UNIT 3

COMPUTER NETWORK

IP ADDRESS

- IP Addresses refer to a number scheme or the way of providing a unique number to every computer or device that connected to the internet/network.

Or

An IP Address is a unique number used to identify a device on a network.

- It is a 32-bit address This is called an IP address or logical address. Which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). Every Host and router on the internet has an IP Address. This IP address is unique and no two devices on the Internet can have the same address at the same time.
- **Each octet** designates either a *network address* or a *host address* on that network. *Which octets are used to designate the network and host address depends on the network class*.

- In any network, when we need to send data to a host device connected to the network, a router uses a broadcast address. Moreover, every network has one unique broadcast address.
- **Broadcast Address** is an address that enables transmission to every node in a local network. The address is the highest numeric value of the address format being used.
- We can simply replace the last bits of a network address by 1, and that would turn into a broadcast address. Therefore, we can determine the broadcast address of any network using the subnet mask and the IP address of that network.
- Let's take a class C IP address: 192.168.1.0. It's a network address. Accordingly, the broadcast address for the given network address would be 192.168.1.255.

- An Ethernet network is type of broadcast network. In a broadcast network any system can send information and all systems receive every message, *although* they discard messages that are not addressed to them.
- Broadcasting is accomplished via the broadcast address. This is the address to use for reaching all other addresses on a network.
- Any address with the host octet set to all 1's, or 255, is by default interpreted as a broadcast address.
- So the **broadcast address** is the address of the subnet, *plus* 255. If a hosts IP address is 129.79.149.0, it's subnet address is 129.79.149 and it's broadcast address would be 129.79.149.255.

TYPES OF IP ADDRESS

- There are **two types** of IP addresses (in terms of *accessibility, uniqueness* & *naming conventions*)

1. Public
2. Private.

- An **IP address** is a number used to identify a host on an IP (Internet Protocol) network.
- In order to successfully communicate on the Internet or any other computer network, a machine must have a network interface and an IP address assigned to it that is unique to that network.

? **Public IP address** is an IP address that is unique to the entire Internet. Public IPs can be accessed globally; therefore, *they are often used by publicly accessible entities such as websites*, *DNS* and *VPN servers*, etc.

➤ Static IP address

- Public static - some times called Dedicated - means the IP address never changes and is tied to a single user, device, server or website.

➤ Dynamic IP address

- Public dynamic - means the IP address can change from time-to-time (for example, when you lose connection and re-connect or the ISP might change the address periodically).
- Most of time for public address to be static or dynamic is done by ISP.

?Private IP address

- Private IP address (Internal) is only used by devices communicating to each other on the same network. Devices with private IP addresses cannot connect to the Internet directly. Likewise, computers or other devices outside the local network cannot connect directly to a device with a private IP.
- **NOTE:**

Also private IP addresses can also be either static or dynamic, just like public IPs. The difference is that private IPs are used inside your local network (LAN) and are not visible on the internet.

- An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks.

- **The following are the three blocks of the IP address space for private networks:-**

i. 10.0.0.0 - 10.255.255.255

ii. 172.16.0.0 - 172.31.255.255

iii. 192.168.0.0 - 192.168.255.255

IP ADDRESS CLASSES

- **IP Address Classes**
- A class - 0 to 126 with default mask of 255.0.0.0
- B class - 128 to 191 with default mask of 255.255.0.0
- C class - 192 to 223 with default mask of 255.255.255.0
- D class - 224 to 247 (Reserved)
- E class - 248 to 255 (Reserved)
- **APIPA** is a mechanism by which a system assign the IP address by itself after the DHCP fail to assign the IP address to it.
- **NOTE:** 127 (It is known as loopback address) is kept for testing internal devices in the motherboard.

