

The Islamic University of Gaza
Engineering Faculty
Department of Computer Engineering

Data Communications

Lab 2

Computer Network Components & Computer Network Models

Computer Network Components

Network Devices:

1. Repeaters
2. Hubs
3. Switches
4. Routers

Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.



Hubs

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 Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.



Switches

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. **Note: Switches work at the data link layer.**



Routers

A router translates information from one network to another. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts. **Routers work at the network layer.** If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet.



Cables and Connectors

Cable is a transmission media used for transmitting a signal.

1- Twisted Pair

cable has pairs of wires with each pair twisted to eliminate electromagnetic interference and prevent crosstalk; each pair forms a circuit which can transmit data. At each end of the cable RJ-45 connectors are installed, The RJ-45 is an eight-wire connector used commonly to connect computers onto an Ethernet local-area network (LAN).

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. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated various categories of wire some of which are shown below.

Category	Maximum Speed	Use
1	1 Mbps	Voice (Telephone wire)
2	4 Mbps	Telephone
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring
5	100 Mbps & 1000 Mbps	100BaseT Ethernet & Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Figure below shows an Unshielded Twisted Pair Cable



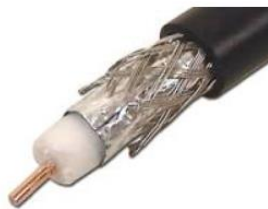
Shielded Twisted Pair Cable (STP) wraps each pair of wire in a metallic foil and further wraps all four pairs of wires in a metallic braid or foil, this further reduces the noise both within the cable from outside the cable. STP cable is more expensive than UTP cable and is much more difficult to install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

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 a copper conductor which is surrounded by an insulation material, over the insulation material is a 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.

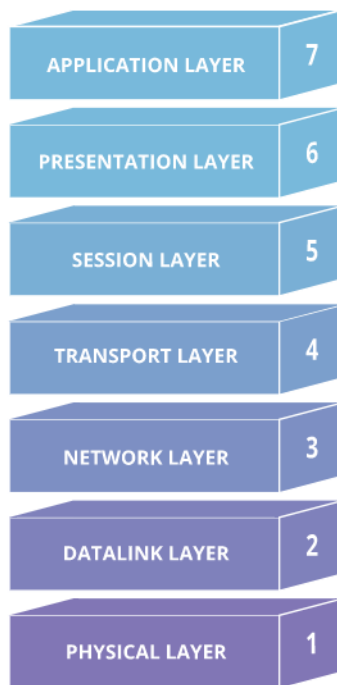
Figure below shows a fiber-optic cable.



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:



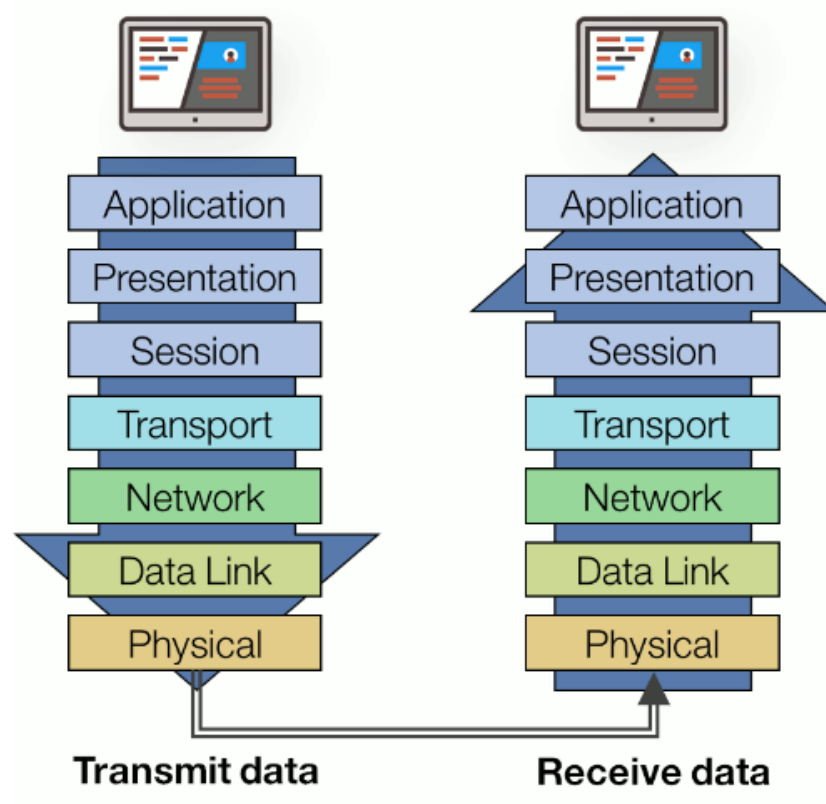
Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself.

