Chapter 4

4.1 Introduction

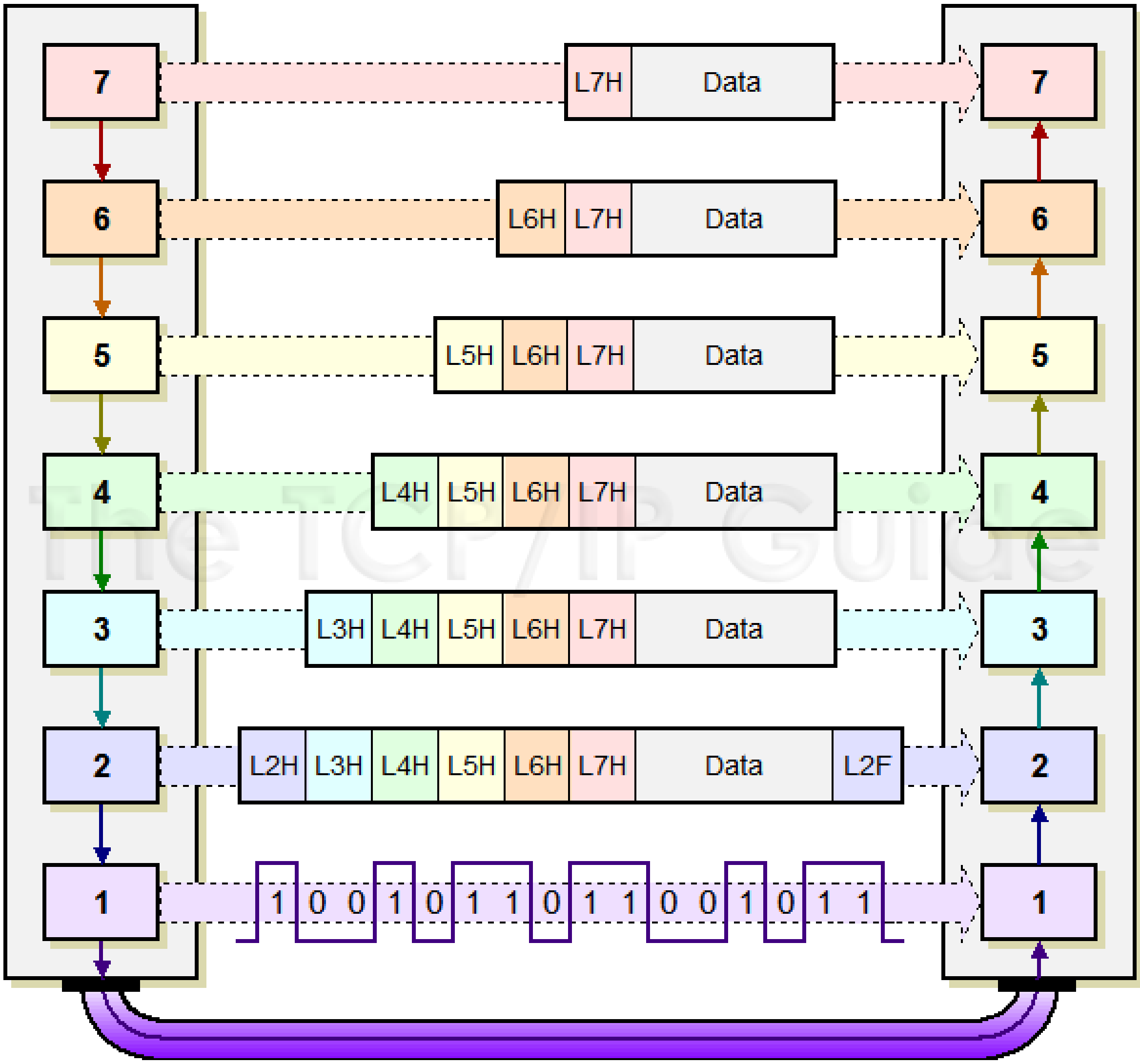
The information that travels on a network is generally referred to as data or a packet. **A packet** is a logically grouped unit of information that moves between computer systems. The **network models** are describing this movement of the packets. The **OSI** and **TCP/IP** models have layers that explain how data is communicated from one computer to another. The models differ in the number and function of the layers. However, each model can be used to help describe and provide details about the flow of information from a source to a destination.

4.2 Using layers to describe data communication

In order for data packets to travel from a source to a destination on a network, it is important that all the devices on the network speak the same language or protocol. A **protocol** is a set of rules that make communication on a network more efficient. For example, while flying an airplane, pilots obey very specific rules for communication with other airplanes and with air traffic control.

A **data communications protocol** is a set of rules or an agreement that determines the format and transmission of data. Layer 4 on the source computer communicates with Layer 4 on the destination computer.

