Chapter 1

DATA COMMUNICATIONS:

- When we communicate, we are sharing information.
- This sharing can be local or remote.
- Data is information.
- Telecommunication: communication at a distance. It includes telephony, telegraph, and television.
- Data communications are the exchange of data between two devices via some form of transmission media, such as a wire cable

data communications system depends on four characteristics:

1. Delivery: The system must deliver data to the correct destination.
2. Accuracy: The system must deliver the data accurately (not altered).
3. Timeliness: The system must deliver data in a timely manner (not late).
4. Jitter: variation in the delay of received packets. Because of network congestion or improper queuing, the delay between packets can vary instead of remaining constant.

A data communications system has five components :

1. Message: is the information (data) to be communicated.
    - E.g. text, numbers, pictures, audio, and video.
2. Sender: is the device that sends the data message.
    - E.g. computer, workstation, telephone handset, video camera.
3. Receiver: is the device that receives the message.
    - E.g. computer, workstation, telephone handset, television.
4. Transmission medium: is the physical path by which a message travels from sender to receiver.
    - E.g. twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. is a set of rules that govern data communications.

Communication between two devices can be: (مُهم جداً)

1. Simplex mode, the communication is unidirectional Only one of the two devices on a link can transmit; the other can only receive.
2. half-duplex mode: each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa and the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
3. full-duplex mode (also called duplex), both stations can transmit and receive simultaneously. In this mode, signals going in one direction share the capacity of the link with signals going in the other direction.

Network is the interconnection of a set of devices capable of communication.

device can be:

- host: laptop, desktop, workstation, cellular phone, or security system.
- Connecting device: router, switch, a modem that changes the form of data.

Network Criteria:

- performance: measured by transit time or response time. evaluated by throughput and delay
- Reliability: measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
- Security: protecting data from damage or unauthorized access, and implementing procedures for recovery from breaches and data losses.

Type of Connection:

- Point-to-Point: The entire capacity of the link is reserved for transmission between two devices.
- Multipoint: More than two devices share a single link. (users must take turns, it is a timeshared connection)

Physical Topology:

Mesh: every device has a dedicated point-to-point link to every other device.

Number of cable: n (n – 1) / 2 duplex-mode links , n is the number of nodes

advantages:

- Eliminate the traffic
- Robust: If one link becomes unusable, it does not incapacitate the entire system.
- Security: message travels along a dedicated line, only the intended recipient sees it.
- point-to-point links make fault identification and fault isolation easy.

disadvantages:

- installation and reconnection are difficult
- the sheer bulk of the wiring can be greater than the available space
- the hardware required to connect each link (I/O ports and cable) can be expensive.

Star: each device has a dedicated point-to-point link only to a central controller called a hub.

Number of cable: N

advantages:

- less expensive than a mesh and easy to install and reconfigure.
- robustness: If one link fails, only that link is affected easy fault identification and Isolation.

disadvantage:

- dependency of topology on the hub. If the hub goes down, the system is dead.
- more cabling than other topologies

bus: is multipoint connection. 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.

- drop line is a connection running between the device and the main cable.
- tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

advantages:

- ease of installation using backbone cable, thus, less cabling than mesh or star.

disadvantage:

- difficult reconnection and fault isolation
- bus is designed to be optimally efficient at installation making it difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality.
- fault or break in the bus cable stops all transmission,

ring: each device has a dedicated point-to-point connection with only the two devices on either side of it

advantages:

- easy to install and reconfigure but the only constraints are media and traffic considerations (maximum ring length and number of devices).
- fault isolation is simplified, because the signal is circulating at all times. If one device does not receive a signal it issues an alarm alerts the network operator to the problem and its location.

disadvantage:

- unidirectional traffic.
- a break in the ring can disable the entire network. Solved by using dual ring or switch.

NETWORKS TYPES:

- Local Area Network(LAN): is usually privately owned and connects some hosts in a single office, building, or campus.
- wide area network (WAN) is also an connection of devices capable of communication.
    - switched WAN is a network with more than two ends.
    - switched WAN is a combination of several point-to-point WANs that are connected by switches.

Switching: An internet is a switched network in which a switch connects at least two links together.

- circuit-switched networks: dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive.
- packet-switched networks: In a computer network, the communication between the two ends is done in blocks of data called packets.

A router in a packet-switched network has a queue that can store and forward the packet. if packets arrive at one router when the thick line is already working at its full capacity, the packets stored and forwarded in the order they arrived.

a packet-switched network: is **more efficient** than a circuit switched network, but the packets may encounter some delays.

The Internet

- backbones are often referred to as international ISPs (Internet Service Providers), they are large networks owned by some communication companies connected through switching systems called peering points
- provider networks are often referred to as national or regional ISPs. They use the services of the backbones for a fee
- customer networks are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services

Accessing the Internet:

- Using Telephone Networks
    - Dial-up service. by adding a modem to convert data to voice , it is slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. used by small business.
    - DSL Service. allows the line to be used simultaneously for voice and data communication. but with higher speed than dial up
- Using Cable Networks
- Using Wireless Networks.
- Direct Connection to the Internet
    - large organization can itself become a local ISP and be connected to the Internet.