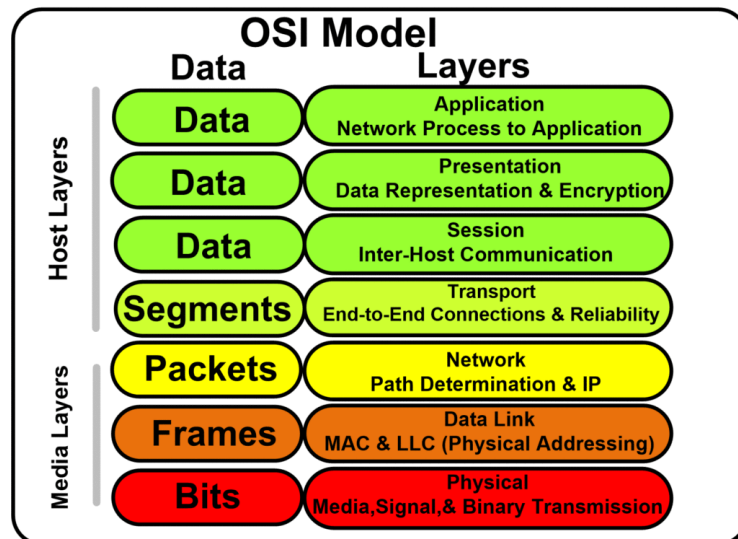
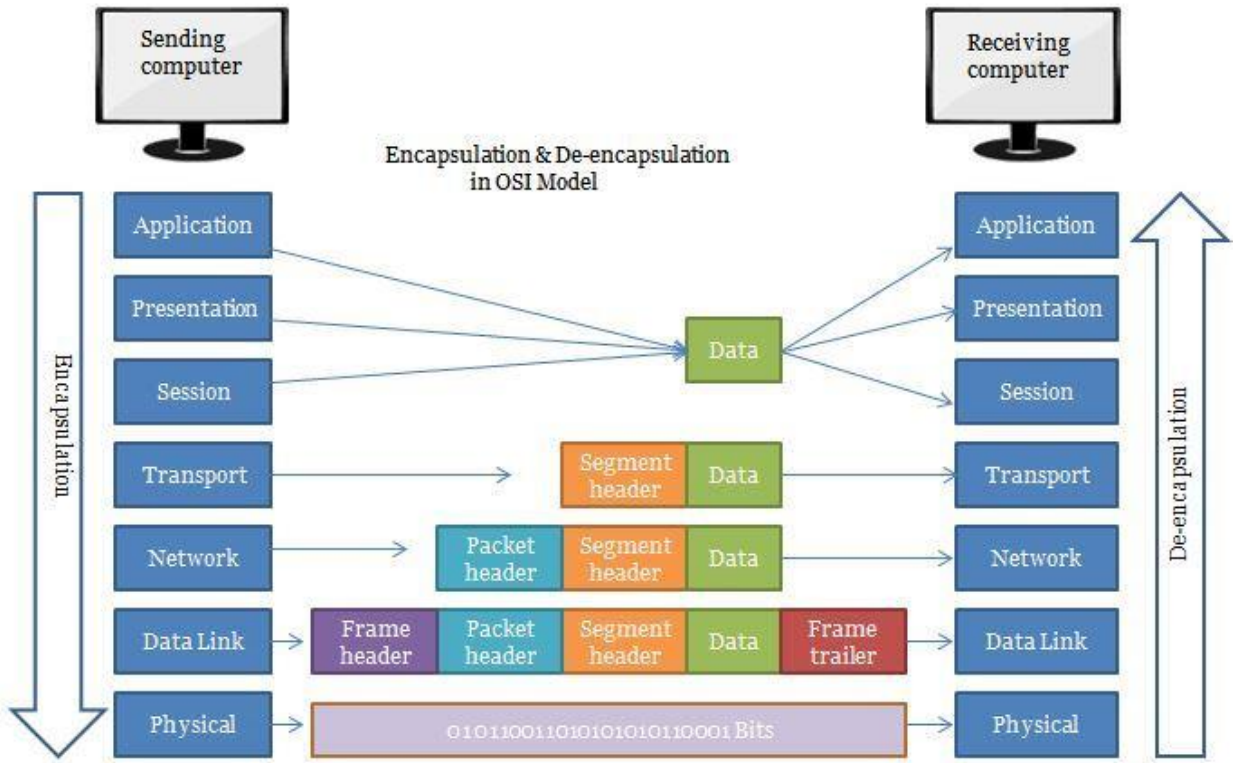
Here is a brief description of each of the layers of the OSI model.