- Part of IP Address

I. Network part
II. Local or Host part

- Services provided by IP

I. Addressing
II. Fragmentation

? IP ADDRESS VERSIONS

➤ IPV4
➤ IPV6

NETWORK ADDRESS TRANSLATION(NAT)

- NAT is the method used to translate your local address to a routable address.
- Use a gateway/router to map invalid address to valid IP addresses
- Router receive one IP address

Either dynamically assigns addresses to all the nodes behind the router,or its assign statically using using non-routable addresses.

If dynamic uses DHCP.

When someone inside the network wants to access a computer outside the local network (the internet),the request is sent to the router which uses NAT to send the request to the internet .

NAT is improve the security because it hide the internal IP from the hacker.

DHCP SERVER

- DHCP (dynamic host configuration protocol) it is used to assign the IP address dynamic instead of configure it manual.
- DHCP server automatically assign a computer an:

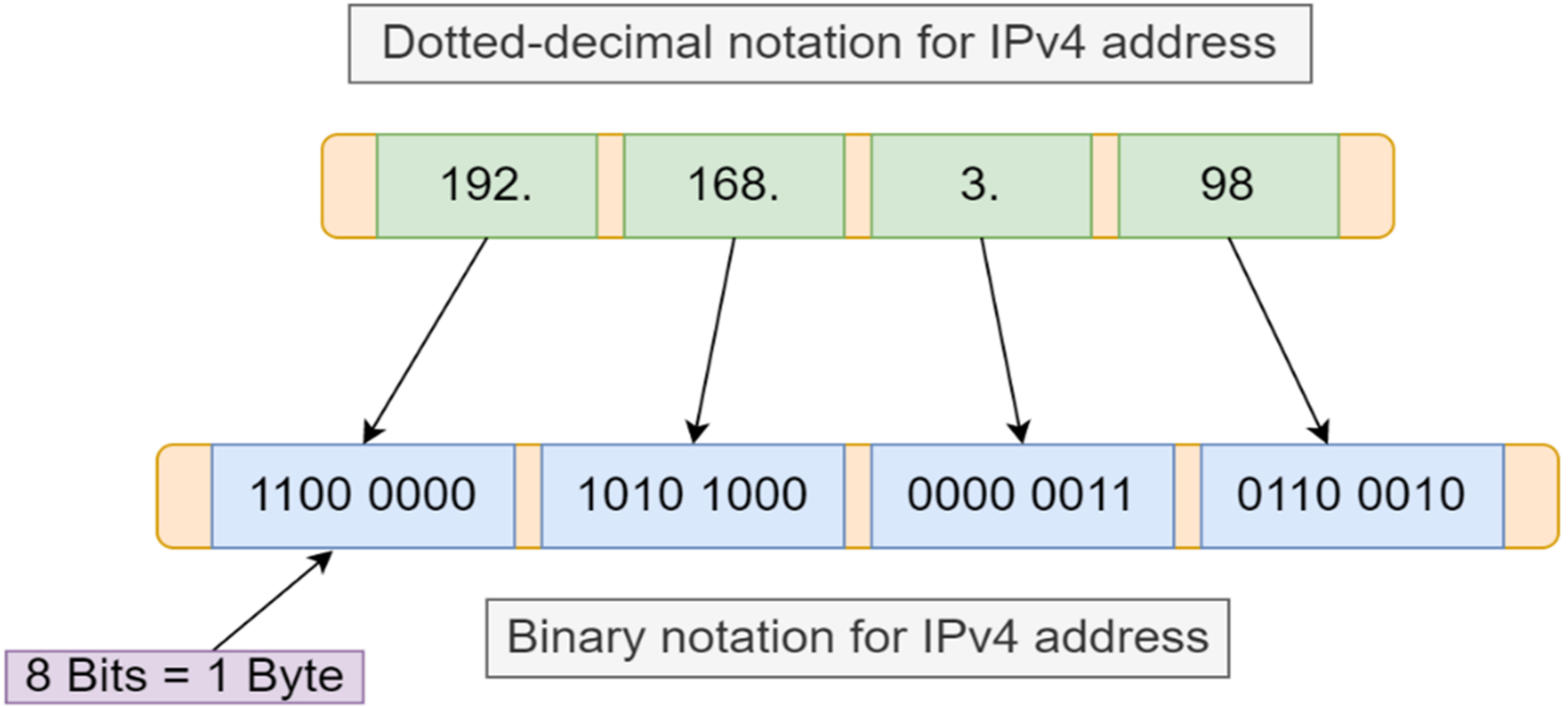
1. IP address
2. Subnet mask
3. Default gateway
4. DNS server

