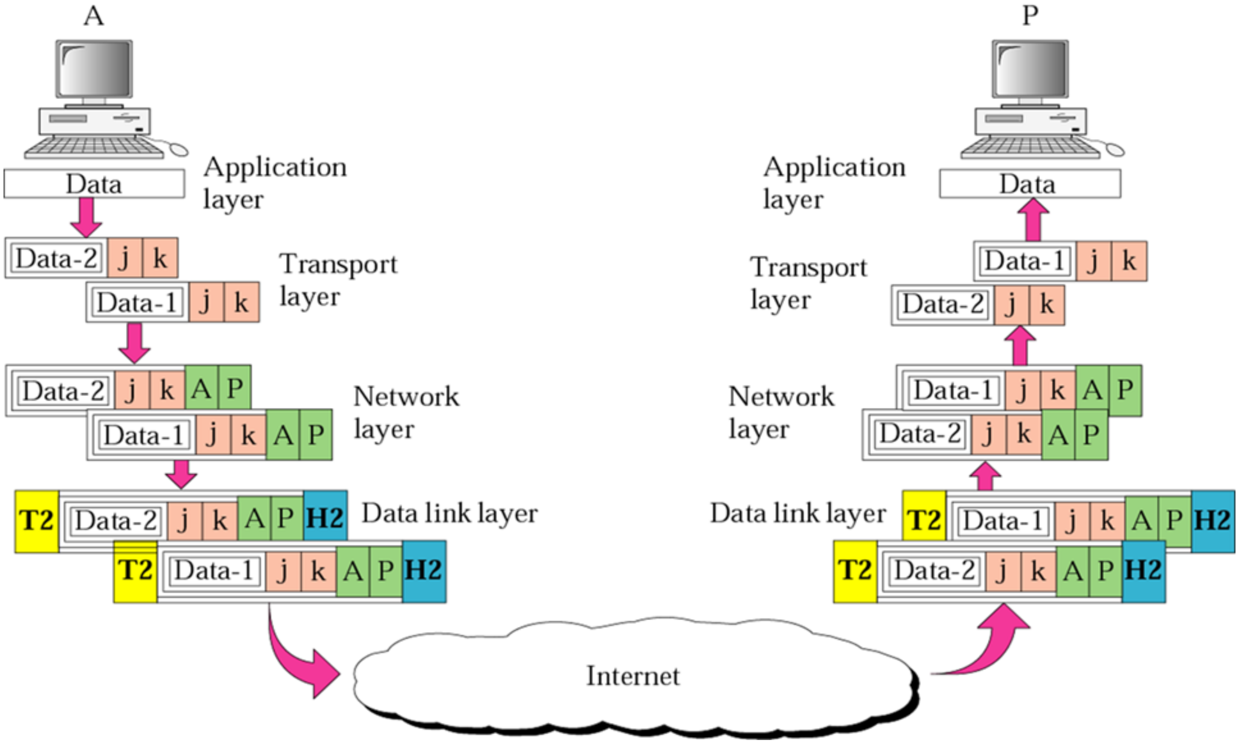
Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. Therefore, we need a method to label the different processes.

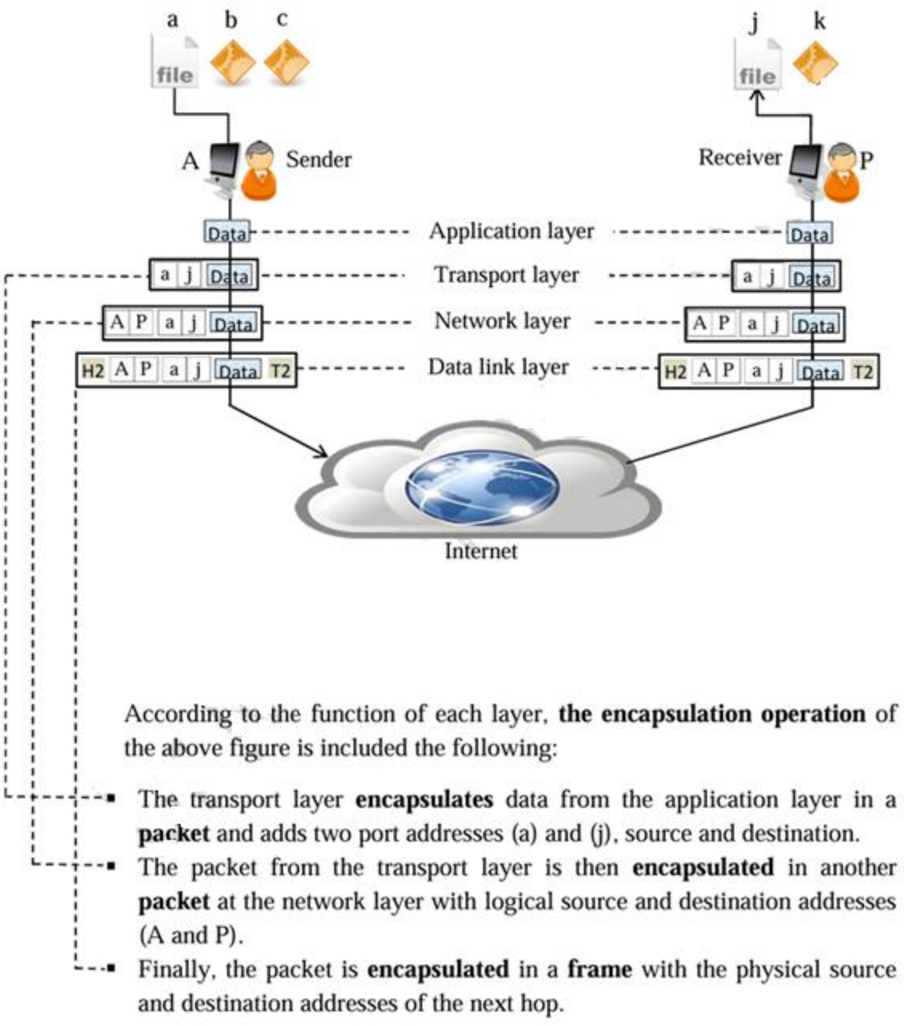
In the TCP/IP architecture, the label assigned to a process is called a port address. A **port address** in TCP/IP is 16 bits in length.

Example 4

Figure 3.6 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses (a), (b), and (c). The receiving computer is running two processes at this time with port addresses (j) and (k). Process (a) in the sending computer needs to communicate with process (j) in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a **client program** and the other is a **server program**.

Note: Although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination (there are some exceptions to this rule).





According to the function of each layer, **the encapsulation operation** of the above figure is included the following:

- The transport layer **encapsulates** data from the application layer in a **packet** and adds two port addresses (a) and (j), source and destination.
- The packet from the transport layer is then **encapsulated** in another **packet** at the network layer with logical source and destination addresses (A and P).
- Finally, the packet is **encapsulated** in a **frame** with the physical source and destination addresses of the next hop.

Figure (3-6): Port address

3.2.4 Specific Addresses

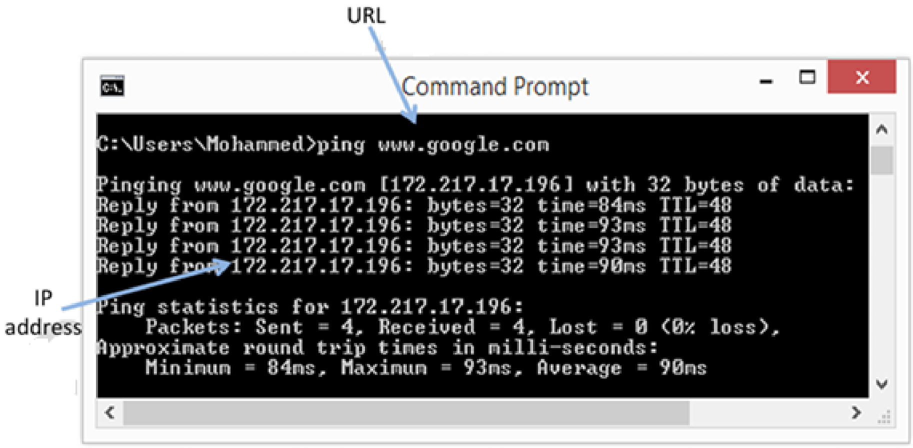
Some applications have user-friendly addresses that are designed for that specific address, for example:

- The e-mail address (for example, someone@gmail.com) that defines the recipient of an e-mail.
- Universal Resource Locator (**URL**) (for **example**, www.google.com) that is used to find a document on the World Wide Web (WWW).

The e-mail and URL addresses **are changed** automatically to the corresponding **port** and **logical addresses** by the sending computer (by **using the DNS**: Domain Name System).

For **example**, Figure 3.7 shows a screenshot of the command prompt window in which the 172.217.17.196 is the logical address of the URL address:

www.google.com.

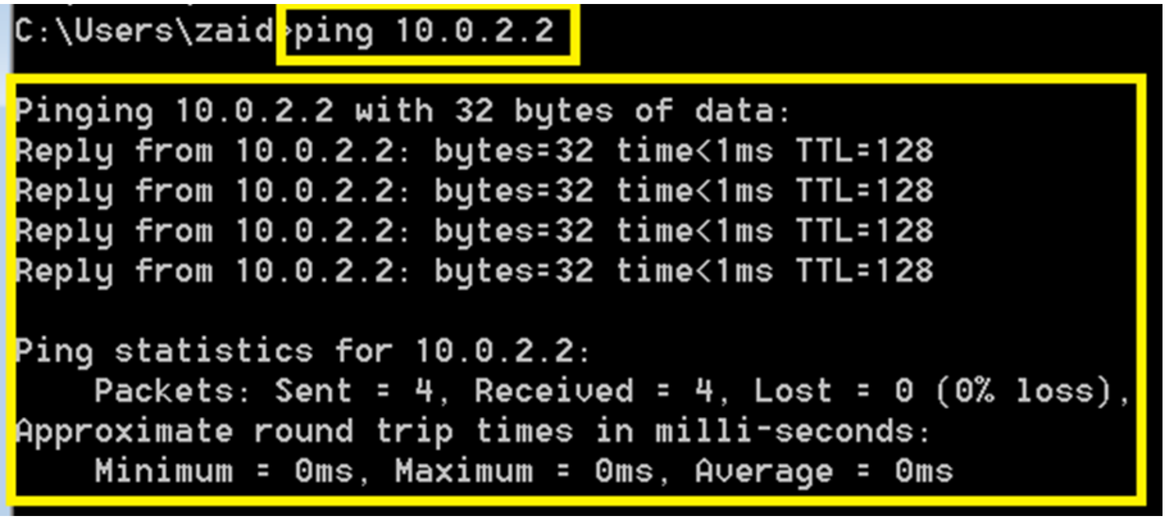


```
C:\Users\Mohammed>ping www.google.com

Pinging www.google.com [172.217.17.196] with 32 bytes of data:
Reply from 172.217.17.196: bytes=32 time=84ms TTL=48
Reply from 172.217.17.196: bytes=32 time=93ms TTL=48
Reply from 172.217.17.196: bytes=32 time=93ms TTL=48
Reply from 172.217.17.196: bytes=32 time=90ms TTL=48

Ping statistics for 172.217.17.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 84ms, Maximum = 93ms, Average = 90ms
```