- **Physical** – defines how to move bits from one device to another. It details how cables, connectors and network interface cards are supposed to work and how to send and receive bits.
- **Data Link** – encapsulates a packet in a frame. A frame contains a header and a trailer that enable devices to communicate. A header (most commonly) contains a source and destination MAC address. A trailer contains the Frame Check Sequence field, which is used to detect transmission errors. The data link layer has two sublayers:

1. **Logical Link Control** – used for flow control and error detection.
 2. **Media Access Control** – used for hardware addressing and for controlling the access method.
- **Network** – defines device addressing, routing, and path determination. Device (logical) addressing is used to identify a host on a network (e.g. by its IP address).
 - **Transport** – segments big chunks of data received from the upper layer protocols. Establishes and terminates connections between two computers. Used for flow control and data recovery.
 - **Session** – defines how to establish and terminate a session between the two systems.
 - **Presentation** – defines data formats. Compression and encryption are defined at this layer.
 - **Application** – this layer is the closest to the user. It enables network applications to communicate with other network applications.

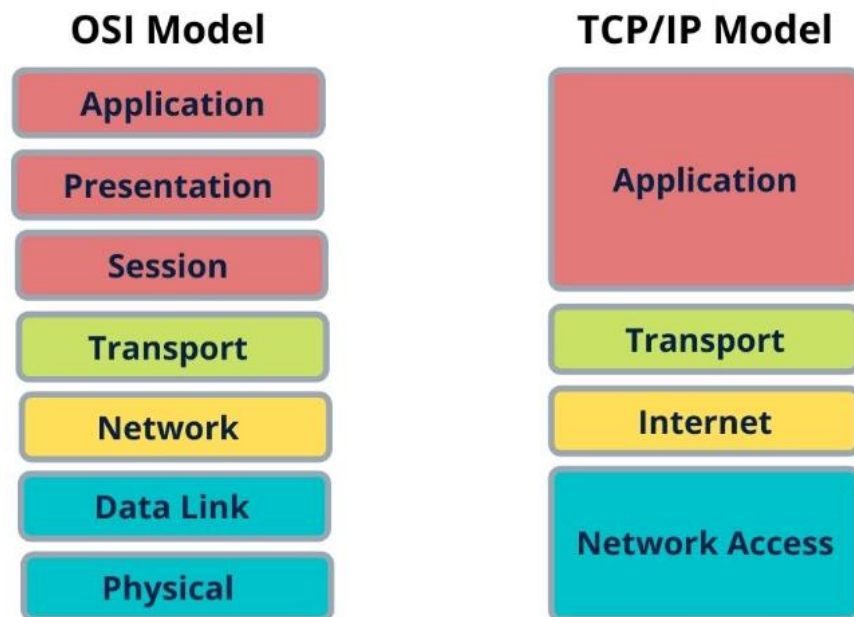
When transmitting data from one machine to another, the data flow starts at the Application layer proceeding down to the Physical layer. Then over the channel to the receiving machine and back up the hierarchy.





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:

OSI Layers	TCP/IP Layers	TCP/IP Protocols				
Application Layer	Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Presentation Layer						
Session Layer						
Transport Layer	Transport Layer	TCP		UDP		
Network Layer	Network Layer	IP				
Data Link Layer	Network Interface Layer	Ethernet	Token Ring	Other Link-Layer Protocols		
Physical Layer						

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. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

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 like broadcast or multitask network transmission.

Network layer protocols:

IP protocol: is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.