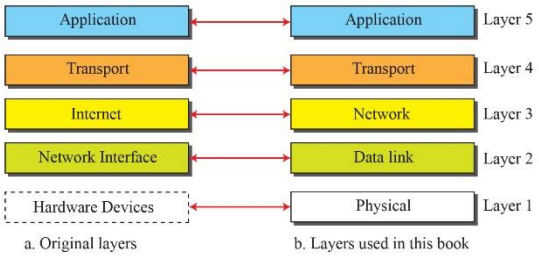
Chapter 2

Protocol: defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

- When communication is simple, we may need only one simple protocol;
- when the communication is complex, we need a protocol at each layer, or protocol layering

Principles of Protocol Layering:

1. dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
2. we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.
3. **TCP/IP** (Transmission Control Protocol/Internet Protocol) is a protocol suite (a set of protocols organized in different layers) used in the Internet today.
   - hierarchical protocol: means that each upper level protocol is supported by the services provided by one or more lower level protocols.



escription of Each Layer:

Physical Layer:

- The lowest layer is responsible for carrying individual bits in a frame across the link. The communication is logical, because there is a hidden layer -transmission media-under the physical layer.
- Two devices are connected by a transmission medium (cable or air) which does not carry bits, it carries electrical or optical signals.
- bits received in a frame from the data-link layer are transformed by some kind of protocol and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.

Data-link Layer:

- The data-link layer is responsible for taking the datagram and encapsulates it in a packet called a frame then moving it across the best link determined by the router.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN with different protocols used with any link type.
- There is no specific protocol for the data-link layer.
- Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, others just one.

Network Layer:

- responsible for host-to-host communication and routing the packet through possible routes.
- we need this layer to separate tasks between different layers and because the routers operate only in this layer which allows us to use fewer protocols on the routers.
- Includes the main protocol IP:
  - defines the format of the packet, called a datagram at the network layer.
  - defines the format and the structure of addresses used in this layer
  - IP responsible for routing a packet from its source to its destination, through multiple routers.
  - IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
  - The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols. A routing protocol does not rout (it is the responsibility of IP), but it creates forwarding tables for routers to help them in the process
- Some protocols that helps IP:
  - Internet Control Message Protocol (ICMP) report some problems when routing a packet.
  - Internet Group Management Protocol (IGMP) helps in multitasking.
  - Dynamic Host Configuration Protocol (DHCP) get the network-layer address for a host.
  - The Address Resolution Protocol (ARP) helps IP to find the link-layer address of a host or a router when its network-layer address is given.

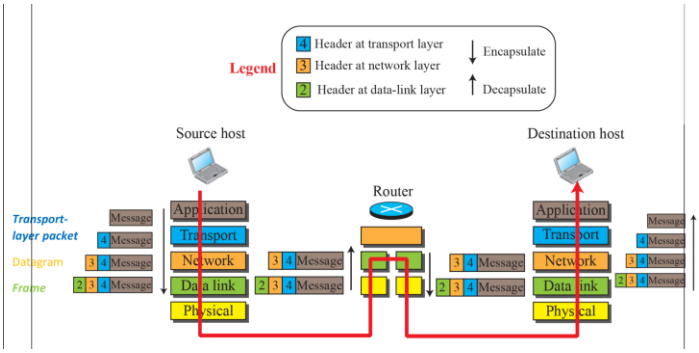
TCP	UDP
Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.	**Reliability**: UDP is connectionless protocol. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.
Ordered: If you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	**Ordered**: If you send two messages out, you don't know what order they'll arrive in i.e. **no ordered**

Transport Layer:

- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet (called a segment or a user datagram) and sends it, through the logical connection, to the transport layer at the destination host. In other words, it is responsible for giving services to the application layer
- logical connection at the transport layer is also end-to-end.
- why we need this layer? the reason is the separation of tasks and duties, and other protocols available in this layer.
- The main protocol, Transmission Control Protocol (TCP):
  - is a connection-oriented protocol that starts a logical connection between transport layers at two hosts before transferring data.
  - provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination).
  - Error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones) and congestion control to reduce the loss of segments due to congestion in the network.
- The other common protocol, User Datagram Protocol (UDP):
  - is a connectionless protocol that transmits user datagrams without first creating a logical connection.
  - in UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).
  - UDP is a simple protocol that does not provide flow, error, or congestion control.
  - Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets.
- A new protocol, Stream Control Transmission Protocol (SCTP):
  - is designed to respond to new applications that are emerging in the multimedia.