Figure 3.7 Using **ping** instruction to know the corresponding IP address of www.google.com



```
C:\Users\zaid>ping 10.0.2.2

Pinging 10.0.2.2 with 32 bytes of data:
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Chapter Four
Data and Signals

4. Data and Signals

One of the major functions of the ***physical layer*** is to move data in the form of electromagnetic signals across a transmission medium. Generally, the data usable to a person or application are not in a form that can be transmitted over a network. For example, a photograph must first be changed to a form that transmission media can accept. Transmission media work by conducting energy along a physical path.

4.1 Analog and Digital Data

Data can be analog or digital. The term ***analog data*** refers to information that is continuous (sounds made by a human voice); ***digital data*** refers to information that has discrete states (data are stored in computer memory in the form of 0s and 1s).

Therefore, data can be analog or digital. Analog data are continuous and take continuous values. Digital data have discrete states and take discrete values.

4.2 Analog and Digital Signals

Signals can be either analog or digital. An *analog signal* has infinitely many levels of intensity over a period of time. A *digital signal* they have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

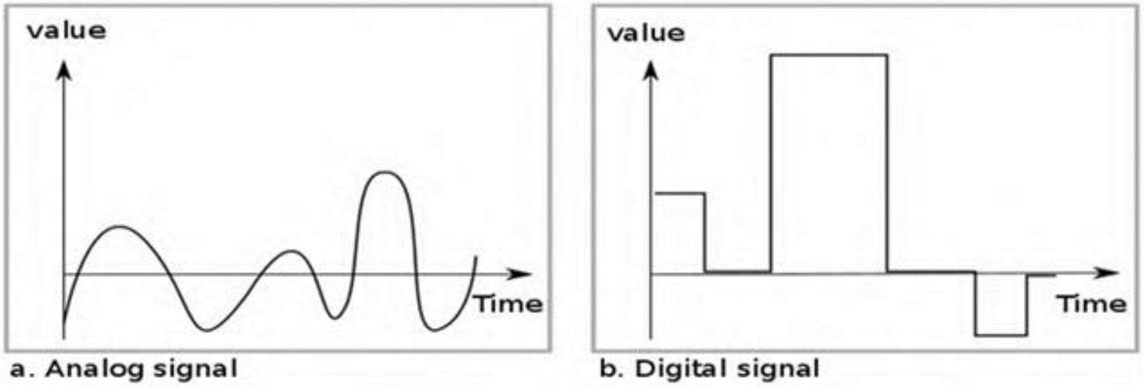


Figure (4-1): Illustrates an analog signal and a digital signal.

The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Therefore, Signals can be analog or digital. *Analog signals* can have an infinite number of values in a range; *digital signals* can have only a limited number of values.

Periodic and Non-Periodic Signals

A **periodic signal** completes a pattern within a measurable time frame, called a period, and repeats that pattern over identical periods. The completion of one full pattern is called a ***cycle***.

A **nonperiodic signal** changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic or nonperiodic.

In data communications (use both), we commonly use periodic analog signals (because they need less bandwidth (*maximum amount of data that can be transmitted over a network connection in a given period MBPS*)) and nonperiodic digital signals (because they can represent variation in data).

4.3 Periodic analog signals

As shown in Figure 4.2 periodic analog signals can be classified as simple or composite.

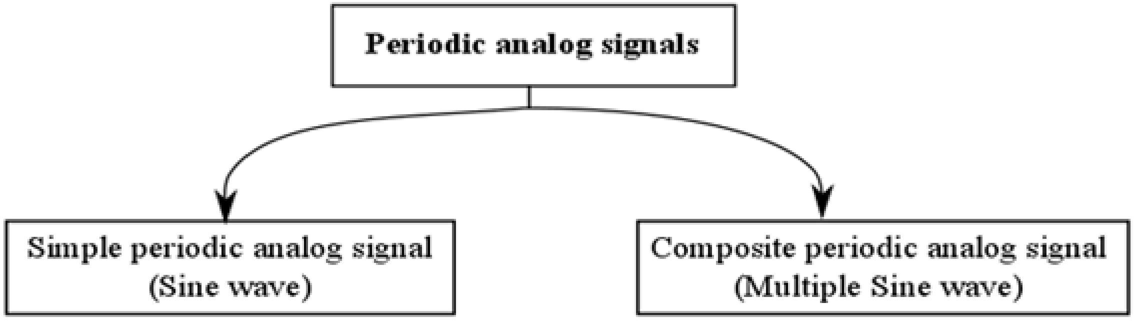

Periodic analog signals
Simple periodic analog signal
(Sine wave)
Composite periodic analog signal
(Multiple Sine wave)

Figure (4-2): Classification of periodic analog signals

4.3.1 Sine Wave

Figure 4.3 shows a sine wave; each cycle consists of a single arc above the time axis followed by a single arc below it. A sine wave can be represented by three parameters:

1) peak amplitude.
2) frequency.
3) phase.

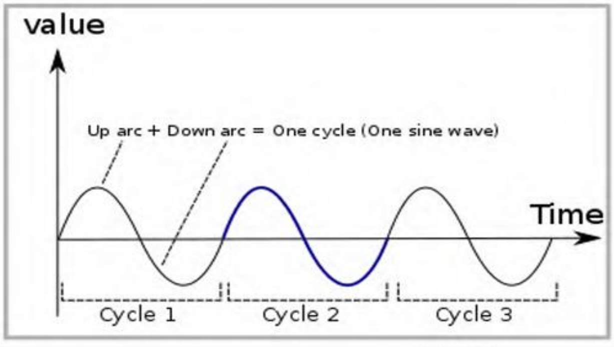


Figure (4-3): Sine wave

1) Peak amplitude

The ***amplitude*** of a signal is the absolute value of its intensity at time **t**. The ***peak amplitude*** of a signal is the absolute value of its highest intensity (the energy). The ***amplitude of a signal*** is proportional to the energy carried by the signal. Figure 4.4 shows two signals and their peak amplitudes. For electric signals, peak amplitude is normally measured in ***volts***. The power in your house can be represented by a sine wave with a peak amplitude of 220 to 240 V.

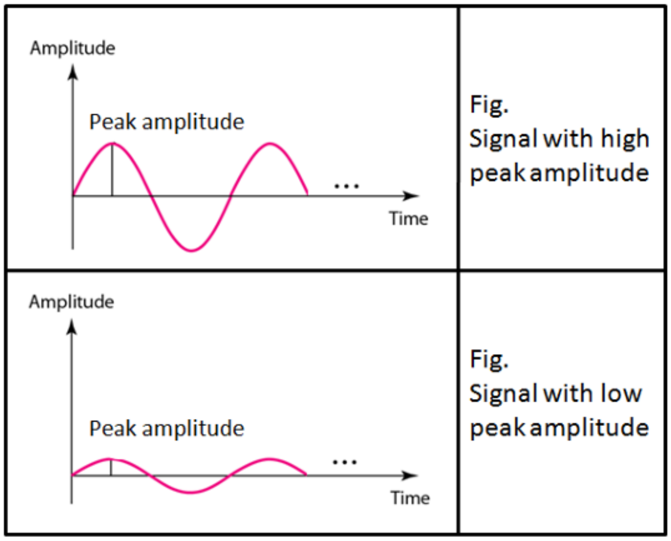


Figure (4-4): Amplitude of a sine wave with different amplitudes

2) Period and Frequency

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. ***Frequency*** refers to the number of cycles completed by the wave in *one second*. Figure (4-5) shows Frequency & Period of a sine wave. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period (i.e. inverse to each other) as the following formulas show.

f=1/T **OR** $T=1/f$

(f: frequency T: time)

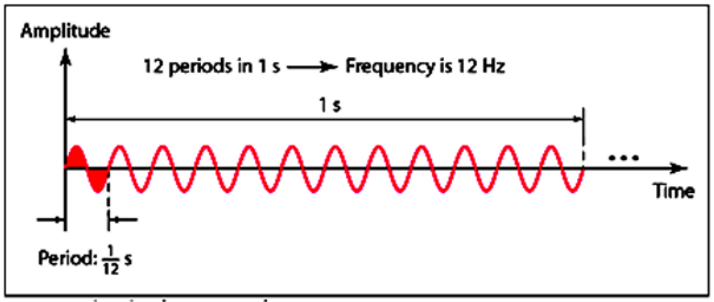


Figure (4-5): Frequency & Period of a sine wave

Period is formally expressed in seconds while the ***frequency*** is formally expressed in Hertz (Hz), which is *cycle per second*. Units of period and frequency are shown in Table 4.1.

Table 4.1 Period and frequency units

Unit	Equivalent	Unit	Equivalent
Seconds (s)	1s	Hertz	1Hz
Milliseconds (ms)	10^{-3} s	Kilohertz	10^{3} Hz
Microseconds (µs)	10^{-6} s	Megahertz	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz	10^{12} Hz

Units of period **Units of frequency**

Example 1

A wave has a frequency of 100 Hz. Its period(T) is given by:

$$T = 1/ F = 1/ 100 = 0.01 \text{ sec}$$

Example 2

The power we use at home has a frequency of 60 Hz. The period of this sine wave can be determined as follows:

$$T=1/f = 1/60 = 0.0166 \text{ s} = 0.0166 \times 10^{3} \text{ ms} = 16.6 \text{ ms}$$

This means that the period of the power for our lights at home is 0.0116 s, or16.6 ms. Our eyes are not sensitive enough to distinguish these rapid changes in amplitude.

Example 3

Express a period of 100 ms in microseconds.

Solution

From Table 4.1 we find the equivalents of 1 ms (1 ms is 10^{-3} s) and 1s (1 is 10^{6} µs). We make the following substitutions:

$$100 \text{ ms} = 100 \times 10^{-3} \times 106 \text{ µs} = 10^{2} \times 10^{-3} \times 10^{6} \text{ µs} = 10^{5} \text{ µs}$$

Example 4

The period of a signal is 100 ms. What is its frequency in kilohertz?

Solution

First we change 100 ms to seconds, and then we calculate the frequency from the period (1 Hz = 10^{-3} kHz).

$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 10^{-1} \text{ s}$
$f = 1/T$
$= 1/10^{-1} \text{ Hz} = 10 \text{ Hz} = 10 \times 10^{-3} \text{ kHz} = 10^{-2} \text{ kHz}$

3) Phase

The term **phase** describes the ***position*** of the waveform relative to time 0. It indicates the status of the ***first cycle*** (how much the wave is shifted from 0 on the time axis).

Looking at Figure 4.6, we can say that

1. A sine wave with a phase of 0° starts at time 0 with a zero amplitude.
The amplitude is increasing.

2. A sine wave with a phase of 90° starts at time 0 with a peak amplitude.
The amplitude is decreasing.

3. A sine wave with a phase of 180° starts at time 0 with a zero amplitude.
The amplitude is decreasing.

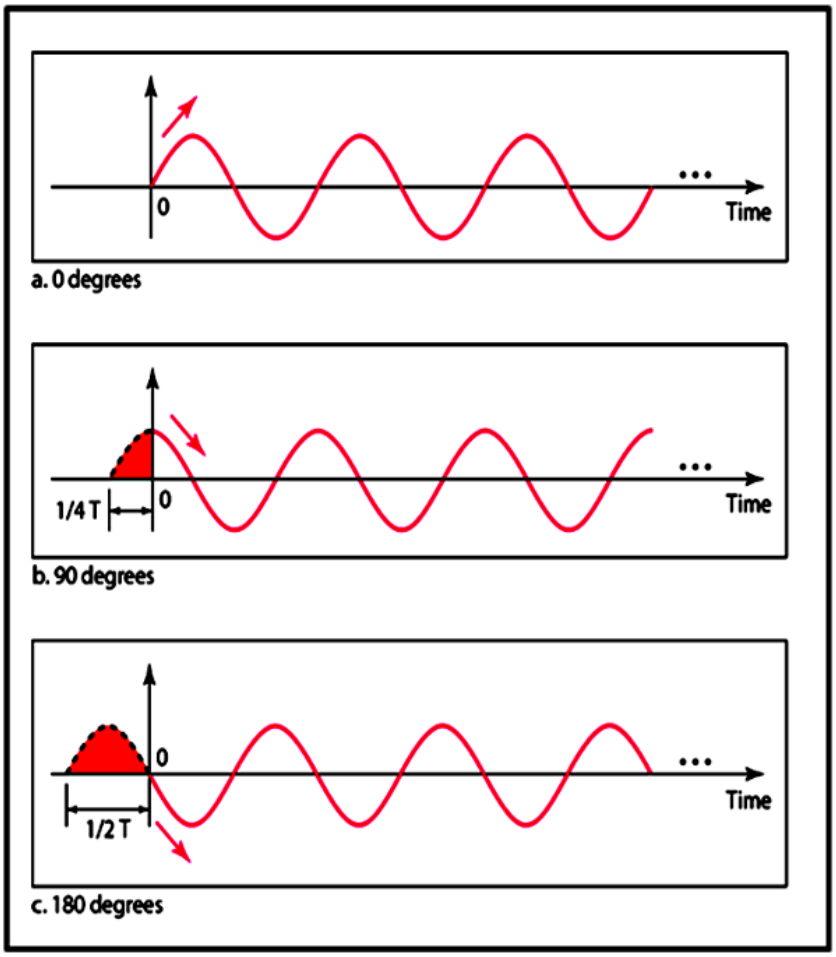
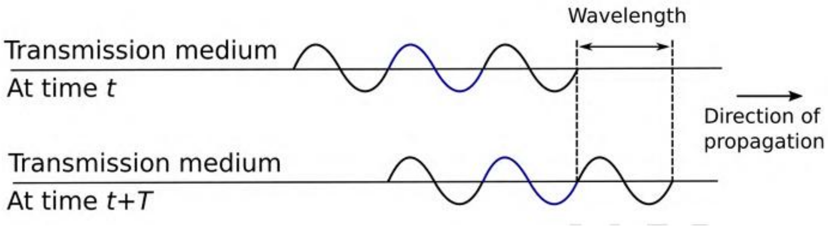


Figure (4-6): Phase of a sine wave with the same amplitude and frequency, but different phases

4) Wavelength

The wavelength of a signal refers to the ***relationship*** between frequency (or period) and propagation speed of the wave through a medium. The *wavelength* is the *distance a signal travels in one period*. (see Figure 4.7).



t = specific time (e.g., 11: 15 :40: 115) refers to a precise second and millisecond
T = Period (e.g., 100 ms). The duration of one complete cycle of a wave or signal. means that every (100) milliseconds, the signal repeats itself.

Figure (4-7): Wavelength and period

The wavelength is normally measured in micrometers (microns) instead of meters. For example, the wavelength of ***red light in air*** is 0.75 µs. But in a ***coaxial*** or ***fiber-optic*** cable the wavelength is shorter (0.5 µs) **because** the propagation speed in the cable is decreased.

4.3.2 Composite Signals

The previous section focused on simple sine waves which have many applications in daily life. We can send a single sine wave to carry electric energy from one place to another. For example, the power company sends a single sine wave with a frequency of 50 Hz to distribute electric energy to houses and businesses.

If we had only one single sine wave to convey يوصل a conversation over the phone, it would make no sense and carry no information. We would just hear a buzz ضجة. Therefore, we need to send a composite signal to communicate data; a single frequency sine wave is **not** useful in data communications.

The composite signal is a combination of simple sine waves with different frequencies, amplitudes سعات , and phases.

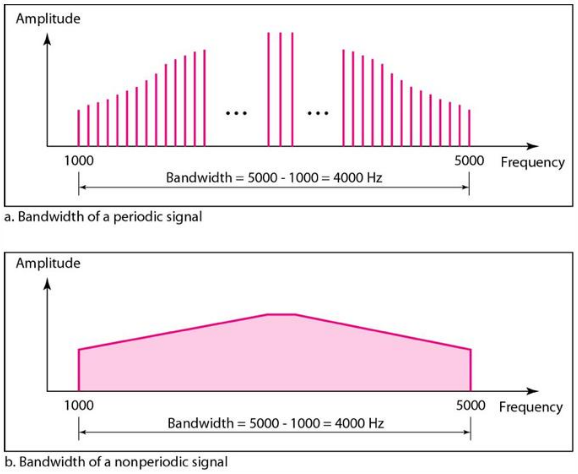
A composite signal can be periodic or non-periodic as shown in the following:

- **A periodic composite signal** can be decomposed into a series of simple sine waves with discrete frequencies (the frequencies that have integer values: 1, 2, 3, and so on).
- **A non-periodic composite signal** can be decomposed into a combination of an infinite number of simple sine waves with *continuous frequencies* (the frequencies that have real values: 0.1, 0.2, 0.3, and so on).

4.3.3 Bandwidth

Bandwidth is the range of frequencies contained in a composite signal. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000.

Figure 4.8 shows the concept of bandwidth. The bandwidth of the periodic signal contains all *integer* frequencies between 1000 and 5000 (1000, 1001, 1002, ...). The bandwidth of the **non-periodic** signals has the same range, but the *frequencies are continuous*.



a. Bandwidth of a periodic signal

b. Bandwidth of a nonperiodic signal

Figure (4-8): The bandwidth of periodic and non-periodic composite signals

Example

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth? Draw the spectrum نطاق, assuming all components have a **maximum amplitude** of 10 V.

Solution

Let ***fh*** be the highest frequency, ***fl*** the lowest frequency, and B the bandwidth.

Then: $B = fh - fl = 900 - 100 = 800$ Hz

The spectrum has only five spikes, at 100, 300, 500, 700, and 900 Hz (see Figure 4.9).

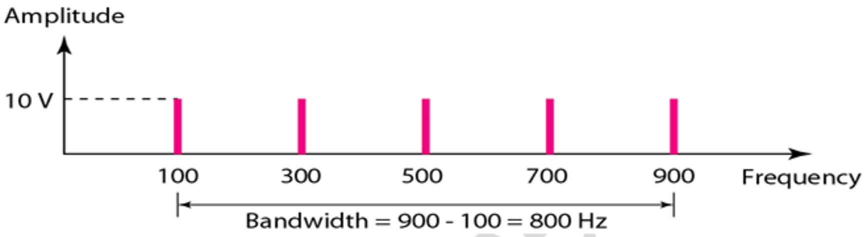


Figure (4-9): The bandwidth

Example

A periodic signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum if the signal contains all frequencies of the same amplitude.

Solution

Let ***fh*** be the highest frequency, ***fl*** the lowest frequency, and B the bandwidth.

Then: B = fh – fl → 20 = 60 – fl → fl = 60 – 20 = 40 Hz

The spectrum contains all integer frequencies. We show this by a series of spikes (see Figure 4.10).

