Standards Organizations

Standards organizations generate, control, and administrate standards. Often competing companies form join committees to create a compromised standard that is accepted to everyone. In the field of our interest there are two main standards organizations.

1- ISO (International Organization for standardization)

2- IAB (Internet Architecture Board)

1-ISO

Created in 1946, ISO is responsible for standardization on a wide range of subjects including graphics, document exchange, system compatibility, quality enhancement and many other fields. Regarding to engineering fields, ISO is responsible for another three main organizations, these are:

- ITU-T (International Telecommunication Union-Telecommunication Sector)

It is the standardization organization of the United Nations. It develops the recommended set of rules for telephone and data communications.

- IEEE (Institute of Electrical and Electronic Engineers)

Even IEEE was found in United Sates, it is now the world's largest professional society with over 200,000 member. It focuses on the fields of electrical, electronic and communication engineering.

- ANSI (American National Standards Institute)

It is the official standards agency for United States. It is responsible for two associations; EIA (Electronics Industry Association) and TIA (Telecommunication Industry Association)

2-IAB

It is a technical advisory group of the Internet society. It focuses on Internet protocols, applications, architectures, and technologies. The two groups IAB responsible of are; IETF (Internet Engineering Task Force) and IRTF (Internet Research Task Force).

Networking Models

Many of the early networks were built using different implementations of hardware and software. This resulted in many of the networks being incompatible and communication between networks was quite difficult. To address this problem, networking models are created as solution for compatibility, development, and study issues. The most common networking models are:

1- OSI Reference Model

2- TCP/IP

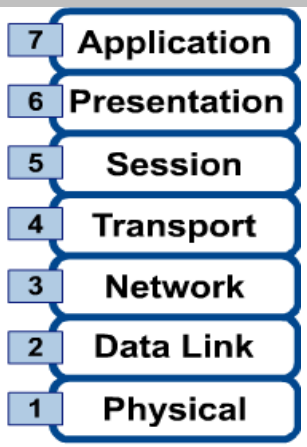
1- The OSI (Open System Interconnection) Reference Model

In the late 1980s and early 1990s there was a significant increase in the number and overall size of networks. ISO recognized that there was a need to create a network model that would help network builders implement networks that could communicate and work together. As a consequence, the Open System Interconnection (OSI) reference model was released in 1984.

The OSI reference model is a framework that you can use to understand how information travels throughout a network. In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function. This separation of networking functions is called layering. The seven layers of the OSI reference model are :-

- Layer 7: The application layer
- Layer 6: The presentation layer
- Layer 5: The session layer
- Layer 4: The transport layer
- Layer 3: The network layer
- Layer 2: The data-link layer
- Layer 1: The physical layer

The 7-layer OSI Reference Model



Dividing the network into these seven layers provides the following advantages:

1. It breaks network communication into smaller parts to make it easier to learn and understand.
2. It standardizes network components to allow multiple-vendor development and support.
3. It allows different types of network hardware and software to communicate with each other.
4. It prevents changes in one layer from affecting the other layers, so that they can develop more quickly.

Most of the protocols commonly used today predate the OSI model, so they don't conform exactly to the seven-layer structure. In most cases, single protocols combine the functions of two or more of the layers in the model, and the boundaries between protocols often don't exactly conform to the model's layer boundaries.

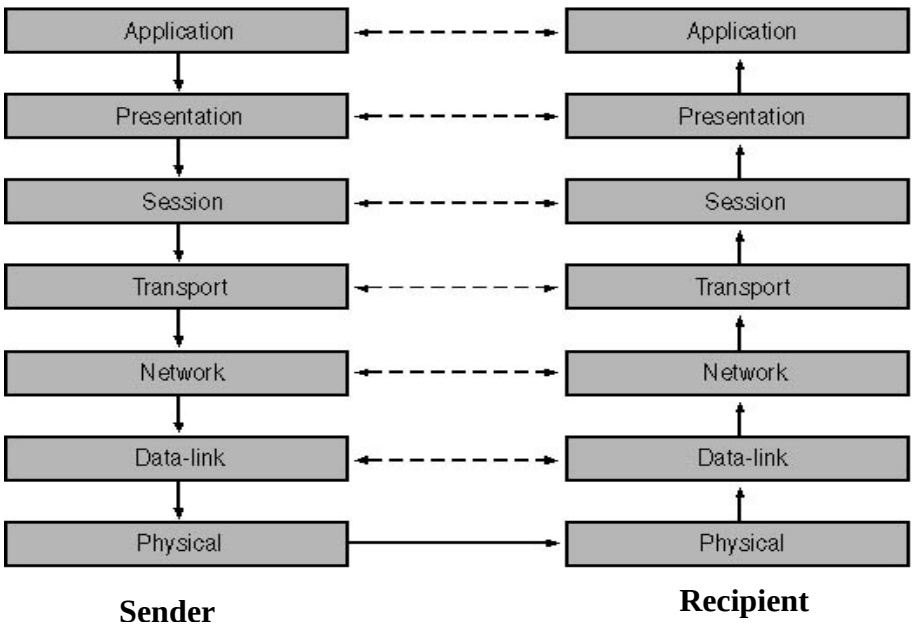
The OSI reference model is the primary model for network communications. Although there are other models in existence, most network vendors, today, relate their products to the OSI reference model, especially when they want to educate users on the use of their products. They consider it the best tool available for teaching people about sending and receiving data on a network.

