Chapter No. 4

Network Reference Model & TCP/IP Fundamentals

Course Outcome

Configure basic network services & the different TCP/IP services.

Content

- **OSI Reference Model – Introduction–** Layered Architecture, Peer-to- Peer Processes
- **Functions of Layers of the OSI Reference Model** (Protocols used) – Physical Layer, Data-Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer.
- **Layered Structure of the TCP/IP Reference Model** – Host-to-Network, Internet, Transport, Application layer.
- **Comparison of the OSI and TCP/IP reference models.**
- **TCP / IP Protocol:** ARP, IP, TCP & UDP, FTP, HTTP, SMTP, TELNET, DNS, DHCP.

Protocol Hierarchies-

Protocol:

A protocol is a set of rules and conventions agreed upon and followed by the communicating entities for data communication.

A protocol outlines the what, how and when of a communication.

The three aspects of a protocol are −

Syntax − It defines the format of data that is to be sent or received.

Semantics − It defines the meaning of each section of bits that are transferred.

Timings − It defines the time at which data is transferred as well as the speed at which it is transferred.

OSI Reference Model

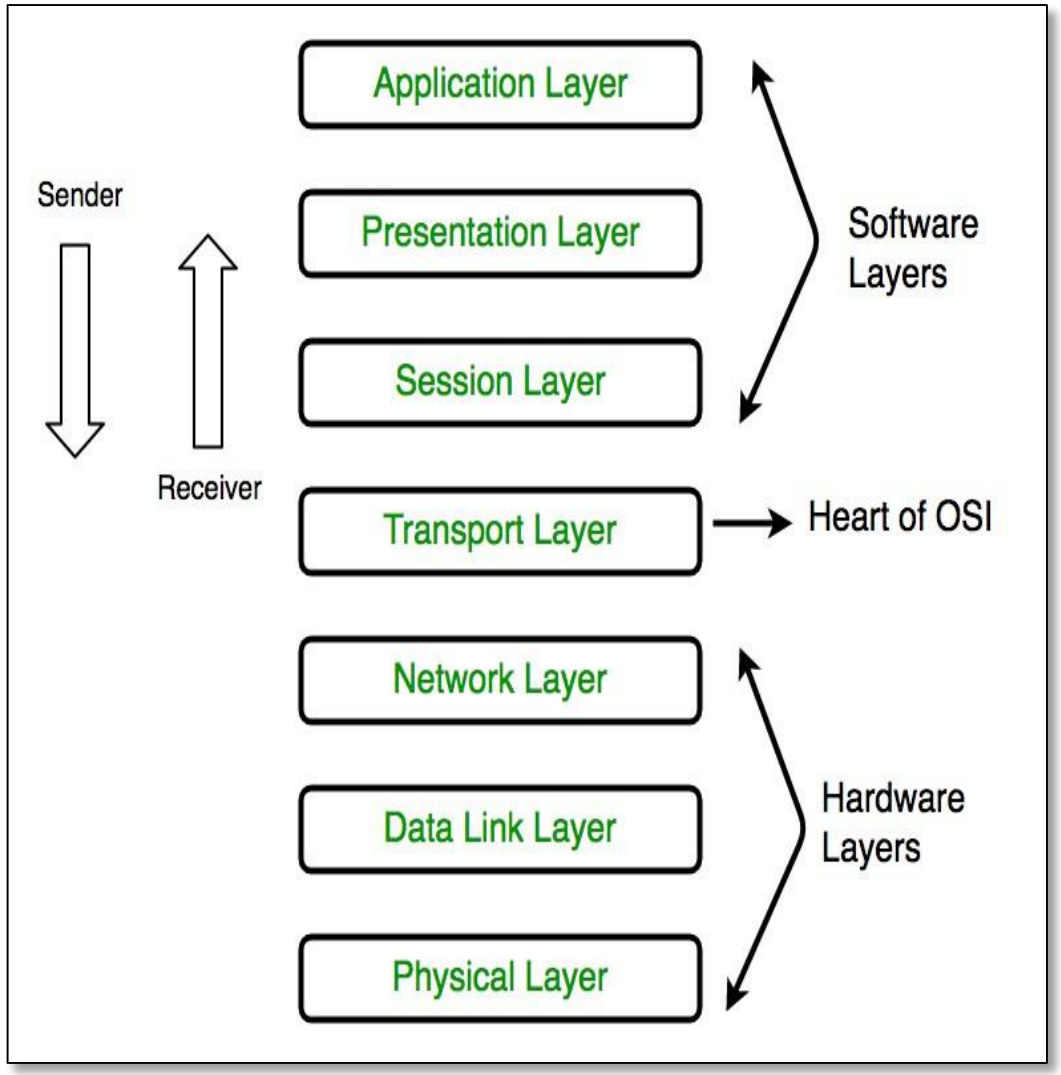
- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- Almost three-fourths of countries in the world are represented in the ISO.
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.
- It was first introduced in the late 1970s.

ISO is the organization; OSI is the model.

OSI Reference Model

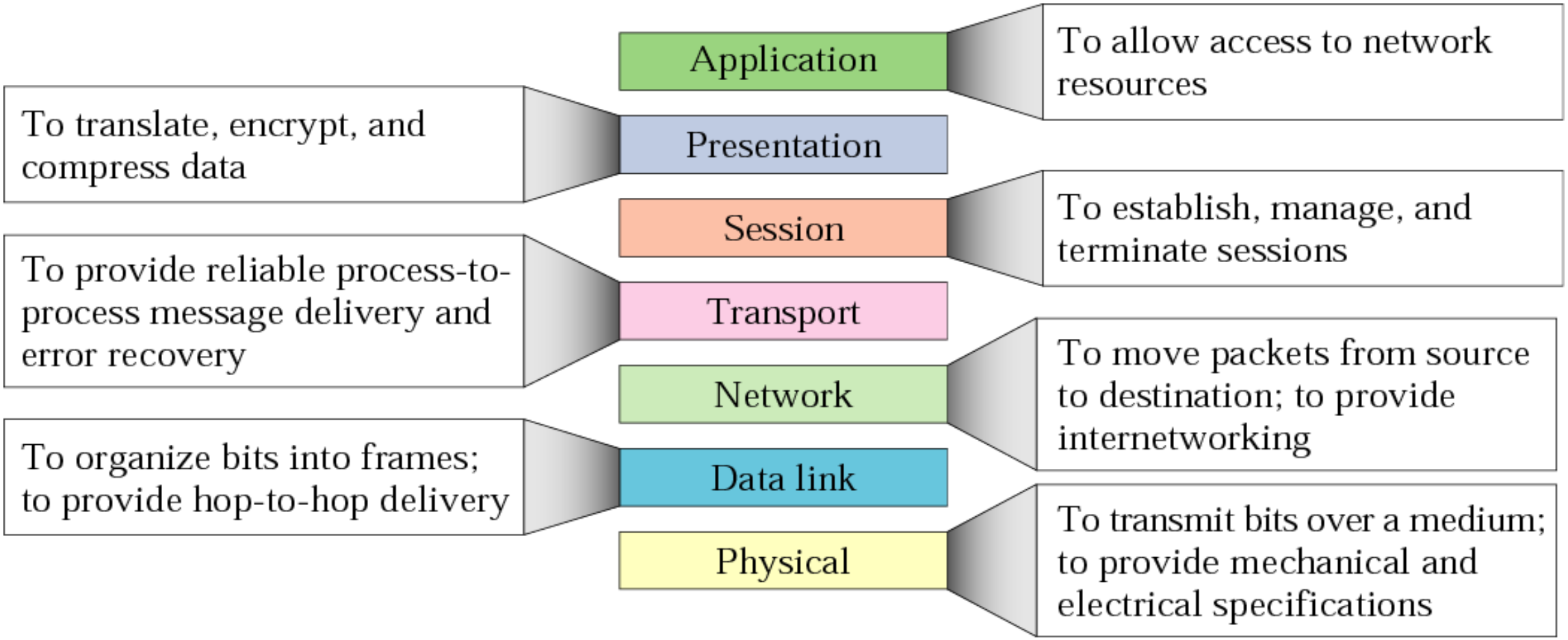
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

OSI Reference Model



- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.3).

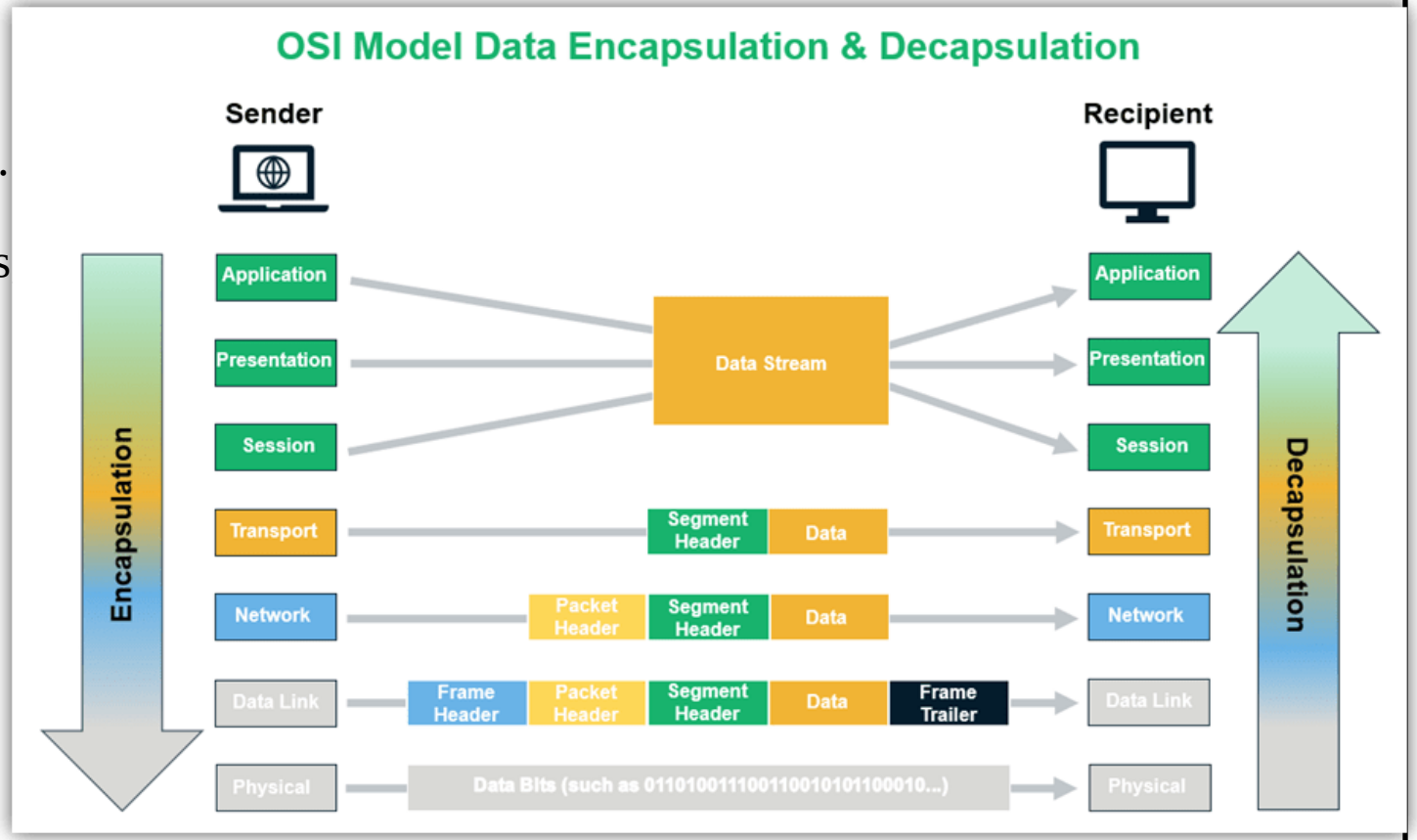
OSI Model


Application
To allow access to network resources
Presentation
To translate, encrypt, and compress data
Session
To establish, manage, and terminate sessions
Transport
To provide reliable process-to-process message delivery and error recovery
Network
To move packets from source to destination; to provide internetworking
Data link
To organize bits into frames; to provide hop-to-hop delivery
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

OSI Model

Each layer contains a Protocol Data Unit (PDU)

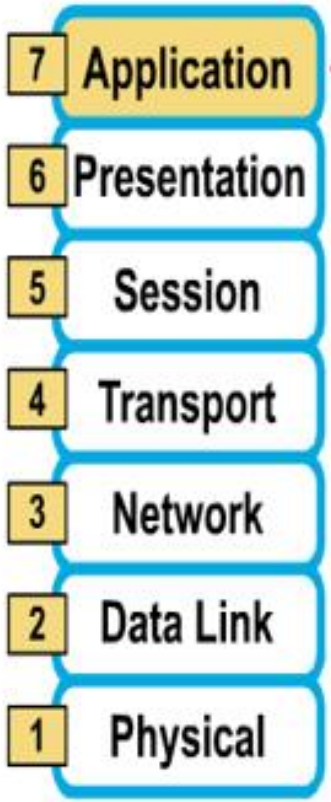
- PDU's are used for peer-to-peer contact between corresponding layers.
- Data is handled by the top three layers then Segmented by the Transport layer.
- The Network layer places it into packets and the Data Link frames the packets for transmission.
- Physical layer converts it to bits and sends it out over the media.
- The receiving computer reverses the process using the information contained in the PDU.



Application Layer

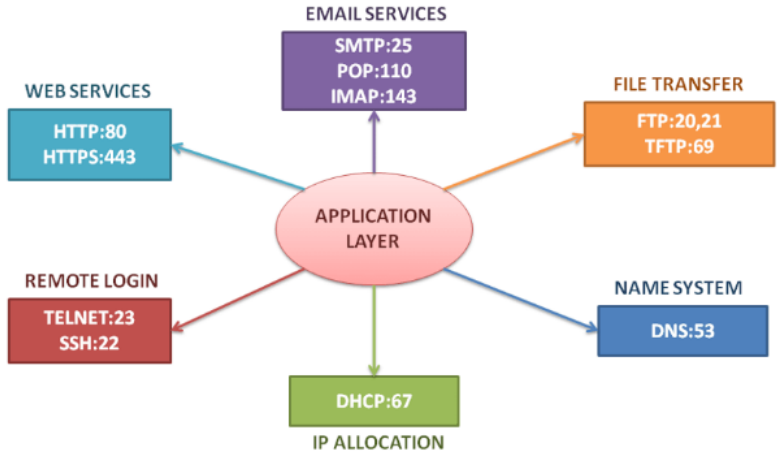
- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which must be transferred over the network.
- This layer also serves as window for the application services to access the network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