The rules and conventions used for this layer are known as Layer 4 protocols. It is important to remember that protocols prepare data in a linear fashion. A protocol in one layer **performs a certain set of operations on data as it prepares the data to be sent over the network**. The *data is then passed to the next layer* where another protocol *performs a different set of operations*. Once the packet has been sent to the destination, the protocols **undo the construction** of the packet that was done on the source side. This is done in reverse order. The protocols for each layer on the destination return the information to its original form, so the application can properly read.



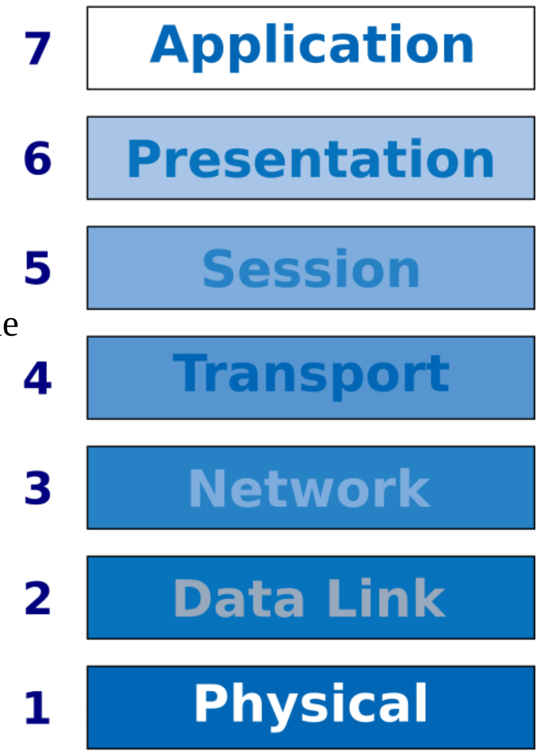
4.3 <u>OSI model</u>

The early development of networks was disorganized in many ways. The early 1980s saw tremendous increases in the number and size of networks. As companies realized the advantages of using networking technology, networks were added or expanded almost as rapidly as new network technologies were introduced.

By the mid-1980s, these companies began to experience problems from the rapid expansion. Just as people that do not speak the same language have difficulty communicating with each other, **it was difficult for networks that used different specifications and implementations to exchange information**. The same problem occurred with the companies that developed private or proprietary networking technologies. Proprietary means that one or a small group of companies controls all usage of the technology. Networking technologies strictly following proprietary rules could not communicate with technologies that followed different proprietary rules.

To address the problem of network incompatibility, the International Organization for Standardization (ISO) researched networking models like Digital Equipment Corporation net (DECnet), Systems Network Architecture (SNA), and TCP/IP in order to find a generally applicable set of rules for all networks. Using this research, the ISO created a network model that helps vendors to create networks that are compatible with other networks. The Open System Interconnection (OSI) reference model released in 1984 was the descriptive network model that the ISO created. It provided vendors with *a set of standards that ensured greater compatibility and interoperability among various network technologies produced by companies around the world.*

The OSI reference model has become the primary model for network communications. Although there are other models in existence, most network vendors relate their products to the OSI reference model. This is especially true when they want to educate users on the use of their products. It is considered the best tool available for teaching people about sending and receiving data on a network. In the Interactive Media Activity, students will identify the benefits of the OSI model.



Memorize name & no of layers

Benefits of the OSI Model:

- Reduce Complexity.
- Standardizes Interfaces.
- Facilitates Modular Engineering.
- Ensures Interoperable Technology.
- Accelerates Evolution.
- Simplifies Teaching and Learning.

The OSI reference model is a framework that is used to understand how information travels throughout a network. The OSI reference model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media. In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function. Dividing the network into seven layers provides the following advantages:

- It breaks network communication into smaller, more manageable parts.

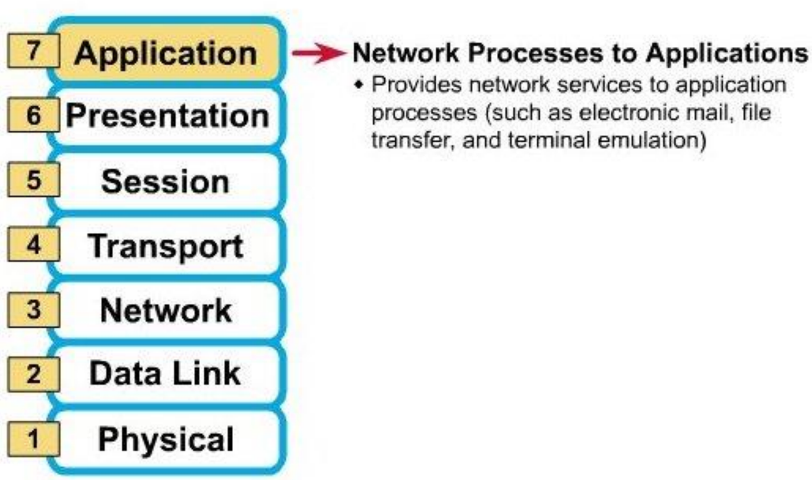
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

4.4 OSI layers

Each individual layer has a set of functions that it must perform in order for data packets to travel from a source to a destination on a network. Below is a brief description of each layer in the OSI reference model.