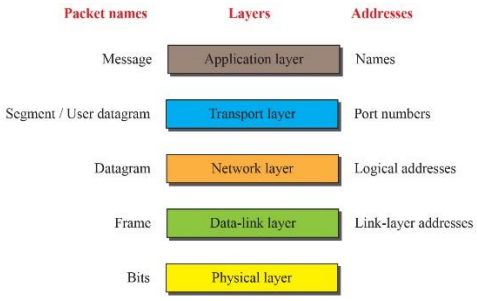
Encapsulation and Decapsulation:

One of the important concepts in protocol layering in the Internet is encapsulation/ Decapsulation



Addressing: source address and destination address.

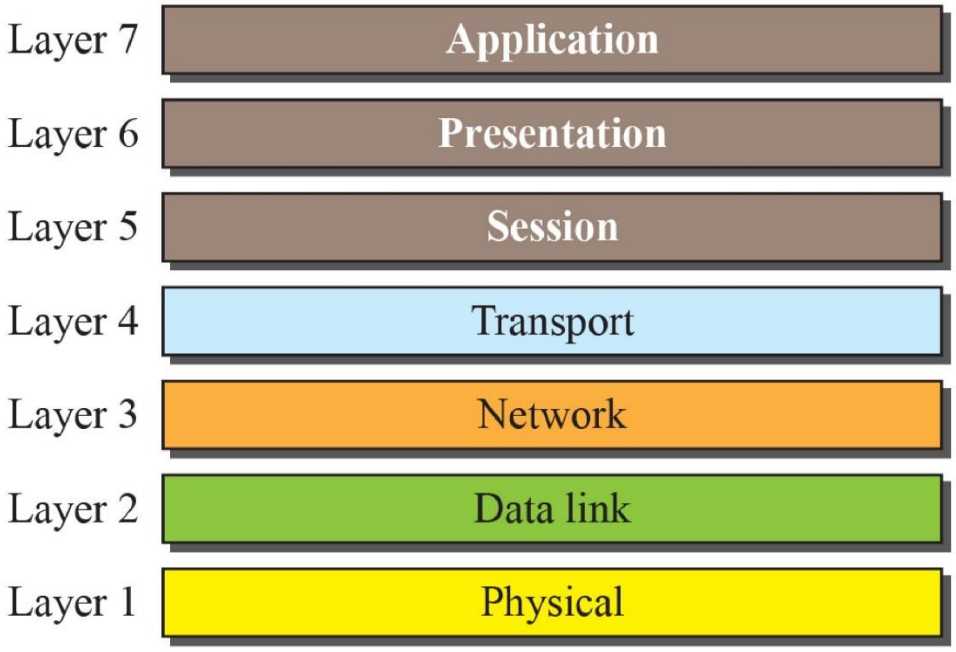
- Any communication that involves two parties needs two addresses: source address and destination address.
- Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four **because** the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address.



Multiplexing and Demultiplexing:

- Multiplexing: a protocol at a layer can encapsulate a packet from several next- higher layer protocols (one at a time).
- Demultiplexing: means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).

OSI MODEL:



Chapter 3

DATA AND SIGNALS:

- For transmission, data needs to be changed to signals.
- One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium.
- Data can be analog or digital.
- **Analog data:** information that is continuous
- **Digital data:** refers to information that has discrete states.

Analog and Digital Signals:

- **analog signal:** has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.
- **digital signal:** can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

Periodic and Nonperiodic:

- **periodic signal:** completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical **periods**. The completion of one full pattern is called a **cycle**.
- **nonperiodic signal:** changes without exhibiting a pattern or cycle that repeats over time.

PERIODIC ANALOG SIGNALS:

Periodic analog signals can be classified as:

- **Simple:** a sine wave, cannot be decomposed into simpler signals.
- **Composite:** is composed of multiple sine waves.

Sine wave: is the most fundamental form of a periodic analog signal.

- **Each cycle consists of a single** arc above the time axis followed by a single arc below
- A sine wave can be represented by three parameters:
    1. The peak amplitude
    2. The frequency.
    3. The phase.

The peak amplitude: of a signal is **the absolute value of its highest intensity**, proportional to the energy it carries. Normally **measured in volts.**

Period: Amount of time, in seconds, a signal needs to complete 1 cycle. Period is expressed in: **seconds**

Frequency: Number of periods in 1 second. Frequency is expressed in: **Hertz** (Hz)

Period is the **inverse** of frequency, and frequency is the **inverse** of period, as the following formulas show: (مهم مراجعه الأمثلة في السلايد ومعرفه طريقة حل المعادلة)

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

Phase: The term phase, or phase shift, **describes the position of the waveform relative to time 0**. Phase is measured in degrees or radians. (مهم مراجعه الأمثلة في السلايد ومعرفه طريقة حل المعادلة)

Wavelength: The distance a simple signal can travel in one period.

Time and Frequency Domains: (معرفه التحويل بالسلايد)

We have been showing a sine wave by using what is called a time domain plot.

