**Computer networks Fundamentals CMP 312**

**Introduction**

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication 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 communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. In general, data communications networks collect data from personal computers and other related devices and transmit those data to a central server. Data communications networks facilitate more efficient use of computers and improve the day-to-day control of a business by providing faster information flow. They also provide message transfer services to allow computer users to talk to one another via email, chat, and video streaming.

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

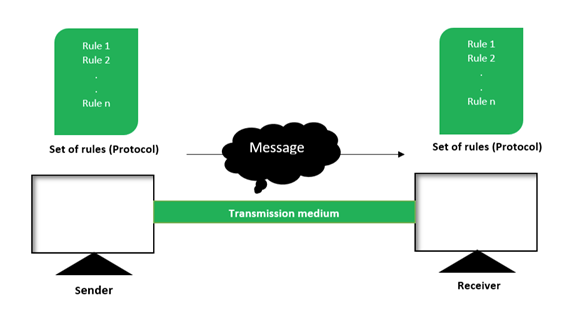
The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
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, in the same order that they are produced, and without significant delay. This kind of delivery is called *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.

**Components of a data communication system**

A data communications system has five components as briefly define below:

1. **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on
4. **Transmission medium**. The transmission medium 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**. A protocol 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.



**Figure 1: Components of a data communication system**

**NETWORK**

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

**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:***

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughputs and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

1. ***Reliability:***

In addition to accuracy of delivery, network reliability is 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.

1. ***Security:***

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

**NETWORK MODELS**

There are many ways to describe and analyze data communications networks. All networks provide the same basic functions to transfer a message from sender to receiver, but each network can use different network hardware and software to provide these functions. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network. All of these hardware and software products have to work together to successfully transfer a message.

One way to accomplish this is to break the entire set of communications functions into a series of **layers**, each of which can be defined separately. In this way, vendors can develop software and hardware to provide the functions of each layer separately. The software or hardware can work in any manner and can be easily updated and improved, as long as the interface between that layer and the ones around it remains unchanged. Each piece of hardware and software can then work together in the overall network.

There are many different ways in which the network layers can be designed. The two most important network models are the Open Systems Interconnection Reference (OSI) model and the Internet model. The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

**Open Systems Interconnection Reference Model**

The **Open Systems Interconnection Reference model** (usually called the **OSI model** for short) helped change the face of network computing.

It is a conceptual model created by the International Organization for Standardization (ISO), which enables diverse communication systems to communicate using standard protocols. In simple terms, the OSI model allows any two different systems to communicate regardless of their underlying architecture.

The OSI Model can be seen as a universal language for computer networking. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

Within a single device, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between devices, layer *x* on one device communicates with layer *x* on another device. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each device that communicate at a given layer are called peer-to-peer processes. Communication between devices is therefore a peer-to-peer process using the protocols appropriate to a given layer. An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

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

|  |
| --- |
| Seven Layers of OSI Model |
| 7. Application |
| 6. Presentation |
| 5. Session |
| 4. Transport |
| 3. Network |
| 2. Data link |
| 1. Physical |

**Organization of OSI Model layers**

The layers are divided into three (3) main subgroup

* + Layers 1,2 and 3 are called network support layers, which deal with physical aspect of moving data from one device to another (such as electric specification, physical connection, physical addressing, support timing and reliability)
  + Layers 5, 6 and 7 can be thought of as a user support layers: they allow interoperability among unrelated software systems
  + Layer 4 is the core layer (that is the transport layer), which links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
  + The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware

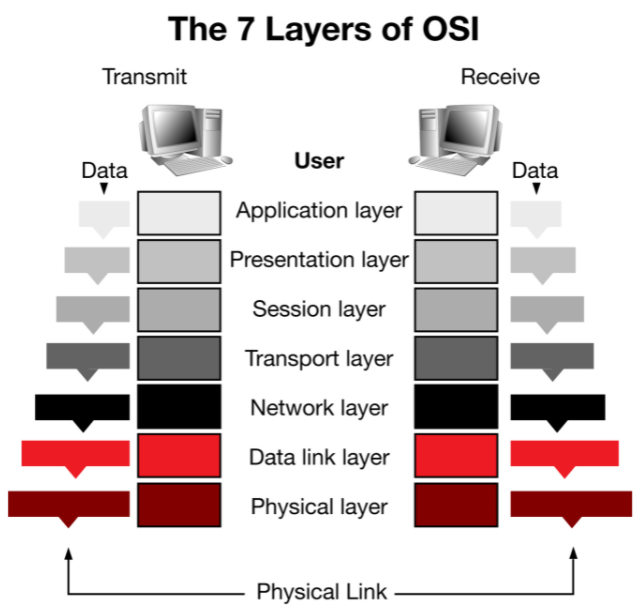
**How data flows through the OSI Model**In order for human-readable information to be transferred over a network from one device to another, the data must travel down the seven layers of the OSI Model on the sending device and then travel up the seven layers on the receiving end.

For example: Mr. Cooper wants to send Ms. Palmer an email. Mr. Cooper composes his message in an email application on his laptop and then hits ‘send’. His email application will pass his email message over to the application layer, which will pick a protocol (SMTP) and pass the data along to the presentation layer. The presentation layer will then compress the data and then it will hit the session layer, which will initialize the communication session.

The data will then hit the sender’s transportation layer where it will be segmented, then those segments will be broken up into packets at the network layer, which will be broken down even further into frames at the data link layer. The data link layer will then deliver those frames to the physical layer, which will convert the data into a bit stream of 1s and 0s and send it through a physical medium, such as a cable.

Once Ms. Palmer’s computer receives the bit stream through a physical medium (such as her Wi-Fi), the data will flow through the same series of layers on her device, but in the opposite order. First the physical layer will convert the bit stream from 1s and 0s into frames that get passed to the data link layer. The data link layer will then reassemble the frames into packets for the network layer. The network layer will then make segments out of the packets for the transport layer, which will reassemble the segments into one piece of data.

The data will then flow into the receiver's session layer, which will pass the data along to the presentation layer and then end the communication session. The presentation layer will then remove the compression and pass the raw data up to the application layer. The application layer will then feed the human-readable data along to Ms. Palmer’s email software, which will allow her to read Mr. Cooper’s email on her laptop screen.



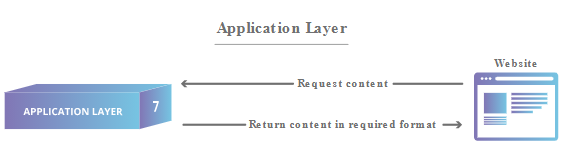
**Figure 2: The data flow across 7 Layers of OSI Model**

* 1. **APPLICATION LAYER**

The **Application Layer** 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, shared database management, and other types of distributed information services. Application layer protocols include HTTP, FTP and SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

Specific services provided by the **application layer** include the following:

1. File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
2. Mail services. This application provides the basis for e-mail forwarding and storage.
3. Directory services. This application provides distributed database sources and access for global information about various objects and services.



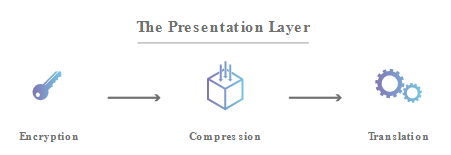
**Figure 3: Application layer**

* 1. **THE PRESENTATION LAYER**

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for **translation**, **encryption** and **compression** of data.

Specific responsibilities of the presentation layer include the following:

1. Translation. Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.
2. Encryption. If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted readable data.
3. Compression. Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

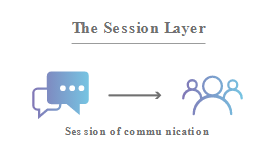


**Figure 4: Presentation layer**

**5. THE SESSION LAYER**

The session layer is responsible for dialog control and synchronization Specific responsibilities of the session layer include the following:

1. Dialog control. This layer is responsible for **opening and closing communication between the two devices**. It 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. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting of the resources.
2. Synchronization. The session layer also **synchronizes data transfer with checkpoints**. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.



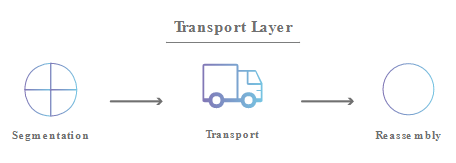
**Figure 5: Session layer**

**4. THE TRANSPORT LAYER**

Layer 4 is responsible for **end-to-end communication between the two devices**. It establishes, maintains, and terminates logical connections for the transfer of data between the original sender and the final destination of the message.

