ASSIGNMENT OSI Model

1. OSI SEVEN LAYERS:

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications.

The OSI model divides networking up into a "vertical stack" consisting 7 layers. We'll describe OSI layers "top down" from the application layer that directly serves the end user, down to the physical layer.

The OSI model consists of the following seven layers:

Layer 7—Application

Layer 6—Presentation

Layer 5—Session

Layer 4—Transport

Layer 3—Network

Layer 2—Data Link

Layer 1—Physical

Layer 7: Application

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS). The application layer sends data to, and receives data from, the presentation layer.

Layer 6: Presentation

The presentation layer handles "syntax processing" – in other words, it converts data from one format to another. The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

ASSIGNMENT OSI Model

Layer 5: Session

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint. Once a “session” is established, the data is passed to or from the Transport Layer.

Layer 4: Transport

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again. Layer 4 Transport examples include SPX, TCP, UDP

Layer 3: Network

The 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 the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

Functions of the Network Layer

Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing

Logical Addressing: To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 3 Network examples include AppleTalk DDP, IP, IPX.

Layer 2: Data Link

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 the DLL to transmit it to the Host using its MAC address.

The Data Link Layer is divided into two sublayers:

Logical Link Control (LLC)

Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the 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.

Functions of the Data Link Layer:

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, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.

Error control: The 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 the amount of data that can be sent before receiving an acknowledgment.

Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 1: Physical

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Layer 1 Physical examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.

Advantages of the OSI model:

The OSI model helps users and operators of networks in a number of ways. It standardizes network communications, as each layer has fixed functions and protocols. Diagnosing network problems is easier with the OSI model. It is easier to improve with advancements as each layer can get updates separately. Having a standard model enables troubleshooting, identifying which network layer is causing an issue and focusing efforts on that layer. The standardized OSI model also helps network device manufacturers and networking software vendors: Create devices and software that can communicate with products from any other vendor, allowing open interoperability. Define which parts of the network their products should work with. Communicate to users at which network layers their product operates – for example, only at the application layer, or across the stack.

ASSIGNMENT OSI Model

2. Working and Functionality of TCP/IP:

There are two network models that are very much used nowadays. One is the OSI model, and the other is the TCP/IP model. TCP/IP vs. OSI is a persistent topic in the networking field, so let's see how both models really differ.

TCP/IP is a data link protocol used on the internet to let computers and other devices send and receive data. TCP/IP stands for Transmission Control Protocol/Internet Protocol and makes it possible for devices connected to the internet to communicate with one another across networks.

TCP/IP Model:

The TCP model stands for Transmission Control Protocol, whereas IP stands for Internet Protocol. A number of protocols that make the internet possibly comes under the TCP/IP model. Nowadays, we do not hear the name of the TCP/IP model much, we generally hear the name of the IPv4 or IPv6, but it is still valid.

This model consists of 4 layer: Network Access, Internet, Transport, and Application.

Here is a brief description of each layer:

Network Access Layer – defines the protocols and hardware required to deliver data across a physical network.

Internet Layer – defines the protocols for logically transmitting packets over the network.

Transport Layer – defines protocols for setting up the level of transmission service for applications. This layer is responsible for the reliable transmission of data and the error-free delivery of packets.

Application Layer – defines protocols for node-to-node application communication and provides services to the application software running on a computer.

TCP/IP determines how computers transfer data from one device to another. This data needs to be kept accurate so that the receiver gets the same information that the sender originally sent.

So what is TCP/IP and how does it work? To ensure that each communication reaches its intended destination intact, the TCP/IP model breaks down data into packets and then reassembles the packets into the complete message on the other end. Sending the data in small packets makes it easier to maintain accuracy versus sending all the data at once.

After a single message is split into packets, these packets may travel along different routes if one route is congested. It's like sending a few different birthday cards to the same household by mail. The cards begin their journey at your home, but you might drop each card into a different mailbox, and each card may take a different path to the recipient's address.

ASSIGNMENT OSI Model

How does the TCP/IP model work?

