

Chapter Four

Protocols and standard Models

Standards (Industry standards) are needed for the purpose of heterogeneous networks can communicate with one another and Standards are necessary to ensure that products from different manufacturers can work together as expected. The two best-known standards are the OSI model and the Internet model.

A protocol is a set of rules that govern data communication; the key elements of a protocol are syntax, semantics, and timing.

Introduction to OSI Model & its layers

The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO). ISO is the organization, while OSI is the model.

It was developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system.

It is a network model that defines the protocols for network communications. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. Physically OSI model breaks the various aspects of a computer network into seven distinct layers. OSI model is also like an onion in that if you start to peel it apart to have a look inside, you 'are bound to shed a few tears. OSI model is a framework into which the various networking standards can fit. OSI model specifies what aspects of a network's operation can be addressed by various network standards.

The first three layers are sometimes called the lower layers. They deal with the mechanics of how information is sent from one computer to another over a network. Layers 4 through 7 are sometimes called the upper layers. They deal with how applications programs relate to the network through application programming interfaces.

Description of Layers in the OSI Model

1. Physical Layer

- I. The Physical Layer provides a standardized interface to physical transmission media, including
 - Mechanical specification of electrical connectors and cables, for example maximum cable length
 - Electrical specification of transmission line
 - Bit-by-bit or symbol-by-symbol delivery
- II. On the sender side, the physical layer receives the data from Data Link Layer and encodes it into signals to be transmitted onto the medium. On the receiver side, the physical layer receives the signals from the transmission medium decodes it back into data and sends it to the Data Link Layer as shown in the figure below:

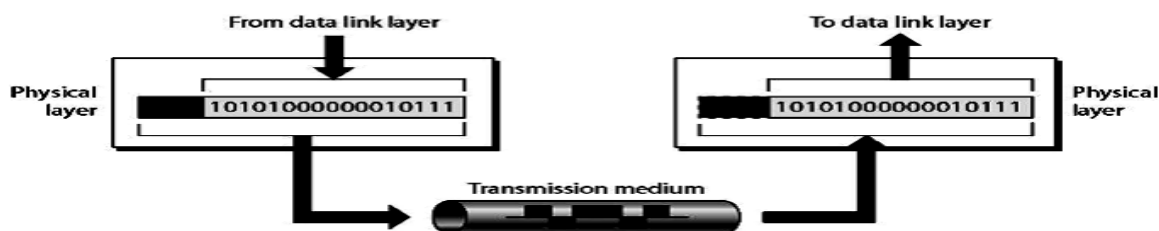


Fig: Transmission of data to and from Physical Layer

- III. **Interface**
The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
- IV. **Representation of bits**
The physical layer is concerned with transmission of signals from one device to another which involves converting data (1's & 0's) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
- V. **Data rate**
The physical layer defines the data transmission rate that means number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.
- VI. **Synchronization of bits**
To interpret correct and accurate data the sender and receiver have to maintain the same bit rate and also have synchronized clocks.
- VII. **Line configuration**
The physical layer defines the nature of the connection .that means a point to point link, or a multi- point link.
- VIII. **Physical Topology**
The physical layer defines the type of topology in which the device is connected to the network. In a mesh topology it uses a multipoint connection and other topologies it uses a point to point connection to send data.
- IX. **Transmission mode**

The physical layer defines the direction of data transfer between the sender and receiver. Two devices can transfer the data in simplex, half duplex or full duplex mode

- X. Main responsibility of the physical layer is Transmission of bits from one hop to the next.

2. Data Link Layer

- I. The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
- II. On the sender side, the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as **Frames** and sends it to the physical layer.
- III. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer. This process is called **Framing**. It is shown in the figure below:

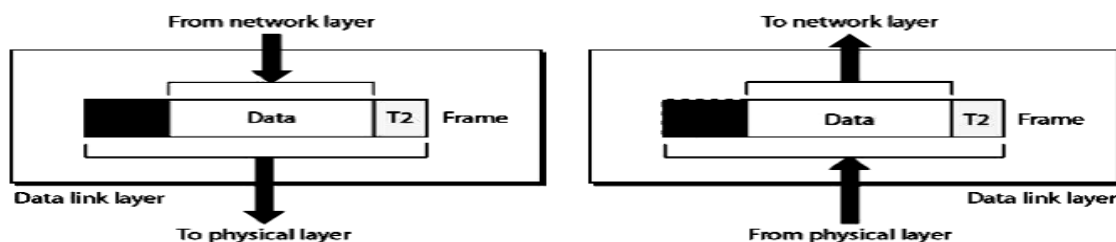


Fig: Data Link Layer: The process of Framing

IV. Physical Addressing (inside / outside sender's network)

- The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
- The physical address contains the address of the sender and receiver.
- In case the receiver happens to be on the same physical network as the sender; the receiver is at only one hop from the sender and the receiver address contains the receiver's physical address.
- In case the receiver is not directly connected to the sender, the physical address is the address of the next node where the data is supposed to be delivered.