Time-domain plot: shows changes in signal amplitude with respect to time (it is an amplitude-versus-time plot).

A frequency-domain plot is concerned with only the peak value and the frequency.

A complete sine wave is represented by one spike.

composite signal: is made of many simple sine waves, with different frequencies, amplitudes, and phases.

A single-frequency sine wave is not useful in data communications

Bandwidth: The range of frequencies contained in the signal. (مسائل مهمه)

How to measure the composite signal Bandwidth?

The bandwidth of a composite signal is the **difference** between the highest and the lowest frequencies contained in that signal.

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.
- If a signal has L levels, each level needs (log2 L) bits. (مسائل مهمه)

bit rate is the number of bits sent in 1s, expressed in bits per second (bps).

bit length: The bit length is the distance one bit occupies on the transmission medium.

Bit length = propagation speed × bit duration

Transmission of Digital Signals: A digital signal is a composite analog signal with an infinite bandwidth.

We can transmit a digital signal by using one of two different approaches:

1. Baseband transmission: means sending a digital signal over a channel without changing the digital signal to an analog signal.
    - requires that we have a **low-pass channel**: a channel with a bandwidth that starts from zero.
    - For example, the entire bandwidth of a cable connecting two computers is one single channel.
2. Broadband transmission: Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.
    - 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.

TRANSMISSION IMPAIRMENT: Signals travel through transmission media, which are not perfect.

- The imperfection causes signal impairment: The signal at the beginning of the medium is not the same as the signal at the end of the medium.

Three causes of impairment are:

1. Attenuation: means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
    - That is why a wire carrying electric signals gets warm, the wire becomes hot after a while because some of the electrical energy in the signal is converted to heat.
    - To **compensate** for this loss, **amplifiers** are used to amplify the signal.
    - 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.
2. Distortion: means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies.
3. Noise: Noise is another cause of impairment. **Several types of noise, such as:**
    1. **Thermal noise:** is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter.
    2. **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.
    3. **Crosstalk:** is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
    4. **Impulse noise:** is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

Signal-to-Noise Ratio (SNR): SNR is the ratio of what is wanted (signal) to what is not wanted (noise).

- **high SNR** means the signal is less corrupted by noise.
- **Low SNR** means the sign al is more corrupted by noise

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

DATA RATE LIMITS: How fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate:

1. **Noiseless Channel: Nyquist Bit Rate**
   - For a noiseless channel, the **Nyquist bit rate** formula defines the theoretical maximum bit rate
   - $\text{BitRate} = 2 \times \text{bandwidth} \times \log_2 L$
     - **Bandwidth** is the bandwidth of the channel.
     - **L** is the number of signal levels used to represent data.
     - **BitRate** is the bit rate in bits per second.
   - Increasing the levels of a signal may reduce the reliability of the system.
2. **Noisy Channel: Shannon Capacity**
   - To determine the theoretical highest data rate for a noisy channel:
   - $\text{Capacity} = \text{bandwidth} \times \log_2(1 + \text{SNR})$
     - **SNR**: signal-to- noise ratio **Capacity**: capacity of the channel in bits per second.

Using Both Limits: The Shannon capacity gives us the upper limit; the Nyquist formula tells us how many signal levels we need.

Bandwidth: One characteristic that measures network performance is bandwidth.

- **Bandwidth in Hertz:** Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.
- **Bandwidth in Bits per Seconds:** The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit.
- an **increase** in bandwidth in hertz means an **increase** in bandwidth in bits per second.

Throughput: is a measure of how fast we can actually send data through a network.

- **Bandwidth** in bits per second and **throughput** are different.
- A link may have a **bandwidth** of B bps, but we can **only** send T bps through this link, with T always **less** than B.

Latency: or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

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

- **Propagation time:** measures the time required for a bit to travel from the source to the destination. Propagation time = Distance / (Propagation Speed)
- **Transmission time:** time between the first bit leaving the sender and the last bit arriving at the receiver. The transmission time of a message depends on the size of the message and the bandwidth of the channel. Transmission time = (Message size) / Bandwidth
- **Queuing time:** the time needed for each intermediate or end device to hold the message before it can be processed.

Bandwidth-Delay Product: The bandwidth-delay product defines the number of bits that can fill the link.

Jitter: Another performance issue that is related to delay is jitter.

- We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, 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 endures jitter.

Describe Data and Signal in the form of Analog and Digital.

	Analog	Digital
Signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Data	The term analog data refers to information that is continuous, Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.	digital data refers to information that has discrete states. Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Chapter 7

Transmission media: are actually located below the physical layer and are directly controlled by the physical layer. We could say that transmission media belong to **layer zero**. In data communications, the transmission medium is usually **free space**, **metallic cable**, or **fiber-optic cable**.

A transmission medium: can be broadly defined as anything that can carry information from a **source** to a **destination**.