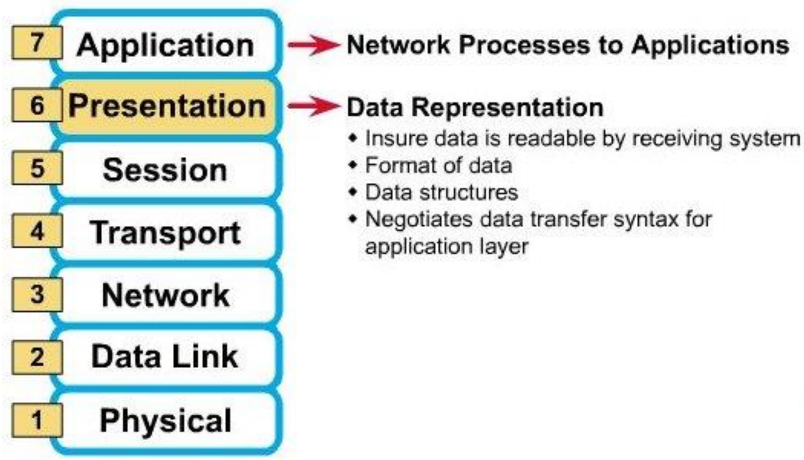
4.4.1 Layer 7: The Application Layer

The application layer is the OSI layer that is closest to the user; it provides networks services to the user's applications. It differs from the other layers in that it does not provide services to any other OSI layer, but rather, only to applications outside the OSI model. Examples of such applications are spreadsheet programs, word processing programs and bank terminal programs. The application layer establishes the availability of intended communication partners synchronizes and establishes agreement on procedures for error recovery and control of data integrity. *If you want to remember layer seven in as few words as possible, think of browsers.*



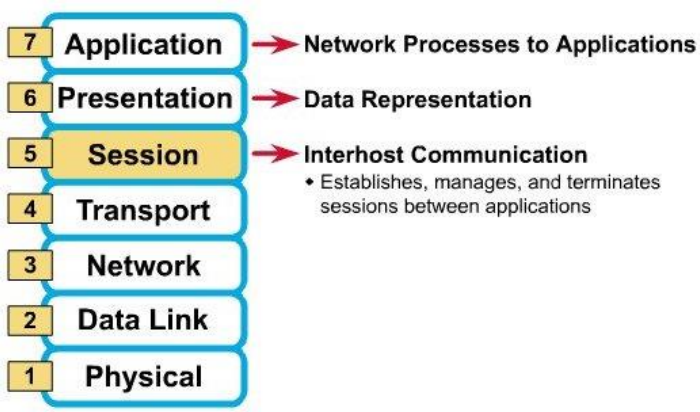
4.4.2 Layer 6: The Presentation Layer

The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system. If necessary, the presentation layer translates between multiple data formats by using a common format. *If you want to think of layer 6 in a few words as possible, think of a common data format.*



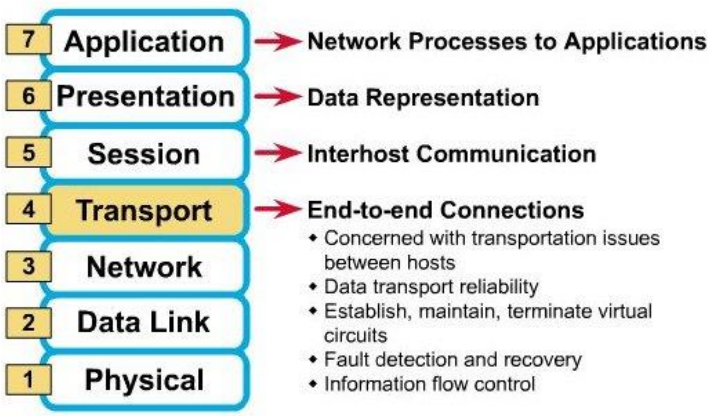
4.4.3 Layer 5: The Session Layer

As its name implies, the session layer establishes, manages, and terminates sessions between two communicating hosts. The session layer provides its services to the presentation layer. It also synchronizes dialogue between the two hosts' presentation layers and manages their data exchange. In addition to session regulation, the session layer offers provisions for efficient data transfer, class of service, and exception reporting of session layer, presentation layer, and application layer problems. *If you want to remember layer 5 in as few words as possible, think of dialogues and conversations.*



4.4.4 Layer 4: The Transport Layer

The transport layer segments data from the sending host's system and reassembles the data into a data stream on the receiving host's system. The boundary between media-layer and transport layer can be thought of as the boundary between media-layer protocols and host-layer protocols. Whereas the application, presentation, and session layers are concerned with application issues, the lower three layers are concerned with data transfer issues.