➢ Protocol Interaction

The protocols operating at the various OSI layers are often referred to as a protocol stack. Generally speaking, the services provided by the protocols are not redundant. Protocols at adjacent layers in the stack provide services to each other, depending on the direction in which the data is flowing.

The data on a transmitting system originates in an application at the top of the protocol stack and works its way down through the layers. Each protocol provides a service to a protocol operating at the layer below it. At the bottom of the protocol stack is the network medium itself, which carries the data to another computer on the network.

When the data arrives at its destination, the receiving computer performs the same procedure as the transmitting computer, except in reverse. The data is passed up through the layers to the receiving application, with each protocol providing an equivalent service to the protocol in the layer above it. For example, if a protocol at layer three on the transmitting computer is responsible for encrypting data, the same protocol at layer three of the receiving system is responsible for decrypting it. In this way, protocols at the various layers in the transmitting system communicate indirectly with their equivalent protocols operating at the same layer in the receiving system.



The following table helps you to remember the layers of the OSI reference model and the Protocol Data Unit (PDU) used in these layers

Layer No.	Layer Name	Mnemonic	PDU
7	Application	All	Data
6	Presentation	People	Data
5	Session	Seem	Data
4	Transport	To	Segment
3	Network	Need	Datagram
2	Data Link	Data	Frame
1	Physical	Processing	Bits

Note: the PDUs in Layers 2,3,4 may be in general called Packets

Layer1: The Physical Layer

The physical layer, at the bottom of the OSI reference model, is, as the name implies, the layer that defines the nature of the network's hardware elements, such as what medium the network uses, how the network is installed, network topology, and the nature of the signals used to transmit binary data over the network.

The physical layer specifications are directly related to the data-link layer protocol used by the network. When you select a data-link layer protocol, you must use one of the physical layer specifications supported by that protocol. For example, in Ethernet - which is a data-link layer protocol - you can use coaxial cables, twisted pair cables or fiber optic cable. The specifications for each of these options include a great deal of detailed information about the physical layer requirements, such as the exact type of cable and connectors to use, how long the cables can be, how many hubs you can have, and many other factors

The other communications element found at the physical layer is the particular type of signaling used to transmit data over the network medium. For copper-based cables, these signals are electrical charges. For fiber optic cables, the signals are pulses of light. Other types of network media can use radio frequencies, infrared pulses, and other types of signals.

In addition to the physical nature of the signals, the physical layer dictates the signaling scheme that the computers use. The signaling scheme is the pattern of electrical signals or light pulses used to encode the binary data generated by the upper layers. For example, Ethernet systems use a signaling scheme called Manchester encoding, and Token Ring systems use a scheme called Differential Manchester.

Layer2: The Data-Link Layer

The protocol at the data-link layer is the conduit between the computer's networking hardware and its networking software. When it comes to designing and building a LAN, the data-link layer protocol you choose is the single most important factor in determining what hardware you buy and how you install it

By far the most popular data-link layer LAN protocol in use today (and throughout the history of the LAN) is Ethernet. IEEE 802.11 WLAN protocols nowadays take second place, followed by other protocols such as Token Ring and Fiber Distributed Data Interface (FDDI). Data-link layer protocol specifications typically include the following three basic elements:

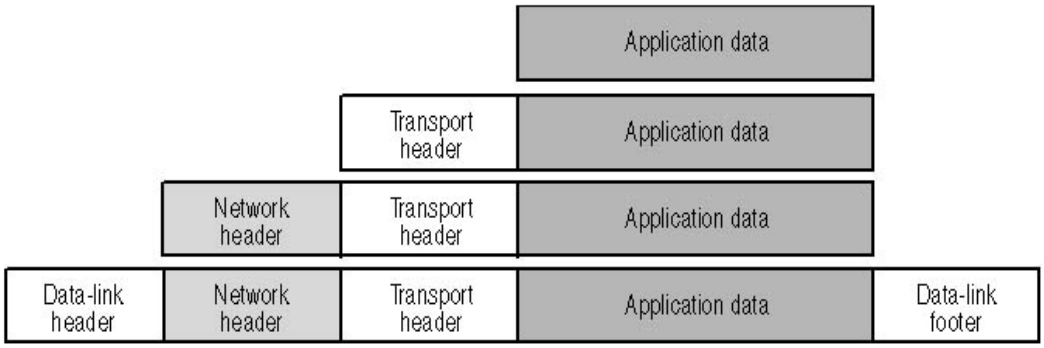
1. A format for the frame
2. A mechanism for controlling access to the network medium
3. One or more physical layer specifications for use with the protocol

➢ Frame Format

The data-link layer protocol adds a header and footer (or trailer) to the data it receives from the Network layer , (the process of adding header and/or footer to a unit of data is known as data encapsulation). It forms now what is called a frame.

A typical data-link layer protocol frame contains- in addition to the Network layer data_ the source and destination address fields, a network layer protocol identifier, and error detection information field.

The following figure illustrates the process of data encapsulation in data- link layer as well as network and transport layers.



❖ Source and Destination Hardware Addresses:

Header and footer usually contain the address of the system sending the packet and the address of its destination system. For LAN protocols like Ethernet and Token Ring, these addresses are 6-byte hexadecimal strings assigned to network interface adapters by their manufacturers. The addresses are referred to as hardware addresses or Media Access Control (MAC) addresses, to distinguish them

from addresses used at other layers of the OSI model. It is important to understand that data-link layer protocols are limited to communications with computers on the same LAN. The hardware address in the header always refers to a computer on the same local network, even if the data's ultimate destination is a system on another network.

❖ **Network Layer Protocol Identifier:**

The other primary functions of the data-link layer frame are to identify the network layer protocol that generated the data in the frame. A computer can use multiple protocols at the network layer, and the data-link layer protocol frame usually contains a code that specifies which network layer protocol generated the data in the packet so that the data-link layer protocol on the receiving system can pass the data to the appropriate protocol at its own network layer.

❖ **The Error Detection Information:**

This can take the form of a cyclical redundancy check (CRC) computation performed on the payload data (the actual data in the frame) by the transmitting system, the results of which are included in the frame's footer. On receiving the packet, the receiving system performs the same computation and compares its results to those in the footer. If the results match, the data has been transmitted successfully. If they do not, the receiving system assumes that the packet is corrupted and discards it.

➢ Media Access Control (MAC)

The computers on a LAN usually share a common medium, making it possible for two computers to transmit data at the same time. When this happens, a packet collision is said to occur, and the data in both packets is lost. One of the main functions of the data-link layer protocol in this type of network is to provide a mechanism that regulates access to the network medium. This mechanism, called a MAC mechanism, provides each computer with an equal opportunity to transmit its data while minimizing the occurrence of packet collisions.

The MAC mechanism is one of the primary defining characteristics of a data-link layer protocol. Ethernet uses a MAC mechanism called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Several other protocols, including Token Ring, use a scheme called token passing.

➢ Physical Layer Specifications

The data-link layer protocols used on LANs often support more than one network medium, and the protocol standard includes one or more physical layer specifications. The data-link layer and physical layer are closely related, because the characteristics of the network medium have a profound effect on the functionality of the protocol's MAC mechanism.

Layer3: The Network Layer

At first glance, the network layer seems to duplicate some of the functions of the data-link layer. This is not so, however, because network layer protocols are responsible for end-to-end communications, whereas data-link layer protocols function only on the local LAN. To say that network layer protocols are responsible for end-to-end communications means that the network layer protocol is responsible for a packet's complete journey from the system that created it to its final destination.

The most popular example of network layer protocols is the Internet Protocol (IP). The Internet Protocol (IP) is the cornerstone of the Transmission Control Protocol/Internet Protocol (TCP/IP). Another example of network layer protocols is the Internetwork Packet Exchange (IPX).

