



Islamic University of Gaza
Faculty of Engineering
Computer Engineering Department
Fall 2025



Data Communications Lab

Lab 2

Fundamentals of data communications and computer networks-part2



Eng. Abdullah Idris Ouda

Eng. Haneen Beram

Computer Network Components

Computer network components are the *major parts* which are needed to *install the software*. Some important network components are **NIC, switch, cable, hub, router, and modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

NIC

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).
- There are two types of NIC:
 - **Wired NIC:** The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.
 - **Wireless NIC:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

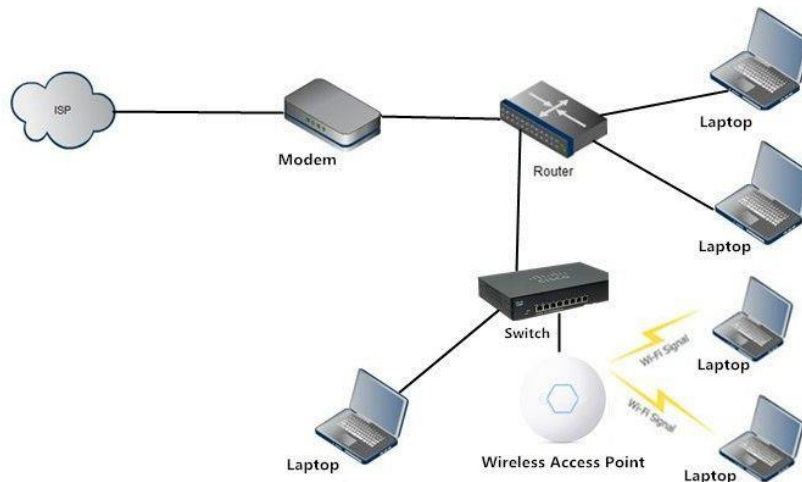
A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- It stands for Modulator/Demodulator.
- It converts the digital data into an analog signal over the telephone lines.
- here are three common types of modem connections:
 - **Dial-up** — A modem that uses a phone line to connect to an ISP. This is the oldest type of modem connection.
 - **DSL** — A digital subscriber line modem uses a phone line to connect to an ISP but with much higher speeds than dial-up.
 - **Cable** — A modem that uses a cable TV line to connect to an ISP. This is the most common type of modem connection.



Transmission Media

For any networking to be effective, raw stream of data is to be transported from one device to other over some medium. Various transmission media can be used for transfer of data. These transmission media may be of two types –

- **Guided** – In guided media, transmitted data travels through cabling system that has a fixed path. For example, copper wires, fiber optic wires, etc.
- **Unguided** – In unguided media, transmitted data travels through free space in form of electromagnetic signal. For example, radio waves, lasers, etc.

Twisted Pair Cable

Copper wires are the most common wires used for transmitting signals because of good performance at low costs. They are most commonly used in telephone lines. However, if two or more wires are lying together, they can interfere with each other's signals. To reduce this electromagnetic interference, pair of copper wires are twisted together in helical shape like a DNA molecule. Such twisted copper wires are called **twisted pair**. To reduce interference between nearby twisted pairs, the twist rates are different for each pair.

There are two sub-categories of Twisted Pair Cables as mentioned below;

- Unshielded Twisted Pair Cable (UTP)
- Shielded Twisted Pair Cable (STP)

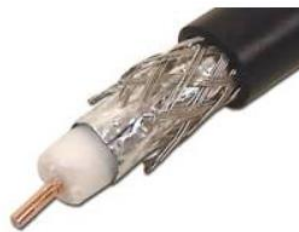
Unshielded Twisted Pair Cable (UTP) is the most common type of cable used in networks. Almost all Ethernet LANs are built using UTP cables. UTP cables are thin and flexible and very cost effective which makes them the ideal choice for Ethernet cabling. Figure below shows an Unshielded Twisted Pair Cable



Shielded Twisted Pair Cable (STP) wraps each pair of wire in a metallic foil and further wraps all four pairs of wires in a metallic braid or foil, this further reduces the noise both within the cable from outside the cable. STP cable is more expensive than UTP cable and is much more difficult to install and manage. Figure below shows a Shielded Twisted Pair Cable.



2- Coaxial cable is the most popular cable in cable television industry, a coaxial cable consists of copper conductor which is surrounded by an insulation material, over the insulation material is copper braid or foil that acts both as the second wire in the circuit and as a shield for the inner conductor thereby protecting it from interference. The coaxial cable is difficult to install and manage but it can support much greater cable lengths. Figure below shows a coaxial cable.