Guided media: provide a conduit from one device to another, include:

1. Twisted-pair cable
2. Coaxial cables
3. Fiber-optic cables

Twisted-Pair Cable: A twisted pair consists of **two** conductors (normally copper), each with its own plastic insulation, twisted together

- 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.
- **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).**

Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each category is suitable for specific uses.

Connectors: The most common UTP connector is **RJ45** (RJ stands for registered jack). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

Performance: One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies.
Note that **gauge** is a measure of the thickness of the wire.

Applications: Twisted-pair cables are used in telephone lines to provide voice and data channels.

Coaxial Cable: Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.

- **Coaxial Cable Standards:** Coaxial cables are categorized by their Radio Government (RG) ratings.
- **Coaxial Cable Connectors:** To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector.
- **Performance:** The attenuation is much higher in coaxial cable than in twisted-pair cable.
- **Applications:** Coaxial cable was widely used in analog telephone networks. Later it was used in digital telephone Networks. Cable TV networks also use coaxial cables.

Fiber-Optic Cable:

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic **core** is surrounded by a **cladding** of less dense glass or plastic.

Propagation modes:

- **Multimode:** Multiple beams from a light source move through the core in different paths.
- **Single-mode:** limits beams to a small range of angles, all close to the horizontal.

Fiber Sizes: Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

Fiber-Optic Cable Connectors: There are three types of connectors for fiber-optic cables:

1. **subscriber channel (SC) connector** is used for cable TV. It uses a push/pull locking system.
2. **straight-tip (ST) connector** is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.
3. **MT-RJ** is a connector that is the same size as RJ45.

Performance: Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually one tenth as many) repeaters when we use fiber-optic cable.

Applications: Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages of Optical Fiber	Disadvantages of Optical Fiber
❑Higher bandwidth. ❑ Less signal attenuation. ❑ Immunity to electromagnetic interference. ❑ Resistance to corrosive materials. ❑ Light weight. ❑ Greater immunity to tapping.	❑Installation and maintenance. ❑ Unidirectional light propagation. ❑ Cost.

Unshielded twisted pair (UTP)		Shielded twisted pair (STP)	
Advantages	Disadvantages	Advantages	Disadvantages
• Easy installation • Capable of high speed for LAN • Low cost	It may be prone to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights)	• Shielded • Faster than UTP and coaxial	• More expensive than UTP and coaxial • More difficult installation

Unguided medium: transport waves without using a physical conductor.

- This type of communication is often referred to as wireless communication.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Unguided signals can travel from the source to the destination in several ways:
    1. ground propagation
        - Radio waves travel through the lowest portion of the atmosphere, hugging the earth.
        - These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
        - Distance depends on the amount of power in the signal: The greater the power, the greater the distance.
    2. sky propagation
        - Higher-frequency radio waves radiate upward into the ionosphere, where they are reflected back to earth.
        - This type of transmission allows for greater distances with lower output power.
    3. line-of-sight propagation.
        - Very high-frequency signals are transmitted in straight lines directly from antenna to antenna.
        - Antennas must be: directional, facing each other, either not affected by the curvature of the earth (tall enough or close enough together)

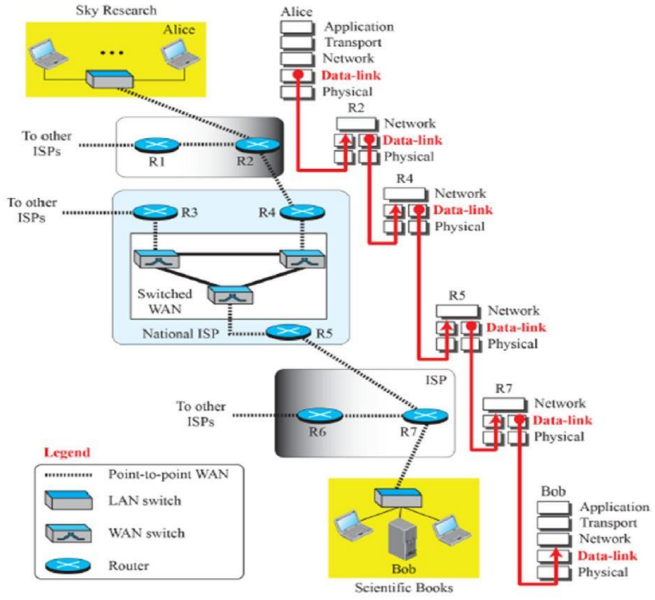
We can divide wireless transmission into three broad groups:

1. **Radio Waves:** Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called **radio waves.**
    - **Applications:** useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio
2. **Microwaves:** Electromagnetic waves having frequencies between 1 and 300 GHz are called **Microwaves**.
    - Microwaves are **unidirectional**. When an antenna transmits microwaves, they can be narrowly focused. This means that the **sending** and **receiving antennas** need to be **aligned**.
    - **Applications:** Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.
3. **Infrared:** **Infrared waves,** with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.
4. **Applications*:*** Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Chapter 9

Communication at the data-link layer:

- Communication at the data-link layer is made up of five separate logical connections between the data-link layers in the path.
- The data-link layer at Alice's computer communicates with the data-link layer at router R2.
- The data-link layer at router R2 communicates with the data-link layer at router R4 and so on.
- Finally, the data-link layer at router R7 communicates with the data-link layer at Bob's computer.
- Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router. The reason is that Alice's and Bob's computers are each connected to a single network, but each router takes input from one network and sends output to another network.



