Unit-4

Reference Model

Protocol stack

The term protocol stack is refer to the collection of protocols (of all layers) of a particular network system. The most commonly used network protocols are:

1. TCP/IP (Transmission Control Protocol/Internet Protocol): TCP/IP is a layered set of protocols. TCP is reliable, but complex transport-layer protocol. It is stream connection-oriented and reliable transport protocol. It adds connection-oriented and reliability features. TCP is responsible for making sure that the data is transmitted to other end. It keeps track of what is sent, and retransmits any data that has not reached its destination.
   The Internet Protocol (IP) is the principal communication protocol used for transmitting data packets across and the network using the Internet Protocol Suite. It is the primary protocol that establishes the Internet.
2. UDP (User Datagram Protocol): UDP is simple, connectionless, unreliable transport protocol. It performs very limited error checking. It is mainly used for transmitting multimedia data, which requires faster transmission and error checking is not used.
3. SMPT (Simple Mail Transfer Protocol): SMPT is a standard protocol for transmitting electronic mail (email) by the Internet. It is an Internet mail protocol. It is a TCP/IP protocol used to send emails.
4. POP (Post Office Protocol): POP is also a protocol for transmitting email. It is simple but has limited functionality. It is an application layer Internet standard protocol used by the local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP3 (POP version 3) is used at present. POP3 is supported by most webmail services such as Hotmail, Gmail, etc.
5. IMAP (Internet Mail Access Protocol): IMAP4 (IMAP version 4) is similar to POP3, but has more features. IMAP4 is more powerful and more complex. It is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the POP. Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server.
6. FTP (File Transfer Protocol): FTP is a standard protocol provided by Internet for copying a file from one computer to another. Although transferring files from one system to another seems simple and straight forward. It may create some problems like, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach.
7. HTTP (Hypertext Transfer Protocol Secure): HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network. HTTPS connections are often used for payment transactions on the

World Wide Web and for sensitive transactions in corporate information systems. The main idea of HTTPS is to create a secure channel over an insecure network.

8. Telnet: Telnet is common network protocol used on the Internet and also inside a LAN. However, due to its lack of security, Telnet has been replaced with Secure Shell (SSH) on most servers. It is one of the simplest ways to exchange data between two computers. It allows two computers anywhere on a computer network, including the worldwide Internet, to exchange text and other data in real time.
9. VoIP (Voice over Internet Protocol): VoIP is a methodology and group of technologies for the transmission of voice communications and multimedia data over Internet Protocol, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, broadband telephony, and broadband phone service.

Networking Model

Networks are organized as a series of stacked layers with each layer stacked over another layer below it. This is done in order to divide the workload and to simplify the systems design. The architecture is considered scalable if it is able to accommodate a number of layers in either large or small scales. For example, a computer that runs an Internet application may require all of the layers that were defined for the architectural model. Similarly, a computer that acts as a router may not need all these layers. Systems design is furthermore simplified because with a layered architecture, the design has to only concern the layer in question and not worry about the architecture in a macro sense.

The depth and functionality of this stack differs from network to network. However, regardless of the differences among all networks, the purpose of each layer is to provide certain services (job responsibilities) to the layer above it, shielding the upper layers from the intricate details of how the services offered are implemented. Every computer in a network possesses within it a generic stack. A *logical* communication may exist between any two computers through the layers of the same "level". Layer-n on one computer may converse with layer-n on another computer. There are rules and conventions used in the communication at any given layers, which are known collectively as the layer-n *protocol* for the nth layer.

Data are not directly transferred from layer-n on one computer to layer-n on another computer. Rather, each layer passes data and control information to the layer directly below until the lowest layer is reached. Below layer-1 (the bottom layer), is the physical medium (the hardware) through which the actual transaction takes place. In *Figure* logical communication is shown by a broken-line arrow and physical communication by a solid-line arrow.