Main functions of network layer protocols are

1. Addressing
2. Fragmenting
3. Routing
4. Identifying the transport layer protocol.

➢ Addressing

The network layer protocol header contains source address and destination address fields, just as the data-link layer protocol does. However, in this case, the destination address is the packet's final destination, which may be different from the data-link layer protocol header's destination address. For example, when you type the address of a Web site in your browser, the packet your system generates contains the address of the Web server as its network layer destination, but the data-link layer destination is the address of the router on your LAN that provides you with Internet access.

IP has its own addressing system that is completely separate from the data-link layer addresses. Each computer on an IP network is assigned a 32-bit IP address. This address identifies both the network on which the computer is located and the computer itself, so that one address can uniquely identify any computer.

➢ Fragmenting

Network layer datagrams may have to pass through many different networks on the way to their destinations, and the data-link layer protocols that the datagrams encounter can have different properties and limitations. One of these limitations is the maximum packet size permitted by the protocol. For example, Token Ring frames can be as large as 4500 bytes, but Ethernet frames are limited to 1500 bytes. When a large datagram that originated on a Token Ring network is routed to an Ethernet network, the network layer protocol must split it into pieces no larger than 1500 bytes each. This process is called fragmentation.

During the fragmentation process, each fragment becomes a packet in itself that continues the journey to the network layer destination. The fragments are not reassembled until all of the packets that make up the datagram reach the destination system. In some cases, datagrams may be fragmented, and their fragments may be fragmented again repeatedly before reaching their destination.

➢ Routing

Routing is the process of directing a datagram from its source, through an internetwork, and to its ultimate destination using the most efficient path possible. On complex internetworks such as the Internet or a large corporate network, there are often many possible routes to a given destination. Network designers usually create redundant links so that, if one of the routers on the network fails, traffic can still find its way to its destination.

There are two types of systems involved in internetwork communications :-

- End systems: which are the source of individual packets and also their ultimate destination. End systems utilize all seven layers of the OSI model,
- intermediate systems: such as Routers. Whereas packets arriving at intermediate systems rise only as high as the network layer of the OSI model.

➢ Identifying the Transport Layer Protocol

The network layer header identifies the transport layer protocol from which it receives the data that it carries. With this information, the receiving system can pass the incoming datagrams to the correct transport layer protocol.

Layer4: The Transport Layer

The transport layer protocols provide services that complement those provided by the network layer. The transport and network layer protocols used to transmit data are often thought of as a matched pair, as seen in the case of TCP/IP. These protocols include TCP. Most protocol suites provide two or more transport layer protocols that provide different levels of service. The alternative to TCP is the User Datagram Protocol (UDP). The IPX protocol suite also provides a choice between transport layer protocols, including the NetWare Core Protocol (NCP) and Sequenced Packet Exchange (SPX).

The headers for transport layer protocols usually include numbers called the port numbers that identify the applications from which the packet originated and for which it is destined.

Transport layer protocols also do segmentation, here the data come from the session layer are divided intro segments, keeping the sequential number of each

segment in the protocol header. This number will help the recipient to reassemble the segment.

The main difference between the protocols provided at the transport is that some are connection-oriented and some are connectionless.

- **Connection-oriented protocol:-**

connection-oriented protocol is one in which the two communicating systems exchange messages to establish a connection before they transmit any application data. This ensures that the systems are both active and ready to exchange messages.

Connection-oriented protocols also provide additional services such as packet acknowledgment, flow control, and end-to-end error detection and correction. Systems generally use this type of protocol to transmit relatively large amounts of information that can't tolerate even a single bit error, such as data or program files, and these services ensure the correct transmission of the data.

The drawback of this type of protocol is that it greatly increases the amount of control data exchanged by the two systems. In addition to the extra messages needed to establish and terminate the connection, the header applied by a connection-oriented protocol is substantially larger than that of a connectionless one. In the case of the TCP/IP transport layer protocols, TCP uses a 20-byte header and UDP uses only an 8-byte one.

- **Connectionless protocol**

A connectionless protocol is one in which there is no preliminary communication between the two systems before the transmission of application data. The sender simply transmits its data to the destination without knowing if the system is ready to receive data, or even if the system exists.

Systems generally use connectionless protocols, such as UDP, for brief transactions that consist only of single requests and responses. The response from the recipient functions as a tacit acknowledgment of the transmission.