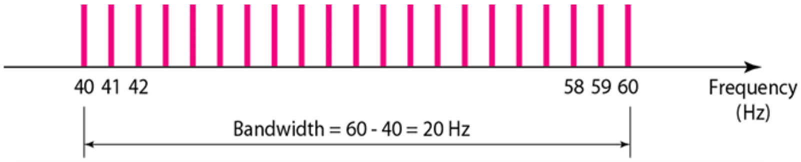
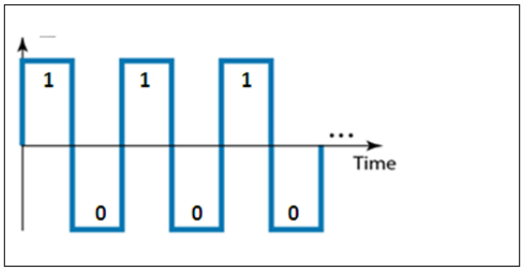


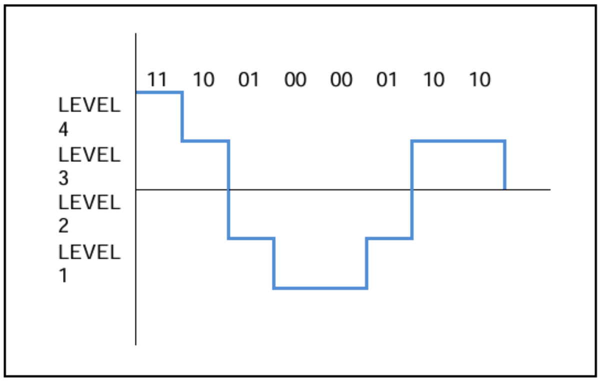
Figure (4-10): The bandwidth

Chapter Five
Digital Signals

5. Digital Signals

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a **1** can be encoded as a positive voltage and a **0** as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 5.1 shows two signals, one with two levels and the other with four. We send 1 bit per level in part (a) of the figure and 2 bits per level in part (b) of the figure.





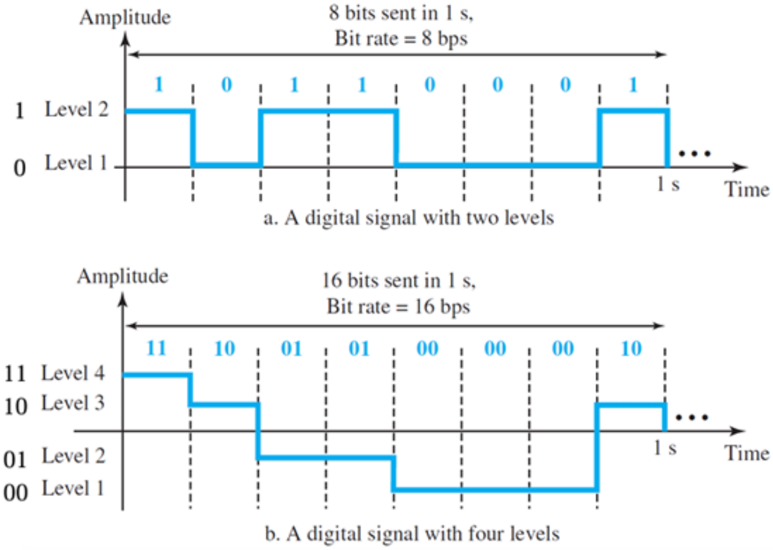
A digital signal with Two levels. „1" represented by a positive voltage and „0" represented by a negative voltage

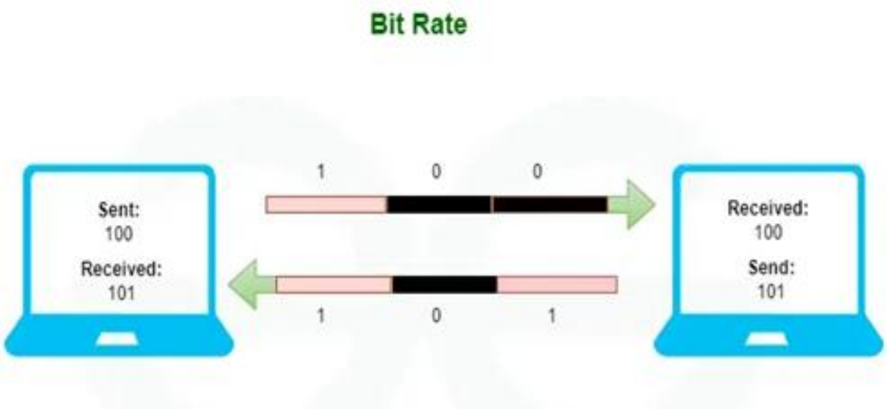
A digital signal with four levels

Figure (5-1): Shows two signals with different levels (2 and 4 levels)

5.1 Bit Rate

Most ***digital signals*** are non-periodic, and thus period and frequency are not appropriate characteristics. Another term—**bit rate** (instead of frequency)—is used to *describe digital signals*. The ***bit rate*** is the number of bits transmitted (sent) in 1s, expressed in bits per second (bps). Figure below shows the bit rate for two signals.





Example

Assume we need to download text documents at the rate of 100 pages per second. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

$$100 \times 24 \times 80 \times 8 = 1{,}536{,}000 \text{ bps} = 1.536 \text{ Mbps}$$

Example

A digitized voice channel is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?

Solution

The bit rate can be calculated as:

$2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}$

Example

What is the bit rate for high-definition TV (HDTV)?

Solution

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16:9 (in contrast to 4:3 for regular TV), which means the screen is wider. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel. We can calculate the bit rate as

$1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000 \approx 1.5 \text{ Gbps}$

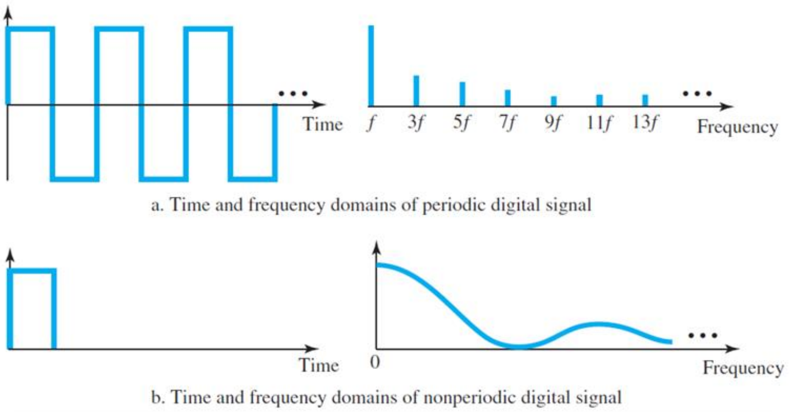
The TV stations reduce this rate to 20 to 40 Mbps through compression.

5.2 Digital Signal as a Composite Analog Signal

https://www.youtube.com/watch?v=07jkx-dZ2JM

Based on Fourier analysis, a digital signal is a composite analog signal with an infinite bandwidth. A ***digital signal***, in the time domain, comprises connected vertical and horizontal line segments as shown in Figure 5.2.

- A *vertical* line in the time domain means a *frequency of infinity* (sudden change in time);
- A *horizontal* line in the time domain means a *frequency of zero* (no change in time).

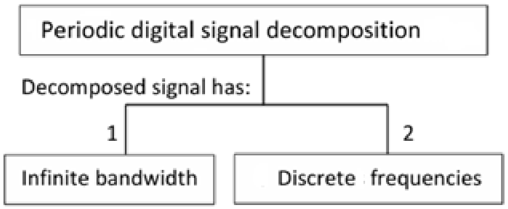


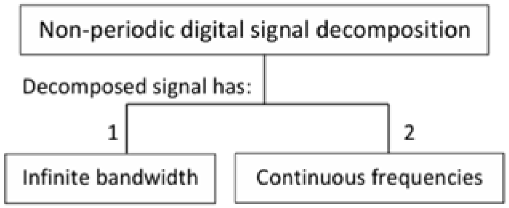
a. Time and frequency domains of periodic digital signal

b. Time and frequency domains of nonperiodic digital signal

Figure (5-2): The time and frequency domains of periodic and non-periodic digital signals

Fourier analysis can be used to decompose a digital signal as shown in the following characteristics:





Note that **both bandwidths** are infinite, but the *periodic signal* has *discrete frequencies* while the *non-periodic* signal has *continuous frequencies*.

5.3 Transmission of Digital Signals

We can transmit a digital signal from point A to point B by using one of two different approaches: **baseband transmission** or **broadband transmission** (using modulation).

For the remainder of this lecture, let us consider the case of a non-periodic digital signal because it is used often in data communications.

5.3.1 Baseband Transmission

Baseband transmission means *sending a digital signal over a channel* **without** changing the digital signal to an analog signal. Figure 5.3 shows baseband transmission.

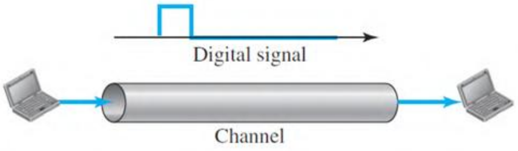


Figure (5-3): Baseband transmission

Baseband transmission requires a ***low-pass channel***, a channel with a bandwidth that starts from zero. This is the case if we have a dedicated medium with a bandwidth constituting only one channel. For example, the entire bandwidth of a cable connecting two computers is one single channel. As another example, we may connect several computers to a bus, but not allow more than two stations to communicate at a time.

5.3.2 Broadband Transmission (Using Modulation)

Broadband transmission or modulation means changing the digital signal to an analog signal for transmission. Modulation allows us to use a ***bandpass channel***—a channel with a bandwidth that does not start from zero. This type of channel is more available than a low-pass channel. Figure 5.4 shows a bandpass channel.

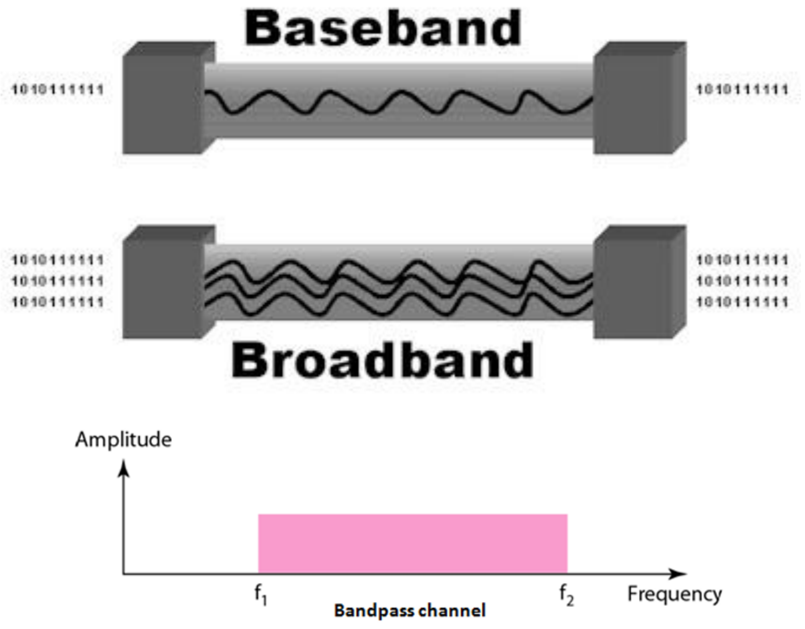


Figure (5-4): Bandpass channel

Figure 5.5 shows the ***modulation of a digital signal***. In the figure, a digital signal is converted to a composite analog signal. We have used a single frequency analog signal (called a ***carrier***); the amplitude of the carrier has been changed to look like the digital signal. The result, however, is not a single frequency signal; it is a composite signal. At the receiver, the received analog signal is converted to digital, and the result is a replica of what has been sent.

If the available channel is a ***bandpass channel***, we cannot send the digital signal directly to the channel; we ***need to convert the digital signal*** to an analog signal before transmission.

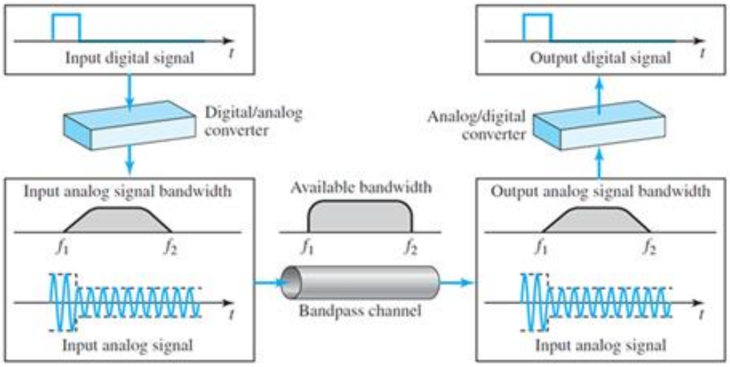


Figure (5-5): Modulation of a digital signal for transmission on a bandpass

Example

An example of broadband transmission ***using modulation*** is the sending of computer data through a telephone lines. The digital signal in the computer is converted to an analog signal, and then sending the analog signal. At the sending and receiving ends we can install two converters to change the digital signal to analog and vice versa. The converter, in this case, is called a **modem** (***mod***ulator/***dem***odulator).

Example

For better reception, the **digital cellular phones** convert the analog audio signal to digital and then convert it again to analog for transmission over a bandpass channel.

Analog audio signal → digital → analog $\xrightarrow{\text{transmission}}$

5.4 Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection **causes signal impairment**. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium (what is sent is not what is received). The causes of impairment are attenuation, distortion, and noise (see Figure 5.6).

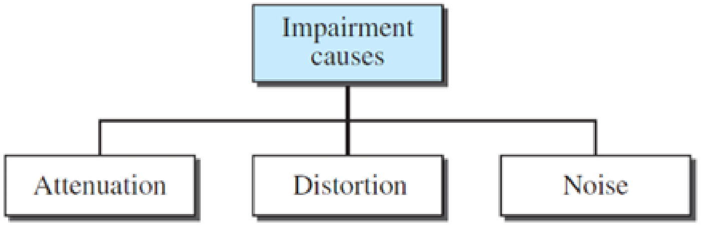


Figure (5-6): Causes of impairment

5.4.1 Attenuation

Attenuation means a *loss of energy*. As signal travels through the medium, its strength decreases as distance increases. As the distance increases attenuation also increases. When a signal (simple or composite) travels through a medium, it loses some of its energy. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To recover this loss, ***amplifiers*** are used to amplify the signal. Figure 5.7 shows the effect of attenuation and amplification.

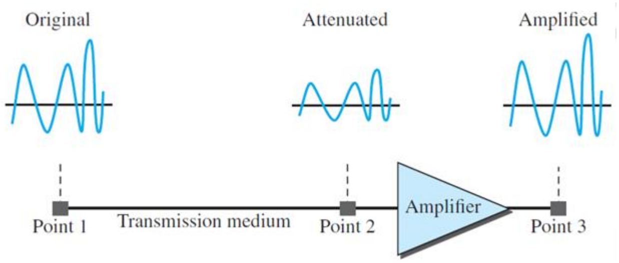


Figure (5-7): Attenuation and amplification

Decibel

To show that a signal has lost or gained strength, engineers use the unit of the **decibel**. The ***decibel*** (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is ***negative*** if a signal is attenuated and ***positive*** if a signal is amplified.

$$\text{dB} = 10 \log_{10} P2/\ P1$$

Variables P1 and P2 are the powers of a signal at points 1 and 2.

The $\log_{10}$ means the logarithm to base 10, which is called the common logarithm or the decimal logarithm.

Example

Suppose a signal travels through a transmission medium and its power is reduced to one-half. This means that P2 = 1/ 2 P1. In this case, the attenuation (loss of power) can be calculated as:

$$10 \log_{10} P2/P1=10 \log_{10} (0.5P1/P1)=10 \log_{10} 0.5=10(-0.3)= -3 \text{ dB}$$

Example

A signal travels through an amplifier, and its power is increased 10 times. This means that P2 = 10P1. In this case, the amplification (gain of power) can be calculated as:

$$\mathbf{10\ log_{10}\ P2/P1=10\ log_{10}\ (10P1/P1)=10\ log_{10}\ 10=10(1)=\ 10\ dB}$$

5.4.2 Distortion

Distortion means that the ***signal changes*** its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. So it is important to have a space (guard space) between the different frequencies. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration (see Figure 5.8).

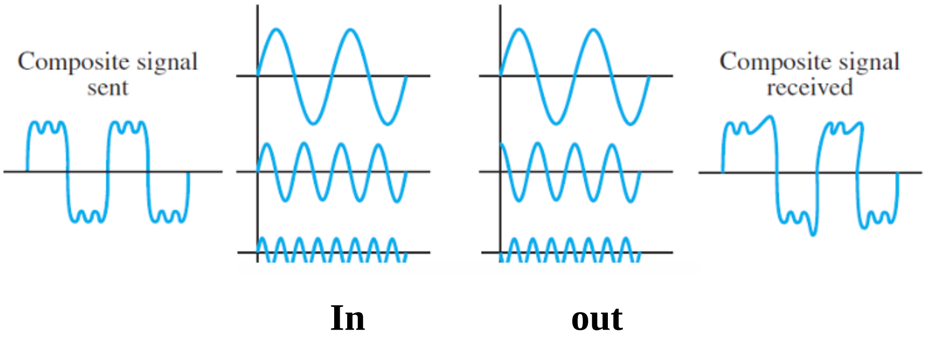


Figure (5-8): Distortion

5.4.3 Noise

Noise is another cause of impairment. **Noise** is defined as an ***unwanted data***. Several types of noise, such as ***thermal noise***, ***induced noise, crosstalk***, and ***impulse noise***, may corrupt the signal. Due to Noise it is difficult to retrieve the original data or information.

- **Thermal noise** is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter.
- **Induced noise** comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.
- **Crosstalk** is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- **Impulse noise** is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

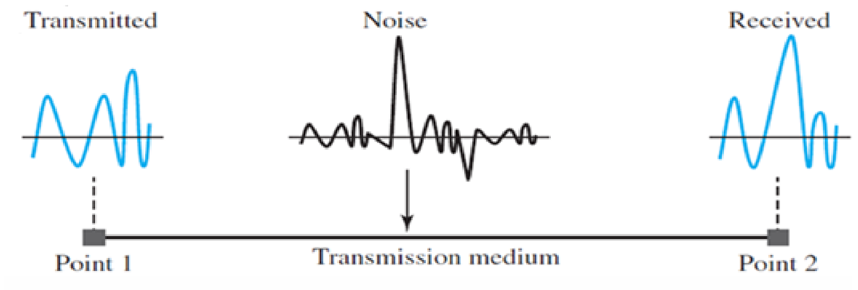


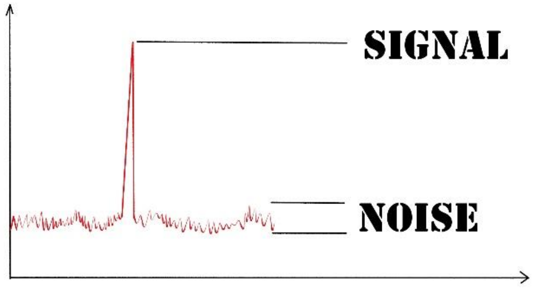
Figure (5-9): Shows the effect of noise on a signal

Signal-to-Noise Ratio (SNR)

The signal-to-noise ratio is defined as:

$$\text{SNR}= \frac{\text{average signal power}}{\text{average noise power}}$$

We need to consider the average signal power and the average noise power because these may change with time. Figure 5.10 shows the idea of SNR.



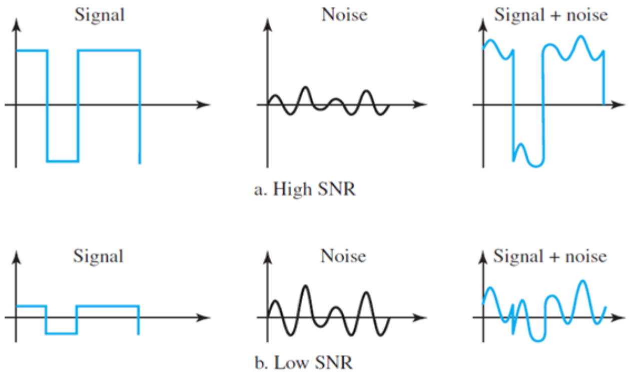


Figure (5-10): Two cases of SNR: a high SNR and a low SNR

SNR is actually the ratio of what is wanted (signal) to what is **not** wanted (noise). A **high SNR** means the signal is less corrupted by noise; a **low SNR** means the signal is more corrupted by noise.

In other words: The higher the SNR value, the better the output. The reason is that there's more useful information (signal) than unwanted data (noise) in a high SNR output. For instance, an SNR of 100dB is better than 70 dB.