- The DHCP server assign the I.P address as a lease.A LEASE is the amount of time an I.P address is assigned to a computer.
- Lease it help to make sure the DHCP server does not run out of I.P addresses
- DHCP RESERVATION is the process of assign the IP address permanent to the devices .eg printer, router,switch.

IPv4 version

- The First Version IPv4 is the most widely used Internet Protocol. IPv4 addresses are written in the form of a string which consists of 4 numbers with a 3 digit section which lies between the ranges of 0-255. Each number separated by a dot. Each section can be represented in binary form with each section having 8 bits. An IP Address can be written in any form, i.e., binary, octal, and hexadecimal if required.

- IPv4 has a 32 bit long address and has 4 octets and each octet contains 8 bits

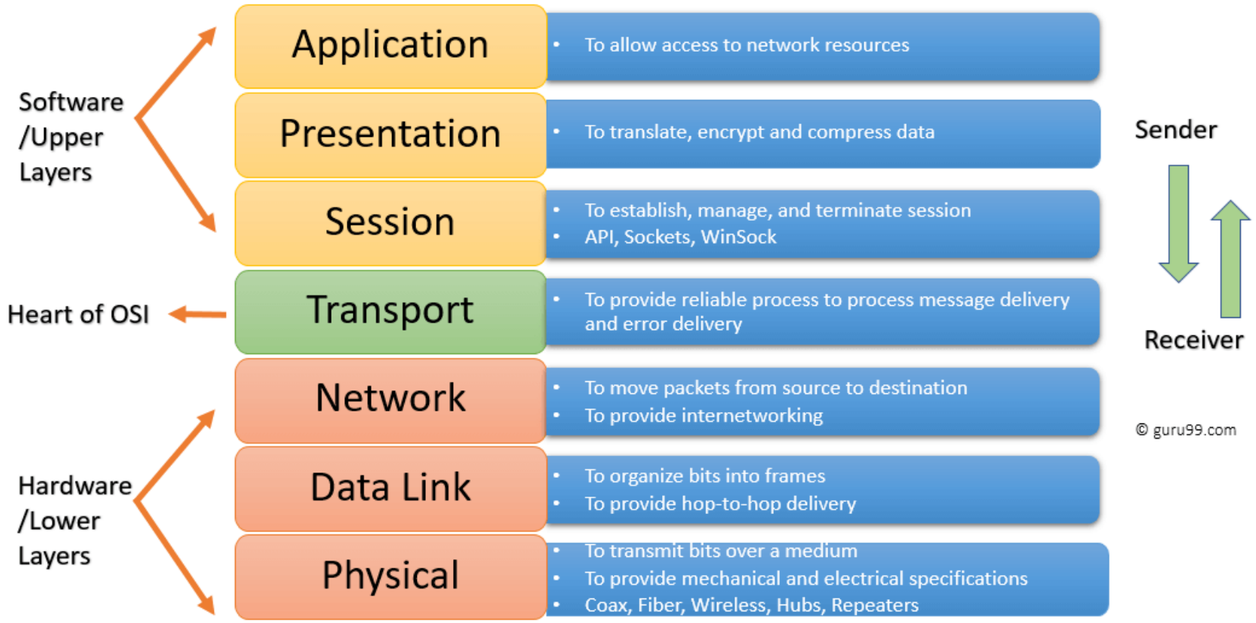


IPv6 Version

- IPv6 Addresses were written using hexadecimal so that they can fit more information using lesser digits. The typical IPv6 address was a long string of numbers in comparison to IPv4. IPv6 uses 128 binary bits to create a single address; the IP address expressed by 8 groups of hexadecimal numbers. Here we used a colon instead of dots to separate the sections of digits. Here if we find 2 colon side by side, that means that all sections between them contain only 0's. Let's see the example of address with and without colons below:
- With double colon -> 2001:0db7::54
- Without double colon -> 2001:0db7:0000:0000:0000:0000:0000:0054

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.