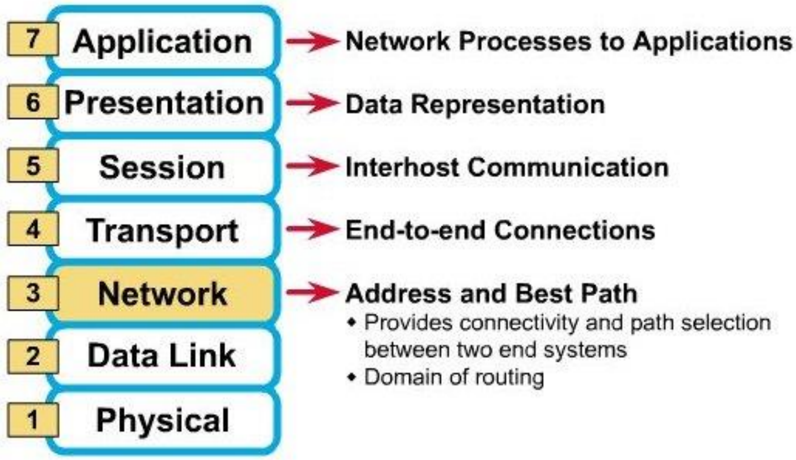


The transport layer attempts to provide a data transfer service that shields the upper layers from transport implementation details. Specifically, issues such as how reliable transport between two hosts is accomplished are the concern of the transport layer. In providing communication service, the transport layer establishes, maintains, and properly terminates virtual recovery and information flow control are used. *If you want to remember layer 4 in as few words as possible, think of quality of service, and reliability.*

4.4.5 Layer 3: The Network Layer

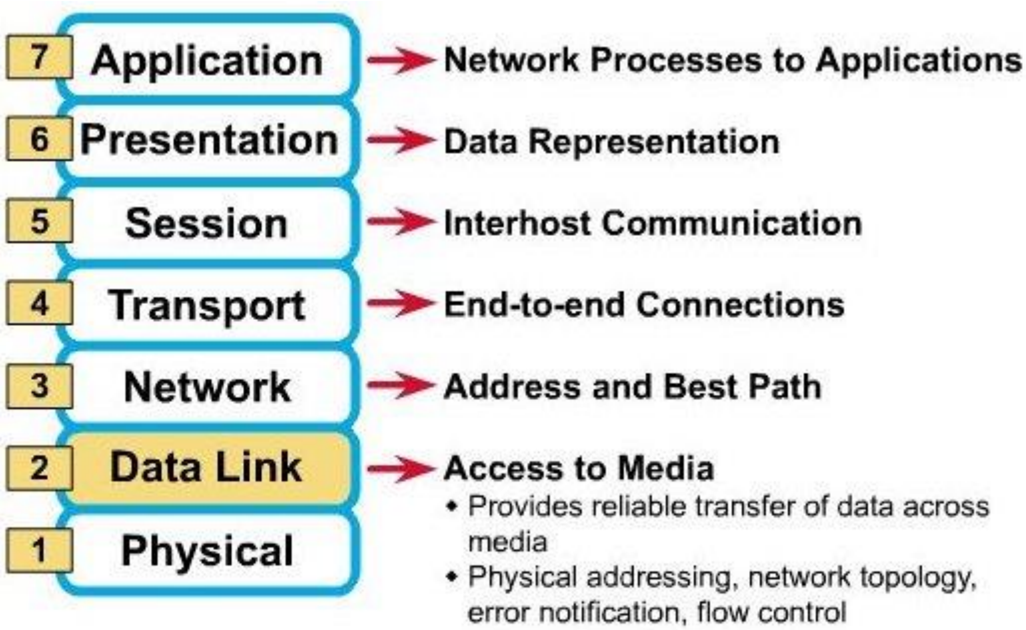
The network layer is a complex layer that provides connectivity and path selection between two host systems that may be located on geographically separated networks.

If you want to remember layer 3 in as few words as possible, think of path selection, routing, and addressing.