V. Flow control

- The data link layer makes sure that the sender sends the data at a speed at which the receiver can receive it else if there is an overflow at the receiver side the data will be lost.
- The data link layer imposes flow control mechanism over the sender and receiver to avoid overwhelming of the receiver.

VI. Error control

- The data link layer imposes error control mechanism to identify lost or damaged frames, duplicate frames and then retransmit them.
- Error control information is present in the trailer of a frame.

VII. Access Control

- The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection scenario.

VIII. The main responsibility of the data link layer is hop to hop transmission of frames.

3. Network Layer

- The network layer makes sure that the data is delivered to the receiver despite multiple intermediate devices.
- The network layer at the sending side accepts data from the transport layer, divides it into packets, adds addressing information in the header and passes it to the data link layer.

At the receiving end the network layer receives the frames sent by data link layer, converts them back into packets, verifies the physical address (verifies if the receiver address matches with its own address) and the send the packets to the transport layer.

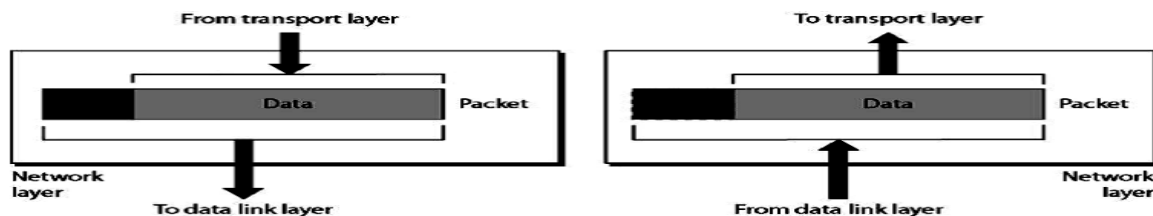


Fig: Network Layer

- The network layer is responsible for source to destination of delivery of data. Hence it may have to route the data through multiple networks via multiple intermediate devices. In order to achieve this the network layer relies on two things:

- Logical Addressing
- Routing

A. Logical Addressing

- The network layer uses logical address commonly known as IP address to recognize devices on the network.
- An IP address is a universally unique address which enables the network layer to identify devices outside the sender's network.
- The header appended by the network layer contains the actual sender and receiver IP address.
- At every hop the network layer of the intermediate node check the IP address in the header, if its own IP address does not match with the IP address of the receiver found in the header, the intermediate node concludes that it is not the final node but an intermediate node and passes the packet to the data link layer where the data is forwarded to the next node.

B. Routing

The network layer divides data into units called packets of equal size and bears a sequence number for rearranging on the receiving end. Each packet

is independent of the other and may travel using different routes to reach the receiver hence may arrive out of turn at the receiver.

Hence every intermediate node which encounters a packet tries to compute the best possible path for the packet. The best possible path may depend on several factors such as congestion, number of hops; etc. This process of finding the best path is called as Routing. It is done using routing algorithms.

- IV. The main responsibility of Network Layer is transmission of packets from source to destination

4. Transport Layer

- I. A logical address at network layer facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other. Hence it is important to deliver the data not only from the sender to the receiver but from the correct process on the sender to the correct process on the receiver. The transport layer takes care of process to process delivery of data and makes sure that it is intact and in order.

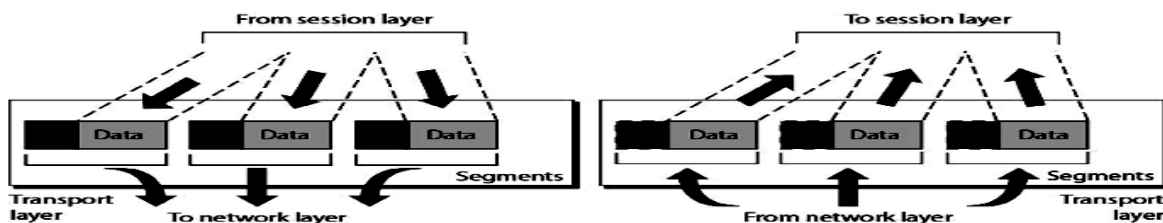


Fig: Transport Layer

- II. To ensure process to process delivery the transport layer makes use of **port address** to identify the data from the sending and receiving process. A Port Address is the name or label given to a process. It is a 16 bit address. Ex. TELNET uses port address 23, HTTP uses port address 80. Port address is also called as Service Point Address

The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private)

- ✓ **Well-known ports.** The ports ranging from 0 to 1023 are assigned and controlled by IANA. These are the well-known ports.
- ✓ **Registered ports.** The ports ranging from 1024 to 49,151 are not assigned or controlled by IANA. They can only be registered with IANA to prevent duplication.
- ✓ **Dynamic ports.** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process. These are the ephemeral ports.