Because SNR is the ratio of two powers, it is often described in ***decibel*** units, SNRdB, defined as

$$\mathrm{SNR}_{\mathrm{dB}} = 10\ \mathbf{log_{10}}\ \boldsymbol{SNR}$$

Example

The power of a signal is 10 mW and the power of the noise is 1 µW; what are the values of SNR and $\mathrm{SNR}_{\mathrm{dB}}$?

Solution

The values of SNR and $\mathrm{SNR}_{\mathrm{dB}}$ can be calculated as follows:

The units must be the same for the calculation. The signal power is converted to microwatts.

$$10\mathrm{mW}\times10\times10^{3}\ \mu\mathrm{W} = 10{,}000\ \mu\mathrm{W}$$

$$\mathbf{SNR = (10{,}000\ \mu W) / (1\ \mu W) = 10{,}000}$$

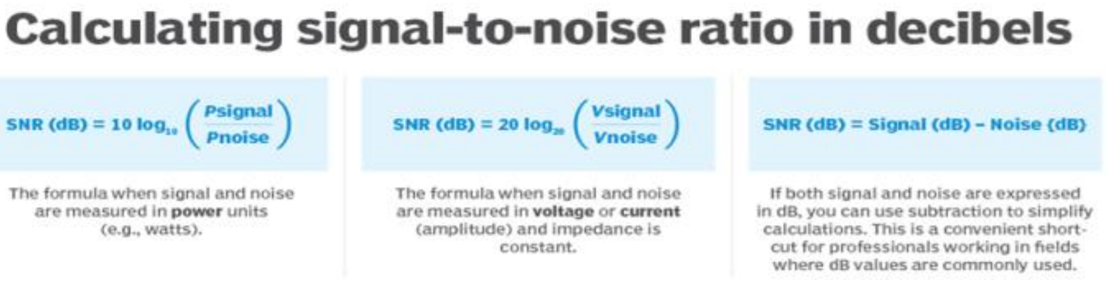
$$\mathbf{SNR_{dB} = 10\ log_{10}\ 10{,}000\ \ =\ \ 10\ log_{10}\ 10^{4}\ = 40\ dB}$$

Example

The values of SNR and $\mathrm{SNR}_{\mathrm{dB}}$ for a noiseless channel are

$$\mathbf{SNR = (signal\ power)/0} = \infty \quad \rightarrow \quad \mathbf{SNR_{db} = 10\ log_{10}} \infty = \infty$$

We can never achieve this ratio in real life; it is an ideal.



Calculating signal-to-noise ratio in decibels

$\mathrm{SNR\ (dB)} = 10 \log_{10}\left(\frac{Psignal}{Pnoise}\right)$

The formula when signal and noise are measured in **power** units (e.g., watts).

$\mathrm{SNR\ (dB)} = 20 \log_{20}\left(\frac{Vsignal}{Vnoise}\right)$

The formula when signal and noise are measured in **voltage** or **current** (amplitude) and impedance is constant.

SNR (dB) = Signal (dB) – Noise (dB)

If both signal and noise are expressed in dB, you can use subtraction to simplify calculations. This is a convenient short-cut for professionals working in fields where dB values are commonly used.

Chapter Six

Network Performance

6. Network Performance

In previous sections, we have discussed the tools of transmitting data (signals) over a network and how the data behave. In this section we discuss ***quality of service***, an overall measurement of network performance.

6.1 Bandwidth

One characteristic that measures network performance is ***bandwidth*** (the maximum amount of data that can be transmitted over a network connection in a given amount of time (bps)). However, the term can be used in two different contexts with two different measuring values: 1) bandwidth in *hertz* and 2) bandwidth in *bits per second*.

1) Bandwidth in Hertz

Analog signal bandwidth is measured in terms of its frequency (hz). For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

2) Bandwidth in Bits per Seconds

digital signal bandwidth is measured in terms of bit rate (bits per second, bps). The term bandwidth can refer to the number of bits per second that a channel or a network can transmit. For example, the bandwidth of an Ethernet network (or the links in this network) is a maximum of 100 Mbps.

Relationship

There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per second. Basically, an ***increase in bandwidth in hertz*** means an ***increase in bandwidth in bits per second***. The relationship depends on whether we have baseband transmission or transmission with modulation. In networking, we use the term bandwidth in two contexts.

- ➢ The first, bandwidth in ***hertz***, refers to the range of *frequencies* in a composite signal or the range of frequencies that a channel can pass.

- ➢ The second, bandwidth in ***bits per second***, refers to the *speed* of bit transmission in a channel or link.

Example 1

The bandwidth of a subscriber line is 4 kHz for voice or data. The bandwidth of this line for data transmission can be up to 56,000 bps using a sophisticated modem to change the digital signal to analog (modulation).

Example

If the telephone company improves the quality of the line and increases the bandwidth to 8 kHz, we can send 112,000 bps by using the same technology as mentioned in Example 1.

Therefore, an increase in bandwidth in hertz means an increase in bandwidth in bits per second.

6.2 Throughput

The throughput is a ***measure*** of *how fast we can actually send data through a network*. The bandwidth in bits per second and throughput are different. For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Imagine a highway designed to transmit 1000 cars per minute from one point to another. However, if there is problem on the road, this number may be reduced to 100 cars per minute. The **bandwidth** is 1000 cars per minute; the **throughput** is 100 cars per minute.

Example

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

The ***throughput*** is almost one-fifth of the ***bandwidth*** in this case.

6.3 Latency (Delay)

The **latency** or delay defines how long it takes for an entire message to completely arrive at the destination. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

❖ Propagation Time

Propagation time ***measures*** the time required for a **bit** to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance / (Propagation Speed)

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal. For example, in a vacuum, light is propagated with a speed of 3 × 108 m/s. It is lower in air; it is much lower in cable.

Example

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution

We can calculate the propagation time as

Propagation time = $(12{,}000 \times 1000) / (2.4 \times 10^8)$

$= 0.05 \text{ s} \times 10^3 = 50 \text{ ms}$

The example shows that a bit can go in only 50 ms: if there is a direct cable between the source and the destination.

❖ Transmission Time

In data communications we don’t send just 1 bit, we send a message. The *transmission time* of a message *depends* on the size of the message and the bandwidth of the channel.

Transmission time = (Message size) / Bandwidth

Example

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission time as

Propagation time = $(12{,}000 \times 1000) / (2.4 \times 10^8) = 50$ ms (dominant factor)

Transmission time = $(2500 \times 8) / 10^9 = 0.00002$ s = 0.02 ms

Note that in this case, because the message is short and the bandwidth is high, the ***dominant factor** is the propagation time*, not the *transmission time*. The transmission time can be ignored.

Example

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission times as

Propagation time = (12,000 × 1000) / (2.4 × 10^8) = 50 ms
Transmission time = (5,000,000 × 8) /10^6 = 40 s (dominant factor)

Note that in this case, because the message is very long and the bandwidth is not very high, the dominant factor is the transmission time, not the propagation time. The propagation time can be ignored.

6.4 Jitter

Another performance issue that is related to delay is ***jitter***. We can say that the jitter problem is happened because:

1. Different packets of data encounter different delays.
2. The application using the data at the receiver site is time-sensitive (audio and video data, for example).

For example, if the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets will make jitter.

6.5 Transmission Media

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. Figure 6.1 shows the position of transmission media in relation to the physical layer.

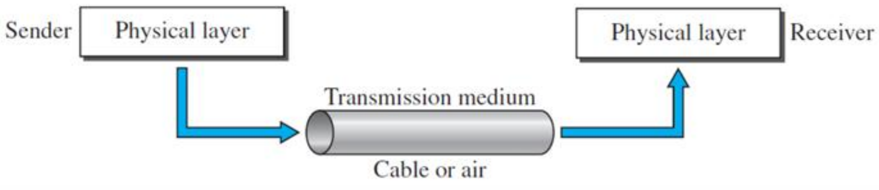


Figure (6-1): Transmission medium and physical layer

A ***transmission medium*** can be defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air.

In ***data communications*** the transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

In ***telecommunications,*** transmission media can be divided into two broad categories: guided and unguided. *Guided media* include twisted-pair cable, coaxial cable, and fiber-optic cable. *Unguided medium* is free space. Figure 6.2 shows this taxonomy.

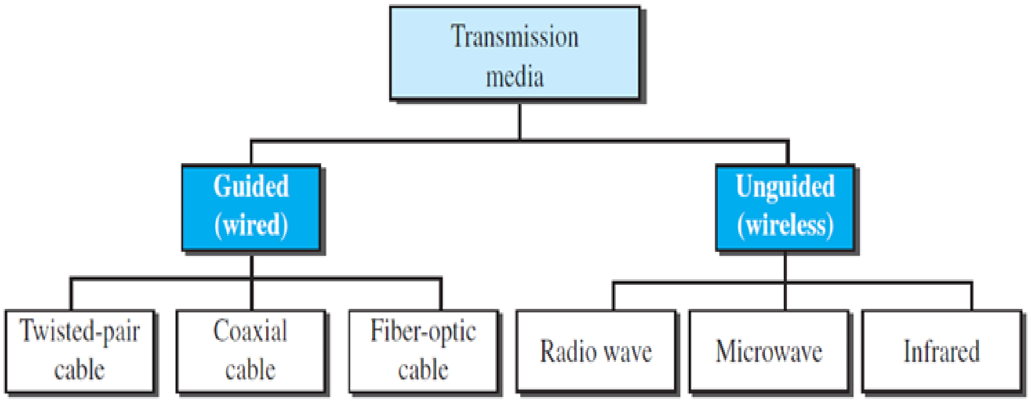


Figure (6-2): Classes of transmission media

6.5.1 Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure 6.3.

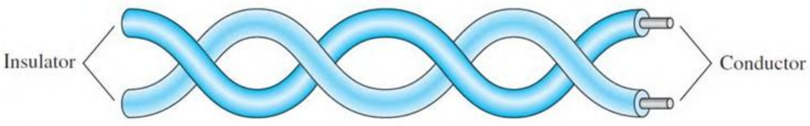


Figure (6-3): Twisted-pair cable

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Twisting makes it probable that both wires are ***equally affected*** by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly cancelled out. The ***number of twists*** per unit of length (e.g., inch) has some effect on the ***quality*** of the cable (more twists → more quality).

6.5.1.1 Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Figure 6.4 shows the difference between UTP and STP.

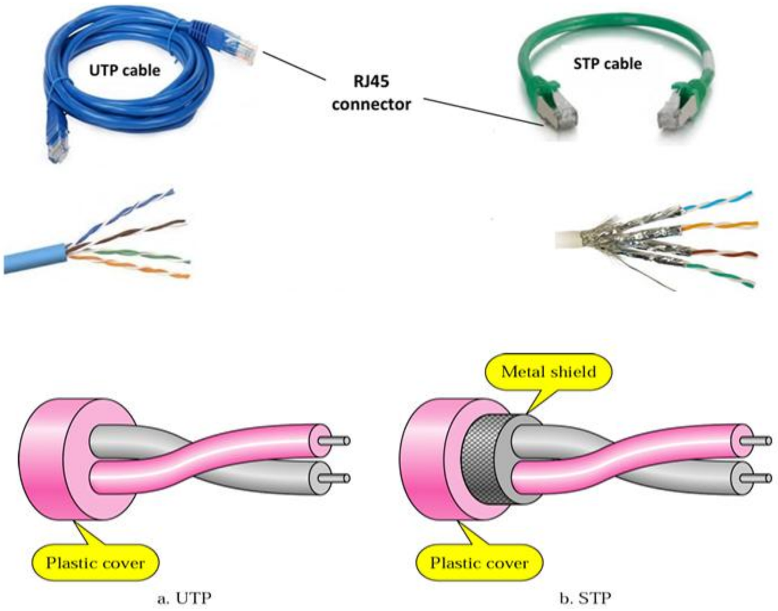


Figure (6-4): UTP and STP

6.5.1.2 Categories

Twisted-pair cables are classified into seven categories. These categories are determined by cable quality, for example:

1. **Category 1** (Cat 1) Unshielded twisted-pair used in *telephone*.
2. **Category 5** (Cat 5) Unshielded twisted-pair used in LANs with 100 Mbps data rate.
3. **Category 6** (Cat 6) A new category that must be tested at a 200-Mbps data rate.
4. **Category 7** Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a metallic foil. The data rate is 600 Mbps.

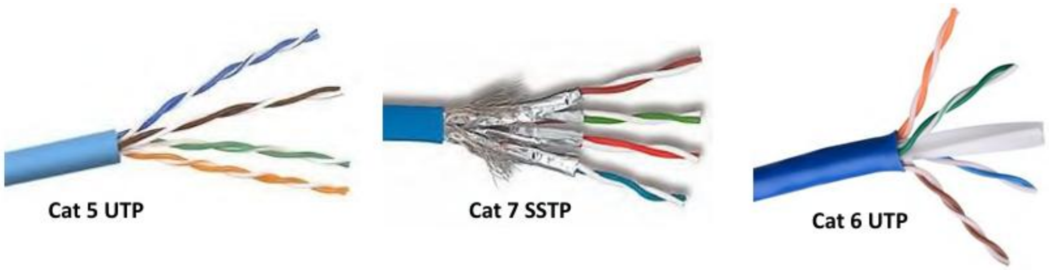


Figure 6.4 UTP and STP cables UTP cable STP cable RJ45 connector

6.5.2 Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. Instead of having two wires, coax has an ***inner core conductor*** of solid wire (usually copper) and ***outer conductor*** serves both as a shield against noise and as the second conductor to complete the circuit (see Figure 6.5).

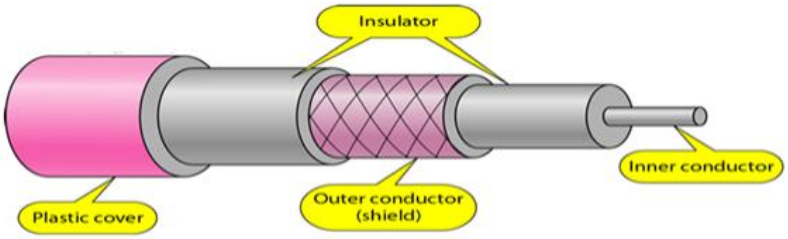


Figure (6-5): Coaxial cable

6.5.2.1 Coaxial Cable Standards

Coaxial cables are categorized by their Radio Government (**RG**) ratings. Each RG number denotes a unique set of *physical specifications*, such as the wire gauge of the inner conductor, the thickness and type of the inner insulator. Each cable defined by an RG rating is adapted for a specialized function, as shown in the following table.

Category of coaxial cable

Category	Impedance	Use
RG-59	75Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

RG-59 cable and connectors