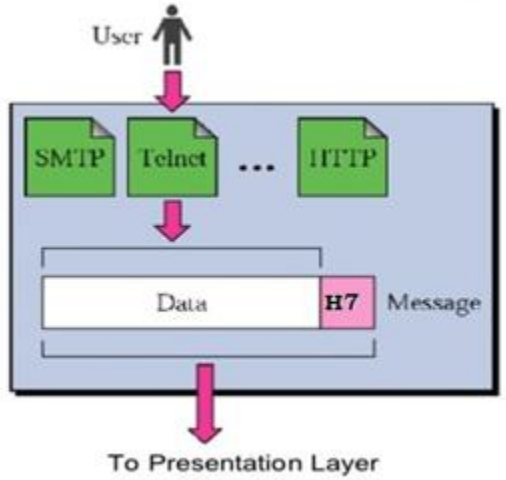
Application Layer

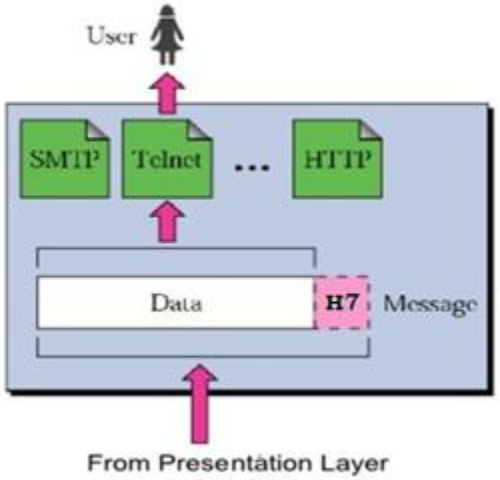


Network Processes to Applications

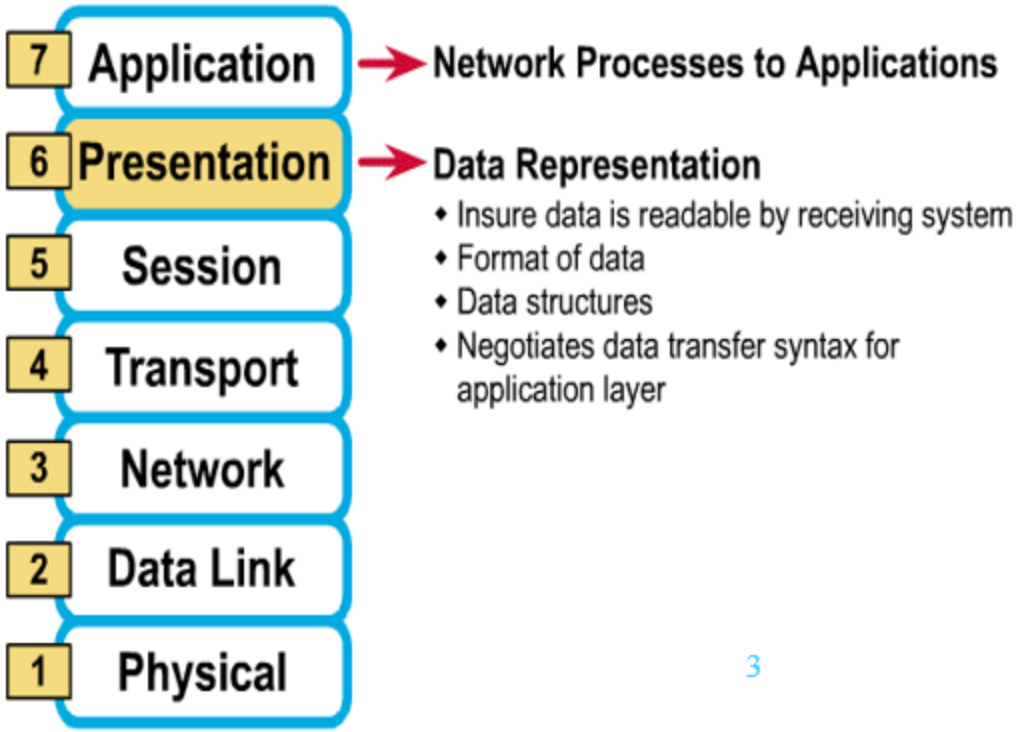
- Provides network services to application processes (such as electronic mail, file transfer, and terminal emulation)







Presentation Layer



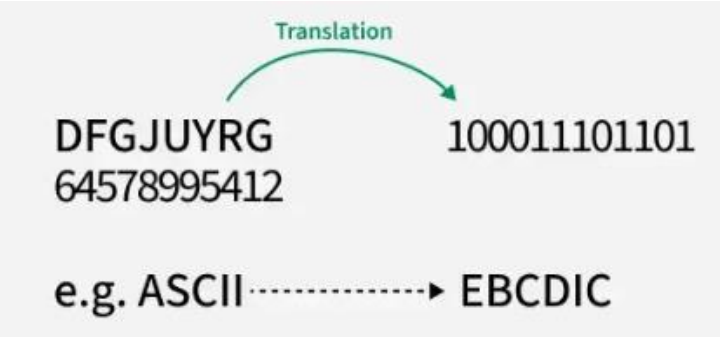
Presentation Layer

- 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 :

1. **Translation :**

- The communication systems usually exchange the information in the form of strings of character , number etc.
- This information need to be changed into bit streams before transmission.
- This layer at the sending end converts the information into a common format and the presentation layer at the receiving end will convert this common format into compatible to the receiver.
- For example, ASCII to EBCDIC.



Presentation Layer

2. Compression:

- The data compression technique is used for reducing the number of bits required to send an information.
- Number of bits are reduced hence the speed of transmission is increased
- May be lossy or lossless compression.
- Real time video/audio transmission

3. Encryption/Decryption:

- For ensuring the security and privacy of the information that is being communicated, a process called data encryption.
- Encryption is carried out at the sending end. In this the sender transforms the original information to another form and sends the transformed information.
- Decryption is carried out in which the received information is transformed back to its original form
- SSL – Secure Socket Protocol

Presentation Layer

Translation

DFGJUYRG
64578995412

eg. ASCII ⟶ EBCDIC

Data Compression

100011101101

1. Lossy
2. Lossless

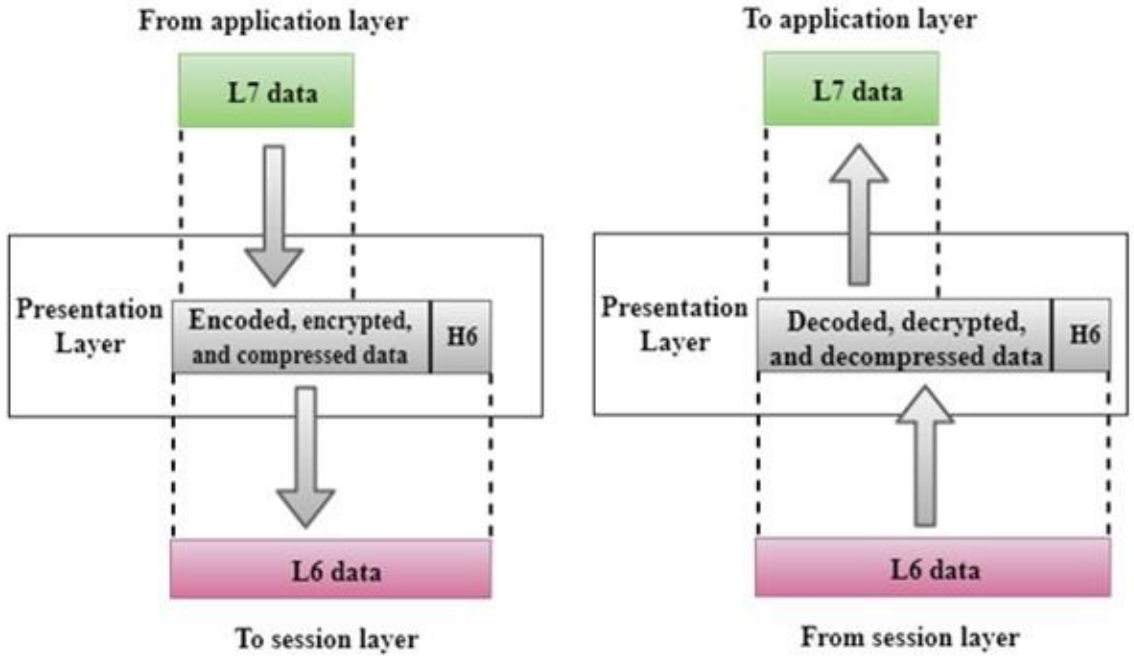
Encryption/Decryption

10101101

10011011

SSL

Secure Sockets Layer

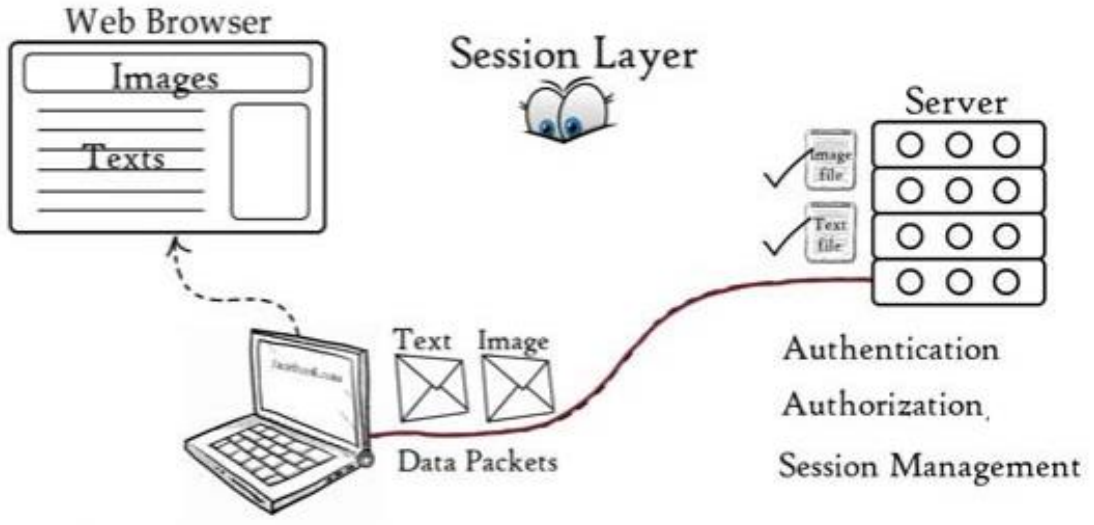


Session Layer

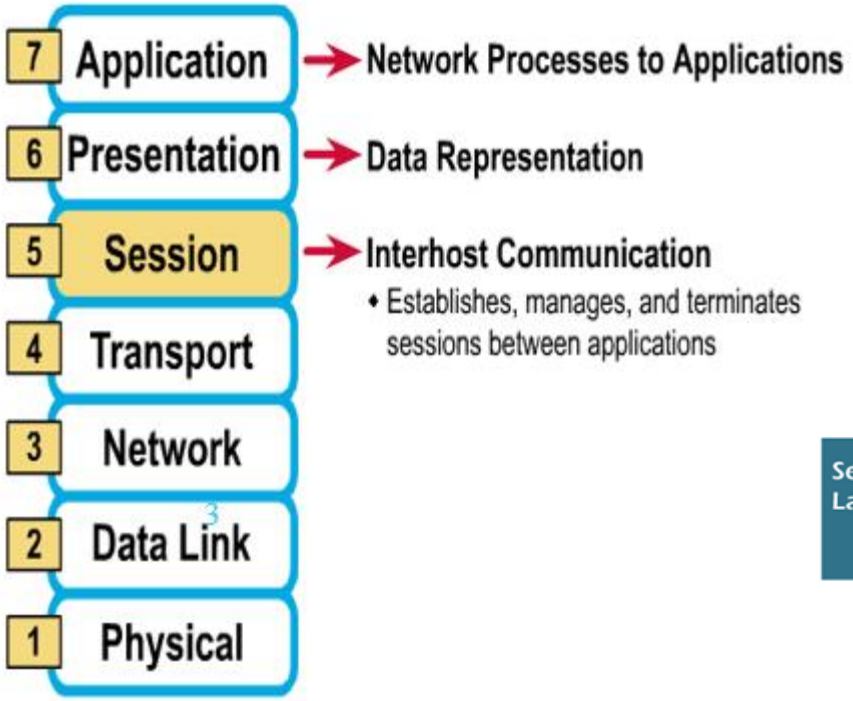
This layer is responsible for establishment of connection, maintenance of sessions, authentication prematurely, ensures security.
The functions of the session layer are :

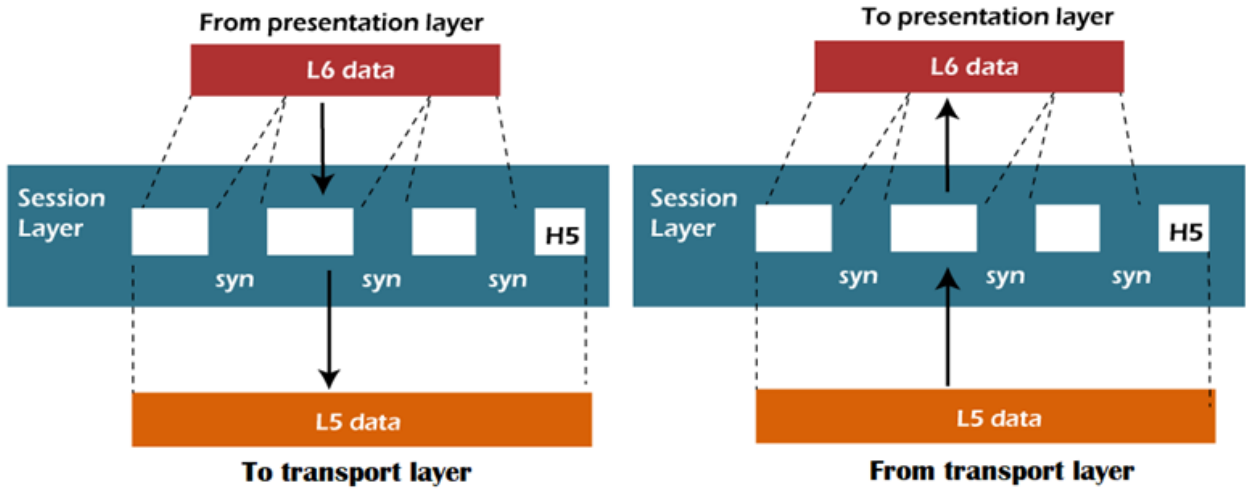
1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point 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.
3. **Dialog Controller :** The session layer determines which device will communicate first and the amount of data that will be sent.

Session Layer



Session Layer





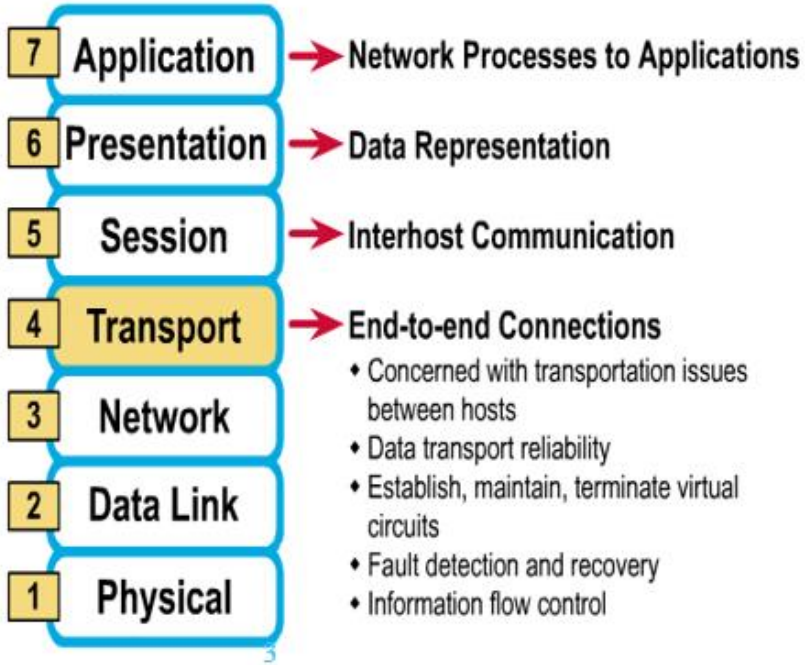
A web Browser performs all these activities for you.

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 also provides the acknowledgement of the successful data transmission and re-transmits the data if error is found.