- **The OSI model is divided into two layers:**

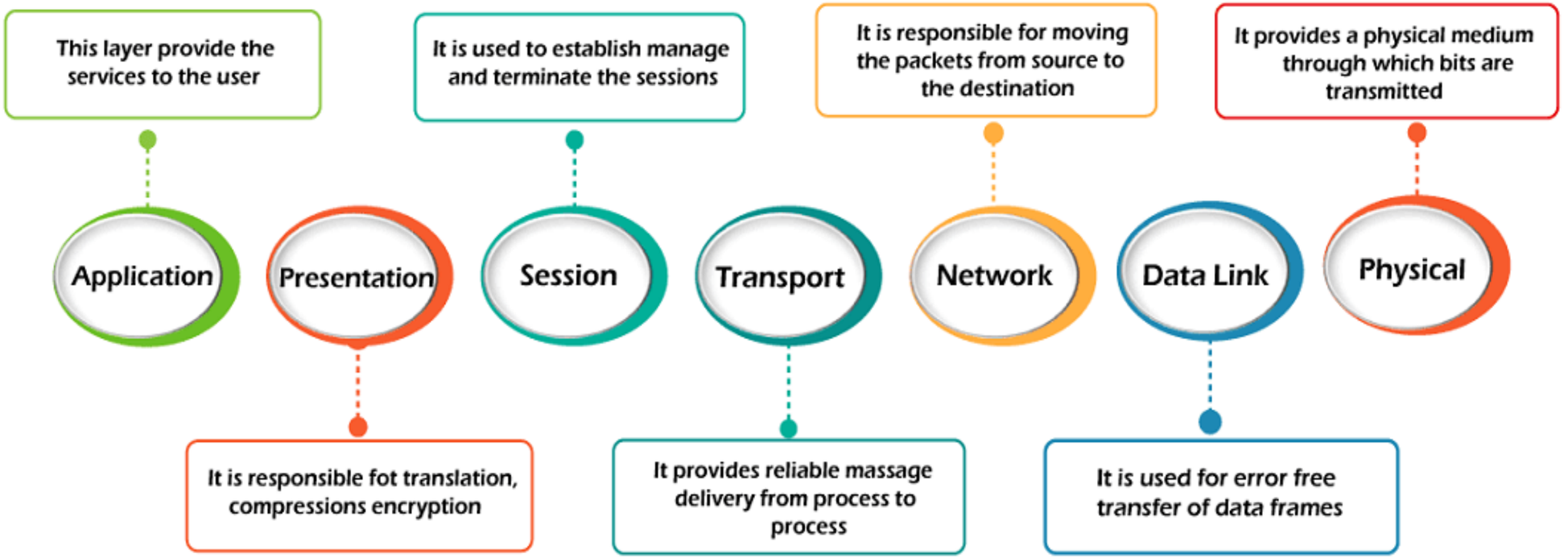
I. upper layers

II. lower layers.

- **The Upper Layers**: It deals with application issues and mostly implemented only in software. The highest is closest to the end system user. In this layer, communication from one end-user to another begins by using the interaction between the application layer. It will process all the way to end-user.
- **The Lower Layers**: These layers handle activities related to data transport. The physical layer and data link layers also implemented in software and hardware

- There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer


This layer provide the services to the user
Application
It is used to establish manage and terminate the sessions
Session
It is responsible for moving the packets from source to the destination
Network
It provides a physical medium through which bits are transmitted
Physical
Presentation
It is responsible fot translation, compressions encryption
Transport
It provides reliable massage delivery from process to process
Data Link
It is used for error free transfer of data frames