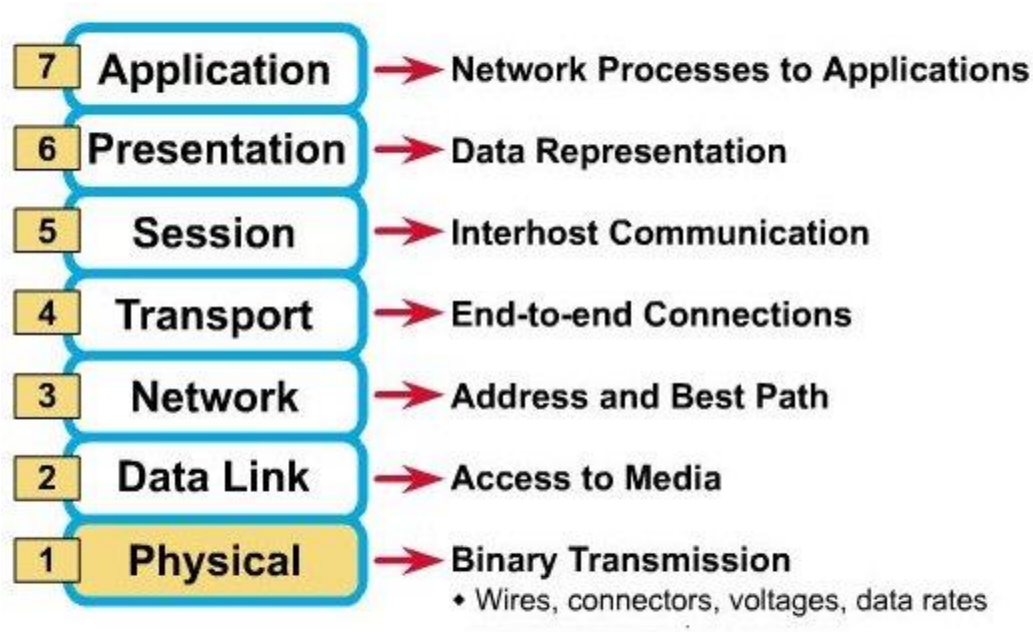
4.4.6 Layer 2: The Data Link Layer

The data link layer provides reliable transmit of data across a physical link in so doing, the data link layer is concerned with physical (as opposed to logical) addressing, network topology, network access, error notification, ordered delivery of frames, and media access control.



4.4.7 Layer 1: The Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other, similar, attributes are defined by physical layer specifications. *If you want to remember layer 1 in as few words as possible, think of signals and media.*



To help remember them in the correct order a common mnemonic is often used from 7 to 1 (top to bottom):

All
People
Seem
To
Need
Data
Processing

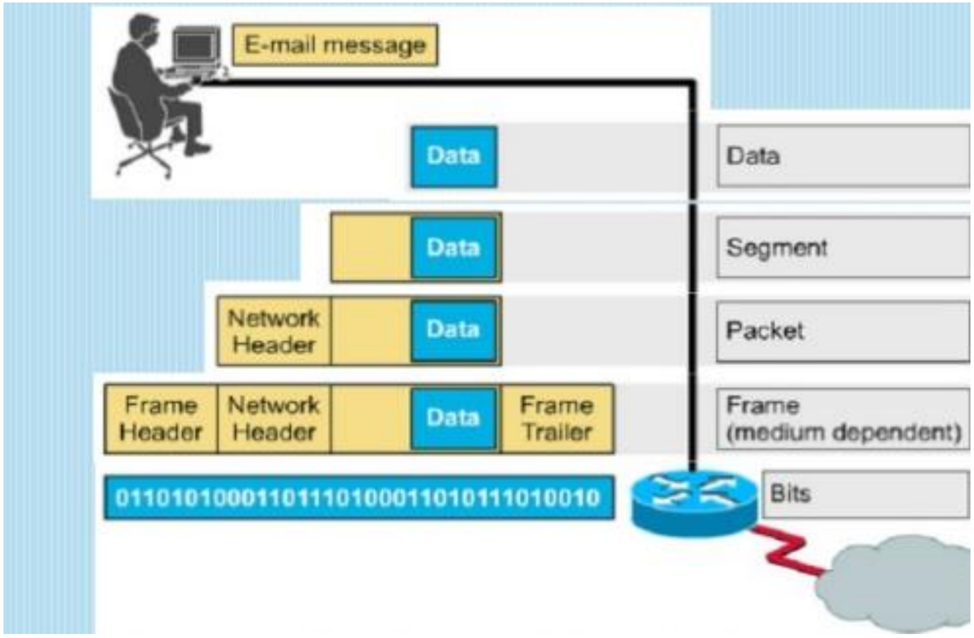
For those of you who like the Domino's or Pappa John's pies, try from 1 to 7 (bottom to top):

Please
Do
Not
Throw
Sausage
Pizza
Away

4.5 Encapsulation

You know that all communications on a network originate at a source, and are sent to a destination, and that the information that is sent on a network is referred to as data or data packets. If one computer (host A) wants to sent data to another (host B), the data must first be packaged by a process called encapsulation. Encapsulation wraps data with the necessary protocol information before

network transit. Therefore, as data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information. (Note: The word "header" means that address information has been added). To see how encapsulation occurs, let's examine the manner in which data travels through the layers. Once the data is sent from the source, it travels through the application layer down through the other layers. As you can see, the packaging and flow of the data that is exchanged goes through changes as the networks perform their services for end-users.