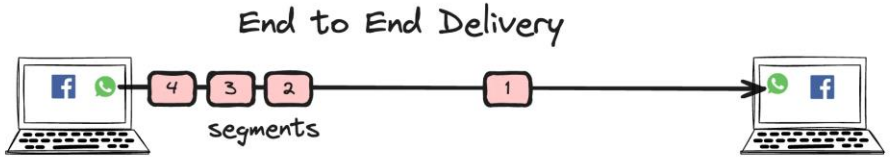
Functions of Transport Layer

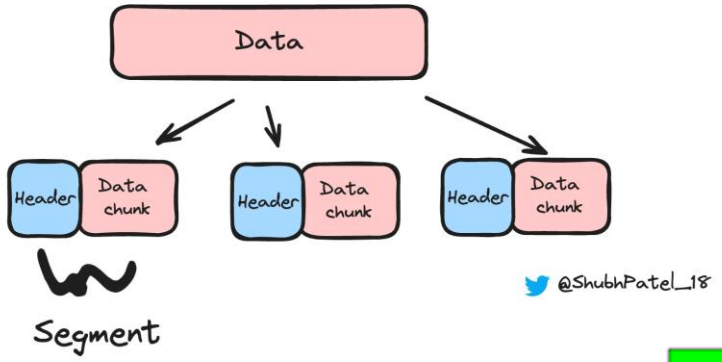
- Segmentation
- Flow Control
- Error Control

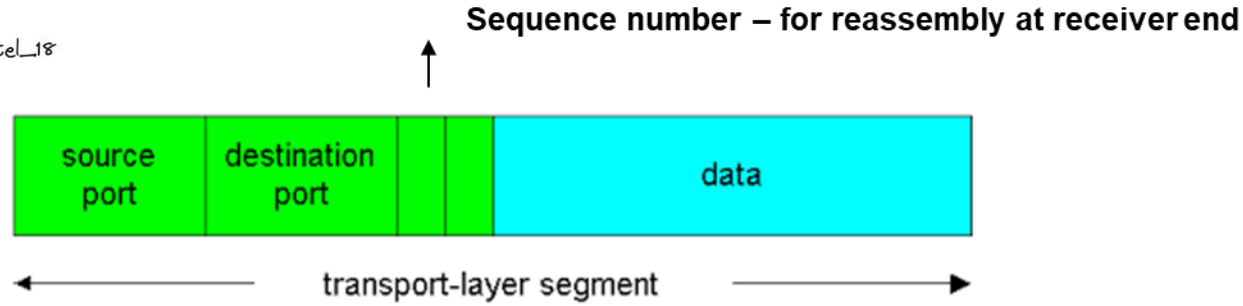


Transport Layer

Segmentation

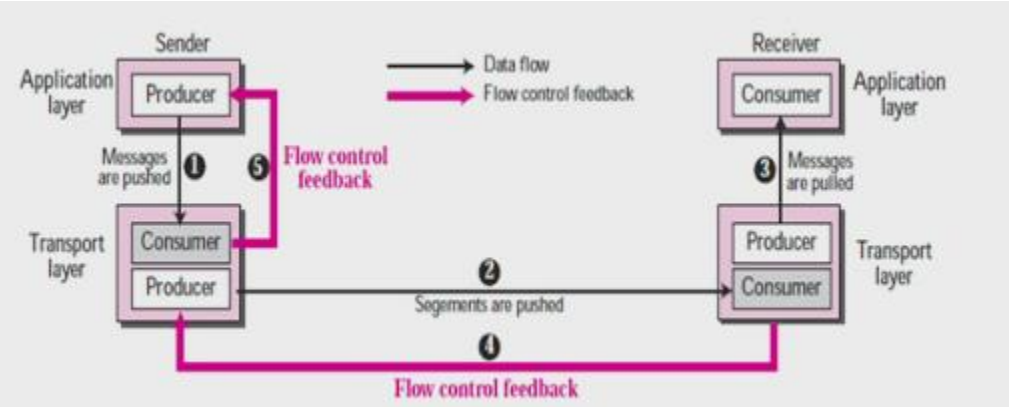






Transport Layer

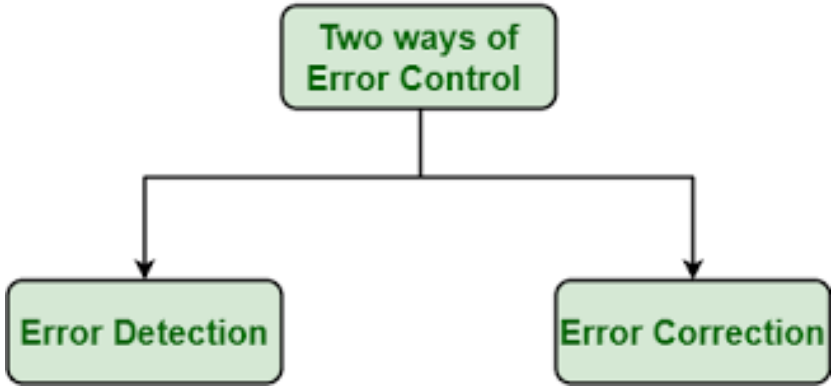
Flow Control



Feedback Based flow control is done. That is speed matching between receiver and sender

Transport Layer

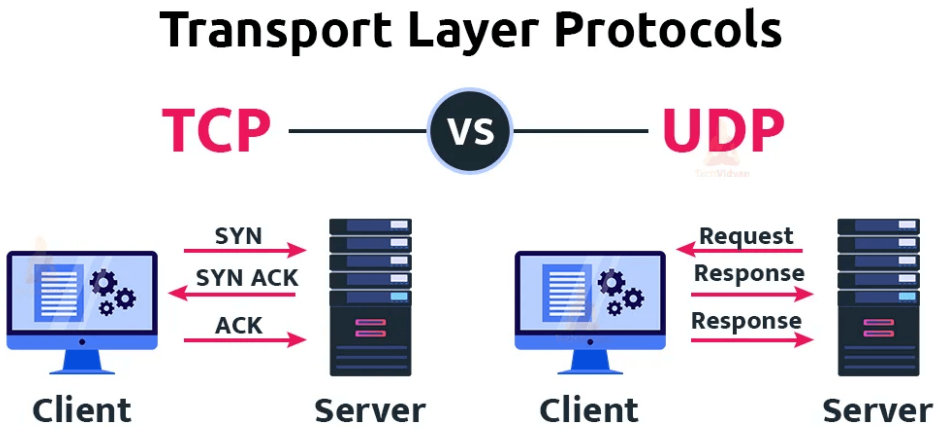
Error Control



- Missing Data
- Checksum
- Parity check
- Cyclic Redundancy Check (CRC)

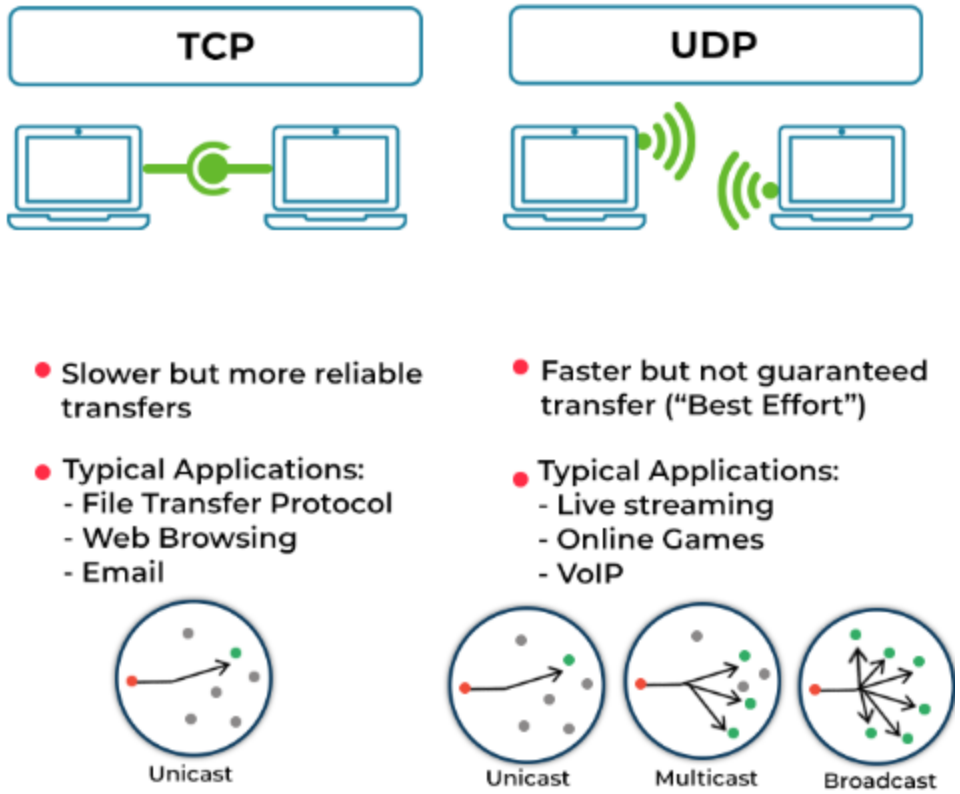
- Forward Error Correction
- Automatic Repeat Request

Transport Layer



Connection Oriented

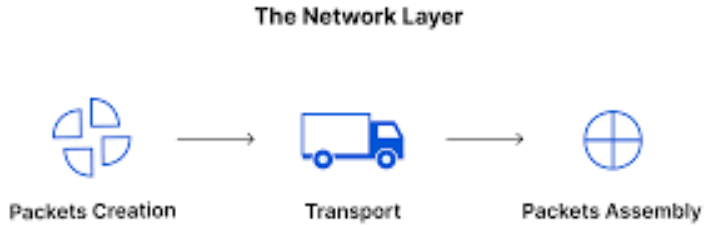
Connectionless



Network Layer

7	Application	Network Processes to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-end Connections
3	Network	Address and Best Path
2	Data Link	
1	Physical	

- Provides connectivity and path selection between two end systems
- Domain of routing



Network Layer

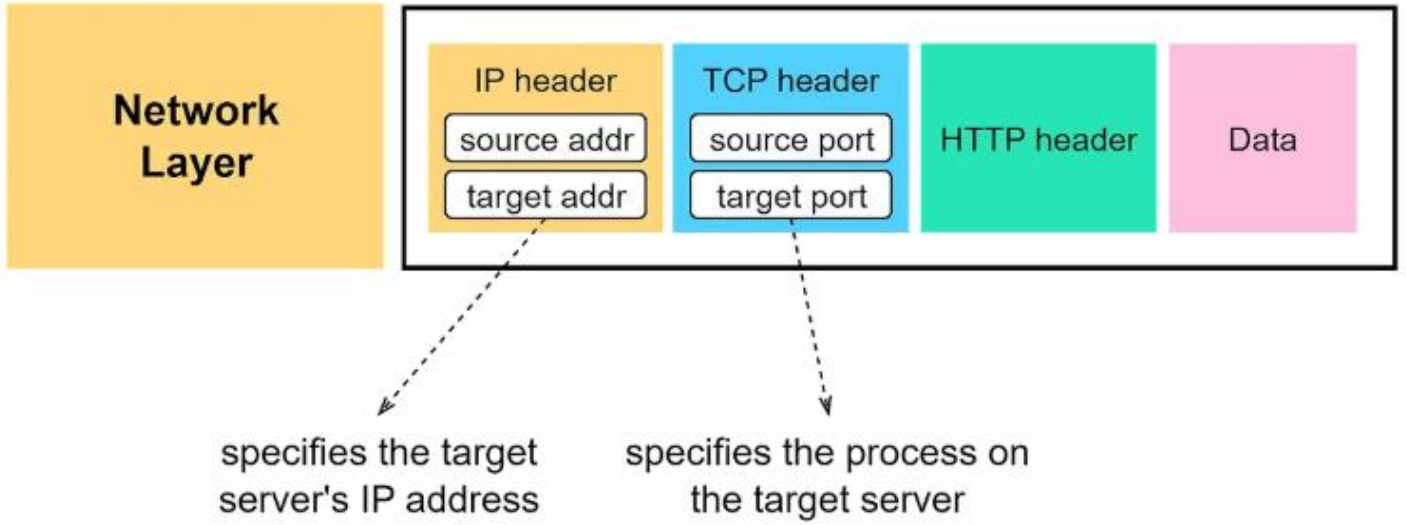
- Network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e., selection of shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** 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.

Network Layer

Logical Addressing

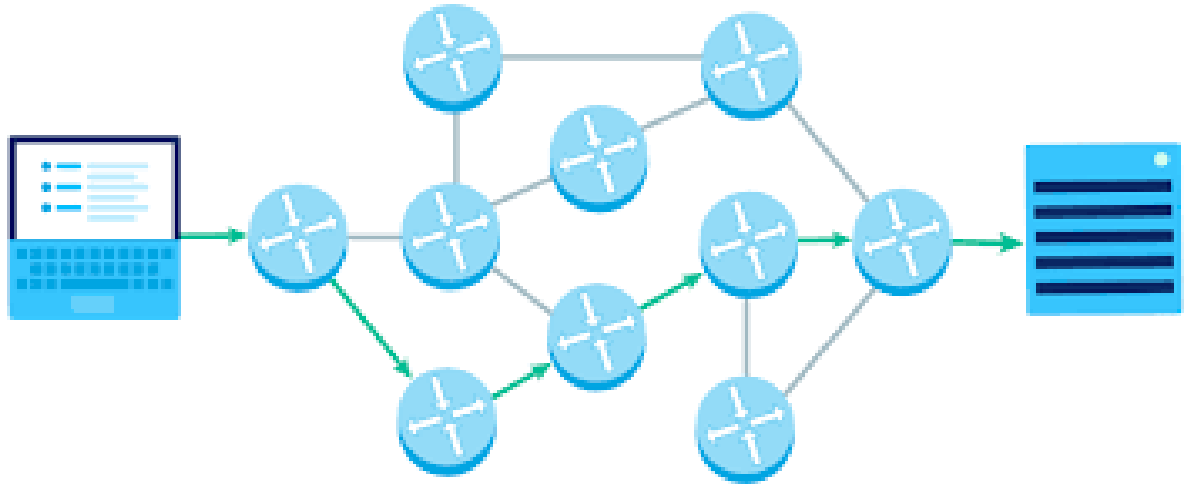


IPV4/IPv6 Addresses are assigned to the segments.
IPv4 + Mask

Network Layer

Routing / Path Determination

OSPF – Open shortest Path First
BGP - Border Gateway Protocol
IS-IS – Intermittent System - IS

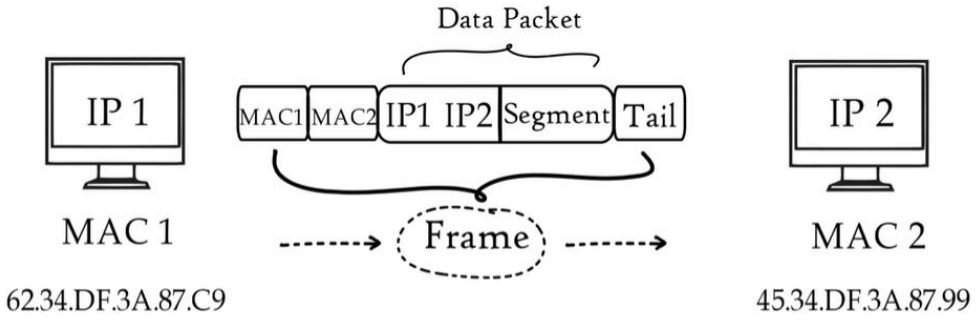


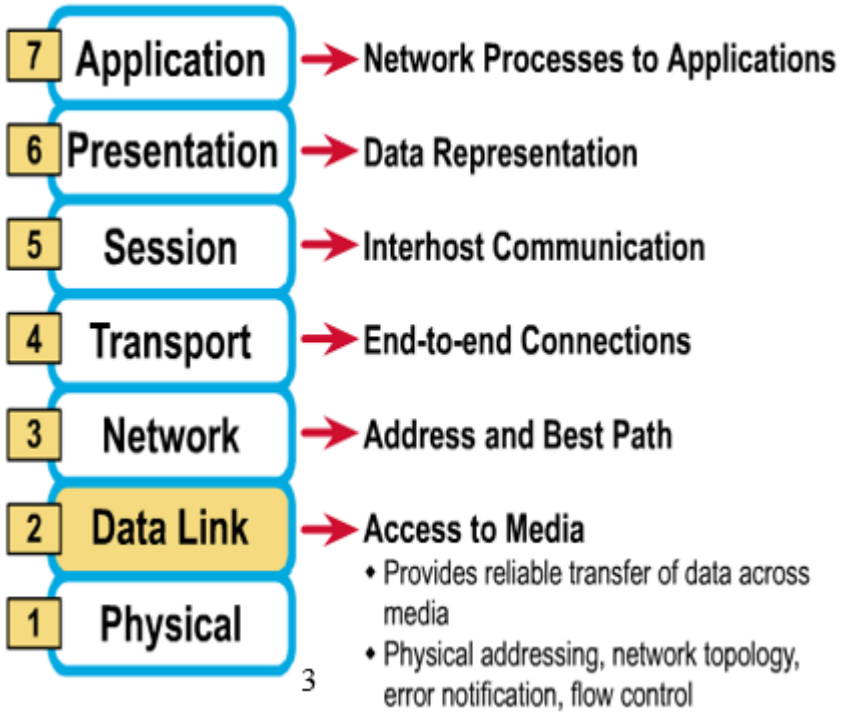
Data Link Layer

- 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)