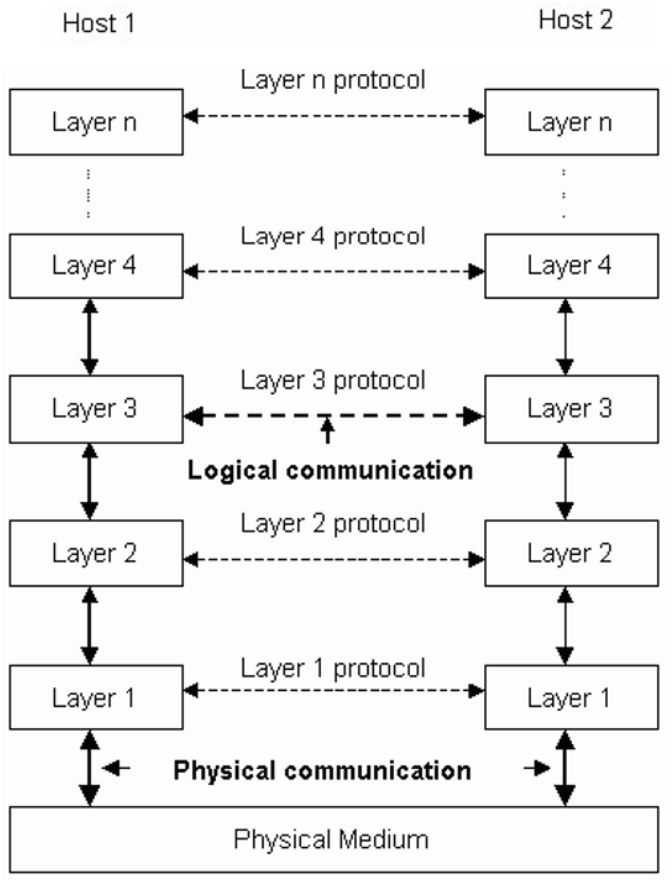

Figure: Layered Network Architecture

Between every pair of adjacent layers is an interface. The interface is a specification that determines how the data should be passed between the layers. It defines what primitive operations and services the lower layer should offer to the upper layer. One of the most important considerations when designing a network is to design clean-cut interfaces between the layers. To create such an interface between the layers would require each layer to perform a specific collection of well-understood functions. A clean-cut interface makes it easier to replace the implementation of one layer with another implementation because all that is required of the new implementation is that, it offers, exactly the same set of services to its neighboring layer above as the old implementation did.

OSI Reference Model

The Open System Interconnection (OSI) model is a set of protocols that attempt to define and standardize the data communications process; we can say that it is a concept that describes how data communications should take place.

The OSI model was set by the International Standards Organisation (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications. The OSI model has the support of most major computer and network vendors, many large customers, and most governments in different countries.

The Open Systems Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers as shown in *Figure* each specifying particular network functions and into these layers are fitted the protocol standards developed by the ISO and other standards bodies. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without affecting the other layers.

The OSI model is modular. Each successive layer of the OSI model works with the one above and below it.

Although, each layer of the OSI model provides its own set of functions, it is possible to group the layers into two distinct categories. The first four layers i.e., physical, data link, network, and transport layer provide the end-to-end services necessary for the transfer of data between two systems. These layers provide the protocols associated with the communications network used to link two computers together. Together, these are communication oriented.

The top three layers i.e., the application, presentation, and session layers provide the application services required for the exchange of information. That is, they allow two applications, each running on a different node of the network to interact with each other through the services provided by their respective operating systems. Together, these are data processing oriented.

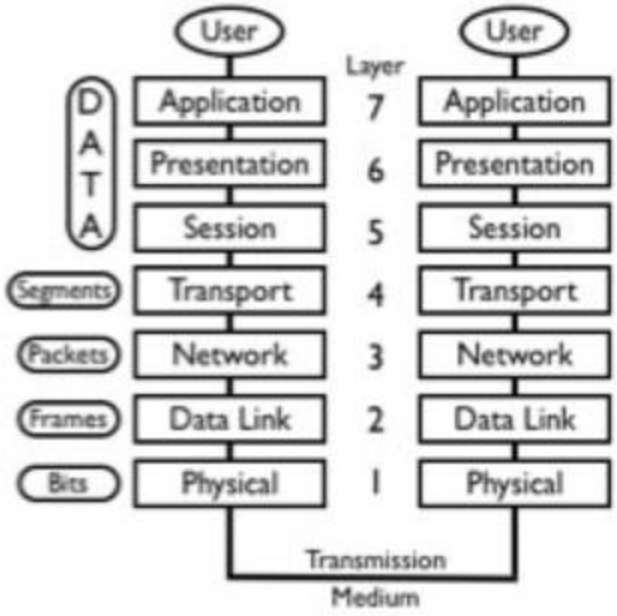

Figure: OSI Reference Model

a) Layer – 1: Physical Layer – The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. **Hub**, **Repeater**, **Modem**, **Cables** are Physical Layer devices.

The functions of the physical layer are :

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- **Bit rate control :** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies :** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
- **Transmission mode :** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

b) Layer – 2 : Data link Layer – The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a

network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sub layers :

- Logical Link Control (LLC)
- Media Access Control (MAC)

Packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

Packet in Data Link layer is referred as Frame and **Switches** and **Bridges** are the data link layer devices.

The functions of the data Link layer are :

- **Framing :** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing :** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
- **Error control :** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control :** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
- **Access control :** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

c) Layer – 3 : Network Layer – Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer. Segment in Network layer is referred as Packet. Devices such as Routers and Layer 3 Switches are Network Layer Devices.

The functions of the Network layer are :

- **Routing :** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
- **Logical Addressing :** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are

placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

d) Layer – 4 : Transport Layer – Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls. Transport Layer is called as Heart of OSI model. Transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if error is found.

- **At sender's side : T**ransport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

  Note : The sender need to know the port number associated with the receiver's application.

  Generally this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

- **At receiver's side :** Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

- **Segmentation and Reassembly :** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing :** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

- **Connection Oriented Service :** It is a three phase process which include Connection Establishment, Data Transfer, Termination/disconnection. In this type of transmission the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

- **Connection less service :** It is a one phase process and includes Data Transfer. In this type of transmission the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

e) Layer – 5: Session Layer – This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

- **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller :** The session layer determines which device will communicate first and the amount of data that will be sent.

f) Layer – 6 : Presentation Layer – Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

- **Translation :** For example, ASCII to EBCDIC.
- **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression :** Reduces the number of bits that need to be transmitted on the network.

g) Layer – 7 : Application Layer – At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as window for the application services to access the network and for displaying the received information to the user. Application Layer is also called as Desktop Layer. Ex: Application – Browsers, Skype Messenger etc.

The functions of the Application layer are :

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services