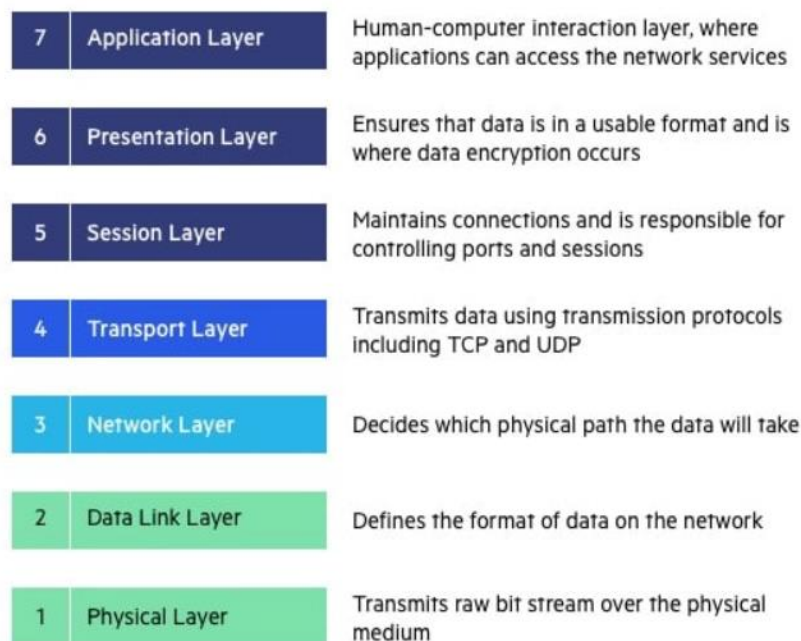
3- Fiber-Optic cable is made up of glass and plastic fibers surrounded by several layers of protective materials. Fiber-optic cables are much more expensive than twisted-pair and coaxial cables. Fiber-optic cables are immune to EMI and can run small and large distances depending upon the type of cable. Fiber-optic cables support very high bandwidth which makes them the preferred choice of cables when high speed connectivity is required. Figure below shows a fiber-optic cable.



OSI model

OSI (Open Systems Interconnection) model was created by the International Organization for Standardization (ISO), an international standard-setting body. It was designed to be a reference model for describing the functions of a communication system. The **OSI model** provides a framework for creating and implementing networking standards and devices and describes how network applications on different computers can communicate through the network media.

The **OSI model** has **seven layers**, with each layer describing a different function of data traveling through a network. Here is the graphical representation of these layers:



Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself.

Here is a brief description of each of the layers of the OSI model.

7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

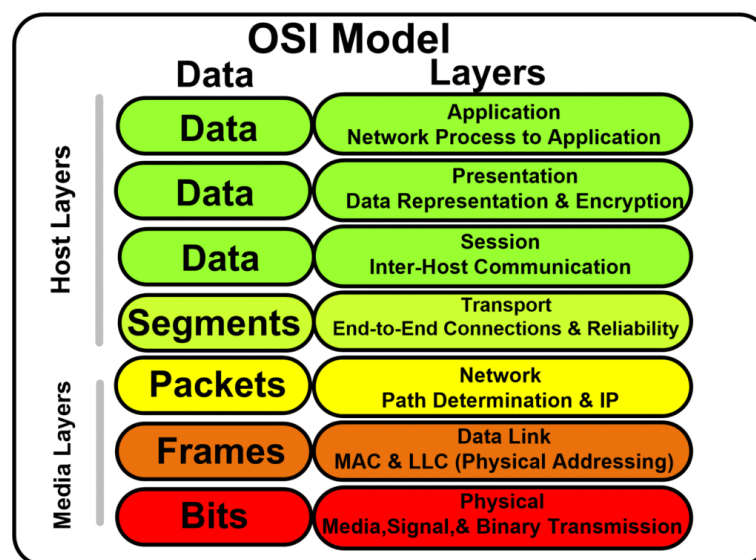
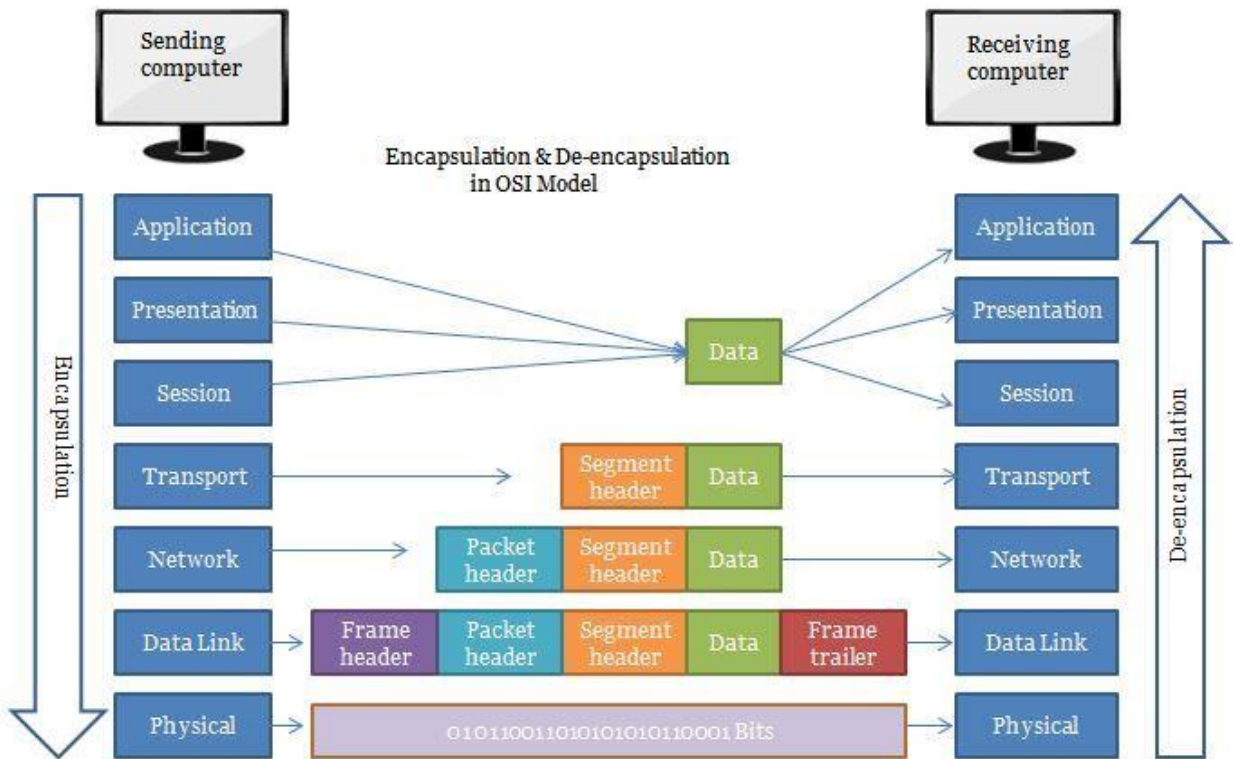
2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