RG-58 cable and connectors

RG-11 cable and connectors

6.5.2.2 Coaxial cable applications

Coaxial cables are mainly used in the following:

1. **Telephone networks**. Coaxial cable was widely used in telephone networks. However, coaxial cable has largely been replaced today with fiber optic cable.

2. **Cable TV networks**. Coaxial cable was widely used in the traditional cable TV network. Later, however, cable TV providers replaced most of the media with fiber-optic cable.

3. **Ethernet LANs**. The 10Base-2 uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m. The ***10Base5*** uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m.

6.5.3 Fiber-Optic Cable

A fiber-optic cable is made of glass (or plastic) and transmits signals in the form of light. The difference in density of the glass and cladding must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it, as shown in Figure 6.6.

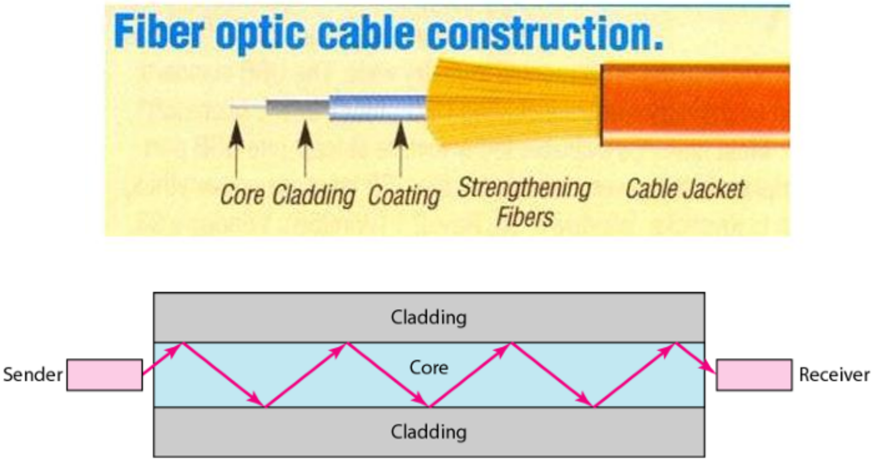


Figure (6-6): Optical fiber

6.5.3.1 Cable Composition

Figure 6.7 shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

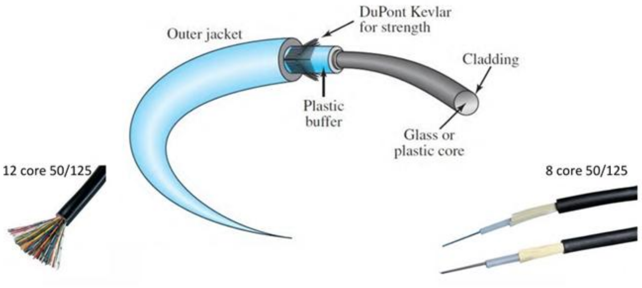


Figure (6-7): Fiber construction

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding both expressed in micrometers (for example 50/125μm or 100/125μm).

6.5.3.2 Fiber-optic applications

1. **Backbone networks**. Fiber-optic cable is often found in backbone networks (central large networks) because its wide bandwidth is cost effective (with data rate of 1600 Gbps).

2. **Cable TV networks**. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.

3. **Ethernet LANs**. Local-area networks such as 100Base-FX network (**Fast Ethernet**) and 1000Base-X also use fiber-optic cable.

6.5.3.3 Advantages of Optical Fiber

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- **Higher bandwidth**. Fiber-optic cable can support higher bandwidths (and hence data rates) than either cables. Bandwidth utilization are limited not by the fiber-optic cable but by the *signal generation and reception technology* available at LAN cards, switches, routers, etc.
- **Less signal attenuation**. A signal can run for 50 km without requiring regeneration.
- **No noise**. Electromagnetic noise cannot affect fiber-optic cables.
- **Resistance to corrosiveness التاكل**. Glass is more resistant to corrosive materials than copper.
- **Light weight**. Fiber-optic cables are much lighter than copper cables.

6.5.3.4 Disadvantages of Optical Fiber

- **Installation and maintenance**. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation**. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost**. The cable and the interfaces are relatively more expensive than those of other copper media.

UNGUIDED MEDIA: WIRELESS

Unguided medium transport electromagnetic waves without using a physical conductor, signals are normally broadcast through free space and thus are available to anyone. Figure 6.8 shows the part of the electromagnetic spectru نطاق, ranging from 3 kHz to 900 THz, used for wireless communication (Unguided medium).

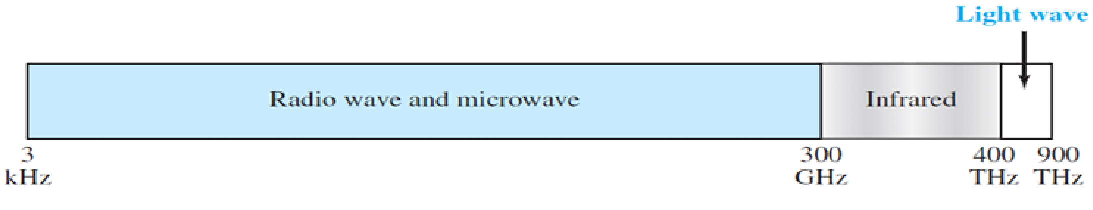


Figure (6-8): Electromagnetic spectrum for wireless communication

Unguided signals can travel from the source to the destination in several ways: ***ground propagation***, ***sky propagation***, and ***line-of-sight propagation*****خط البصر**, as shown in Figure 6.9.

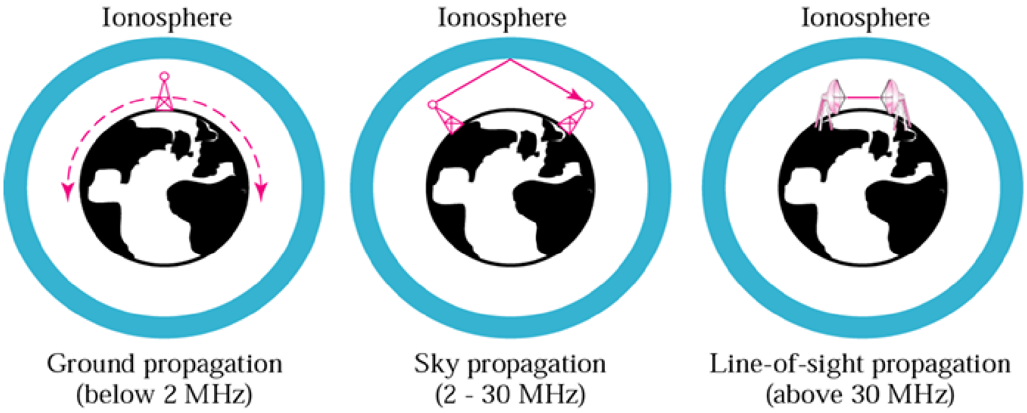


Figure (6-9): Propagation methods

In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth.

In **sky propagation**, higher-frequency radio waves radiate تشع upwardاعللا into the ionosphere (the layer of atmosphere غلاف جوي) where they are reflected back to earth.

In **line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional.

6.5.4 Radio Waves

Radio waves are omnidirectional متعدد الاتجاهات, when an antenna transmits radio waves; they are propagated in all directions. This means that the sending and receiving antennas **do not have to be aligned**. متوازية

Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long distance broadcasting such as AM radio.

6.5.4.1 Omnidirectional Antenna

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure 6.10 shows an omnidirectional antenna.

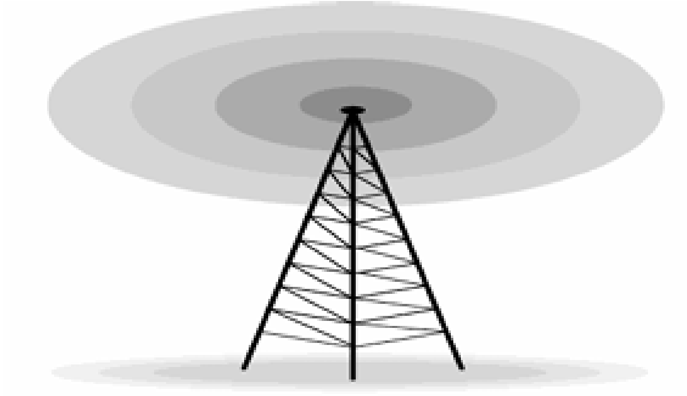


Figure (6-10): Omnidirectional antenna

6.5.4.2 Radio waves applications

The omnidirectional characteristics of radio waves make them useful for **multicasting**, in which there is one sender but many receivers. AM radio, FM radio and television are examples of multicasting.

6.5.5 Microwaves

Microwaves have frequencies between 1 and 300 GHz. Microwaves are unidirectional. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Following describes some **characteristics** of microwave propagation:

- **Microwave propagation is line-of-sight**.خط البصر Since the towers with the mounted مثبتة antennas need to be in direct sight of each other.
- **Very high-frequency microwaves cannot penetrate walls**.
- **The microwave band is relatively wide**, almost 299 GHz.

6.5.5.1 Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. **Two types of antennas** are used for microwave communications: the **dish antenna** and the **horn antenna** (see Figure 6.11).

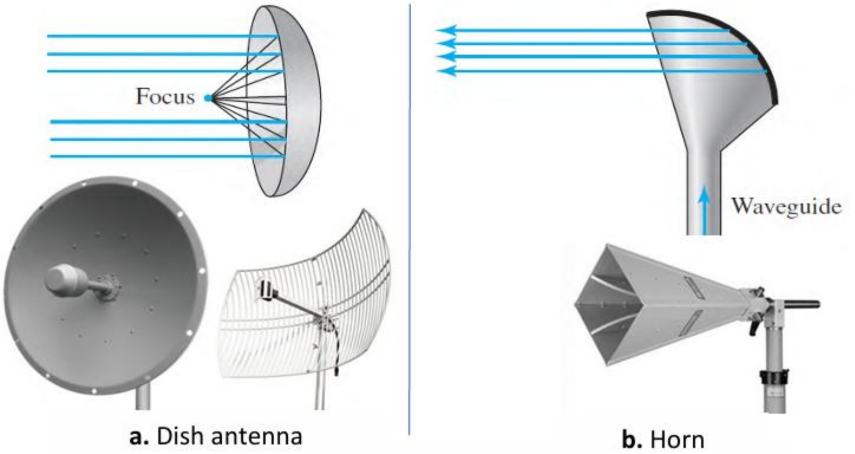


Figure (6-11): Unidirectional antennas

6.5.5.2 Microwave Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, **satellite networks**, and **wireless LANs**.

6.5.6 Infrared waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This **advantageous** characteristic prevents interference between one system and another. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. We ***cannot*** use infrared waves outside a building ***because*** the sun’s rays contain infrared waves that can interfere with the communication.

Infrared Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

The **Infrared Data Association منظمة** (IrDA), an association which has established standards for using these signals for communication between devices such as **keyboards**, **mice**, **PCs**, and **printers**.

Infrared signals defined by IrDA transmit through **line of sight**; the IrDA port on the keyboard needs to point to the PC for transmission to occur.

Chapter Seven
IPv4 address

7. IPv4 address

The identifier used in the IP layer of the TCP/IP protocol suite to *identify each device connected to the Internet* is called the ***Internet address*** or ***IP address***. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

Two devices on the Internet can **never have** the same address at the same time. However, if a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

7.1 Address Space

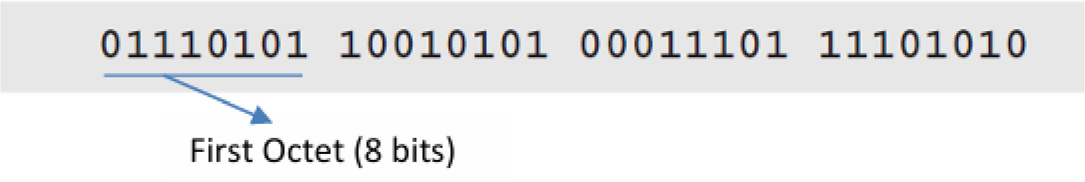
An address space is the *total number of addresses* used by the protocol. If a protocol uses **b** bits to define an address, the address space is **2b** because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion). Theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

7.2 Notation

There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).

Binary Notation: Base 2

In binary notation, an IPv4 address is displayed as 32 bits (in four octets). Each octet (8 bits) is often referred to as a byte. The following is an example of an IPv4 address in binary notation:



Dotted-Decimal Notation: Base 256

To make the IPv4 address more compact and easier to read, an IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes.

Note that because each byte (octet) is only 8 bits, each number in the dotted decimal notation is between 0 and 255 (see Figure 7.1).

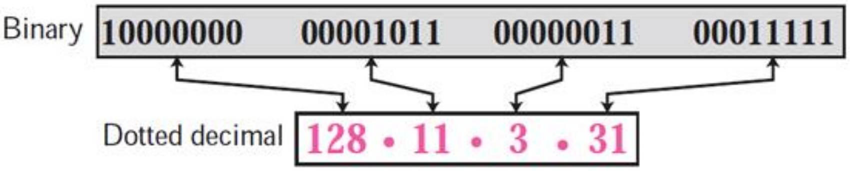


Figure (7-1): Dotted-decimal notation

Example 1

Change the following IPv4 addresses **from** binary notation **to** dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation:

a. 129.11.11.239

b. 193.131.27.255

Example 2

Change the following IPv4 addresses **from** dotted-decimal notation **to** binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent:

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 3

Find the **error**, if any, in the following IPv4 addresses:

a. 111.56.**0**45.78

b. 221.34.7.8.20

c. 75.45.**301**.14

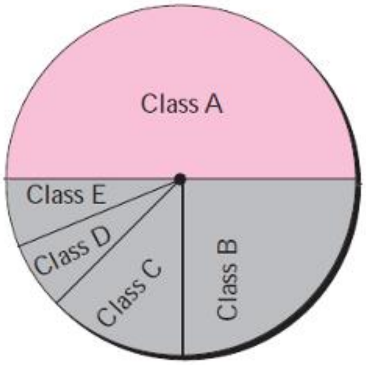
d. **11100010**.23.14.67

Solution

a. There should be no leading zeroes in dotted-decimal notation (045).
b. We may not have more than 4 bytes in an IPv4 address.
c. Each byte should be less than or equal to 255; 301 is outside this range.
d. A mixture of binary notation and dotted-decimal notation is not allowed.

7.3 Classful addressing

In classful addressing, the IP address space is divided into **five classes**: A, B, C, D, and E. Each class occupies some part of the whole address space. Figure 7.2 shows the class occupation of the address space.



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

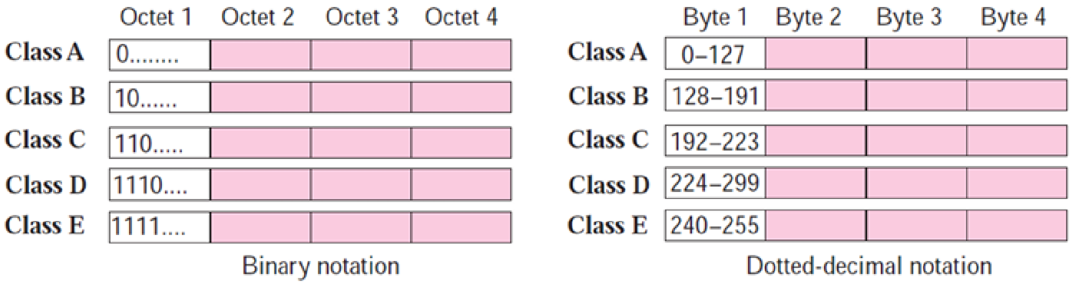
Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Figure (7-2): Occupation of the address space

7.3.1 Recognizing Classes

We can find the class of an address when the address is given either in binary or dotted decimal notation. In the **binary notation**, the ***first few bits*** can immediately tell us the ***class*** of the address; in the **dotted-decimal** notation, the ***value of the first byte*** can give the ***class*** of an address (Figure 7.3).



	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0........			
Class B	10......			
Class C	110.....			
Class D	1110....			
Class E	1111....			

Binary notation

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–299			
Class E	240–255			

Dotted-decimal notation

Figure (7-3): Finding the class of an address

Example 5

Find the **class** of each address:

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 10100111 11011011 10001011 01101111

d. 11110011 10011011 11111011 00001111

Solution

a. The first bit is 0. This is a class A address.
b. The first 2 bits are 1; the third bit is 0. This is a class C address.
c. The first bit is 1; the second bit is 0. This is a class B address.