Other responsibilities of the **transport layer** include the following:

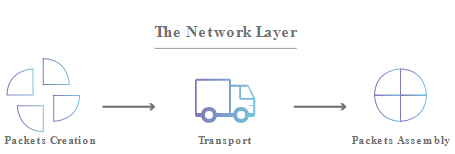
1. Segmentation and reassembly. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.
2. Flow control. Like the data link layer, the transport layer also is responsible for flow control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn’t overwhelm a receiver with a slow connection. However, flow control at this layer is performed end to end rather than across a single link.
3. Error control. Like the data link layer, the transport layer is responsible for error control. The transport layer performs error control on the receiving end by ensuring that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.



**Figure 6: Transport layer**

**3. THE NETWORK LAYER**

The network layer is responsible for **facilitating data transfer between two different networks**. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer **breaks up segments from the transport layer into smaller units, called packets**, on the sender’s device, and reassembling these packets on the receiving device.



**Figure 7: Network layer**

Other responsibilities of the network layer include the following:

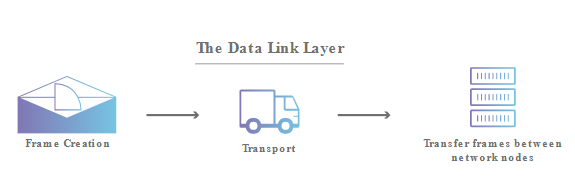
1. Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
2. Routing. The network layer also finds the **best physical path** for the data to reach its destination; this is known as **routing**.

**2. THE DATA LINK LAYER**

The data link layer is very similar to the network layer, except the data link layer **facilitates data transfer between two devices on the SAME network**.

Other responsibilities of the data link layer include the following:

1. Framing. The data link layer takes packets from the network layer and breaks them into smaller pieces **called frames**. Because layer 1 accepts and transmits only a raw stream of bits without understanding their meaning or structure, the data link layer must create and recognize message boundaries; that is, it must mark where a message starts and where it ends.
2. Flow control. Like the network layer, the data link layer is also responsible for **flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
3. Error control. Another major task of layer 2 is to solve the problems caused by damaged, lost, or duplicate messages so the succeeding layers are shielded from transmission errors. Thus, layer 2 performs error detection and correction. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
4. Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



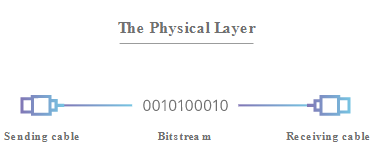
**Figure 8: Data link layer**

**1. THE PHYSICAL LAYER**

This layer includes the **physical equipment** involved in the data transfer, such as the **cables and switches**. This is also the layer where the **data gets converted into a bit stream**, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

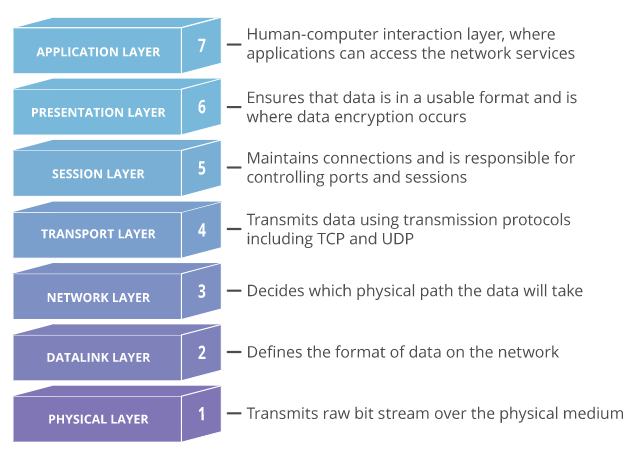
The physical layer is also concerned with the following:

1. Representation of bits. The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s are changed to signals).
2. Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
3. Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
4. Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a specified topology, for example mesh topology, etc.
5. Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.



**Figure 9: Physical layer**

**Summary of OSI Layers**



**Figure 10: OSI Model layers**