1. Physical Layer

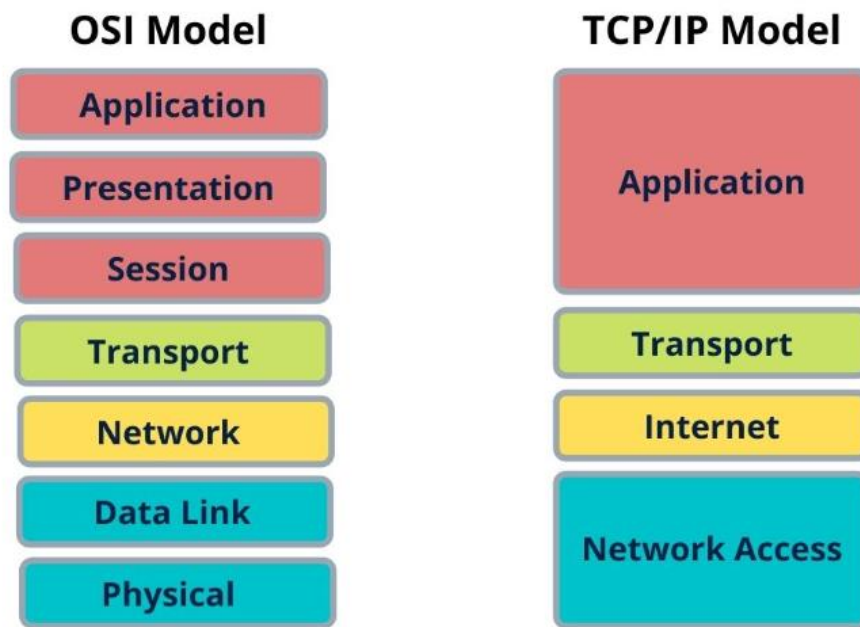
The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

When transmitting data from one machine to another, the data flow starts at the Application layer proceeding down to the Physical layer. Then over the channel to the receiving machine and back up the hierarchy.



TCP/IP model:

The **TCP/IP (Transmission Control Protocol/Internet Protocol) model** was introduced before the OSI model. This model helps users understand how a specific computer should be connected to the internet and how data can transmit between them. TCP/IP is used more compared to the OSI model for providing communication between computers over the internet.