Data Link Layer

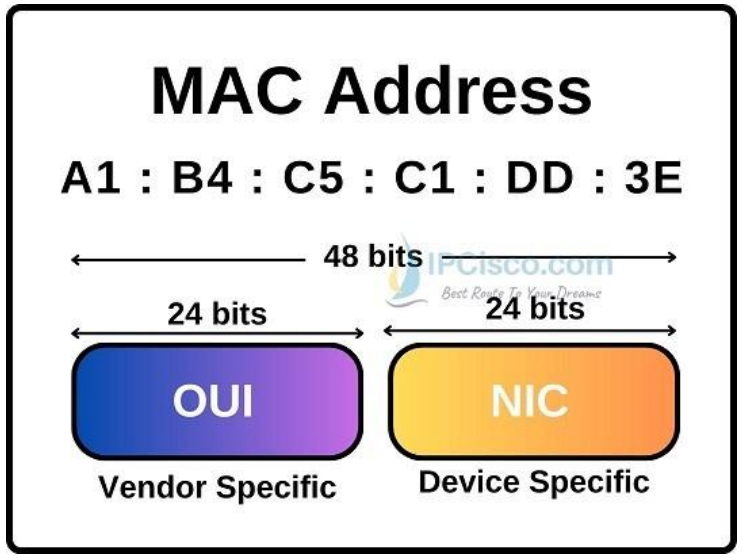
- Network layer deals with logical address
- Data link layer deals with Physical Address

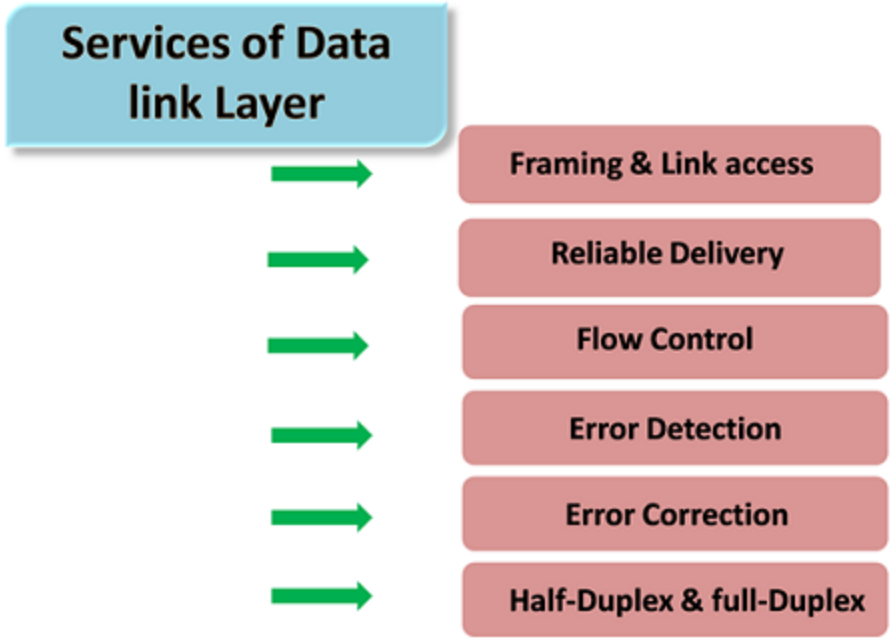




Data Link Layer

- Network layer deals with logical address
- Data link layer deals with Physical Address





Organizationally Unique Identifier (OUI)

Network Interface Card (NIC)

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.

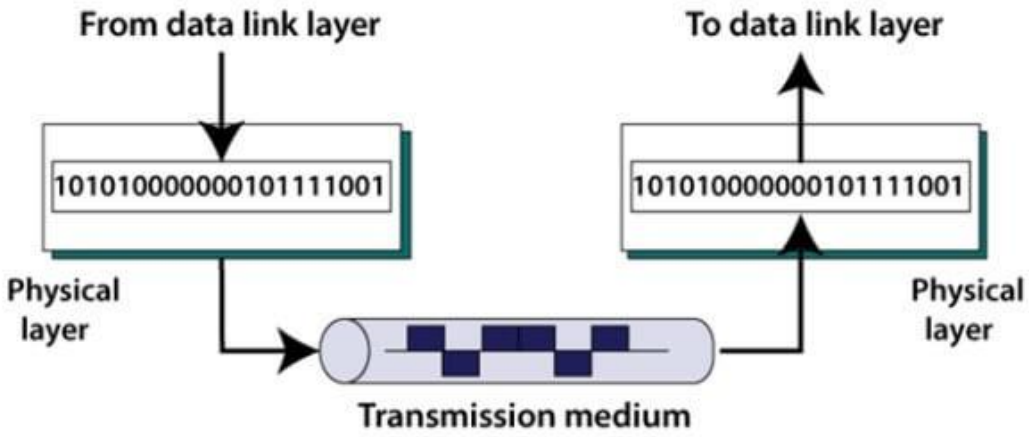
The functions of the physical layer are :

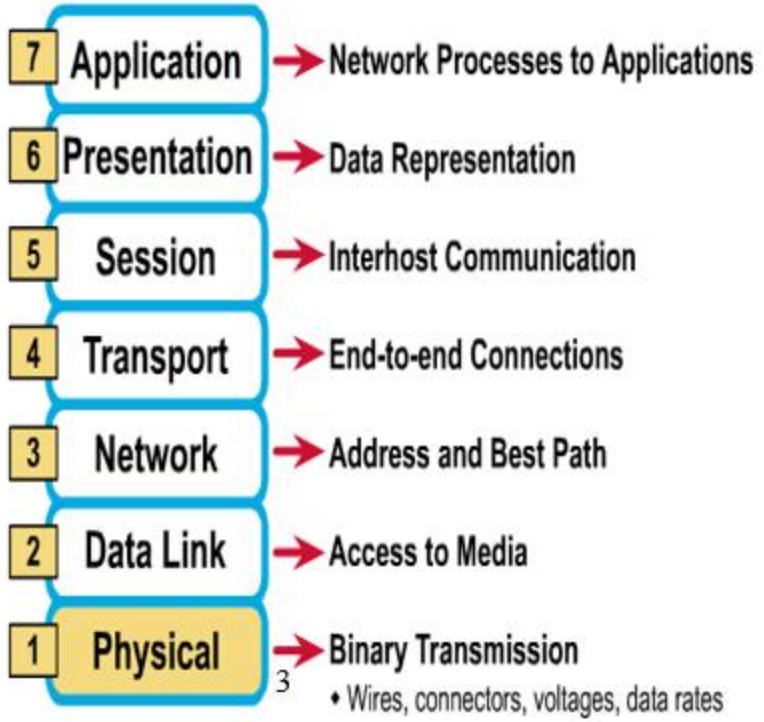
- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- **Bit rate control**: The Physical layer also defines the transmission rate are the number of bits sent per second.
- **Physical topologies**: Physical layer specifies the way in which the different, devices/nodes are arranged in a network are bus, star or mesh topology.
- **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.

Devices

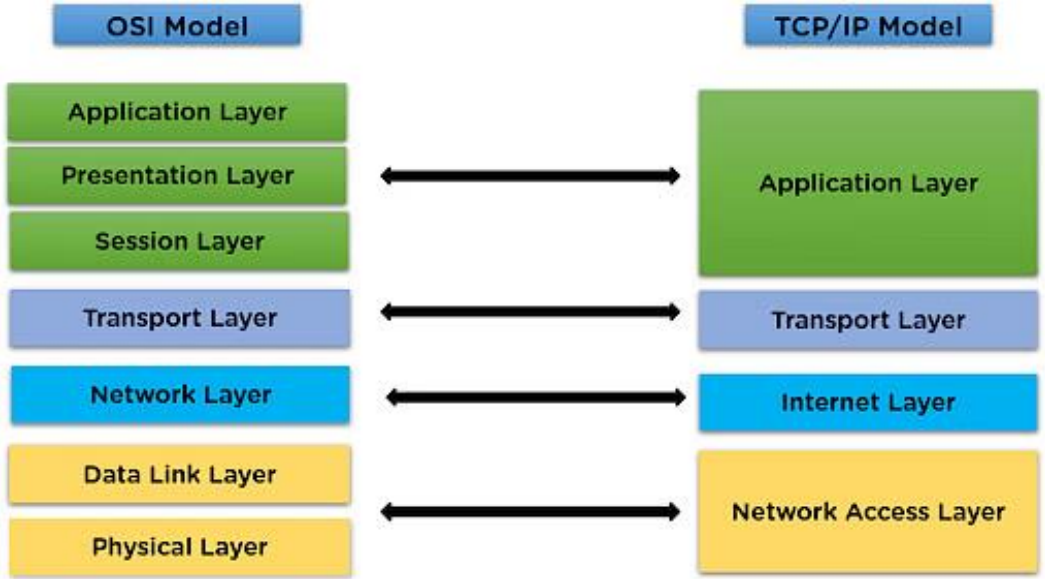
- Hub, Repeater, Modem, Cables are Physical Layer devices.