PHYSICAL LAYERS

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

FUNCTIONS OF A PHYSICAL LAYER

- **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 the 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 how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

DATA-LINK LAYER

- This layer is responsible for the error-free transfer of data frames.It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

DATA LINK LAYER FUNCTIONS

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

NETWORK LAYER

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

NETWORK LAYER FUNCTIONS

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

TRANSPORT LAYER

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

FUNCTIONS OF TRANSPORT LAYER

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

SESSION LAYER

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **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 that are considered synchronization points in the data. These synchronization points 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 allows two systems to start communication with each other in half-duplex or full-duplex.

.

PRESENTATION LAYER

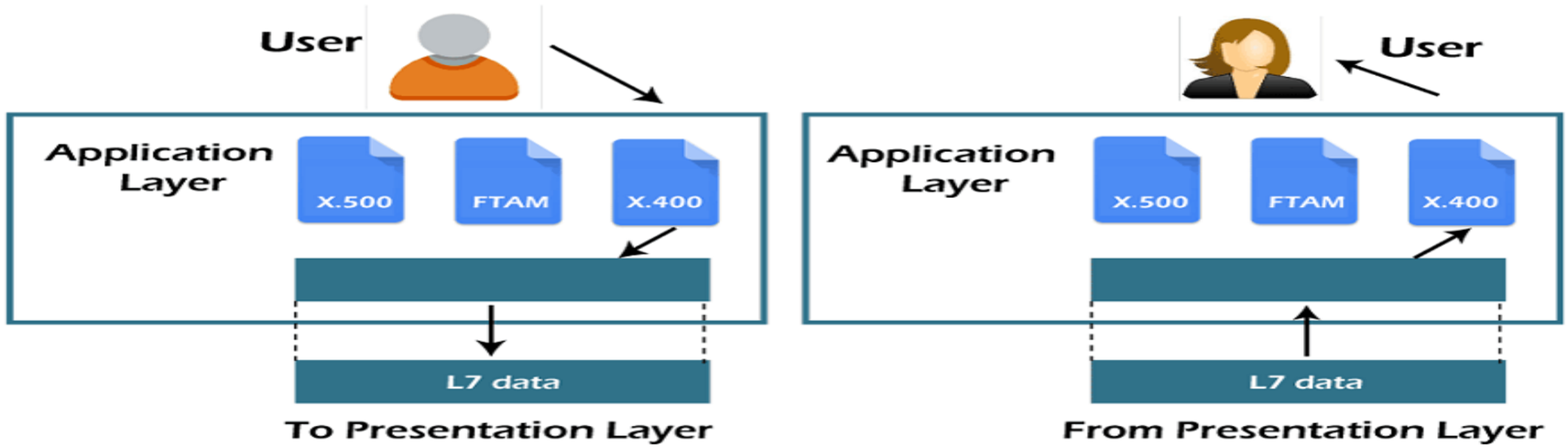
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

FUNCTIONS OF PRESENTATION LAYER

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

APPLICATION LAYER

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.



FUNCTIONS OF APPLICATION LAYER

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

Protocols supported at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable , etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

ADVANTAGES OF OSI MODEL

The OSI model has a number of advantages, including the following:

- It's considered a standard model in computer networking.
- The model supports connectionless, as well as connection-oriented, services. Users can take advantage of connectionless services when they need faster data transmissions over the internet and the connection-oriented model when they're looking for reliability.
- It has the flexibility to adapt to many protocols.
- The model is more adaptable and secure than having all services bundled in one layer.

DISADVANTAGES OSI MODEL

The disadvantages of the OSI model include the following:

- It doesn't define any particular protocol.
- The session layer, which is used for session management, and the presentation layer, which deals with user interaction, aren't as useful as other layers in the OSI model.
- Some services are duplicated at various layers, such as the transport and data-link layers.
- Layers can't work in parallel; each layer must wait to receive data from the previous layer

CABLES

- I gave it as assignment