d. The first 4 bits are 1s. This is a class E address.

Example 6

Find the **class** of each address:

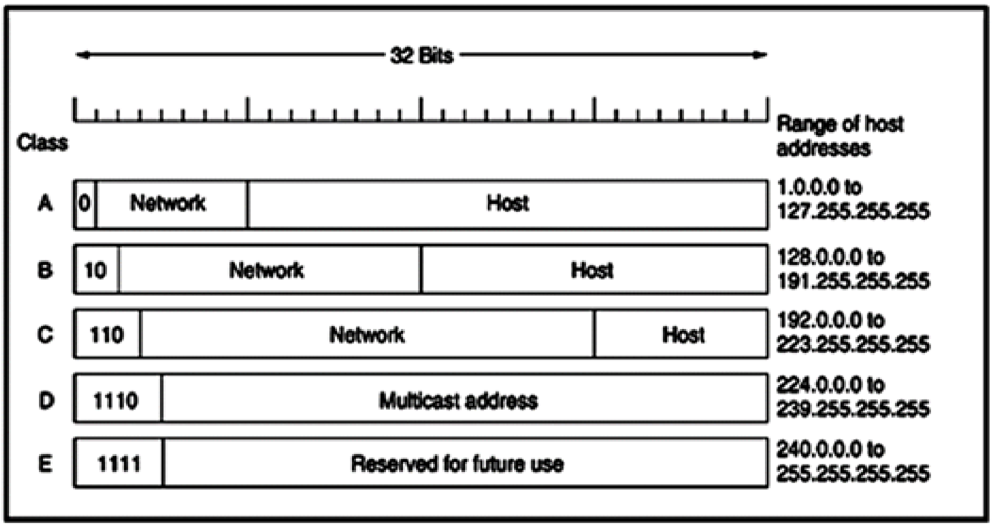
a. 227.12.14.87
b. 193.14.56.22
c. 14.23.120.8
d. 252.5.15.111

Solution

a. The first byte is 227 (between 224 and 239); the class is D.
b. The first byte is 193 (between 192 and 223); the class is C.
c. The first byte is 14 (between 0 and 127); the class is A.
d. The first byte is 252 (between 240 and 255); the class is E.

7.3.2 NetId and HostId

In classful addressing, an IP address in classes A, B, and C is divided into NetId and HostId. Figure 7.4 shows the NetId and HostId bytes. Note that classes **D and E** are **not divided** into NetId and HostId.


32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

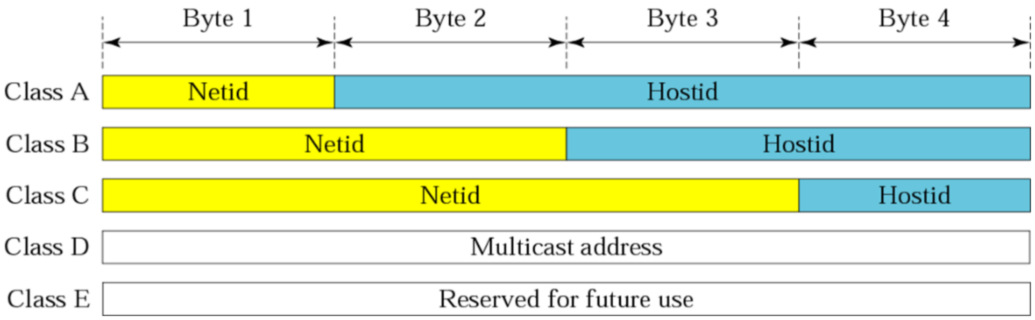
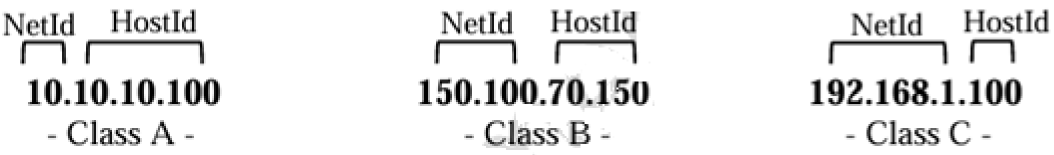
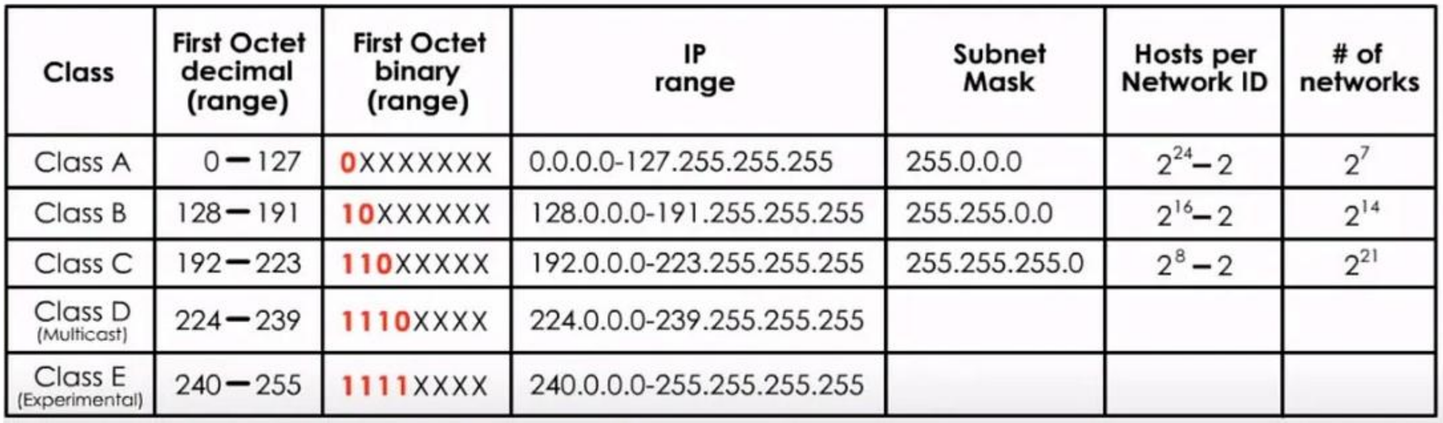


Figure (7-4): NetId and HostId





Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 — 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 — 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 — 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 — 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 — 255	1111XXXX	240.0.0.0-255.255.255.255			

Class D

There is just one block of class D addresses. It is designed for ***multicasting*** (one-to-many communication). Each address in this class is used to define ***one group of hosts*** on the Internet. When a group is assigned an address in this class, every host that is a member of this group will have a multicast address in addition to its normal (unicast) address. Used for applications like video/audio streaming, gaming, and real-time data delivery.

Class E

There is just ***one block*** of class E addresses. It was designed for use as reserved addresses for future purposes.

7.3.3 Extracting Information in a Block

The block size shows the number of IP addresses contained in a specific range. Given any address in the block, we normally like to know ***three pieces of information*** about the block: the number of addresses, the first address, and the last address. After the class of the block is found, ***we know the value of n*** (the length of NetId in bits). We can now find these three pieces of information as shown in the following:

1. The **number of addresses** in the block, **N**, can be found using N = 2^{32-n}.

2. To find the **first address**, we keep the **n** leftmost bits and set the (32− n) rightmost bits all to 0s.

3. To find the **last address**, we keep the **n** leftmost bits and set the (32− n) rightmost bits all to 1s.

Example 7

An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address, and the last address.

Solution

Since 73 is between 0 and 127, the class of the address is **A**. The value of **n** for class A is 8. Figure 7.8 shows a possible configuration of the network that uses this block. Note that we show the value of **n** in the network address after a slash.

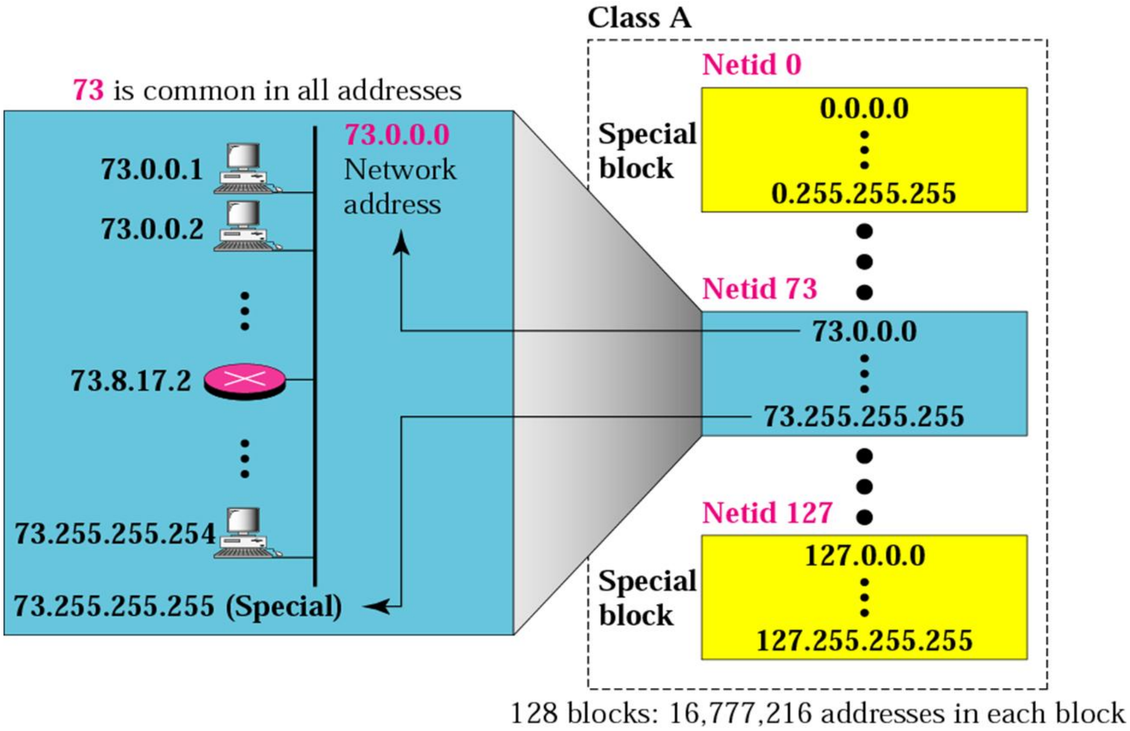


Figure (7-8): Solution to Example 7 (Blue)

1. The number of addresses in this block is N = $2^{32-n} = 2^{24}$ = 16,777,216.

2. The first address is 73.0.0.0/8 in which **8** is the value of **n**. The first address is called the **network ID** and is not assigned to any host. It is used to define the network.

3. The last address is 73.255.255.255. The last address (or called the **broadcast ID**) is normally used for a special purpose.

Example 8

An address in a block is given as 180.8.17.9. Find the number of addresses in the block, the first address, and the last address.

Solution

1. The number of addresses in this block is N = $2^{32-n} = 2^{32-16} = 2^{16}$= 65,536.
2. The first address (network address) is 18.8.0.0/16, in which **16** is the value of **n**.
3. The last address is 18.8.255.255.

Number of Addresses

The given IP address is 180.8.17.9.

1. The first octet, 180, falls between 128 and 191.
2. This indicates that the address belongs to a Class **B** network.
3. In a Class B network, the **first 16 bits** are used for the **network ID**.
4. The number of addresses in the block is calculated using the formula $N = 2^{32-n}$, where $\boldsymbol{n}$ is the number of bits in the network ID.
5. The number of addresses is $N = 2^{32-16} = 2^{16}$.
6. The total number of addresses is 65536.

First Address

1. The first address is found by *keeping* the network ID and *setting* the host ID to all zeros.
2. The network ID consists of the first 16 bits, which correspond to the first two octets.
3. The first two octets are 180.8.
4. The host ID consists of the last 16 bits, which correspond to the last two octets.
5. The last two octets are set to 0.0.
6. The first address in the block is 180.8.0.0.

Last Address

1. The last address is found by **keeping** the ***network ID*** and **setting** the ***host ID*** to ***all ones***.
2. The network ID consists of the first 16 bits, which correspond to the first two octets.
3. The first two octets are 180.8.
4. The host ID consists of the last 16 bits, which correspond to the last two octets.
5. The last two octets are set to 255.255.
6. The last address in the block is 180.8.255.255.

Final Answer

The number of addresses in the block is 65536. The first address is 180.8.0.0. The last address is 180.8.255.255.

Example 9

Figure 7.9 shows a hypothetical part of an internet with three networks.

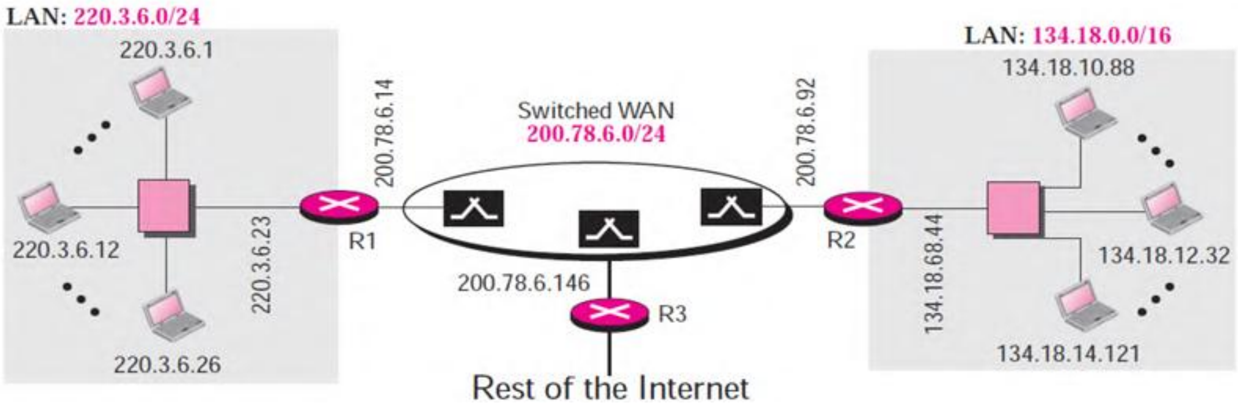


Figure (7-9): Sample internet

We have

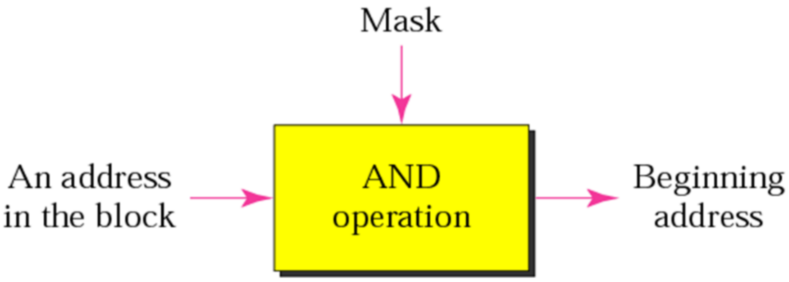
1. A LAN with the network address 220.3.6.0 (class C).

2. A LAN with the network address 134.18.0.0 (class B).

3. A switched WAN (class C), that can be connected to many routers. We have shown three. **One** router connects the WAN to the left LAN, **one** connects the WAN to the right LAN, and **one** connects the WAN to the rest of the internet.

7.4 Network Mask

A network mask or a ***default mask*** in classful addressing is a 32-bit number with ***n*** leftmost bits all set to **1s** and (32 − n) rightmost bits all set to **0s**. Since **n** is different for each class in classful addressing, we have three default masks in classful addressing as shown in Figure 7.10.



Class	*Mask in binary*	*Mask in dotted-decimal*
A	**11111111** 00000000 00000000 00000000	**255.**0.0.0
B	**11111111 11111111** 00000000 00000000	**255.255.**0.0
C	**11111111 111111111 11111111** 00000000	**255.255.255.**0

Figure (7-10): Network mask

The routers in the Internet normally use an algorithm to extract the network address from the destination address of a packet. A router uses the **AND** operation. When the ***destination*** address is **AND**ed with the ***default mask***, the ***result*** is the ***network address***.

How it Works (Example)

1. **Binary Operation**: A bitwise AND operation between an IP address and its subnet mask isolates the network address.
2. **Dotted-Decimal Notation**: Commonly shown as four numbers separated by dots (e.g., 255.255.255.0).
3. **CIDR Notation**: Sometimes represented by a forward slash and a number (e.g., /24), indicating the number of '1' bits in the mask.

Example: 192.168.1.100 with Mask 255.255.255.0 (/24)

- The mask's '1's (255.255.255.) cover the first three octets, making the ***network part*** "192.168.1".
- The mask's '0' (255.255.255.**0**) signifies the ***host part***, meaning all devices from 192.168.1.0 to 192.168.1.255 are on the same local network.

Example 10

A router receives a packet with the destination address 201.24.67.32. Show how the router finds the network address of the packet.

Solution

Step 1: Identify the IP **class**

- The destination IP is 201.24.67.32
- Since the first octet is (which falls between 192–223), this is a Class **C** address.
- Default subnet mask for Class C = 255.255.255.0

Step 2: Convert to binary

IP Address: 11001001.00011000.01000011.00100000

Subnet Mask: 11111111.11111111.11111111.00000000

Network Addr.: 11001001.00011000.01000011.00000000

Step 3: Convert back to decimal

- Network address = **201.24.67.0**

The router determines that the packet with destination 201.24.67.32 belongs to the network **201.24.67.0/24.**

7.5 Special Addresses

Some blocks of addresses are reserved for ***special purposes*** and cannot be used as normal IP addresses as shown in the following:

1- **All-Zeros Address.** The block **0.0.0.0/32**, which contains only **one single address**, is reserved for communication when a host needs to send an IPv4 packet but it does **not** know its own address. The host sends an IPv4 packet to a bootstrap server (called DHCP server) using this address as the source address and a **limited broadcast address** (255.255.255.255) as the destination address to find its own address (see figure 7.11).

2- **All-Ones Address.** The block 255.255.255.255/32, which contains **one single address**, is reserved for **limited broadcast address** in the current network.

3- **Loopback Addresses**. The block 127.0.0.0/8 is used to test the software on a machine. When this address is used, a **packet never leaves the machine**; it simply returns to the protocol software.

4- **Network ID and broadcast ID**. The network ID is the first address (with the suffix set all to 0s) in a block **defines the network address**. Broadcast ID is the last address in a block or subnet (with the suffix set all to 1s) can be used as a direct broadcast address. **This address is usually used by a router to send a packet to all hosts in a specific network**.

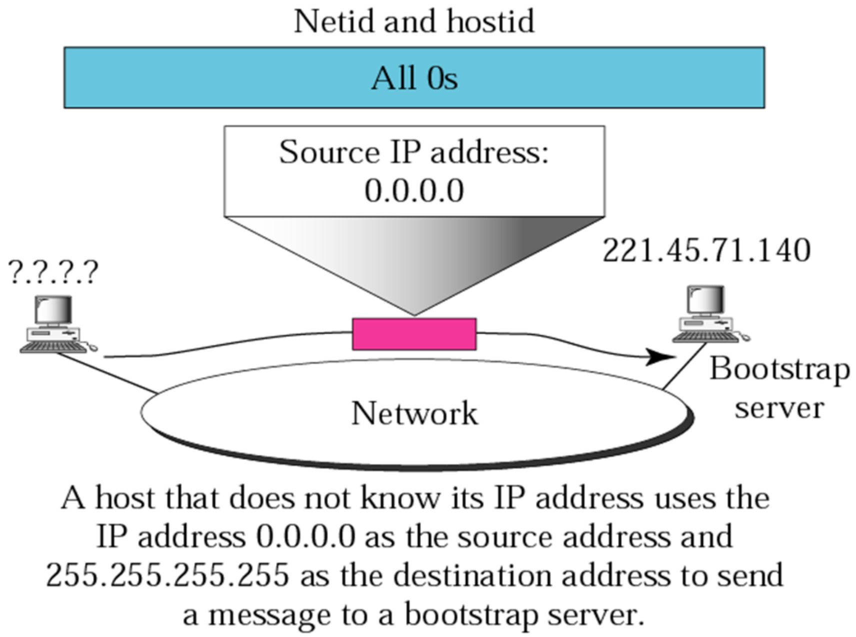

Netid and hostid
All 0s
Source IP address:
0.0.0.0
?.?.?.?
221.45.71.140
Bootstrap server
Network
A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

Figure (7-11): Examples of using the all-zeros addresses

7.6 Internet Protocol version 6 (IPv6)

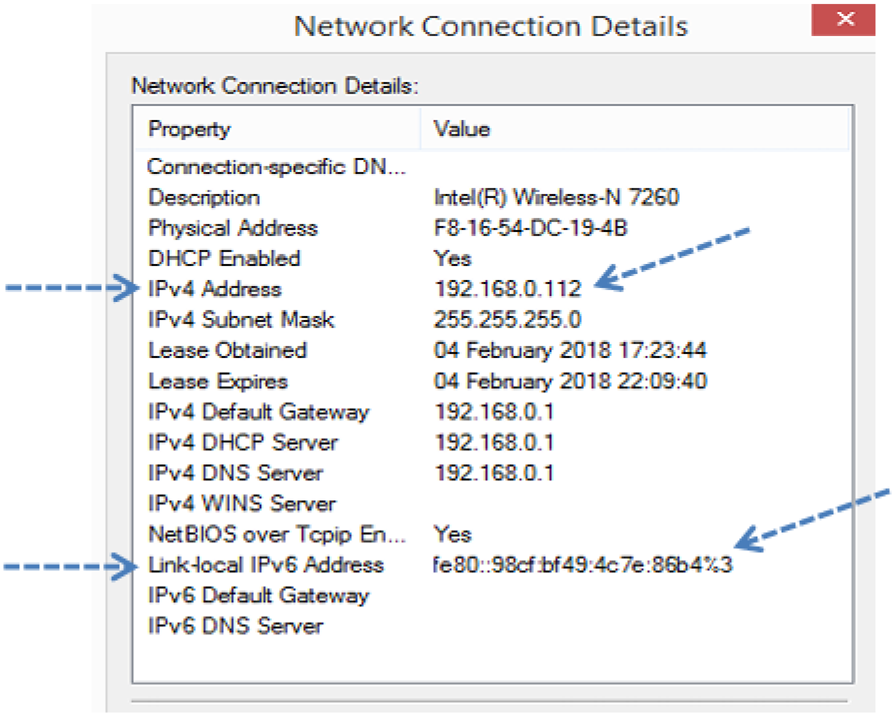