Physical Layer



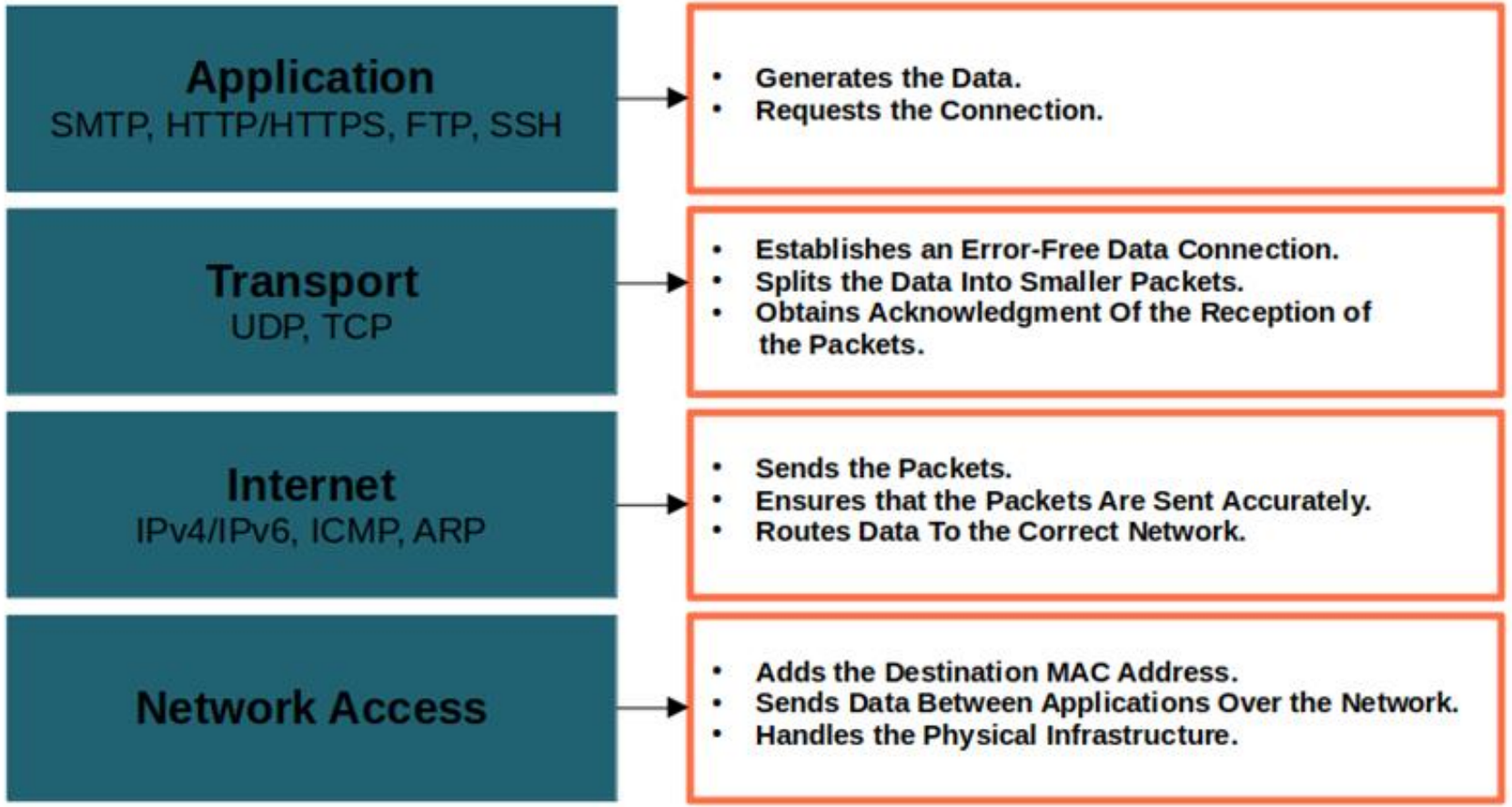


TCP/IP Protocol Suite

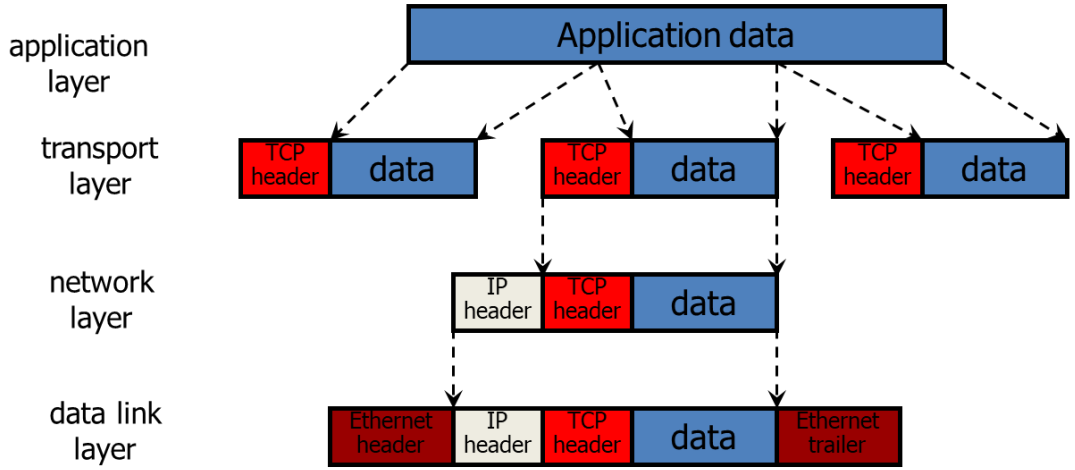


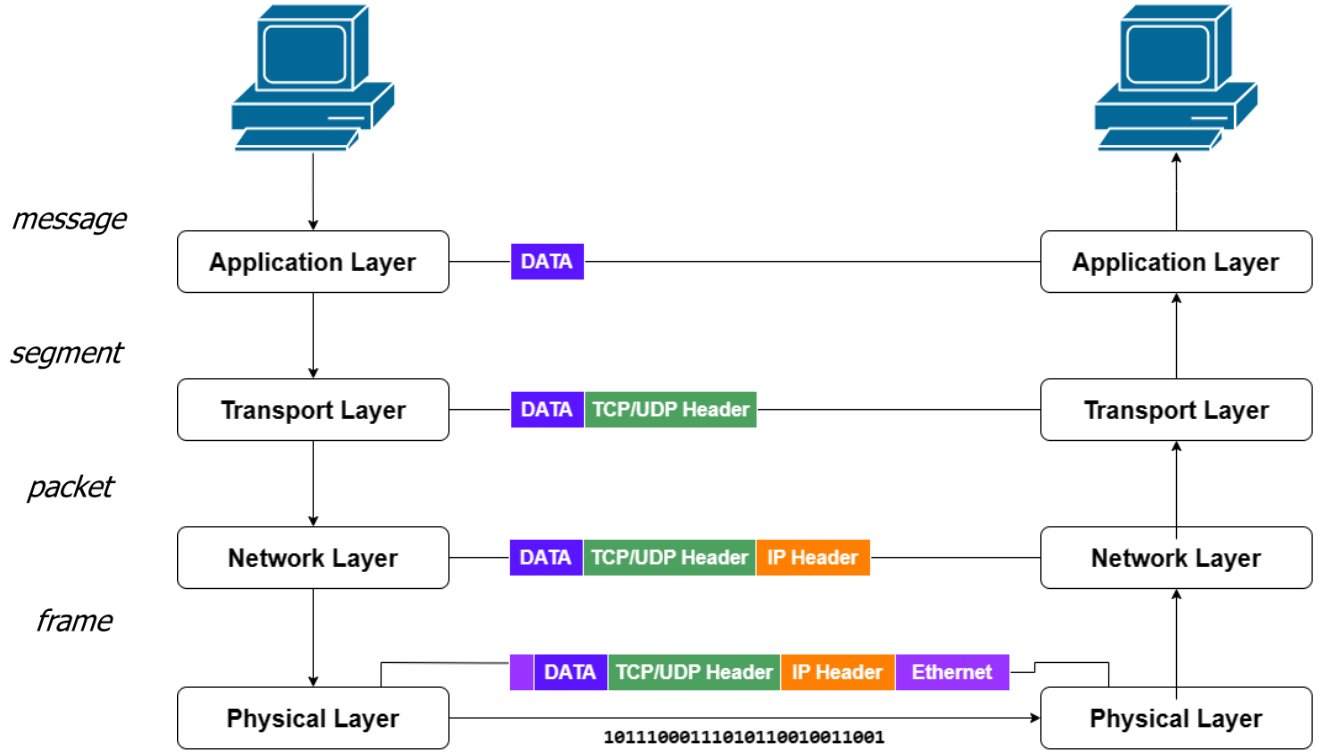
TCP/IP Protocol Suite

The Four Layers Of the TCP/IP Model and Their Functions

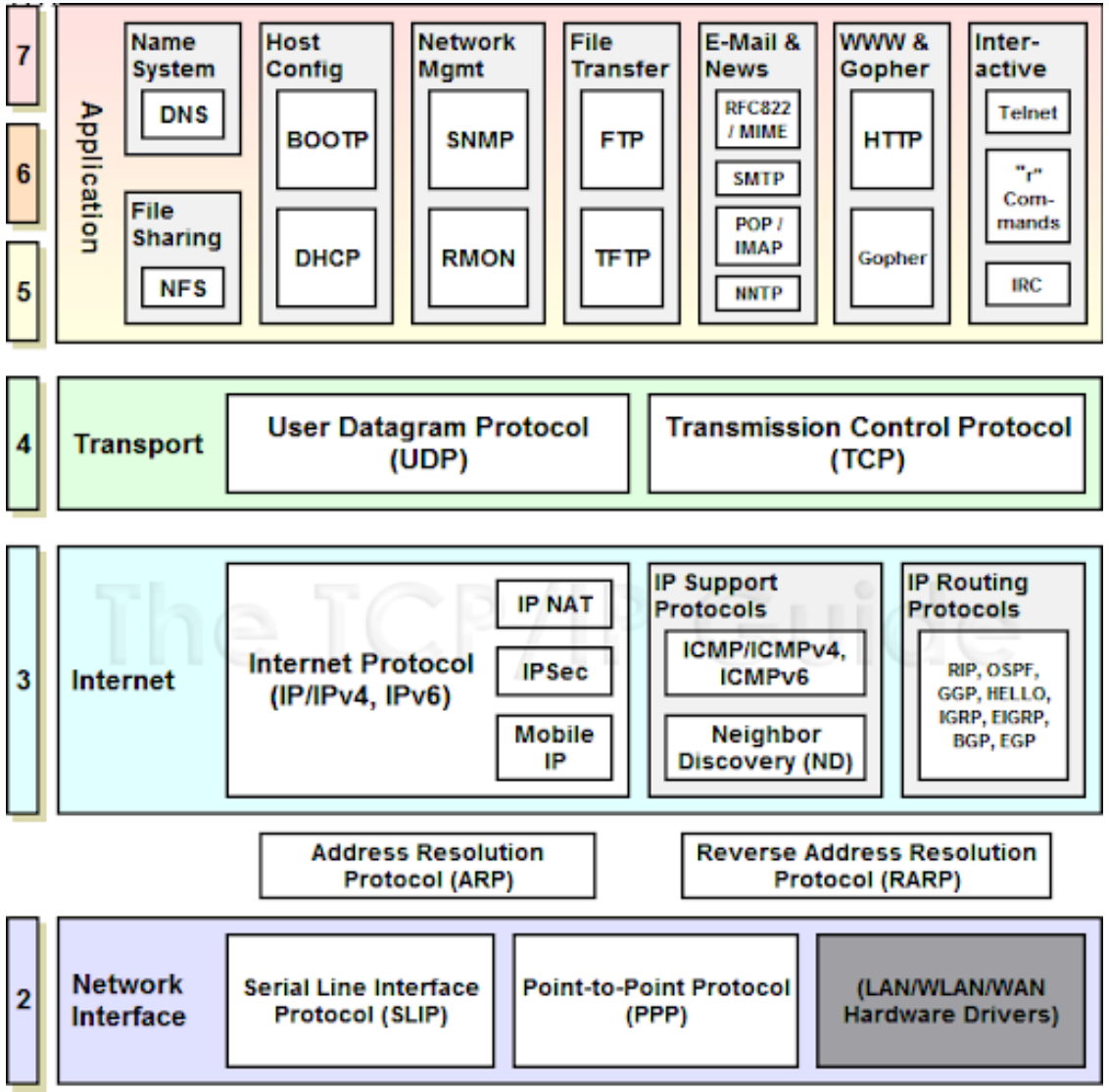


TCP/IP Protocol Suite





TCP/IP Protocol Suite



OSI vs TCP/IP

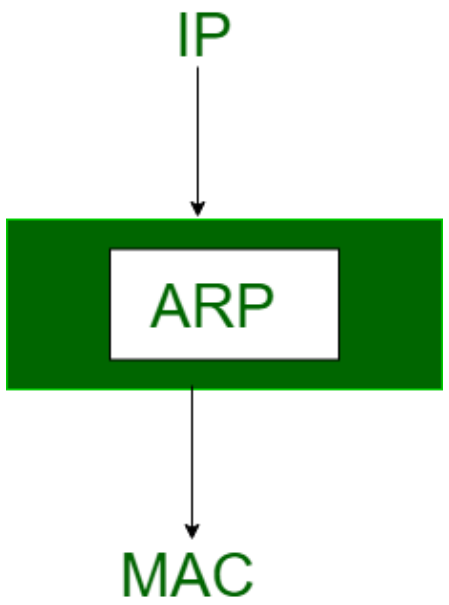
TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical mode
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard
Protocols are not strictly defined	Stricter boundaries for the protocols

OSI = TCP/IP

Similarities between the TCP/IP and OSI models

- Both models are based on layered structuring.
- In both models, data are mainly used to convert raw data into packets and help them reach their destination node.
- In both models, protocols are defined in a layer-wise manner.
- The layers in the models are compared with each other.
- The physical layer and the data link layer of the OSI model correspond to the link layer of the TCP/IP model.
- The session layer, the presentation layer and the application layer of the OSI model together form the application layer of the TCP/IP model.
- The network layers and the transport layers are the same in both models.

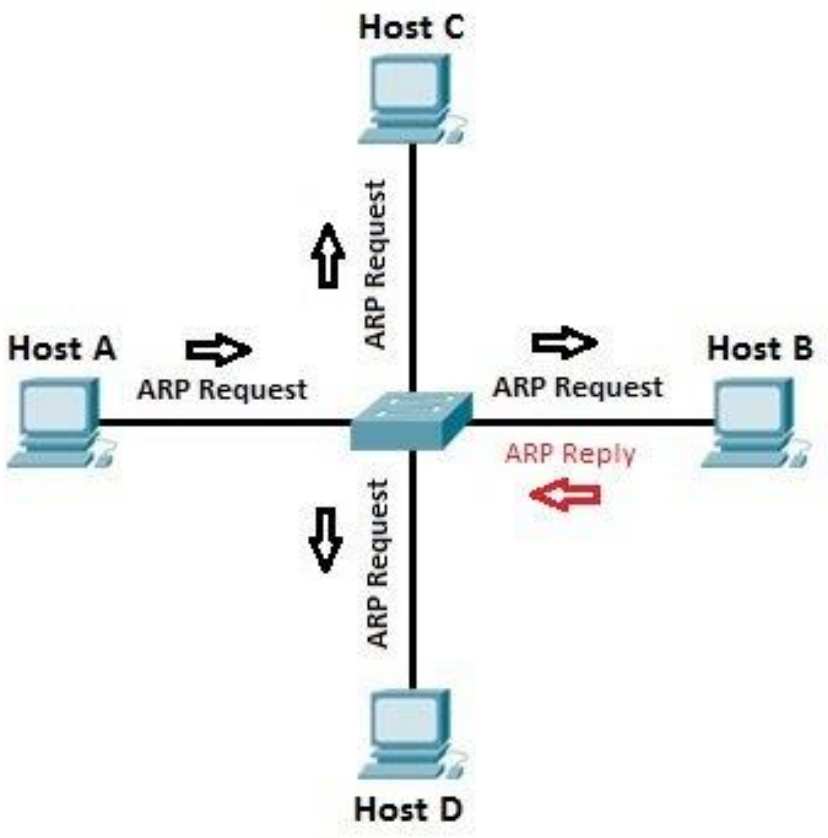
TCP / IP Protocol: ARP

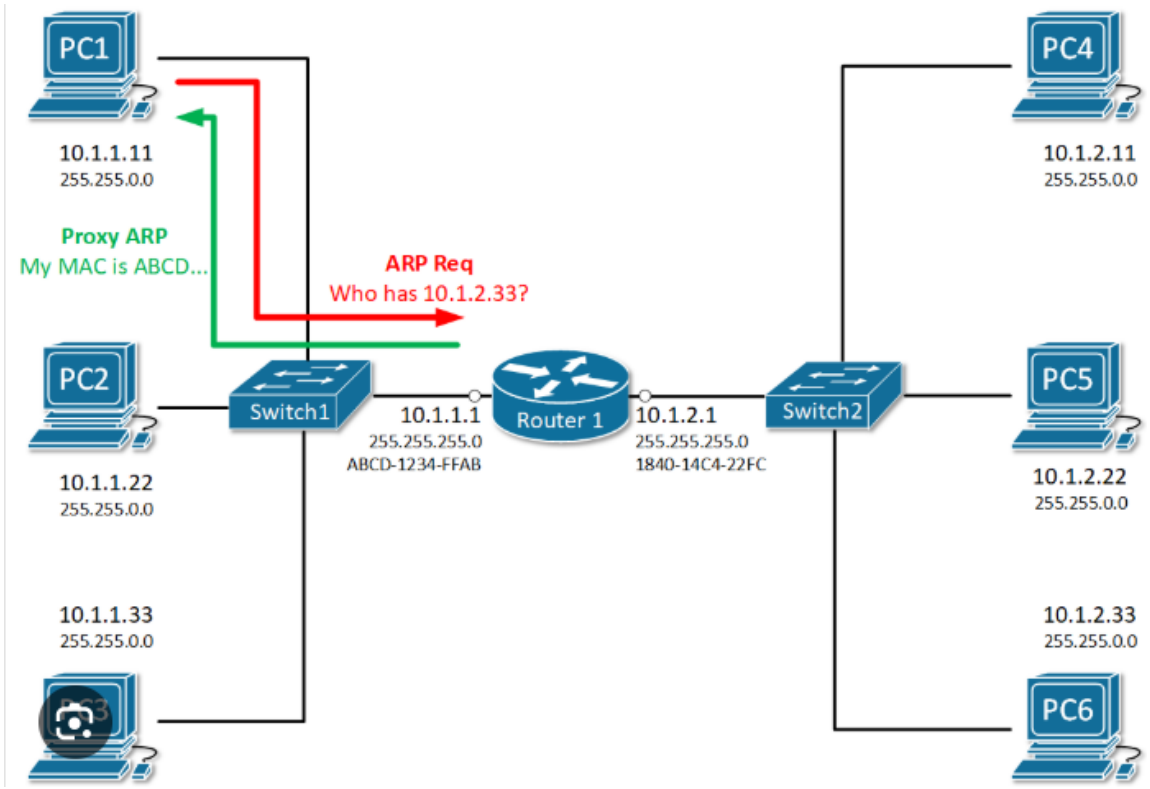


ARP (Address Resolution Protocol):-

- Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however, the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of the OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses.
- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address.
- This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

TCP / IP Protocol: ARP





TCP / IP Protocol: ARP

Steps to be followed

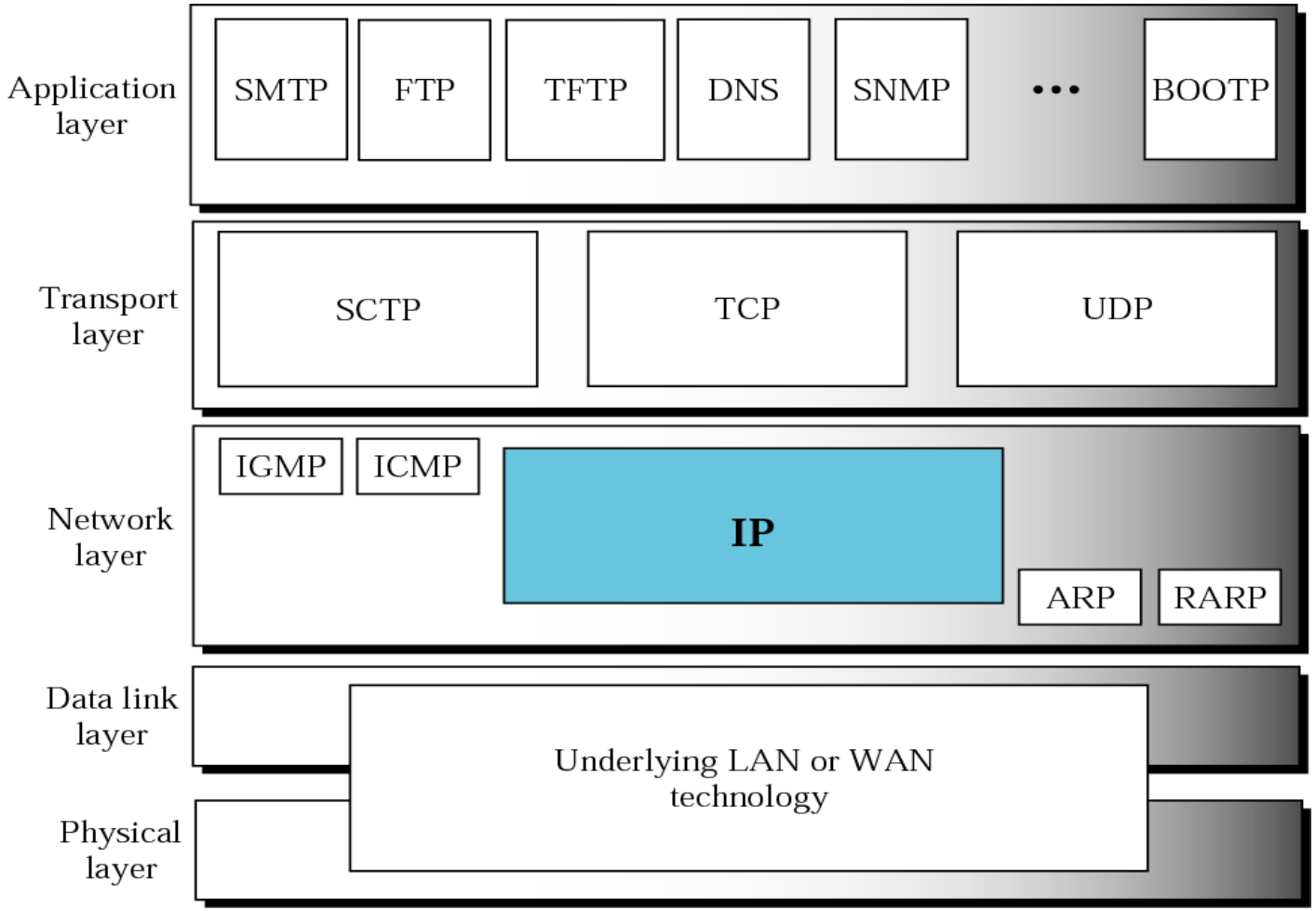
1. The sender knows the IP address of the target. We will see how the sender obtains this shortly.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address.
3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine.
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

TCP / IP Protocol

IP (Internet Protocol):-

- IP is the host to host delivery protocol which belongs to the network layer & is designed for the Internet.
- The Internet Protocol (IP) is the **connectionless** transmission mechanism used by the TCP/IP protocol.
- IP is an unreliable and connectionless datagram—a best-effort delivery service. It ensures no guarantee of successfully transmission of data.
- The term best-effort means that IP provides no error checking or tracking.
- IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
- If reliability is important, IP must be paired with a reliable protocol such as TCP
- IP supports two formats: IPv4 (32-bit addresses) and IPv6 (128-bit addresses), with IPv6 offering virtually unlimited addressing capacity.