The following are the **four layers** of the TCP/IP model:

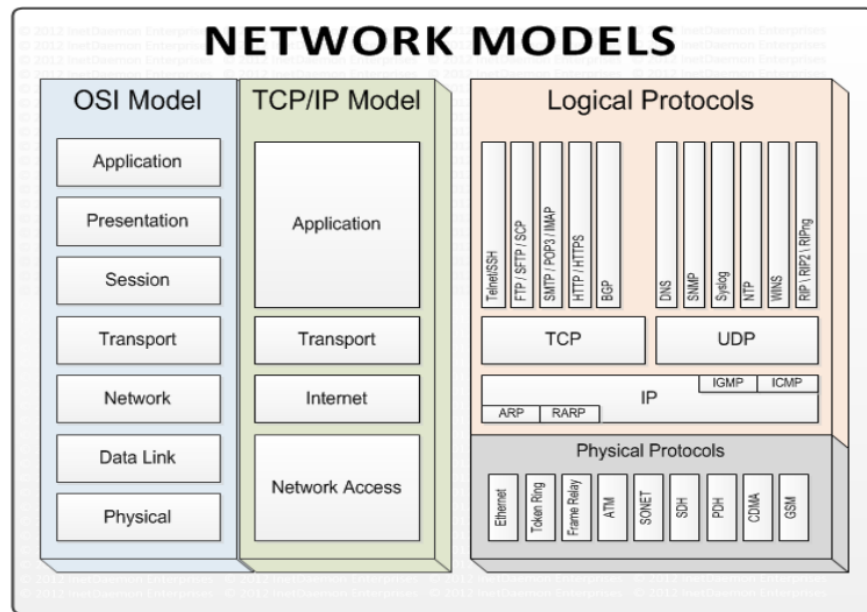
Network Access Layer: It is the lowest layer of the TCP/IP Model that helps in the transmission of data between two devices on the same network. This layer is a combination of the Physical and Data Link layer of the OSI model.

Internet Layer: Helps in moving packets from destination to source. This layer corresponds to the Network layer of the OSI Model.

Transport Layer: Responsible for reliable and error-free process to process message delivery. It is parallel to the Network layer of the OSI Model.

Application Layer: This layer provides access to network resources. When the Application, Presentation, and Sessions layers of the OSI model are combined, they perform similar functions as the Application layer of the TCP/IP model.

Some of important protocols:



Application layer protocols:

HTTP: HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video.

FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

TELNET: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

Transport layer protocols:

1- TCP

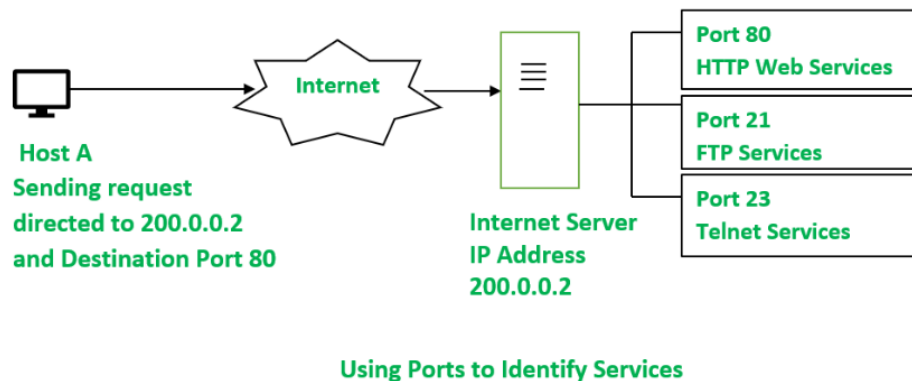
Transmission Control Protocol (TCP) is connection-oriented, meaning once a connection has been established, data can be transmitted in two directions. TCP has built-in systems to check for errors and to guarantee data will be delivered in the order it was sent, making it the perfect protocol for transferring information like still images, data files, and web pages.

But while TCP is instinctively reliable, its feedback mechanisms also result in a larger overhead, translating to greater use of the available bandwidth on your network.

2- UDP

User Datagram Protocol (UDP) is a simpler, connectionless Internet protocol wherein error-checking and recovery services are not required. With UDP, there is no overhead for opening a connection, maintaining a connection, or terminating a connection; data is continuously sent to the recipient, whether or not they receive it.

Although UDP isn't ideal for sending an email, viewing a webpage, or downloading a file, it is largely preferred for real-time communications.



Network layer protocols:

Internet Protocol (IP): This protocol is responsible for addressing and routing data packets across the internet. It works by assigning a unique numerical address, called an IP address, to each device on a network. This allows data packets to be forwarded to the correct device based on the IP address.

Internet Control Message Protocol (ICMP): This protocol is used to transmit error messages and other information between devices on a network. It is often used to troubleshoot network issues or to send diagnostic information.

Address Resolution Protocol (ARP): This protocol is used to map IP addresses to physical addresses, such as a device's media access control (MAC) address. This allows devices to communicate with each other on a network.