- III. The data can be transported in a connection oriented or connectionless manner. If the connection is connection oriented then all segments are received in order else they are independent of each other and are received out of order and have to be rearranged.

- IV. The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers. This numbering enables the receiving transport layer to rearrange the segments in proper order.
- V. **Flow Control & Error control:** the transport layer also carries out flow control and error control functions; but unlike data link layer these are **end to end** rather than node to node.

VI. **Main Responsibility**

The main responsibility of the transport layer is process to process delivery of the entire message.

5. **Session Layer**

- I. The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
- II. The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called synchronization bits and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the **checkpoints** inserted previously and passes the data to the presentation layer.
- III. The checkpoints or synchronization points is a way of informing the status of the data transfer. Ex. A checkpoint after first 500 bits of data will ensure that those 500 bits are not sent again in case of retransmission at 650th bit.
- IV. Main responsibility of session layer is dialog control and synchronization.

6. **Presentation Layer**

- I. The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
- II. The presentation layer at sending side receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer. At the receiving side, the presentation layer receives data from the session layer decompresses and decrypts the data as required and translates it back as per the encoding scheme used at the receiver.

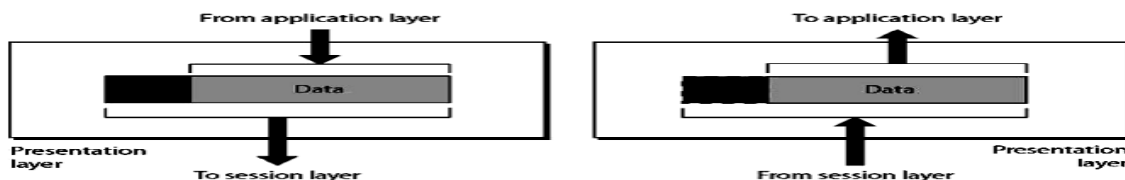


Fig : Presentation Layer

- III. **Translation:** The sending and receiving devices may run on different platforms (hardware, software and operating system). Hence it is important that they understand the messages that are used for

communicating. Hence a translation service may be required which is provided by the Presentation layers.

IV. **Compression**

Compression ensures faster data transfer. The data compressed at sender has to be decompressed at the receiving end, both performed by the Presentation layer.

V. **Encryption**

It is the process of transforming the original message to change its meaning before sending it. The reverse process called decryption has to be performed at the receiving end to recover the original message from the encrypted message.

VI. The main responsibility of the Presentation layer is translation, compression and encryption.

7. **Application Layer**

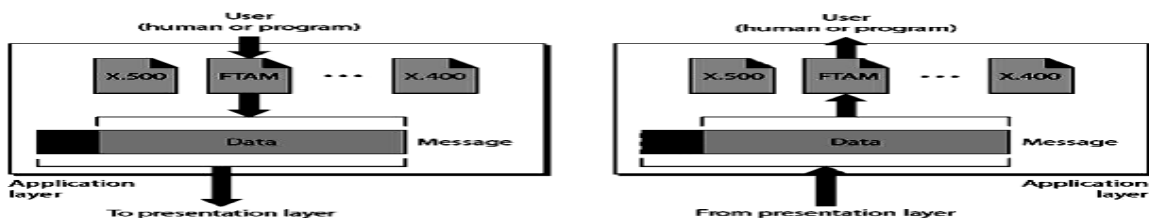
I. The application layer enables the user to communicate its data to the receiver by providing

Application Layer

Some of the better-known Application layer protocols are:-

- ✓ DNS (Domain Name System) for resolving Internet domain names.
- ✓ FTP (File Transfer Protocol) for file transfers.
- ✓ SMTP (Simple Mail Transfer Protocol) for e-mail.
- ✓ SMB (Server Message Block) for file sharing in Windows networks.
- ✓ NFS (Network File System) for file sharing in UNIX networks.
- ✓ Telnet for terminal emulation.