TCP / IP Protocol



Position of IP in TCP/IP Protocol Suite

- The network layer in the TCP/IP suite as well as internet layer are: ARP, RARP, IP, ICMP & IGMP.
- Out of these protocols **IP** is the most important protocol it is responsible for host to host delivery of datagrams from a source to destination.
- IP takes help from **ARP** in order to find the **MAC (physical)** address of the next hop.
- IP uses the services of **ICMP** during the delivery of the datagram packets to handle unusual situations such as presence of an error.

UDP(User Datagram Protocol):

- Above Figure shows the relationship of the **User Datagram Protocol (UDP) to the other** protocols and layers of the TCP/IP protocol suite.
- UDP is located between the application layer and the IP layer, and serves as the intermediary between the application programs and the network operations.
- UDP is a **connectionless, unreliable transport protocol.**
- UDP provides a connectionless packet service that offers unreliable 'best effort' delivery. This means that arrival of packets is not guaranteed, nor is the correct sequencing of delivered packets.

TCP / IP Protocol

UDP(User Datagram Protocol):

- To create a process-to-process communication, UDP uses port numbers to accomplish this.
- To provide control mechanisms at the transport level, UDP does not provide flow control & acknowledgment for received packets.
- **It does not add anything** to the services of IP except for providing process-to-process communication.

Advantages of UDP

- UDP is a very simple protocol using a minimum of overhead.
- If a process wants to send a small message and does not care much about reliability, it can use UDP.
- Sending a small message using UDP takes much less interaction between the sender and receiver than using TCP.

TCP / IP Protocol

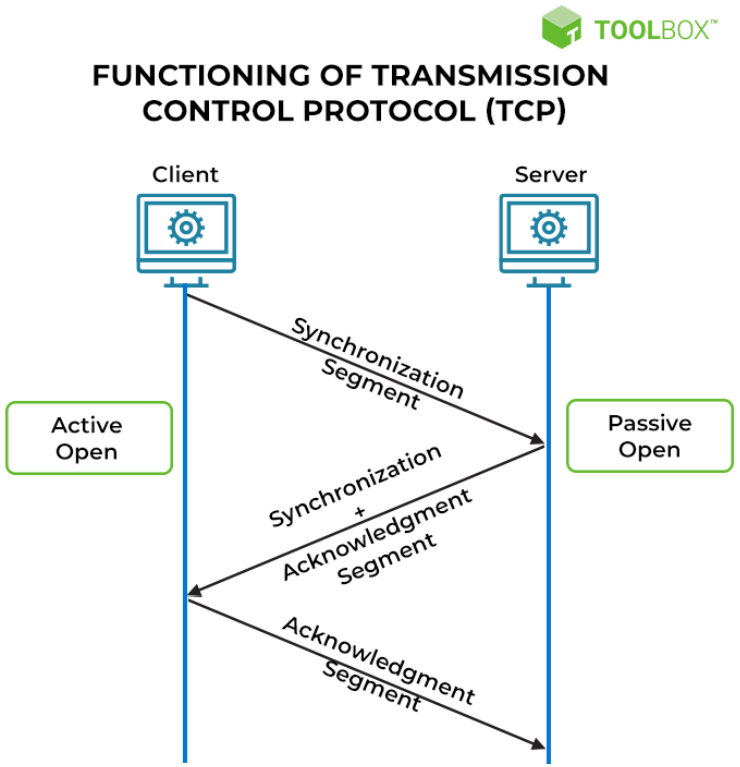
Transmission Control Protocol (TCP)

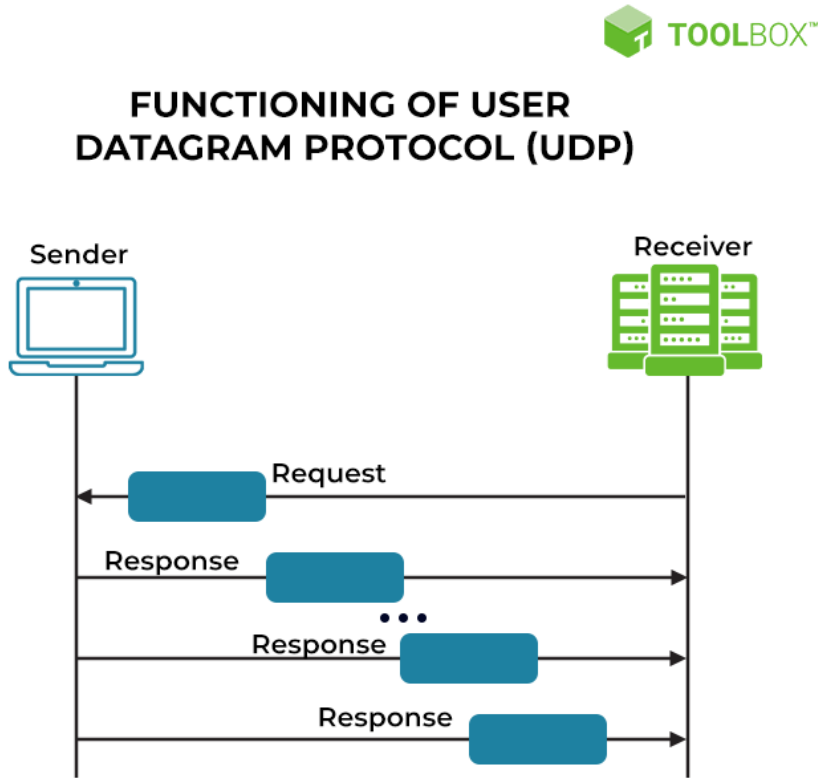
- TCP is a **reliable** connection oriented protocol. i.e. a connection is established between the sender & receiver before the data can be transmitted.
- TCP divides the data it receives from the upper layer into segments & tags a sequence number to each segment which is used at the receiving end for reordering of data.
- TCP serves as the intermediary between application programs (application layer) & the network operations.(Network layer)

TCP Services

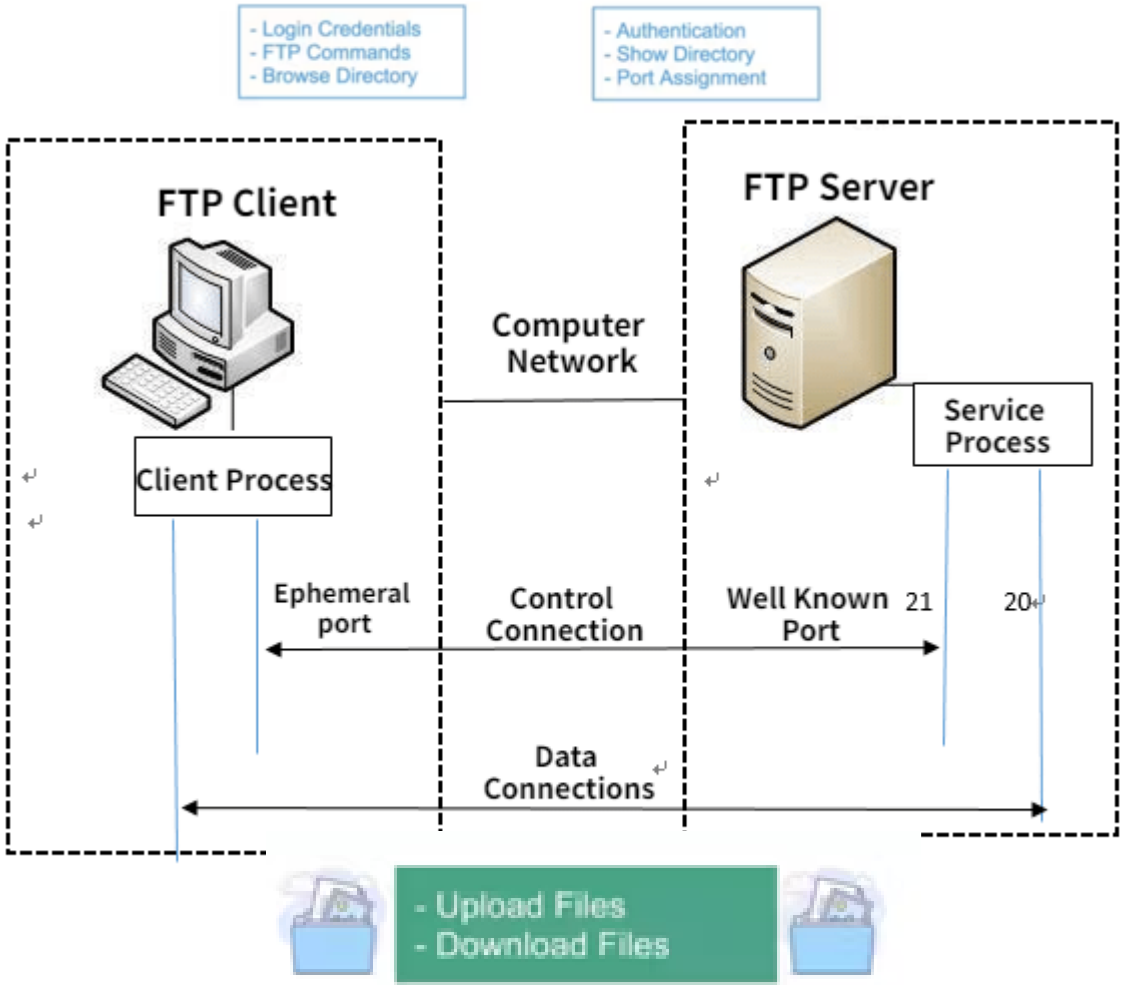
- Process-to-Process Communication
- Stream Delivery Service
- Full-Duplex Communication
- Multiplexing and Demultiplexing
- Connection-Oriented Service
- Reliable Service

TCP / IP Protocol





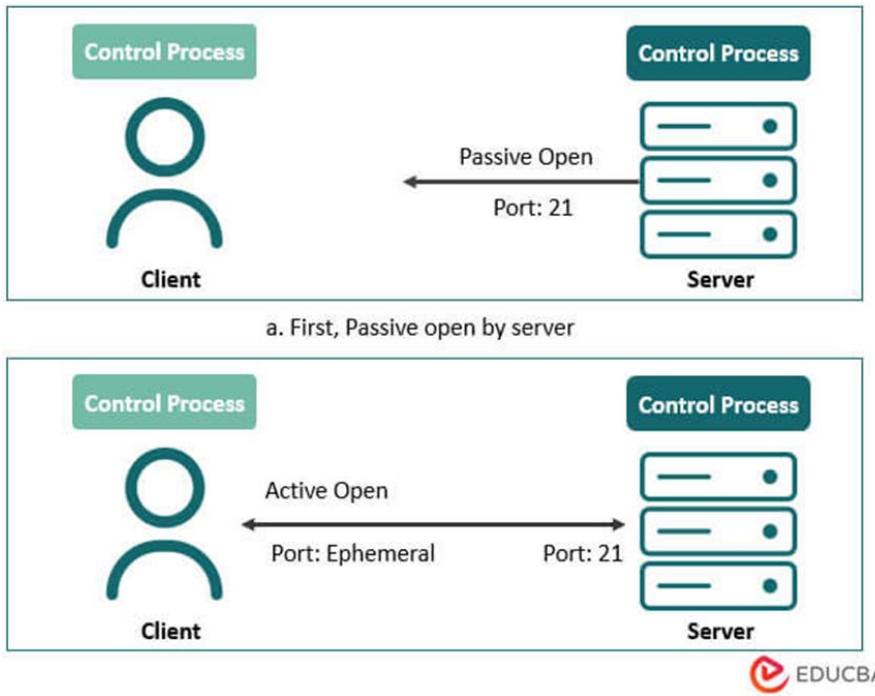
FTP (File Transfer Protocol)



Working Principle of FTP

- FTP differs from other client-server applications in that it establishes two connections between the hosts.
- One connection is used for data transfer, the other for control information (commands and responses).
- Separation of commands and data transfer makes FTP more efficient.
- FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

Architecture of FTP



- The user types commands and expects to receive responses without significant delay.
- shows the initial connection between the server and the client.

- When a user starts an FTP session, the control connection opens.
- While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

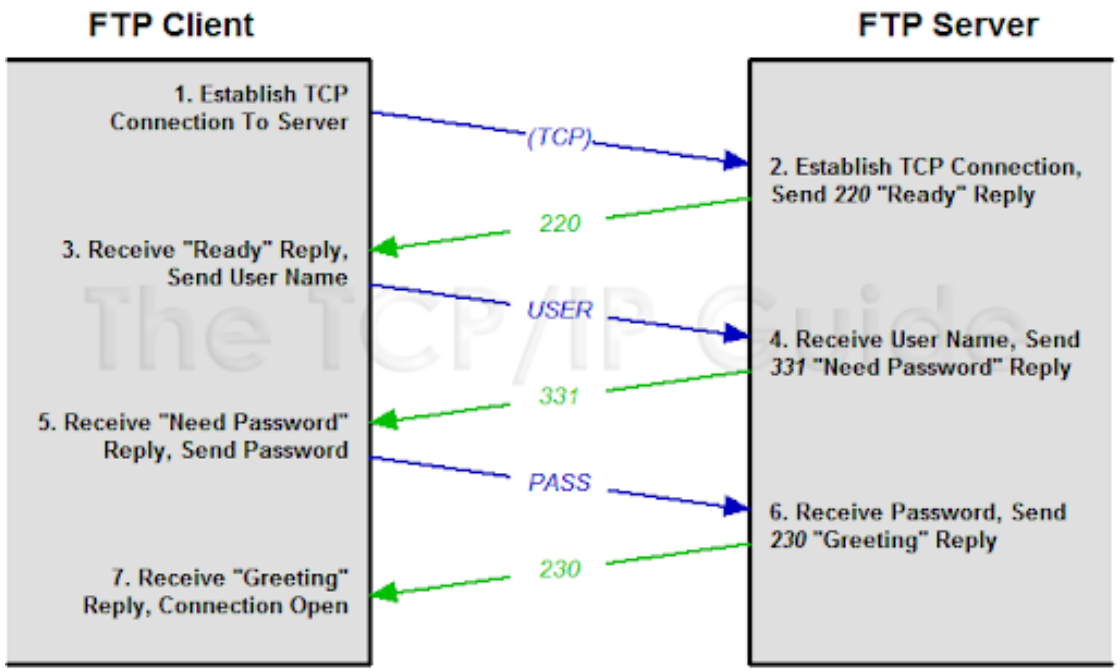
1. Control Connection

- The control connection is created in the same way as other application programs described so far.

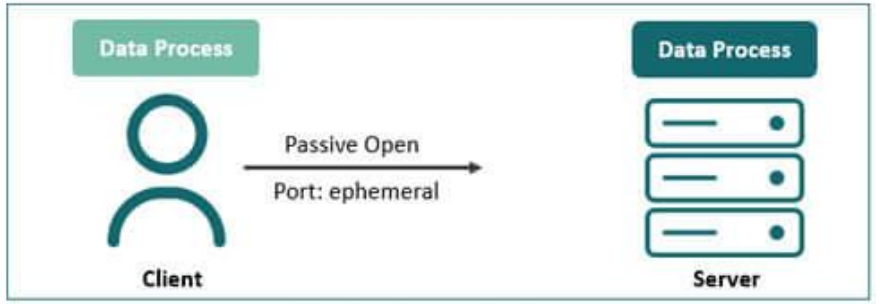
There are two steps:

- The server issues a passive open on the well-known port 21 and waits for a client.
- The client uses an ephemeral port and issues an active open.
- The connection remains open during the entire process. The service type, used by the IP protocol, is *minimize delay because this is an interactive connection between a user* (human) and a server.