Whenever you send something over the internet — a message, a photo, a file — the TCP/IP model divides that data into packets according to a four-layer procedure. The data first goes through these layers in one order, and then in reverse order as the data is reassembled on the receiving end.

The TCP/IP model works because the whole process is standardized. Without standardization, communication would go haywire and slow things down — and fast internet service relies on efficiency. As the global standard, the TCP/IP model is one of the most efficient ways to transfer data over the internet.

Differences Between TCP/IP vs OSI Model:

The difference between the two models is that the OSI model segments multiple functions that the TCP/IP model groups into single layers. This is true of both the application and network access layers of the TCP/IP model, which contain multiple layers outlined within the OSI model.

The TCP/IP model is not that specific. It can be said that the OSI model prescribes and TCP/IP model describes.

ASSIGNMENT OSI Model

3. Working of TCP & UDP Protocols Working of HTTP, HTTPs & ICMP Protocol

TCP and UDP protocols:

TCP stands for Transmission Control Protocol. UDP stands for User Datagram Protocol. Both protocols allow network applications to exchange data between nodes. The main difference between both is that TCP is a connection-oriented protocol while UDP is a connectionless protocol.

When the TCP protocol is used, a special connection is opened up between two network devices, and the channel remains open to transmit data until it is closed. On the other hand, a UDP transmission does not make a proper connection and merely broadcasts its data to the specified network address without any verification of receipt.

TCP VS UDP:

TCP:

The TCP stands for Transmission Control Protocol. If we want the communication between two computers and communication should be good and reliable. For example, we want to view a web page, then we expect that nothing should be missing on the page, or we want to download a file, then we require a complete file, i.e., nothing should be missing either it could be a text or an image. This can only be possible due to the TCP. It is one of the most widely used protocols over the TCP/IP network.

UDP:

The UDP stands for User Datagram Protocol. Its working is similar to the TCP as it is also used for sending and receiving the message. The main difference is that UDP is a connectionless protocol. Here, connectionless means that no connection establishes prior to communication. It also does not guarantee the delivery of data packets. It does not even care whether the data has been received on the receiver's end or not, so it is also known as the "fire-and-forget" protocol. It is also known as the "fire-and-forget" protocol as it sends the data and does not care whether the data is received or not. UDP is faster than TCP as it does not provide the assurance for the delivery of the packets.

HTTP (Hypertext Transfer Protocol):

HTTP is often called the protocol of the Internet. HTTP received this designation because most Internet traffic is based on HTTP. When a user requests a Web resource, it is requested using HTTP. The following is a Web request:

http://www.example.com

When a client enters this address into a Web browser, DNS is called to resolve the Fully Qualified Domain Name (FQDN) to an IP address. When the address is resolved, an HTTP get request is sent to the Web server. The Web server responds with an HTTP send response. Such communication is done several times throughout a single session to a Web site. HTTP uses TCP for communication between clients and servers. HTTP operates on port 80.

ASSIGNMENT OSI Model

HTTPS (Hypertext Transfer Protocol Secure):

HTTPS is for Web sites using additional security features such as certificates. HTTPS is used when Web transactions are required to be secure. HTTPS uses a certificate-based technology such as VeriSign.

Certificate-based transactions offer mutual authentication between the client and the server. Mutual authentication ensures the server of the client identity and ensures the client of the server identity. HTTPS, in addition to using certificate-based authentication, encrypts all data packets sent during a session.

ICMP (Internet Control Message Protocol):

ICMP provides network diagnostic functions and error reporting. ICMP also provides a little network help for routers. When a router is being overloaded with route requests, the router sends a source quench message to all clients on the network, instructing them to slow their data requests to the router.

ICMP was primarily designed for devices that work in the path that connects the sender device to the receiver device. The most common device that works in the middle of the path is the router. ICMP is not restricted to routers. Any device in the network can use ICMP and send messages to another device. ICMP provides a single mechanism for all control and information messages.

The main functions of ICMP are the following:

- Allow routers to inform a source when an IP packet sent by the source is undeliverable.
- Allow a source to discover all available paths to the destination device.
- Allow a source to check whether the destination device is online and up.
- Allow administrators to test connectivity and debug connectivity-related issues.