Networks must perform the following five conversion steps in order to encapsulate data:

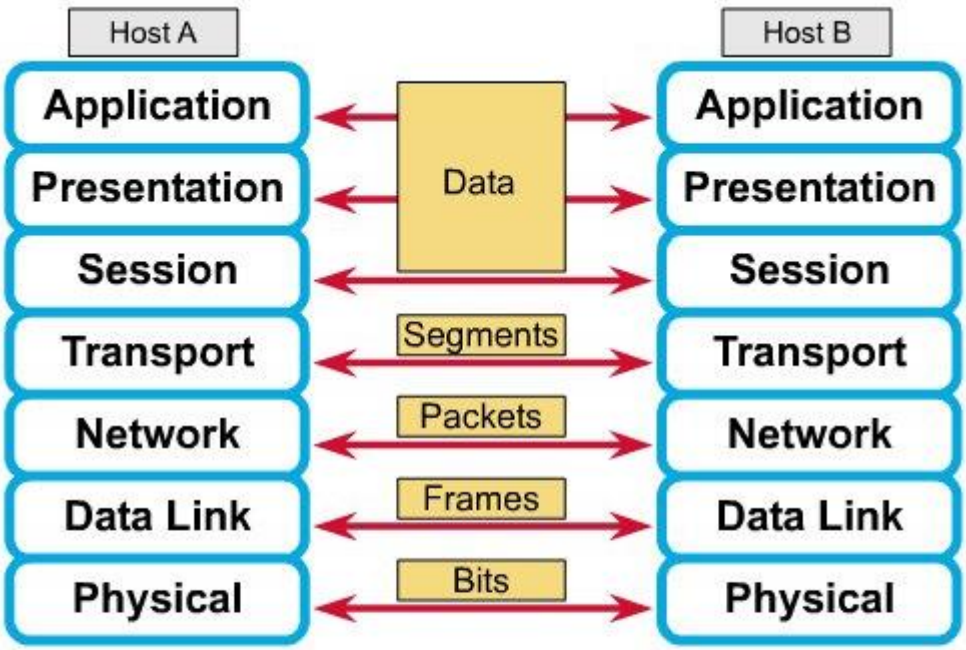
1- **Build the data (application layer):** As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.
2- **Package the data for end-to-end transport (transport layer):** The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.
3- **Append (add) the network address to the header (network layer):** The data is put into a packet or datagram that contains a network header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.
4- **Append (add) the local address to the data link header (data link layer):** Each network device must put the packet into a frame. The frame allows

connection to the next directly-connected network device on the link. Each device in the chosen network path requires framing in order for it to connect to the next device.

5- **Convert to bits for transmission (physical layer):** The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium (usually a wire). A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN. Headers and trailers are added as data moves down though the layers of the OSI model.

4.6 Peer-to-peer communications

In order for data to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as peer-to-peer. During this process the protocols of each layer exchange information, called protocol data units (PDUs). Each layer of communication on the source computer communicates with a layer-specific PDU, and with its peer layer on the destination computer as illustrated in figure.



Data packets on a network originate at a source and then travel to a destination. Each layer depends on the service function of the OSI layer below it. To provide this service, the lower layer uses encapsulation to put the PDU from the upper layer into its data field. Then it adds whatever headers and trailers the layer needs to perform its function. Next, as the data moves down through the layers of the OSI model, additional headers and trailers are added. After Layers 7, 6, and 5 have added their information, Layer 4 adds more information. This grouping of data, the Layer 4 PDU, is called a segment.

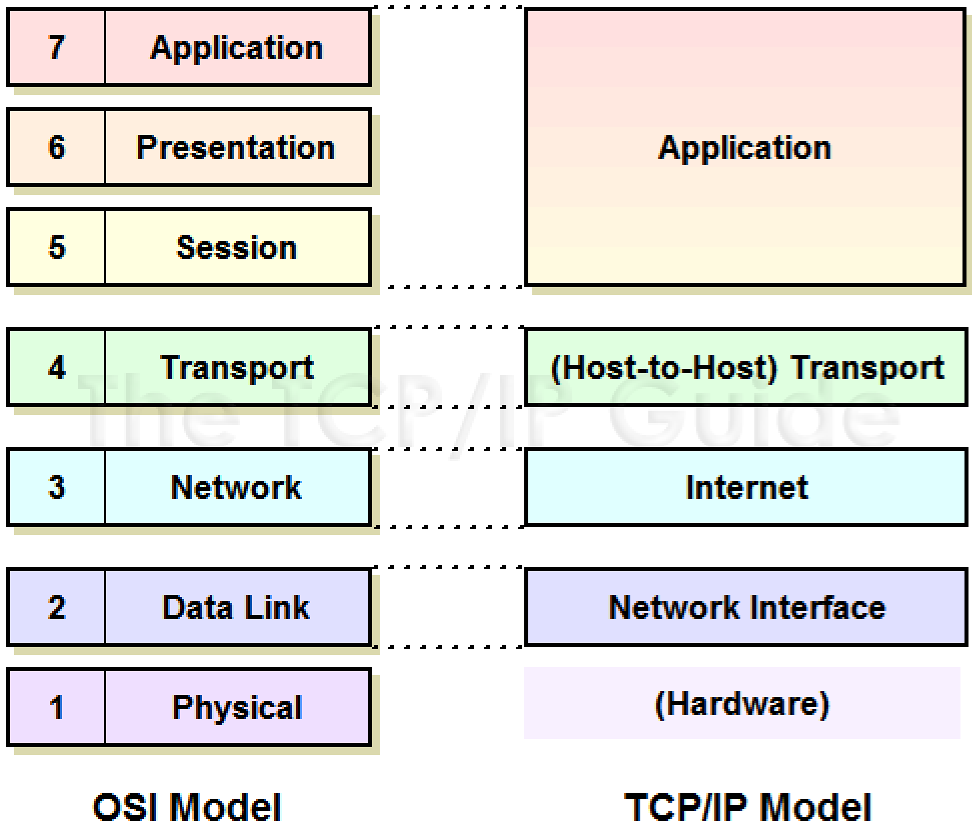
The network layer provides a service to the transport layer, and the transport layer presents data to the internetwork subsystem. The network layer has the task of moving the data through the internetwork. It accomplishes this task by encapsulating the data and attaching a header creating a packet (the Layer 3 PDU). The header contains information required to complete the transfer, such as source and destination logical addresses. The data link layer provides a service to the network layer. It encapsulates the network layer information in a frame (the Layer 2 PDU). The frame header