Layer5: The Session Layer

There are no separate session layer protocols as there are at the lower layers. Session layer functions are instead integrated into other protocols that also include presentation and application layer functions.

The transport, network, data-link, and physical layers are concerned with the proper transmission of data across the network, but the protocols at the session layer and above are not involved in that part of the communications process.

As its name implies, the session layer establishes, manages, and terminates sessions between two communicating hosts. The session layer provides about 22 services, many of which are concerned with the ways in which networked systems exchange information. The most important of these services are dialog control and

dialog separation. Where the term dialog refers to the exchange of information between two systems on the network.

- Dialog Control :- is the selection of a mode that the systems will use to exchange messages. When the dialog is begun, the systems can choose one of two modes:-
    1. Two-way alternate (TWA) mode:- (for two communicating computers, only one is permitted to transmit at a time)
    2. Two-way simultaneous (TWS) mode:- (is more complex where the two communicating computers, can transmit at the any time, and even simultaneously)
- Dialog separation :- is the process of creating checkpoints in a data stream that enable communicating systems to synchronize their functions.

Layer6: The Presentation Layer

There is main one function found at the presentation layer: the translation of syntax between different systems. This translation may also include compression and Encryption. In some cases, computers communicating over a network use different syntaxes, and the presentation layer enables them to negotiate a common syntax for the network communications. When the communicating systems establish a connection at the presentation layer, they exchange messages containing information about the syntaxes they have in common, and together they choose the syntax they will use during the session.

Both of the systems involved in the connection have an abstract syntax, which is their native form of communication. Computers running on different platforms can have different abstract syntaxes. During the negotiation process, the systems choose a transfer syntax, which is an alternative syntax that the two have in common. The transmitting system converts its abstract syntax to the transfer syntax, and after the transmission, the receiving system converts the transfer syntax to its own abstract syntax.

Layer7: The Application Layer

The application layer is the OSI layer that is closest to the user. It provides network 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. Most application layer protocols provide services that programs use to access the network, such as the Simple Mail Transfer Protocol (SMTP), which most e-mail programs use to send e-mail messages. In some cases, as with File Transfer Protocol (FTP), the application layer protocol is a program in itself.

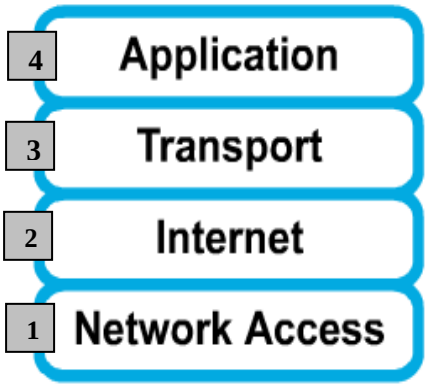
Application layer protocols often include the session and presentation layer functions. As a result, a typical protocol stack consists of four separate protocols that run at the application, transport, network, and data-link layers.

TCP/IP Model

Another model used to describe networking is the TCP/IP (Transmission Control Protocol/Internet Protocol) . This model is developed by DoD (Department of Defense) in USA. This model consists of four layers. These layers are:-

- Layer 4: The application layer
- Layer 3: The Transport layer
- Layer 2: The Internet layer
- Layer 1: The Network Access layer

The 4-layer TCP/IP Reference Model



Note: It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model. Do not confuse the layers of the two models, because the application layer has different functions in each model.

• Network Access Layer

The name of this layer is very broad and somewhat confusing. It is also called the host-to-network layer. It is the layer that is concerned with all of the issues that an IP packet requires to actually make a physical link. It includes all the details in the OSI physical and data link layers.

• Internet Layer

The purpose of the internet layer is to send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks 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.

• Transport Layer

The transport layer deals with issues like 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.

- **Application Layer**

The designers of TCP/IP felt that the higher level protocols should include the session and presentation layer details. They simply created an application layer that handles high level protocols, issues of representation, encoding, and dialog control. The TCP/IP combines all issues related to application into one layer, and assures this data is properly packaged for the next layer.

TCP/IP vs. OSI :-

If you compare the TCP model and the OSI model, you will notice that they have similarities and differences. Examples include:

Similarities

- Both are layered models
- Both have application layers, though they include very different services
- Both have comparable transport and network (internet) layers
- Packet-switched (not circuit-switched) technology is assumed

Differences

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into one layer
- TCP/IP appears simpler because it has fewer layers, however this is a misconception. The OSI reference model, with its less complex and multiple layers, is simpler to develop and troubleshoot.