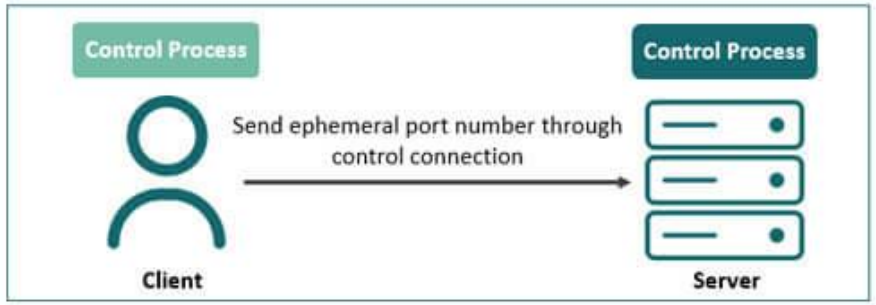
FTP (File Transfer Protocol)



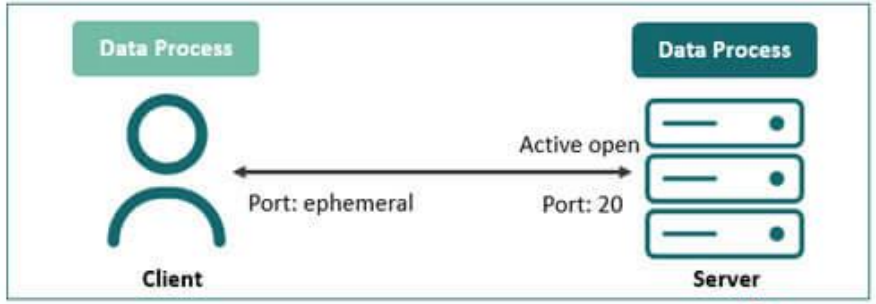
Architecture of FTP



a. First, Passive open by client



b. Second sending of ephemeral port

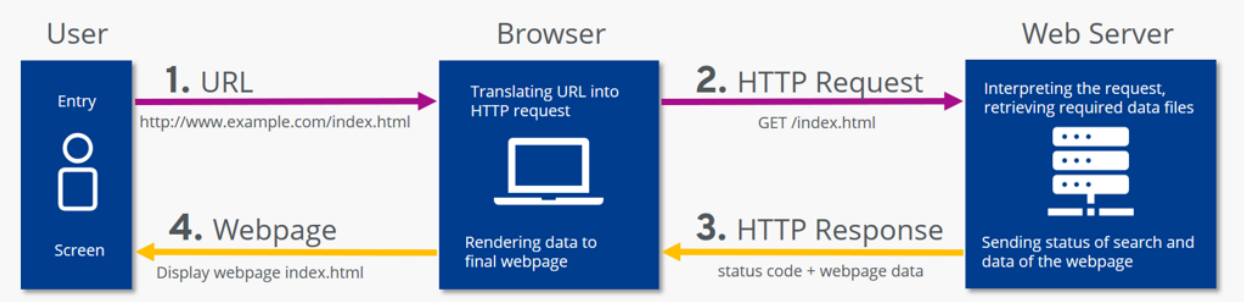


EDUCBA

2. *Data Connection*

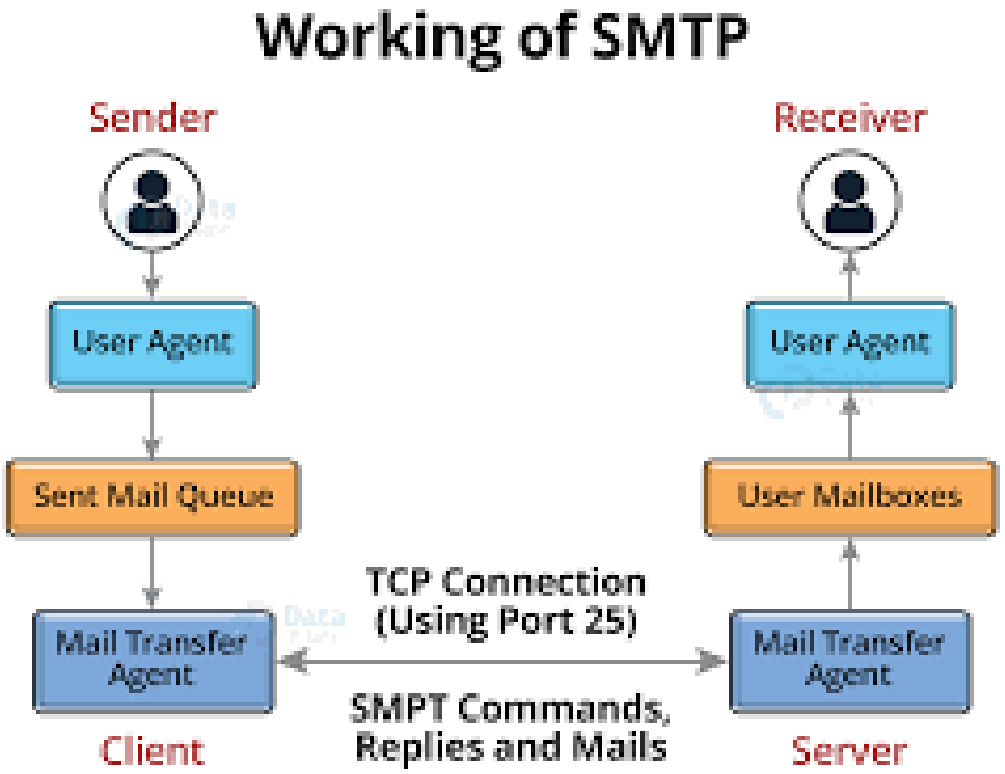
- The **data connection uses the well-known port 20 at the server site.** The following shows how FTP creates a data connection:
  1. **The client, not the server, issues a passive open using an ephemeral port. This must be** done by the client because it is the client that issues the commands for transferring files.
  2. **The client sends this port number to the server using the PORT command (we will** discuss this command shortly).
  3. **The server receives the port number and issues an active open using the well-known** port 20 and the received ephemeral port number.

HTTP(Hypertext Transfer Protocol)



- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP functions like a combination of FTP and SMTP.
- It is similar to FTP because it transfers files and uses the services of
  TCP.
- However, it is much simpler than FTP because it uses only one TCP connection.
- There is no separate control connection; only data are transferred between the client and the server.
- HTTP is like SMTP because the data transferred between the client and
  the server look like SMTP messages.
- HTTP uses the services of TCP on well-known port 80.

Simple Mail Transfer Protocol(SMTP)

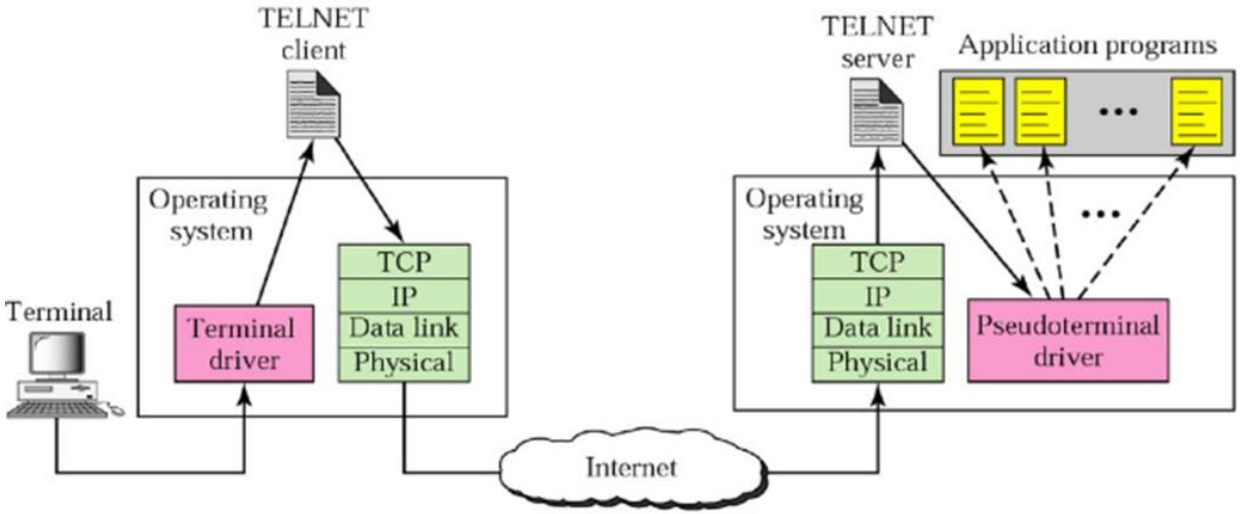


- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e- mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
- It can send a single message to one or more recipients.
- Sending message can include text, voice, video or graphics.
- It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers.
- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers
- SMTP simply defines how commands and responses must be sent back and forth.
- Each network is free to choose a software package for implementation.

Remote Login

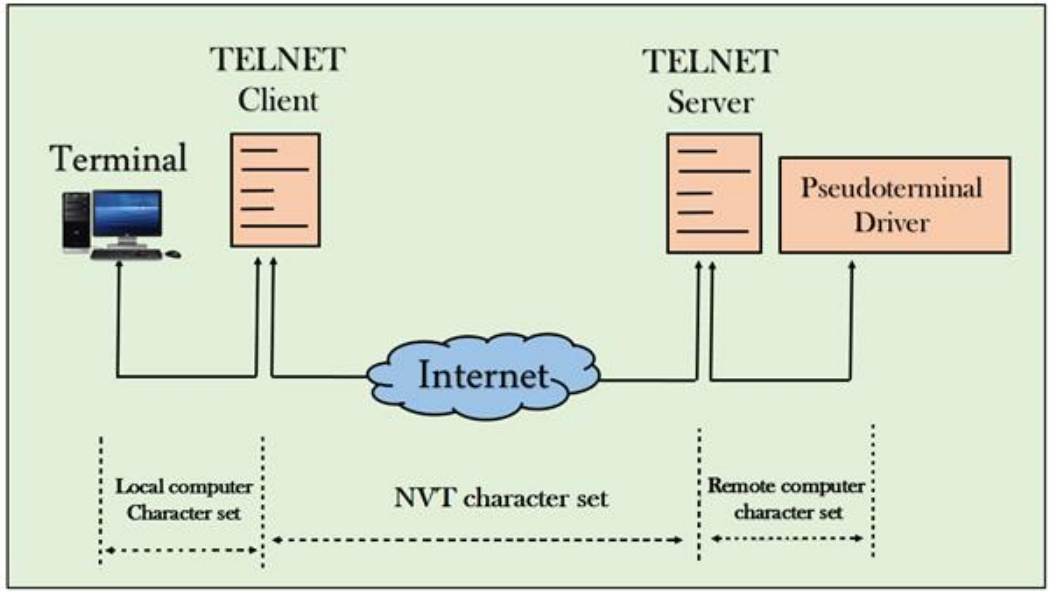
- Remote access refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location.
- This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.
- Remote access can be set up using a local area network (LAN), wide area network (WAN) or even a virtual private network (VPN) so that resources and systems can be accessed remotely.
- Remote access is also known as remote login.
- When a user wants to access an application program or utility located on a remote machine, he or she performs **remote login.**

Remote Login



- Here the TELNET client and server programs come into use.
- The user sends the keystrokes to the terminal driver where the local operating system accepts he characters but does not interpret them.
- The characters are sent to the TELNET client, which transforms the characters to a universal character set called *Network Virtual Terminal (NVT) characters and delivers* them to the local TCP/IP stack

Telnet



- **TELNET is an abbreviation for *TErminaL NETwork.***
- ***It is the standard TCP/IP protocol*** for virtual terminal service as proposed by ISO.
- TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.
- The main task of the internet is to provide services to users.
- For example, users want to run different application programs at the remote site and transfers a result to the local site.
- This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.

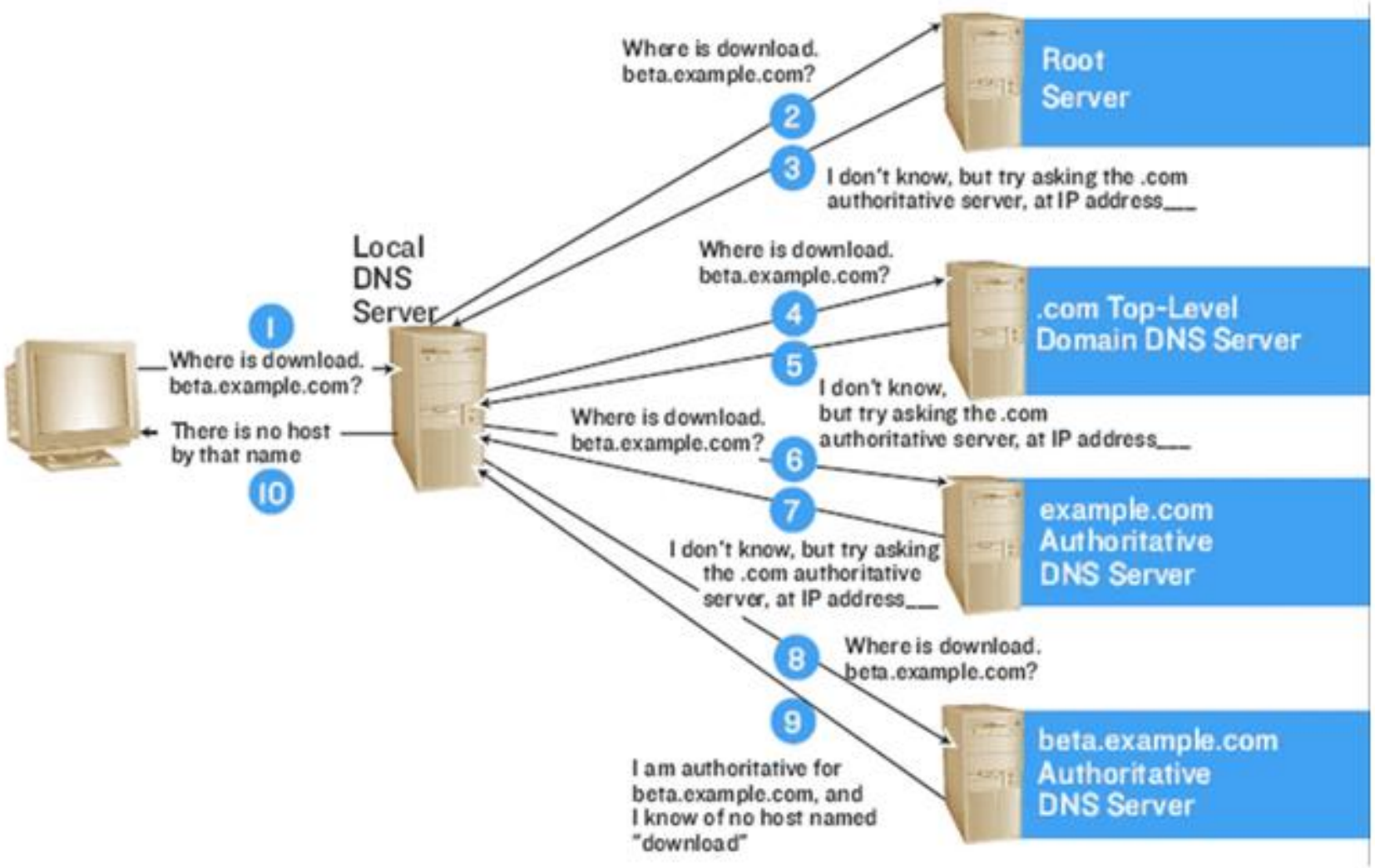
Telnet

- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer.
- Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands.