contains information (for example, physical addresses) required to complete the data link functions. The data link layer provides a service to the network layer by encapsulating the network layer information in a frame. The physical layer also provides a service to the data link layer. The physical layer encodes the data link frame into a pattern of 1s and 0s (bits) for transmission in the medium (usually a wire) at layer 1.

4.7 TCP/IP model

The U.S. Department of Defense (DoD) created the TCP/IP reference model, because it wanted to design a network that could survive any conditions, including a nuclear war. In a world connected by different types of communication media such as copper wires, microwaves, optical fibers and satellite links, the DoD wanted transmission of packets every time and under any conditions. This very difficult design problem brought about the creation of the TCP/IP model. Unlike the proprietary networking technologies mentioned earlier, TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard. The TCP/IP model has the following four layers:

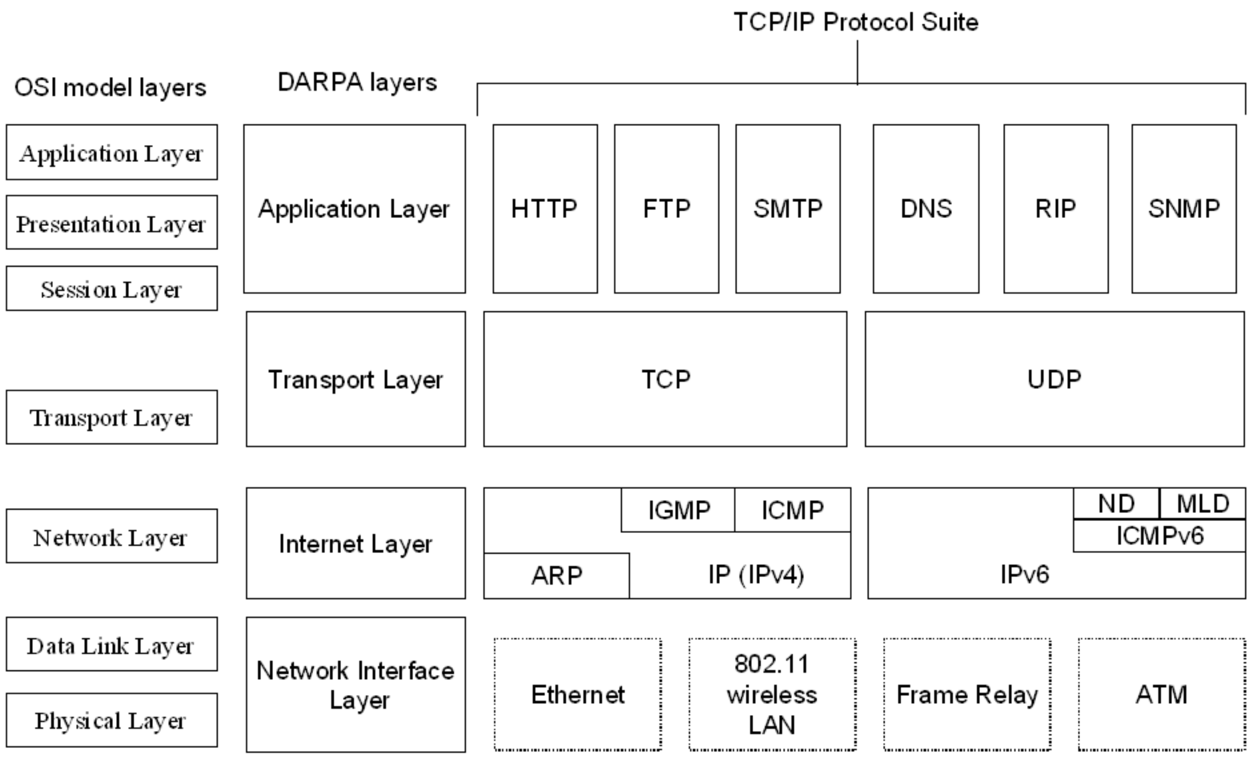
1- Application layer
2- Transport layer
3- Internet layer
4- Network access layer