IPv6 was developed to deal with the problem of IPv4 address. IPv6 is ***intended to replace*** IPv4. With the rapid growth of the Internet after the 1990s, far more addresses would be needed to connect devices than the IPv4 address space had available.

By 1998, the IPv6 had been formalized with 128-bit, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses, whereas IPv4 uses only **32-bit** addresses and provides approximately 2^{32}, or 4.3 billion addresses.

IPv6 addresses are represented as ***eight groups*** of ***four hexadecimal digits*** with the groups being ***separated by colons***, for example:

3501**:**0cb8**:**0000**:**0052**:**0000**:**7a5e**:**0b70**:**9335

But methods are existed to abbreviate this full notation as shown in Figure 7.12.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Wireless-N 7260
Physical Address	F8-16-54-DC-19-4B
DHCP Enabled	Yes
IPv4 Address	192.168.0.112
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 February 2018 17:23:44
Lease Expires	04 February 2018 22:09:40
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::98cf:bf49:4c7e:86b4%3
IPv6 Default Gateway	
IPv6 DNS Server	

Figure (7-12): Example of IPv6 and IPv4 addresses in a host computer

7.7 Subnetting

Subnetting is a process of breaking large network in small networks known as ***subnets***.

Method of subnetting

In subnetting we need to find the following:

a. Finding the subnet mask

To find the subnet mask, we 1) need to write down the default subnet mask, 2) find the host bits borrowed to create subnets, and 3) put the borrowed bits (1s bits) in the left side instead of the 0s bits.

For example: find the subnet mask of address 188.25.45.48/**20**

1. The default subnet mask is 255.255.0.0 (/**16**),
2. The number of borrowed bits from HostId portion is 4 (20 - 16 = 4).
3. The subnet mask in binary would be 11111111. 11111111. 11110000. 00000000.

Then subnet mask in decimal is **255.255.240.0**

IP address: 188.25.45.48/20   subnet mask: 255.255.240.0

b. Finding the number of subnets

To calculate the number of subnets (sub-networks) provided by given subnet mask we use 2^b, where b = number of bits borrowed from HostId bits to create subnets.

For example: find the number of subnets in 192.168.1.0/**27**

The number of borrowed bits is **3** because 27-24=3. (24 is the default value of Class C IP).
Then the number of subnets is $2^3 = 8$
This means that we can make **8** sub-networks with the IP range 192.168.1.0/**27**.

c. Finding the total hosts

Total hosts are the hosts available per subnet. 2H = Total hosts. H is the number of host bits. For **example** in address 192.168.1.0/**26** we have 32 - 26 = 6 (where 32 is the total bits in IP address). Total hosts per subnet would be $2^6 = 64$.

Valid number of hosts

As we mentioned previously, we need to reduce two addresses per block (or subnet), one for network ID and another for broadcast ID. Therefore,

Valid hosts = Total hosts - 2.

In above example we have 64 hosts per subnet, so valid hosts in each subnet would be 64-2 = 62.

network ID → 192.168.1.0 broadcast ID → 192.168.1.63 (First subnet)
network ID → 192.168.1.64 broadcast ID → 192.168.1.127 (Second subnet)
network ID → 192.168.1.128 broadcast ID → 192.168.1.191 (Third subnet)
network ID → 192.168.1.192 broadcast ID → 192.168.1.255 (Forth subnet)

In the following we include some examples only from class C (**Class C Subnetting**).

Example: assume an organization has purchased the IP range: 192.168.55.0 and they need to use this IP range through four buildings with 55 host computer in each building. Find the 1) suitable subnet mask, 2) number of subnet, 3) number of hosts in each subnet, 4) valid number of hosts, 5) the network ID, broadcast ID and unused IPs of the third subnet.

Solution

Because we need to distribute the IP range through four buildings or networks, then the number of bits that will be borrowed from HostId is 2 as shown in the following:

Default subnet mask

Six bits available for Host address **(H)=6**

11111111.11111111.11111111.11000000

b=2

Using **2** HostId bits for NetId bits to extend the default subnet mask

Decimal notation for the subnet mask: 255.255.255.192 (/**26**)

Example:

Assume that we have the IP address 200.10.73.0/**28**, find each of following:

1) subnet mask,
2) number of subnets,
3) number of hosts in each subnet,
4) valid number of hosts,
5) the network ID, broadcast ID of the second subnet.

Default subnet mask

four bits available for Host address **(H)=4**

11111111.11111111.11111111.11110000

b=4

Using 4 HostId bits for NetId bits to extend the default subnet mask

Binary notation for the subnet mask: 255.255.255.240(/28)

Solution

The binary notation for the subnet mask is as shown below:

1) Subnet mask: 255.255.255.240 (/**28**) IP address: 200.10.73.0/**28**
2) Number of subnets: $2^b = 2^4 = 16$
3) Number of host in each subnet: $2^H = 2^4 =$ **16** available hosts
4) Valid number of hosts: 16-2=14
5) Network ID → 192.168.1.16, broadcast ID → 192.168.1.31 (for second subnet)

Chapter Eight

Wired LANs –Ethernet–

8. Wired LANs –Ethernet–

The Computer Society of the IEEE started a project, called **Project 802**, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI model or TCP/IP protocol suite. The relationship of the 802 Standard to the TCP/IP protocol suite is shown in Figure 8.1. The IEEE has subdivided the data-link layer into two sub-layers: **logical link control (LLC)** and **media access control (MAC).**

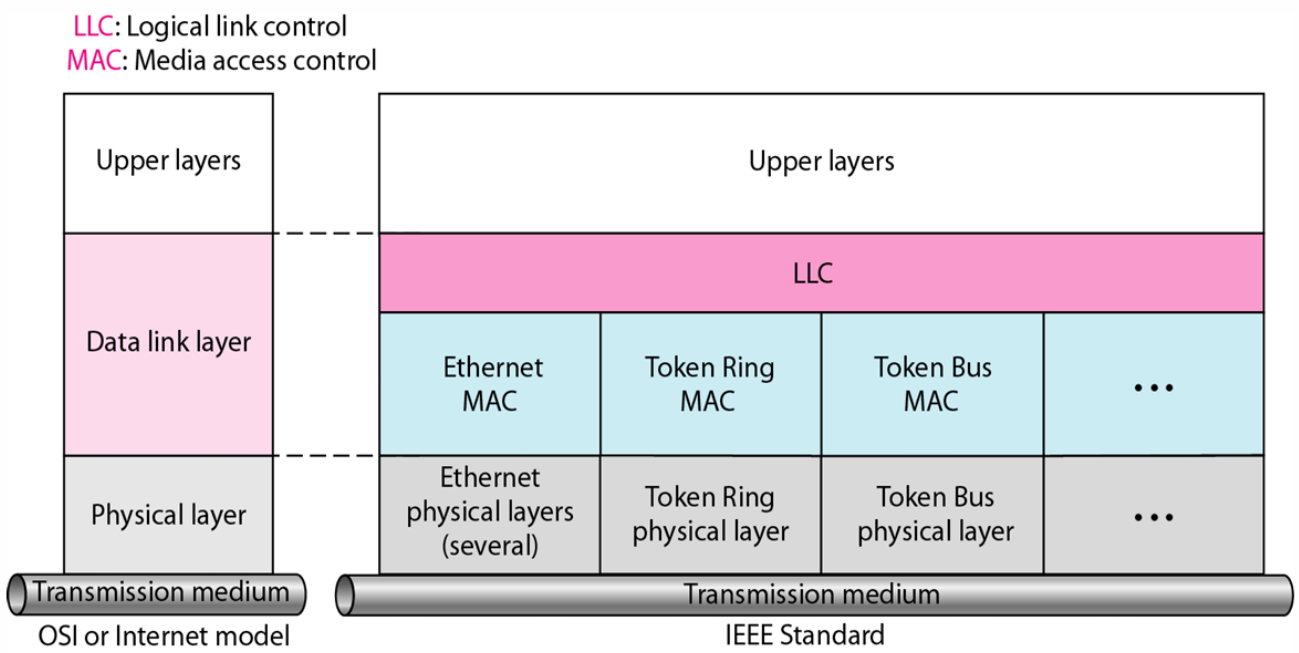


Figure (8-1): IEEE standard for LANs

Ethernet Evolution

The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Since then, it has gone through four generations: ***Standard Ethernet*** (10 Mbps), ***Fast Ethernet*** (100 Mbps), ***Gigabit Ethernet*** (1 Gbps), and ***10 Gigabit Ethernet*** (10 Gbps), as shown in Figure 8.2.

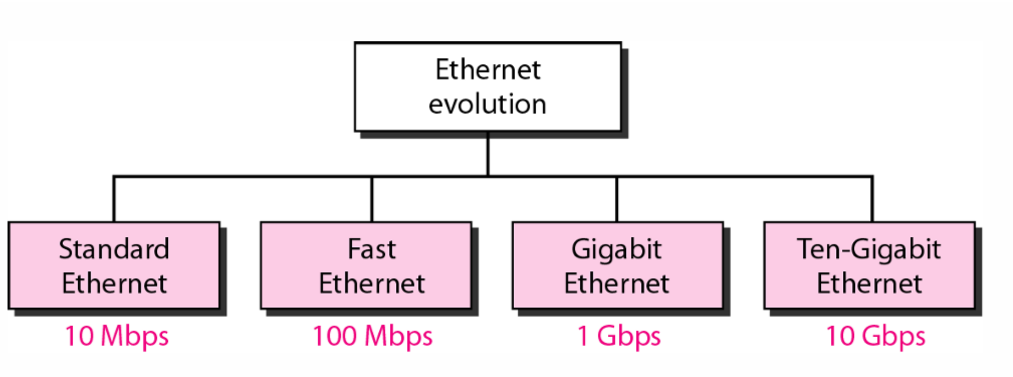


Figure (8-2): Ethernet evolutions through four generations

8.1 Standard Ethernet

We refer to the original Ethernet technology with the data rate of 10 Mbps as the ***Standard Ethernet***. Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution.

8.1.1. Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own **network interface card** (NIC). The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation. For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

Transmission of Address Bits

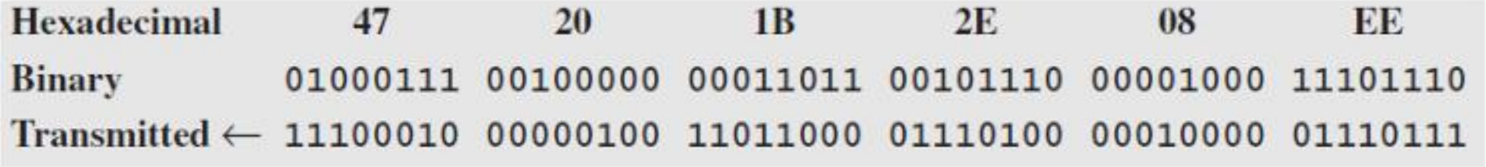
The transmission is left to right, **byte by byte**; however, for each byte, the least significant **bit** is sent first and the most significant bit is sent last. This means that the bit that defines an address as unicast or multicast arrives first at the receiver. This helps the receiver to immediately know if the packet is unicast or multicast.

Example 1

Show how the address 47:20:1B:2E:08:EE is sent out online.

Solution

The address is **sent left to right**, byte by byte. But for each byte, it is sent right to left, bit by bit, as shown below:



Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast, Multicast, and Broadcast Addresses

A **source address** is always a unicast address—the frame comes from only one station. The **destination address**, however, can be unicast, multicast, or broadcast. Figure 8.3 if the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast. The broadcast address is a special case of the multicast address. A broadcast destination address is forty-eight 1s.

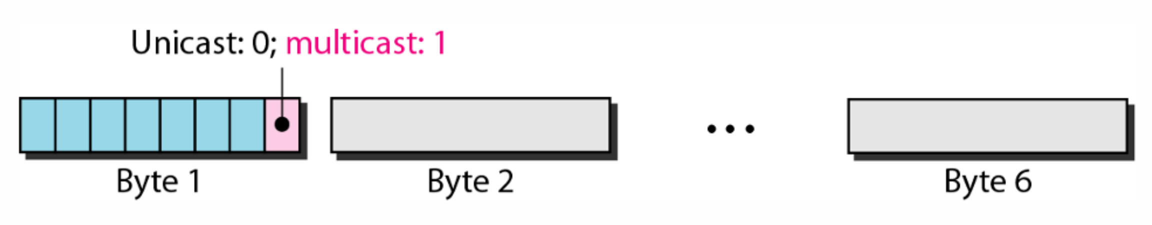


Figure (8-3): Unicast and multicast addresses

Example 2

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

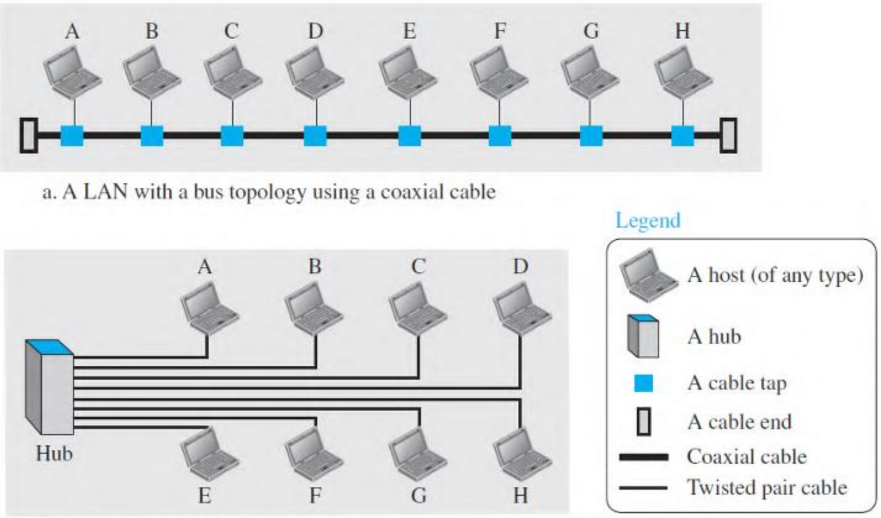
Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are Fs, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

Distinguish Between Unicast, Multicast, and Broadcast Transmission Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology) as shown in Figure 8.4.

We need to know that transmission in the standard Ethernet is always broadcast, no matter if the intention is unicast, multicast, or broadcast. In the bus topology, when station A sends a frame to station B, all stations will receive it. In the star topology, when station A sends a frame to station B, the hub will receive it. Since the hub is a passive element, it regenerates the bits and sends them to all stations except station A.



a. A LAN with a bus topology using a coaxial cable

b. A LAN with a star topology using a hub

Figure (8-4): Implementation of standard Ethernet

The question is, then, how the actual unicast, multicast, and broadcast transmissions are distinguished from each other. The answer is in the way the frames are **kept** or **dropped**.

- In a unicast transmission, all stations will receive the frame, the **intended recipient** keeps and handles the frame; the rest discard it.
- In a multicast transmission, all stations will receive the frame, the stations that are **members of the group** keep and handle it; the rest discard it.
- In a broadcast transmission, **all stations** (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

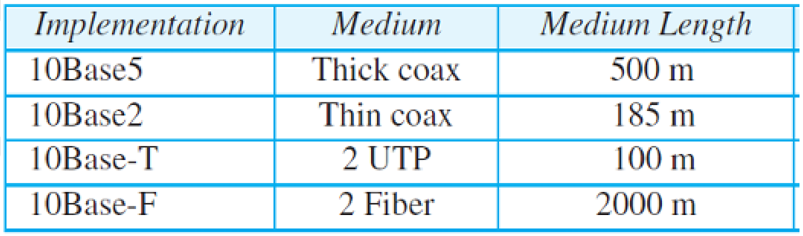
8.1.2 Access Method

Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium. The standard Ethernet uses the protocol CSMA/CD as an access method.

8.1.3 Implementation

The Standard Ethernet defined several implementations, but only four of them became popular during the 1980s. Table 8.1 shows a summary of Standard Ethernet implementations.

Table 8.1 Summary of Standard Ethernet implementations



Implementation	*Medium*	*Medium Length*
10Base5	Thick coax	500 m
10Base2	Thin coax	185 m
10Base-T	2 UTP	100 m
10Base-F	2 Fiber	2000 m

In the term 10BaseX, the number defines the data rate (10 Mbps), the term Base means baseband (digital) signal, and X approximately defines either the maximum size of the cable in 100 meters (for example 5 for 500 or 2 for 185 meters) or the type of cable, T for unshielded twisted pair cable (UTP) and F for fiber-optic. The standard Ethernet uses a baseband signal, which means that the bits are changed to a digital signal and directly sent on the line.