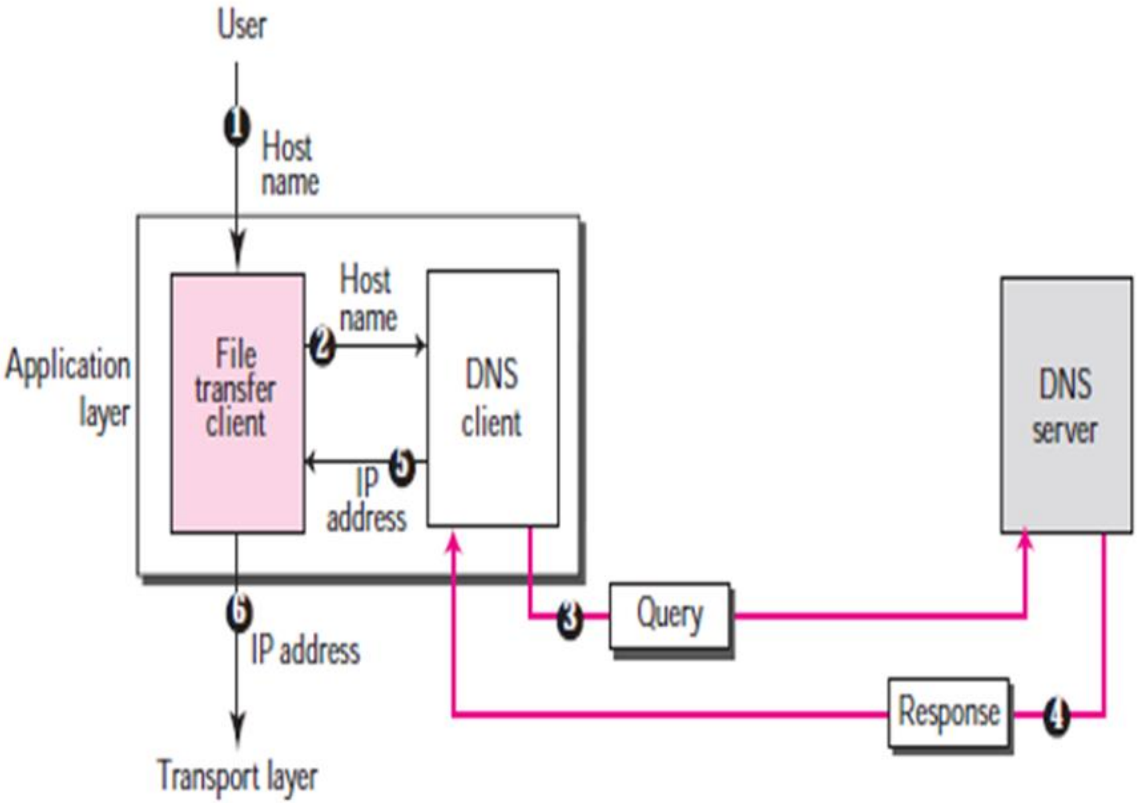
Network Virtual Terminal (NVT)

- The mechanism to access a remote computer is complex. This is because every computer and its operating system accepts a special combination of characters as tokens.
- For example, the end-of-file token in a computer running the DOS operating system is Ctrl+z, while the UNIX operating system recognizes Ctrl+d.

DNS - Domain Name System



DNS - Domain Name System



NEED FOR DNS

- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of numeric addresses.
- Therefore, we need a system that can map a name to an address or an address to a name.

Concept of Domain Name Space

- The names must be unique because the addresses are unique.
- A **name space that maps each address to a unique name can be organized in two ways:** flat or hierarchical.

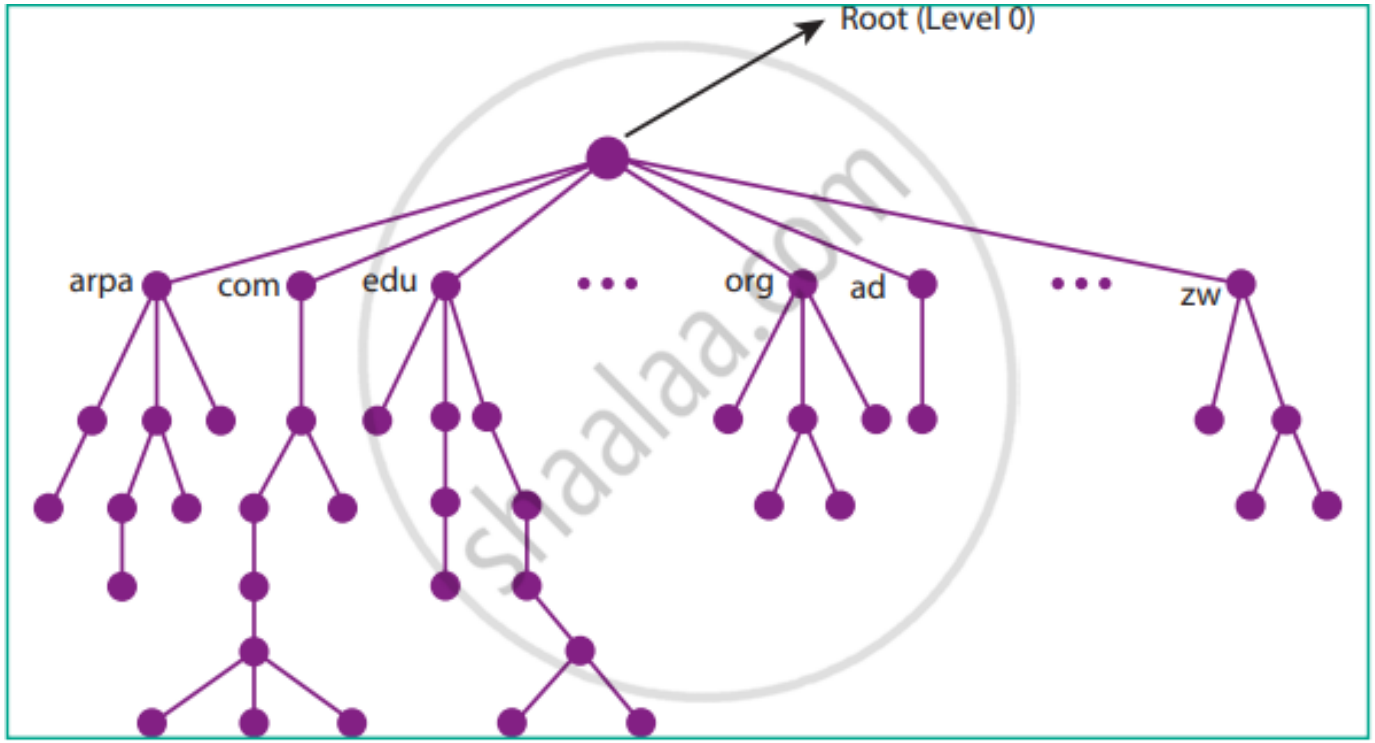
1. **Flat Name Space**
    - In a flat name space, a name is assigned to an address.
    - A name in this space is a sequence of characters without structure.
    - The names may or may not have a common section; if they do, it has no meaning.
    - The main disadvantage of a flat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

Concept of Domain Name Space

2. Hierarchical Name Space

- In a **hierarchical name space, each name is made of several parts.**
- **The first part can** define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on.
- In this case, the authority to assign and control the name spaces can be decentralized.

Domain Name Space



- To have a hierarchical name space, a **domain name space was designed.**
- **In this design** the names are defined in an inverted-tree structure with the root at the top.
- The tree can have only 128 levels: level 0 (root) to level 127

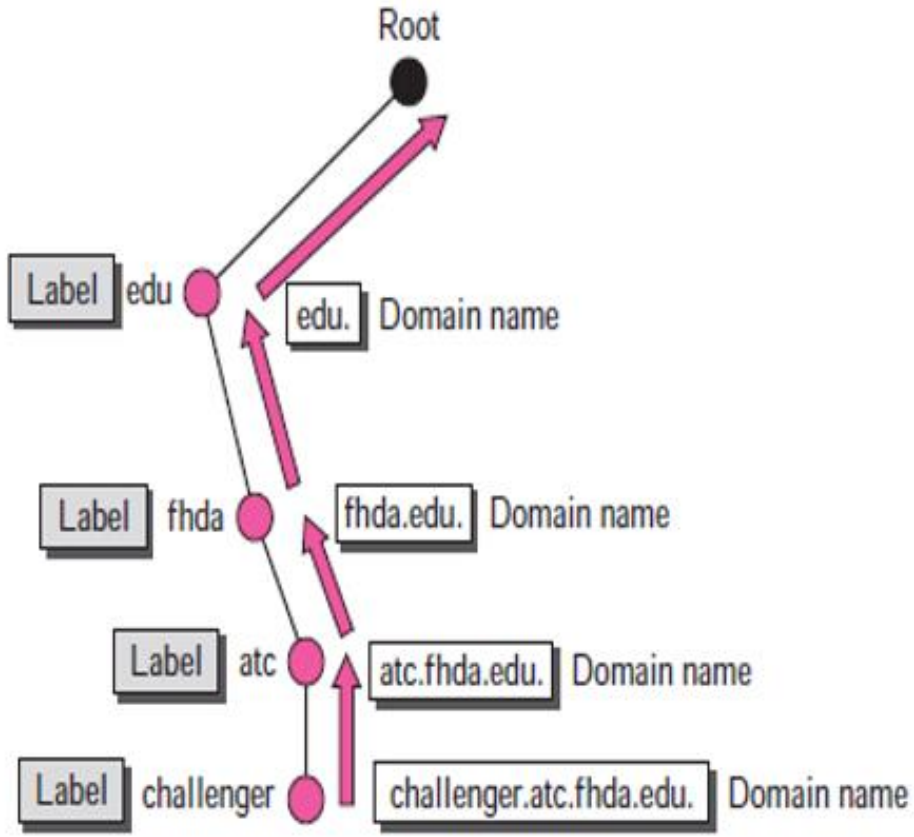
Domain Name Space

Label

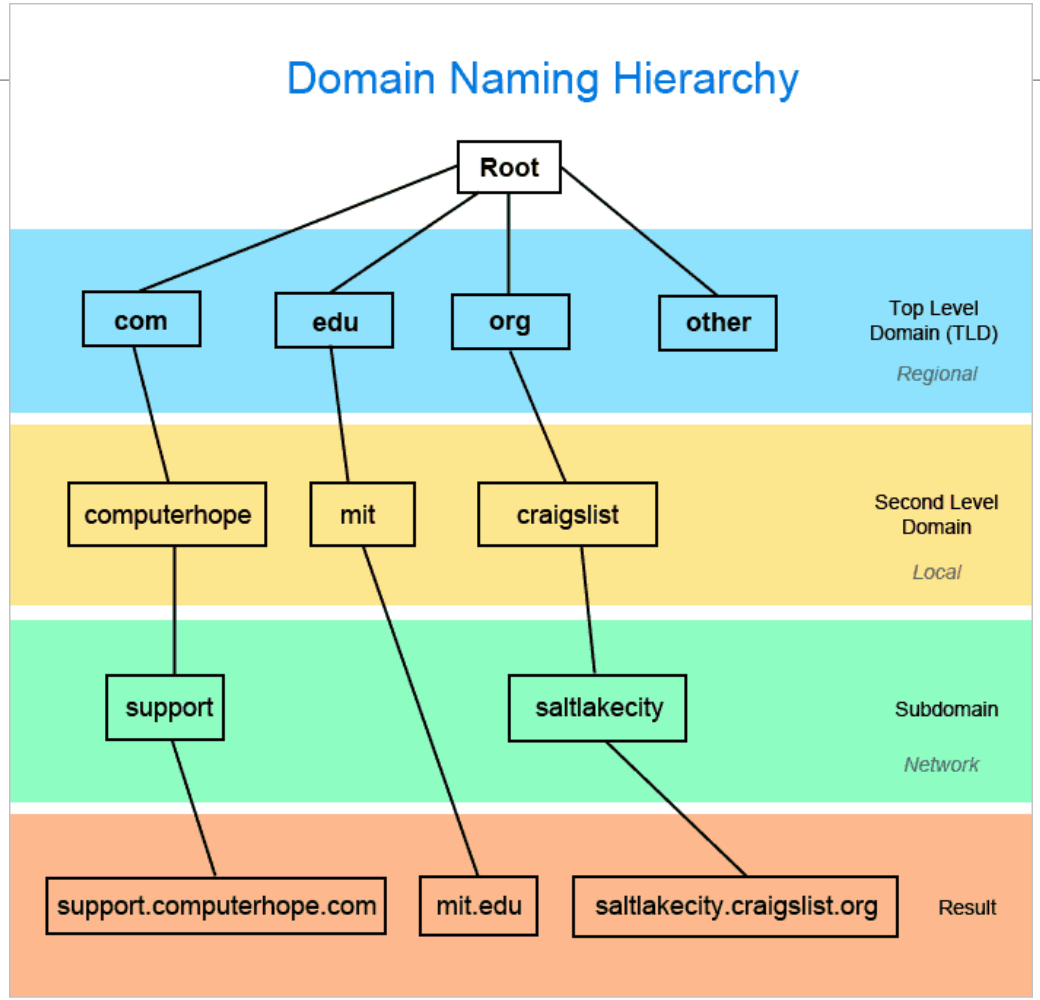
- Each node in the tree has a **label, which is a string with a maximum of 63 characters.**
- The root label is a null string (empty string).
- DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

Domain Name

- Each node in the tree has a domain name.
- A full **domain name is a sequence of labels** separated by dots (.).
- The domain names are always read from the node up to the root.



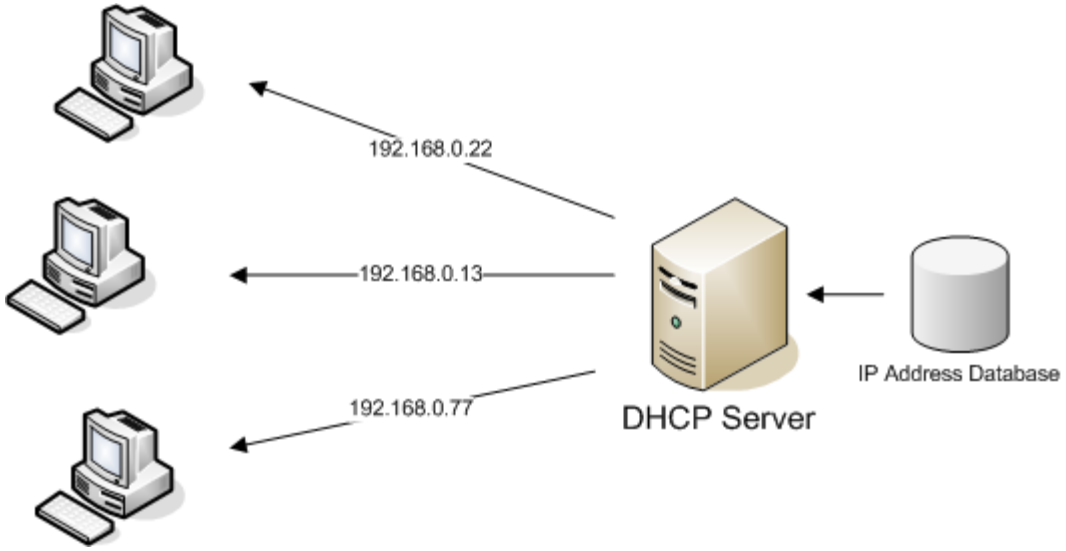
Level of Domain Name Space

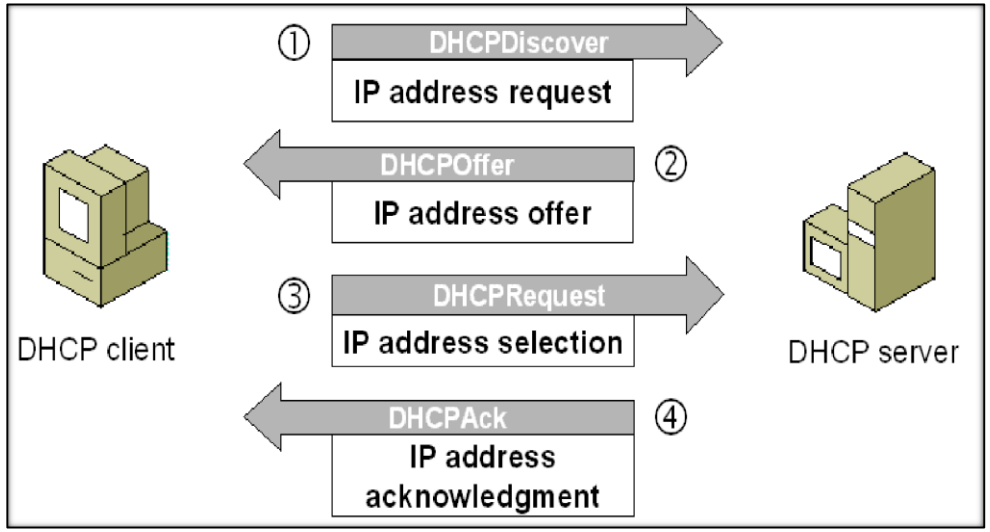


Dynamic Host Configuration Protocol (DHCP)

- The **Dynamic Host Configuration Protocol** (**DHCP**) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address.
- A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.
- In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an APIPA address, which will not enable it to communicate outside its local subnet.
- **Port number for DHCP is 67, 68.**

DHCP OPERATION





DHCP OPERATION

1. **DHCP discover message –**
- This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server.

2. DHCP offer message –
- The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server.

3. **DHCP request message –**
- When a client receives a offer message, it responds by broadcasting a DHCP request message.

4. **DHCP acknowledgement message –**
- In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time.