Nodes and Links:

- Communication at the data-link layer is **node-to-node**.
- A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point.
- Theses LANs and WANs are connected by routers.
- It is customary to refer to:
  - The two end: **hosts**.
  - The routers: **nodes**.
  - The networks in between as: **links**.

Services:

- The data-link layer is located between the physical and the network layers.
- The data-link layer provides services to the network layer;

services provided by a data-link layer as shown below:

1. **Framing:** The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a frame (data-link-layer packect) before sending it to the next node. The node also needs to decapsulate the datagram from the frame received on the logical channel.
2. **Flow Control:** The sending data-link layer is a producer of frames; the receiving data-link layer is a consumer. If the rate of produced frames is higher than consumed ones, frames at the receiving end need to be **buffered** waiting to be consumed (processed). We cannot have unlimited buffer size so we have to **either** let the receiving end to drop frames when it is full or to send feedback to the sending end to ask it to stop or slow down.
3. **Error Control:** At the sending node, a frame needs to be changed to bits, then to electromagnetic signals, and transmitted through the transmission media. At the receiving node these signals are received transformed to bits, and put together to create a frame.
4. **Congestion Control:** a link may be congested with frames, which result in frame loss, most data-link-layer protocols do not directly use a congestion control to alleviate congestion.

Two Categories of Links: (مهم)

1. **point-to-point link**: the link is dedicated to the two devices. Example: traditional home phones
2. **broadcast link:** the link is shared between several pairs of devices. Example: cell phone.

Two Sublayers:

1. **The data link control sublayer (DLC)** deals with all issues common to both point-to-point and broadcast links
2. **The media access control sublayer (MAC)** deals only with issues specific to broadcast links.

LINK-LAYER ADDRESSING:

- the IP addresses in a datagram should not be changed. If the destination IP address in a datagram changes, the packet never reaches its destination
- **link-layer addresses** of the two nodes, sometimes called a **link address**, or a **physical address**, or a **MAC address**.
- The destination link layer address is determined by using the Address Resolution Protocol (ARP)

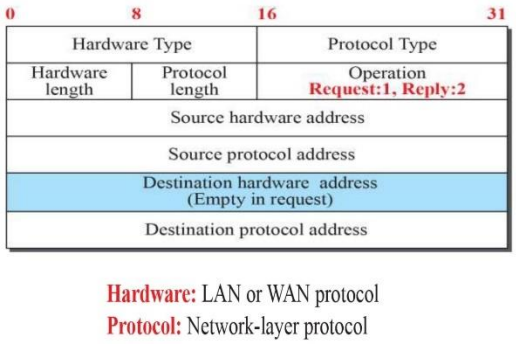
Three Types of addresses:

1. **Unicast:** Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.
    - **48 bits (six bytes)** that are presented as **12 hexadecimal** digits separated by colons
    - The second digit needs to be an even number. (0,2,4,6,8,A,C,E)
    - A**2**:34:45:11:92:F1
2. **Multicast**: **one-to-many** communication. However, the jurisdiction is local (inside the link).
    - **48 bits (six bytes)** that are presented as **12 hexadecimal** digits separated by colons
    - The second digit needs to be an odd number. (1,3,5,7,9,B,D,F)
    - A**3**:34:45:11:92:F1
3. **Broadcast**: **one-to-all** communication. A frame with a destination broadcast address is sent to all entities in the link.
    - **48 bits (six bytes)** that are presented as **12 hexadecimal** digits separated by colons
    - The All digit needs to be **F** **(**FF:FF:FF:FF:FF:FF**)**

Address Resolution Protocol (ARP):

- The ARP protocol is one of the network layer protocols.
- ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.
- ARP Request is **Broadcast**, ARP Reply is **Unicast**

ARP packet:

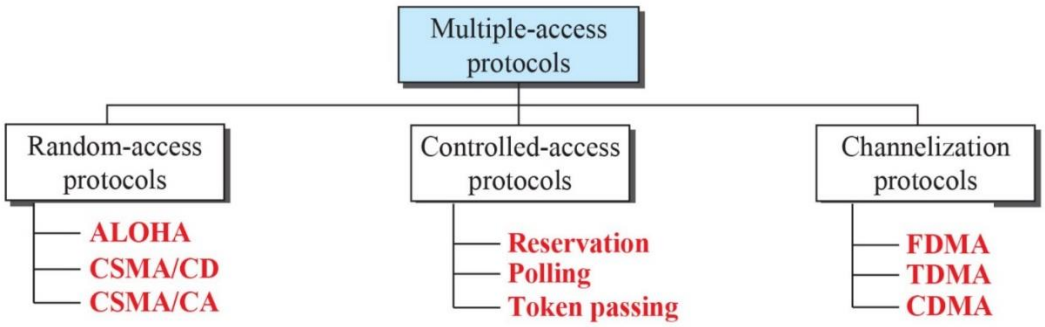


- **hardware type** field defines the type of the link-layer protocol; Ethernet is given the type 1.
- **protocol type** field defines the network-layer protocol: IPv4 protocol is (0800)16
- **source hardware and source protocol addresses** are variable-length fields defining the linklayer and network-layer addresses of the sender.
- **destination hardware address and destination protocol address** fields define the receiver link-layer and network-layer addresses. An ARP packet is encapsulated directly into a datalink frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

Chapter 12

multiple-access protocols:

- when nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.
- Many protocols have been devised to handle access to a shared link.
- All of these protocols belong to a sub-layer in the data-link layer called media access control (MAC)



RANDOM ACCESS: Two features give this method its name:

1. First, there is no scheduled time for a station to transmit. Transmission is random among the stations -random access-.
2. Second, no rules specify which station should send next. They compete to access the medium-contention methods-.

random-access methods have three main protocols:

1. **ALOHA** protocol, used carrier sense multiple access **(CSMA). designed for a radio (wireless) LAN, but it can be used on any shared medium.**
2. carrier sense multiple access with collision detection **(CSMA/CD)** tells the station what to do when a collision is detected
3. carrier sense multiple access with collision avoidance **(CSMA/CA),** which tries to avoid the collision.

CSMA:

- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- CSMA can reduce the possibility of collision, but it cannot eliminate it. because of propagation delay

Vulnerable time in CSMA: The Vulnerable time for CSMA is the propagation time

Persistence methods:

- **1-Persistent method:** It is simple and straightforward. The station finds the line idle then sends its frame immediately (with probability 1). This method has the **highest chance of collision** because two or more stations may find the line idle and send their frames immediately. **Ethernet** uses this method.
- **No persistent method:** a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. This method **reduces the chance of collision** because it is unlikely that two or more stations will wait the same amount of time and retry to send at the same time. However, this method **reduces the efficiency of the network** because the medium remains idle when there may be stations with frames to send.
- **p-Persistent method:** It is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. This method combines the advantages of the other two strategies. It **reduces the chance of collision and improves efficiency**. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame. 2. With probability q = 1 − p, the station waits for the beginning of the next time slot and checks the line again.
2. If the line is idle, it goes to step 1.
3. If it is busy, it acts as a collision has occurred and uses the back off procedure.

CSMA/CD: In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. **The frame transmission time (Tfr)** Must be **at least Two times** the maximum propagation time Tp

Energy Level: We can say that the level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level.

Throughput: The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
Traditional Ethernet: One of the LAN protocols that used CSMA/CD is the traditional Ethernet with the data rate of 10 Mbps.

CSMA/CA: Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for **wireless networks.** Collisions are avoided through the use of CSMA/CA's **three strategies:**

- interframe space (IFS)
- contention window
- acknowledgments

CONTROLLED ACCESS: In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three controlled access methods:

- Reservation: station needs to make a reservation before sending data. **Time is divided into intervals**. In each interval, a reservation frame **precedes** the data frames sent in that interval.
- Polling: works with topologies in which one device is a **primary station** and the others are **secondary stations**. All data exchanges **must** be made through the primary device even when the destination is a secondary device. **The primary device controls the link**; the secondary devices follow its instructions., This method uses **poll** and **select functions** to prevent collisions
- Token passing: the stations in a network are organized in a **logical ring**. In other words, for each station, there is a **predecessor** and a **successor**. The predecessor is the station which is logically **before** the station in the ring; the successor is the station which is **after** the station in the ring.

CHANNELIZATION: Channelization (or channel partition, as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code. **three protocols:**

- frequency-division multiple access (FDMA): the available bandwidth of the common channel is divided into bands that are separated by guard bands.
- time-division multiple access (TDMA): the bandwidth is just one channel that is timeshared between different stations.
- Code-division multiple access (CDMA): one channel carries all transmissions simultaneously.

Chips: CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called **chips**

Data Representation: We follow these rules for encoding:

- If a station needs to send a **0 bit**, it encodes it as **–1**;
- if it needs to send a **1 bit**, it encodes it as **+1**.
- When a station is **idle,** it sends no signal, which is interpreted as a **0.**

Chapter 13

Ethernet Evolution (four generations):

1. Standard Ethernet (10 Mbps).
2. Fast Ethernet (100 Mbps).
3. Gigabit Ethernet (1 Gbps)
4. 10 Gigabit Ethernet (10 Gbps).