8.2 Fast Ethernet (100 Mbps)

Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the ***Fast Ethernet***. The designers of the Fast Ethernet needed to make it compatible with the Standard Ethernet. The goals of

Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.

8.2.1 Access Method

Fast Ethernet is 10 times faster than Standard Ethernet. In order to achieve this, the Fast Ethernet came with two solutions (it can work with either choice):

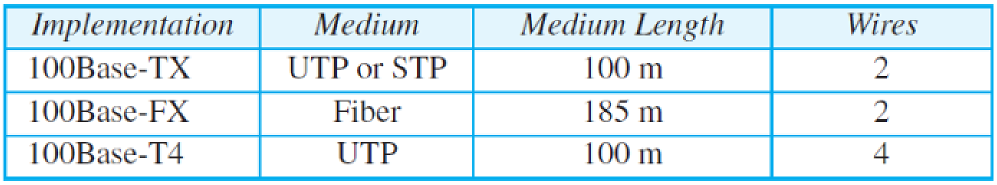
1. The first solution was to totally drop the bus topology and use a passive hub and star topology but make the maximum size of the network 250 meters instead of 2500 meters as in the Standard Ethernet. This approach is kept for compatibility with the Standard Ethernet.

2. The second solution is to use a link-layer switch (instead of physical-layer hub) with a buffer to store frames and a full-duplex connection to each host to make the transmission medium private for each host. In this case, there is no need for CSMA/CD because the hosts are not competing with each other.

8.2.2 Implementation

Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either shielded twisted pair (STP), which is called 100Base-TX, or fiber-optic cable, which is called 100Base-FX. The four-wire implementation is designed for unshielded twisted pair (UTP), which is called 100Base-T4 (see Table 8.2).

Table 8.2 Summary of Fast Ethernet implementations



Implementation	*Medium*	*Medium Length*	*Wires*
100Base-TX	UTP or STP	100 m	2
100Base-FX	Fiber	185 m	2
100Base-T4	UTP	100 m	4

8.3 Gigabit Ethernet

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps). The IEEE committee calls it the Standard **802.3z**. The goals of the Gigabit Ethernet design can be summarized as follows:

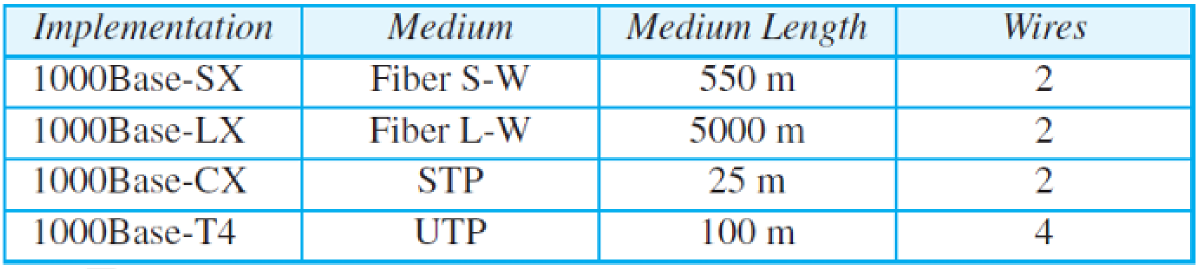
1. Upgrade the data rate to 1 Gbps.

2. Make it compatible with Standard or Fast Ethernet.

Implementation

Table 8.3 is a summary of the Gigabit Ethernet implementations. S-W and L-W mean short-wave and long-wave respectively.

Table 8.3 Summary of Gigabit Ethernet implementations



Implementation	*Medium*	*Medium Length*	*Wires*
1000Base-SX	Fiber S-W	550 m	2
1000Base-LX	Fiber L-W	5000 m	2
1000Base-CX	STP	25 m	2
1000Base-T4	UTP	100 m	4

8.4 10 Gigabit Ethernet

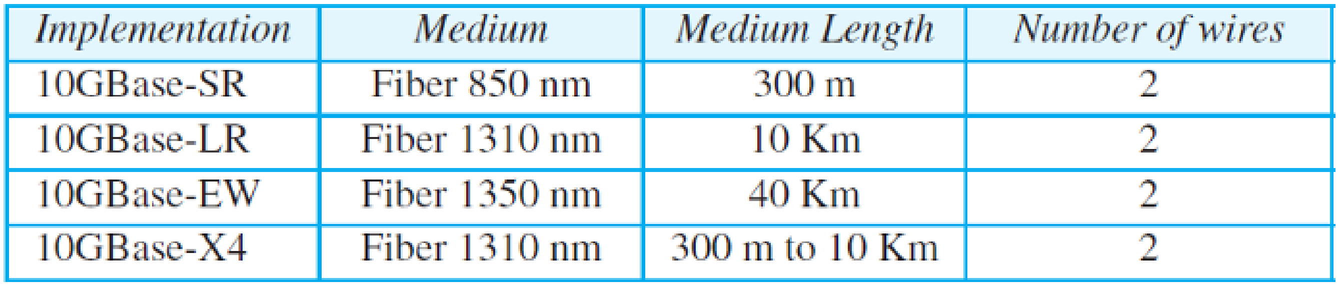
In recent years, there has been another look into the Ethernet for use in metropolitan areas. The idea is to extend the Ethernet, such that it can be used as LAN and MAN. The IEEE committee created 10 Gigabit Ethernet and called it Standard **802.3ae**.

The goals of the 10 Gigabit Ethernet design can be summarized as upgrading the data rate to 10 Gbps. This data rate is possible only with fiber-optic technology at this time.

Implementation

10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention i.e., CSMA/CD is not used in 10 Gigabit Ethernet. Table 8.4 shows the summary of the 10 Gigabit Ethernet implementations.

Table 8.4Summary of 10 Gigabit Ethernet implementations



Implementation	*Medium*	*Medium Length*	*Number of wires*
10GBase-SR	Fiber 850 nm	300 m	2
10GBase-LR	Fiber 1310 nm	10 Km	2
10GBase-EW	Fiber 1350 nm	40 Km	2
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2

Chapter Nine

Wireless LANs –WiFi–

9. Wireless LANs –WiFi–

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. In the following three sections, we make three comparisons between wired and wireless LANs depending on architecture, characteristics and access control.

9.1 Architectural Comparison

Let us compare the architecture of wired and wireless LANs to give some idea about the following issues:

Medium

In a wired switched LAN, with a link-layer switch, the communication between the hosts is ***point-to-point*** and ***full-duplex*** (bidirectional). In a wireless LAN, the medium is air, the signal is generally ***broadcast***. When hosts in a wireless LAN communicate with each other, they are ***sharing the same medium*** (multiple access).

Hosts

In a wired LAN, before the host can use the services of the Internet, it needs to be physically connected to the Internet. In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network. Therefore, the mobility are totally different issues.

Isolated LANs

A wired isolated LAN is a set of hosts connected via a link-layer switch (in the recent generation of Ethernet). A wireless isolated LAN, called an ***ad hoc network*** in wireless LAN terminology, is a set of hosts that communicate freely with each other. The concept of a link-layer switch does not exist in wireless LANs. Figure 9.1 shows two isolated LANs, one wired and one wireless.

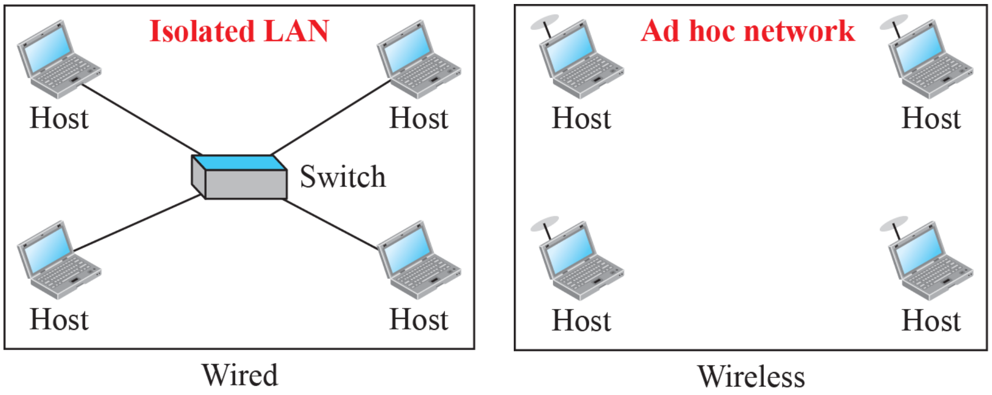


Figure (9-1): Isolated LANs: wired versus wireless

Connection to Other Networks

A wired LAN can be connected to another network or an internetwork such as the Internet using a router. In Figure 9.2, the wireless LAN is referred to as an infrastructure network, and the connection to the wired infrastructure, such as the Internet, is done via a device called an **access point (AP)**.

Note that the role of the access point ***is completely different*** from the role of a link-layer switch in the wired environment. An ***access point*** is gluing two different environments together: one wired and one wireless.

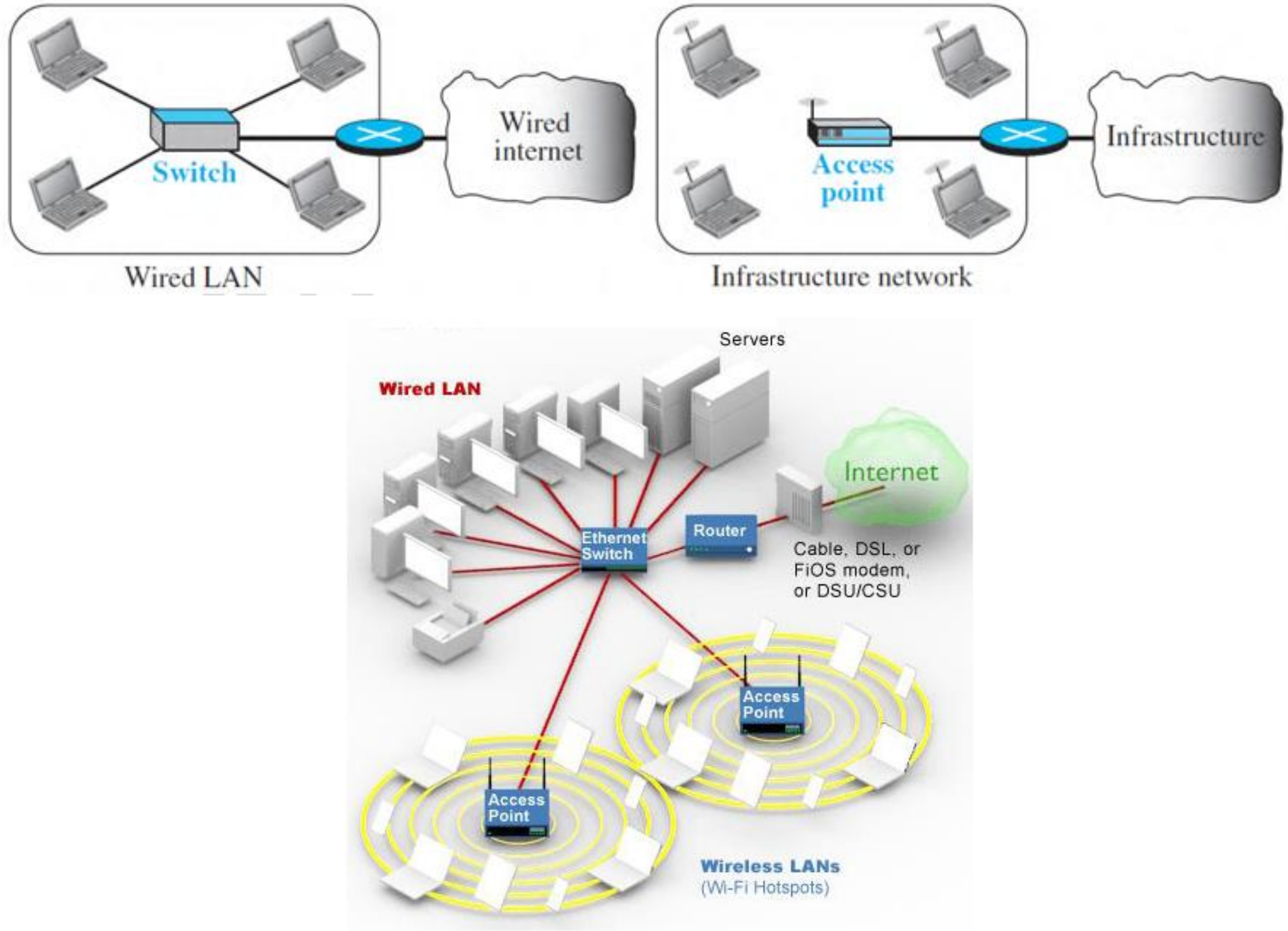


Figure (9-2): Connection of a wired LAN and a wireless LAN to other networks

Moving between Environments

In order to move from the wired environment to a wireless environment, we need to change the network interface cards designed for wired environments to the ones designed for wireless environments and replace the link-layer switch with an access point.

9.2 Characteristic Comparison

There are several characteristics of wireless LANs that either do not apply to wired LANs or can be ignored.

Attenuation

The strength of electromagnetic signals ***decreases rapidly*** because the signal disperses in all directions; only a small portion of it reaches the receiver.

Interference

Another issue is that a receiver may receive signals not only from the true sender, but also from ***other senders*** if they are using the same frequency band.

Multipath Propagation

A receiver may receive more than one signal from the ***same sender*** because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.

Error

With the above characteristics of a wireless network, we can expect that errors are ***more serious issues*** in a wireless network than in a wired network. For example, we can think about the error level in the measurement of **signal-to noise ratio** (SNR).

9.3 Access control

In the previous chapter, we discussed that the Standard Ethernet (in wired LAN) uses the **CSMA/CD** algorithm. Because of some problems, the CSMA/CD does ***not*** work in wireless LANs. Therefore, the **Carrier Sense Multiple Access with Collision Avoidance** (CSMA/CA) was invented for wireless LANs.

9.4 IEEE 802.11 project (wireless LAN)

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. Some countries, including the United States, use the term WiFi (short for wireless fidelity) as a synonym for wireless LAN.

9.4.1 Architecture

The standard defines two kinds of services:

1. Basic Service Set

IEEE 802.11 defines the **basic service set** (BSS) as the building blocks of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure (9-3) shows two sets in this standard.

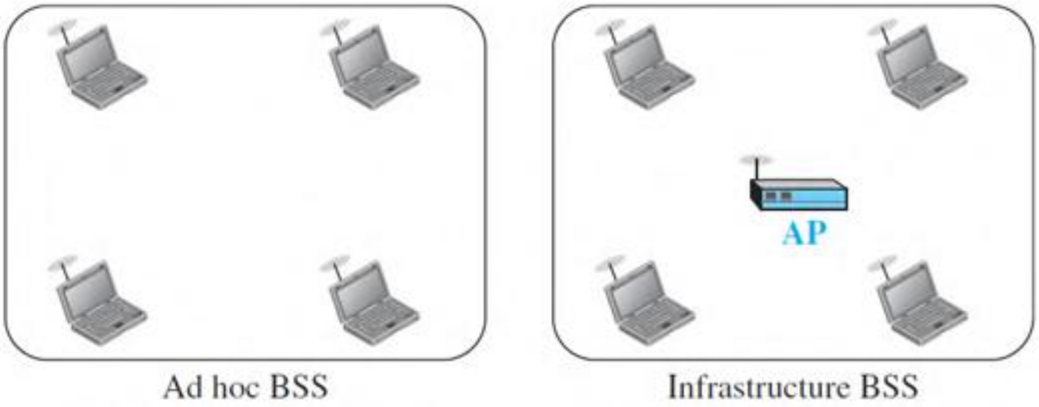


Figure (9-3): Basic service sets (BSSs)

The BSS without an AP is an independent network and cannot send data to other BSSs. It is called an ***ad hoc architecture***. A BSS with an AP is sometimes referred to as an infrastructure BSS.

2. Extended Service Set

An **extended service set** (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network. The distribution system connects the APs in the BSSs. Figure 9.4 shows an ESS.

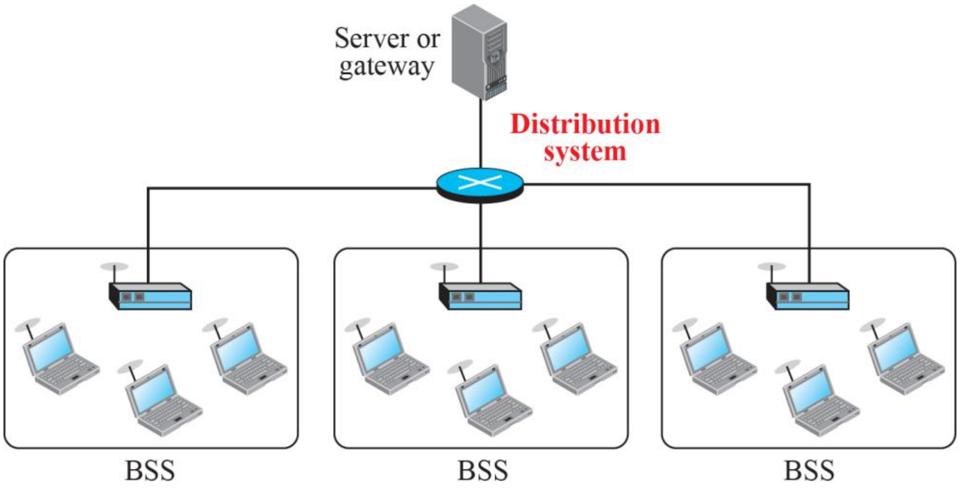


Figure (9-4): Extended service set (ESS)

9.5 Specification of IEEE 802.11

IEEE creates several specifications for the wireless LANs as described in the following:

IEEE 802.11 In 1997, the IEEE created the first WLAN standard with a maximum network ***bandwidth of 2 Mbps*** - too slow for most applications.

IEEE 802.11b IEEE expanded in July 1999, creating the 802.11b specification. It supports ***bandwidth up to 11 Mbps***, and uses radio signaling frequency (**2.4 GHz**).

IEEE 802.11a was created at the same time of 802.11b, but in a higher cost. IEEE 802.11a is usually found on business networks. It supports bandwidth up to 54 Mbps and signals in frequency **5 GHz**.

IEEE 802.11g was created in 2002 to combine the best of both 802.11a and 802.11b. IEEE 802.11g supports bandwidth up to ***54 Mbps***, and it uses the ***2.4 GHz*** frequency.

IEEE 802.11n (or "Wireless N") uses multiple wireless signals and antennas called MIMO (multiple-input multiple-output antenna) instead of one. It was created in 2009 with specifications providing for up to ***300 Mbps*** of network bandwidth.

IEEE 802.11ac is the newest generation of Wi-Fi which can utilize dual-band connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. It offers bandwidth rated up to ***1300 Mbps*** on the **5 GHz** band plus up to ***450 Mbps*** on ***2.4 GHz***.

WR543G Wireless AP/Client Router **IEEE 802.11b/g**

TP-LINK TL-WR940N **IEEE 802.11n** Wireless Router

LINKSYS WRT54G WIRELESS G BROADBAND ROUTER **54Mbps** **IEEE 802.11g** 4Router **2.4 GHz**)

Asus RT-AC3200 **IEEE 802.11ac** Ethernet Wireless Router **2.4, 5 GHz**

المصادر

1- **Computer networks, 5th Edition, 2011, By:** ANDREWS.TANENBAUM, Vrije Universiteit, Amsterdam, The Netherlands and DAVIDJ. WETHERALL, University of Washington, Seattle, WA.

2- **Data and Computer Communications, By:** William STALING 5th Edition, Prentice Hall 1997.

3- **Data Communication And Networking, By:** Behrouz A. Forouzan , Mc Graw Hill, 2007.

4- **Internet.**