Although some of the layers in the TCP/IP model have the same name as layers in the OSI model, the layers of the two models do not correspond exactly. Most notably, the application layer has different functions in each model. The designers of TCP/IP felt that the application layer should include the OSI session and presentation layer details. They created as application layer that handles issues of representation, encoding, and dialog control. The transport layer deals with the quality of service issues of reliability, flow control, and error correction. One of its protocols, the transmission control protocol (TCP), provides excellent and flexible ways to create reliable, well flowing, low-error network communications. TCP is a connection-oriented protocol. It maintains a dialogue between source and destination while packaging application layer information into units called segments. Connection-oriented does not mean that a circuit exists between the communicating computers. It does mean that Layer 4 segments travel back and forth between two hosts to acknowledge the connection exists logically for some period. The purpose of the Internet layer is to divide TCP segments into packets and send them from any network. The packets arrive at the destination network independent of the path they took to get there. The specific protocol that governs this layer is called the Internet Protocol (IP). Best path determination and packet switching occur at this layer. The relationship between IP and TCP is an important one. IP can be

thought to point the way for the packets, while TCP provides a reliable transport. The name of the network access layer is very broad and somewhat confusing. It is also known as the host-to-network layer. This layer is concerned with all of the components, both physical and logical, that are required to make a physical link. It includes the networking technology details, including all the details in the OSI physical and data link layers.

The following figure illustrates some of the common protocols specified by the TCP/IP reference model layers.



Some of the most commonly used application layer protocols include the following:

1. File Transfer Protocol (FTP)
2. Hypertext Transfer Protocol (HTTP)
3. Simple Mail Transfer Protocol (SMTP)
4. Domain Name System (DNS)
5. Trivial File Transfer Protocol (TFTP)

The common transport layer protocols include:

1. Transport Control Protocol (TCP)
2. User Datagram Protocol (UDP)

The primary protocol of the Internet layer is:

1. Internet Protocol (IP)

The network access layer refers to any particular technology used on a specific network. Regardless of which network application services are provided and which transport protocol is used, there is only one Internet protocol, IP. This is a deliberate design decision. IP serves as a universal protocol that allows any computer anywhere to communicate at any time. A comparison of the OSI model and the TCP/IP model will point out some similarities and differences.

Similarities include:

1. Both have layers.
2. Both have application layers, though they include very different services.
3. Both have comparable transport and network layers.
4. Both models need to be known by networking professionals.
5. Both assume packets are switched. This means that individual packets mat take different paths to reach the same destination. This is contrasted with circuit-switched networks where all the packets take the same path.

Differences include:

1. TCP/IP combines the presentation and session layer issues into its application layer.
2. TCP/IP combines the OSI data link and physical layers into the network access layer.
3. TCP/IP appears simpler because it has fewer layers.
4. TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, networks are not usually built on the OSI protocol, even though the OSI model is used as a guide.

Although TCP/IP protocols are the standards with which the Internet has grown, this curriculum will use the OSI model for the following **reasons**:

1. It is a generic, protocol-independent standard.
2. It has more details, which make it more helpful for teaching and learning.
3. It has more details, which can be helpful when troubleshooting. Networking professionals differ in their opinions on which model to use.

Due to the nature of the industry it is necessary to become familiar with both. Both the OSI and TCP/IP models will be referred to throughout the curriculum. The focus will be on the following:

1. TCP as an OSI layer 4 protocol
2. IP as an OSI Layer 3 protocol

3. Ethernet as a Layer 2 and Layer 1 technology

Remember that there is a difference between a model and an actual protocol that is used in networking. The OSI model will be used to describe TCP/IP protocols.

Transmission Control Protocol (TCP)

Transmission Control Protocol, TCP, is a connection oriented protocol that functions on the Transport layer of the OSI model. When two computers on a network need to communicate, TCP opens a connection between the computers. When the data packet is ready to be sent, TCP adds to the packet header information that contains flow control and error checking.

Internet Protocol (IP):

The Internet protocol, IP, is a connectionless protocol that operates at the Network layer of the OSI model. When data packets ate sent over the network, IP is responsible for addressing the packets and routing them through the network. Attached to each packet is and IP header that contains the sending address and receiving address. When the packets reach their final destination, the IP puts all the packets together again in the correct order.

User Datagram Protocol (UDP):

The user Datagram Protocol (UDP) provides a datagram service. Datagram is a way of sending messages with a minimum of overhead. Delivery is not guaranteed. No checking for missing or out-of-sequence packet is performed, and no acknowledgments are sent.

File Transfer Protocol (FTP):

File Transfer Protocol, or FTP, is used for file sharing between computers that use TCP/IP to communicate. FTP allows users to log on to a remote computer on a network and see that files are on the computer. It allows users to also upload and download files between the two computers. FTP is a widely used Application layer protocol because an FTP service exists for almost every operating system.

Simple Mail Transfer Protocol (SMTP):

Simple Mail Transfer Protocol (SMTP) makes sure that e-mail is delivered from the sender's service to the intended recipient's e-mail server. It does not handle the delivery to the final e-mail desktop location. SMTP is an Application layer protocol.