Standard Ethernet characteristics:

5. Connectionless and Unreliable Service:
    1) connectionless service means each frame sent is independent of the previous or next frame.
    2) If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless
    3) Ethernet is also unreliable like IP and UDP. If a frame is corrupted during transmission and the receiver finds out about the corruption, the receiver drops the frame silently.
2. Frame Format: The Ethernet frame contains seven fields:
    1) **Preamble:** This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock
    2) **Start frame delimiter (SFD):** added at the physical layer. this field is a flag(1 byte: 10101011) signals the frame beginning and to warn rec for last chance for synch, The last 2 bits are (11)2 and alert the receiver that the next field is the destination address.
    3) **Destination address (DA):** 6 bytes (48 bits) and contains the link-layer address of the destination to receive the packet when see it decapsulates the frame and passes the data to the upper layer protocol defined by the value of the type field.
    4) **Source address (SA):** 6 bytes field and contains the link-layer address of the sender of the packet.
    5) **Type:** defines the upper-layer protocol whose packet is encapsulated in the frame e.g. IP. used for multiplexing and demultiplexing.
    6) **Data:** carries data with max 1500 and min 46 value, if it is more than max, it is fragmented, if it is less than min it is padded with extra 0s.
    7) **CRC:** error detection information, receiver calculate it over the addresses, types, and data field., if it is 0 _interrupted it is discarded.
3. Frame Length:
    1) Minimum frame length: 64 bytes
    2) Maximum frame length: 1518 bytes
    3) Minimum data length: 46 bytes
    4) Maximum data length: 1500 bytes

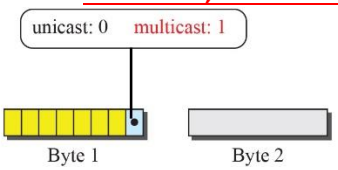
Addressing: Each station on an Ethernet network (such as a PC, workstation, or printer) has its own **network interface card (NIC).** The NIC fits inside the station and provides the station with a **link-layer Address (MAC address).** The Ethernet address is **6 bytes (48 bits) written in hexadecimal notation** example (4A:30:10:21:10:1A)

Transmission of Address Bits: The way the addresses are sent out online is **different** from the way they are **written** in hexadecimal notation. 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.
The address is sent left to right, byte by byte; 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.
- If the **least** significant bit of the first byte in a destination address is **0**, the address is **unicast, otherwise, it is multicast.**



Distinguish Between Unicast, Multicast, and Broadcast Transmission:
Standard Ethernet uses a coaxial cable (bus topology) packet is send to all stations, transmission in the standard Ethernet is **always broadcast**, but we can distinguish between the 3 ways of transmission in the way the frames are kept or dropped:

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

Access Method: standard Ethernet protocol is a broadcast network, standard Ethernet chose CSMA/CD with 1-persistent method.

Efficiency of Standard Ethernet: is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station

Efficiency = 1 / (1 + 6.4 x a)

- a: number of frames that can fit on the medium
- a = (propagation delay)/(transmission delay)

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

Implementation:

- **10BaseX**, the number defines the **data rate** (10 Mbps)
- **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)
- **F** for fiber-optic

goals of Fast Ethernet can be summarized as follows:

1) Upgrade the data rate to 100 Mbps.
2) Make it compatible with Standard Ethernet.
3) Keep the same 48-bit address.
4) Keep the same frame format.

Access Method: CSMA/CD depends on the transmission rate, the minimum size of the frame, and the maximum network length. If we want to keep the minimum size of the frame, the maximum length of the network should be changed. So the Fast Ethernet came with two solutions:

1) is to 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
2) to use a link-layer switch with a buffer to store frames and a fullduplex connection to each host to make the transmission medium private for each host. so, there is no need for CSMA/CD . And the shared medium is changed to many point-to- point media, and there is no need for contention.

Autonegotiation: A new feature added to Fast Ethernet. It was designed particularly for these purposes:

- To allow incompatible devices to connect to one another. E.g., a device with a max capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but which can work at a lower rate).
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

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.
3) Keep the same 48-bit address.
4) Keep the same frame format.
5) Keep the same minimum and maximum frame lengths.
6) Support Autonegotiation as defined in Fast Ethernet.

MAC Sublayer of the Gigabit Ethernet

- Full-Duplex Mode
- Half-Duplex Mode

Physical Layer: physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet.

goals of the 10 Gigabit Ethernet design can be summarized as:

- upgrading the data rate to 10 Gbps, this is possible only with fiber-optic technology
- keeping the same frame size and format
- allowing the interconnection of LANs, MANs, and WAN possible.

The standard defines two types of physical layers:

- LAN PHY: is designed to support existing LANs
- WAN PHY. defines a WAN with links connected through SONET OC-192.