II. Main Responsibility of Application layer is to provide access to network resources.



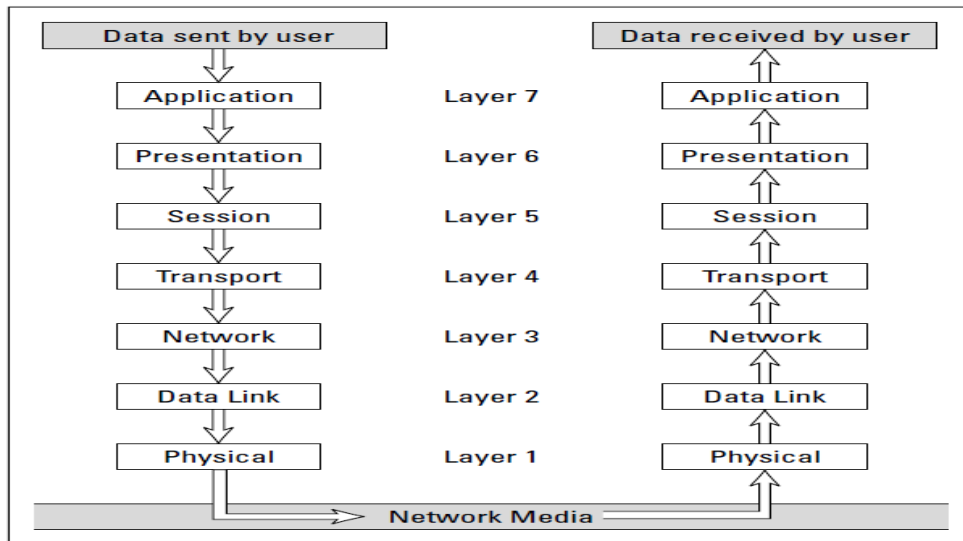


Figure:

How data travels through ..

■ Transport Control Protocol /Internet Protocol (TCP/IP)Model

It is also called as the TCP/IP protocol suite. It is a collection of protocols. IT is a hierarchical model, there are multiple layers and higher layer protocols are supported by lower layer protocols. It existed even before the OSI model was developed. Originally had four layers (bottom to top):

1. Host to Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

- The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.
- The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.
- The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model
- The Network layer of TCP/IP model corresponds to the Network Layer of OSI model
- The Host to network layer of TCP/IP model corresponds to the Physical and Data link Layer of OSI model.

SIMILARITIES

The main similarities between OSI and TCP/IP models include the following:

- They share similar architecture. - Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.
- They share a common application layer.- Both of the models share a

common "application layer". However in practice this layer includes different services depending upon each model.

- Both models have comparable transport and network layers.- This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.
- Knowledge of both models is required by networking professionals.- According to article obtained from the internet networking professionals "need to know both models".
- Both models assume that packets are switched.- Basically this means that individual packets may take differing paths in order to reach the same destination.

DIFFERENCES

The main differences between the two models are as follows:

OSI	TCP / IP
Application (Layer 7)	Application
Presentation (Layer 6)	
Session (Layer 5)	Transport
Transport (Layer 4)	
Network (Layer 3)	Internet
Data Link (Layer 2)	Host to Network
Physical (Layer 1)	

- TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a generic, protocol-independent standard.
- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears to be a simpler model and this is mainly due to the fact that it has fewer layers.
- TCP/IP is considered to be a more credible model- This is mainly due to the fact because TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason. Where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.
- The OSI model consists of 7 architectural layers whereas the TCP/IP only has 4 layers.

Functions of the Layers of TCP/IP model:

A. Host to Network Layer

This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers.

B. Network Layer or IP

Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.

The Internetworking Protocol (IP) is an **connection-less & unreliable protocol**.

It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.

IP transports data by dividing it into **packets or datagram's** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.

In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination. Hence, the word **connection-less**.

The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an **unreliable** protocol.

Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.

IP is a combination of four protocols:

- | | |
|---------|---------|
| 1. ARP | 3. ICMP |
| 2. RARP | 4. IGMP |

1. ARP - Address Resolution Protocol

- ✓ It is used to resolve the physical address of a device on a network, where its logical address is known.
- ✓ Physical address is the 48 bit address that is imprinted on the NIC or LAN card, Logical address is the Internet Address or commonly known as IP address that is used to uniquely & universally identify a device.

2. RARP- Reverse Address Resolution Protocol

- ✓ It is used by a device on the network to find its Internet address when it knows its physical address.

3. ICMP- Internet Control Message Protocol

- ✓ It is a signaling mechanism used to inform the sender about datagram problems that occur during transit.
- ✓ It is used by intermediate devices.

- ✓ In case and intermediate device like a gateway encounters any problem like a corrupt datagram it may use ICMP to send a message to the sender of the datagram.

4. IGMP- Internet Group Message Protocol

- ✓ It is a mechanism that allows to send the same message to a group of recipients.

C. Transport Layer

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.

The transport layer contains three protocols:

1. TCP
2. UDP
3. SCTP

1. TCP - Transmission Control Protocol

- ✓ TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.
- ✓ It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.

2. UDP - User Datagram Protocol

- ✓ UDP is a simple protocol used for process to process transmission.
- ✓ It is an unreliable, connectionless protocol for applications that do not require flow control or error control.
- ✓ It simply adds port address, checksum and length information to the data it receives from the upper layer.

3. SCTP - Stream Control Transmission Protocol

- ✓ SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.
- ✓ It combines the features of TCP and UDP.
- ✓ It is used in applications like voice over Internet and has a much broader range of applications

D. Application Layer

The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.