Computer Networks

Unit : Computer Network

- Introduction to Data Communication and Computer Network, Network Topologies, classification of computer network, Parallel & Serial Transmission, Transmission Models, Transmission Channel, Data Rate, Bandwidth Signal Encoding Schemes, Data Compression, Transmission Impairments, Layering and Design Issues, OSI Model and TCP/ IP model.

Unit : Computer Network

- Data Link Layer: Need for Data Link Control, Frame Design Consideration, Flow Control & Error Control. MAC sublayer, contention based and polling based MAC protocols.

- Network Layer: Routing, Congestion control, Internetworking principles, Internet Protocols (IPv4, packet format, Hierarchal addressing sub netting, ARP, PPP), Bridges, Routers. Classless IP address.

Unit : Computer Network

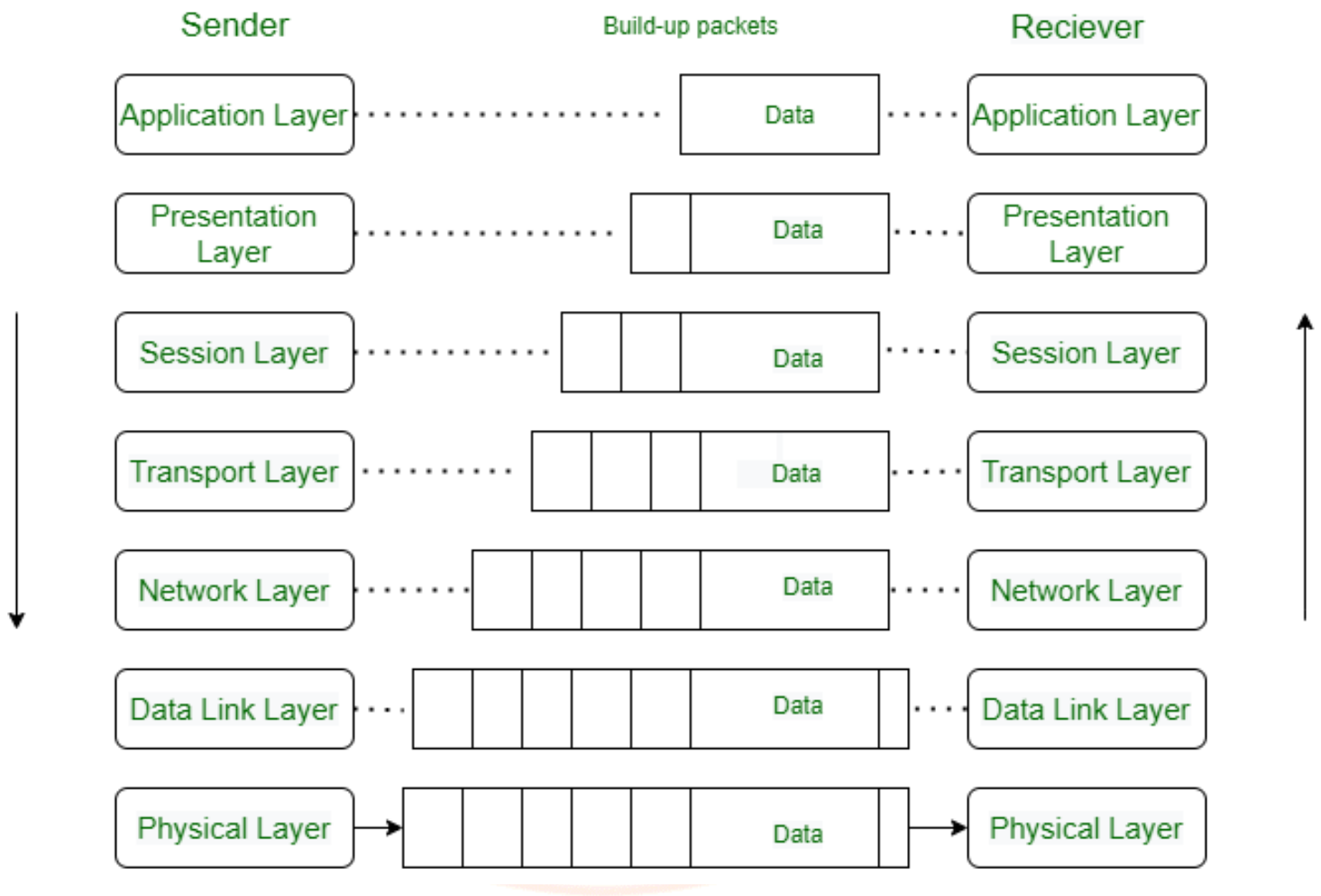
- Datalink Layer: Process to process communication. Socket meaning and socket address. Upward and downwards multiplexing. UDP and TPDU.

- Application Layer: HTTP, FTP, Telnet, SMTP, SNMP

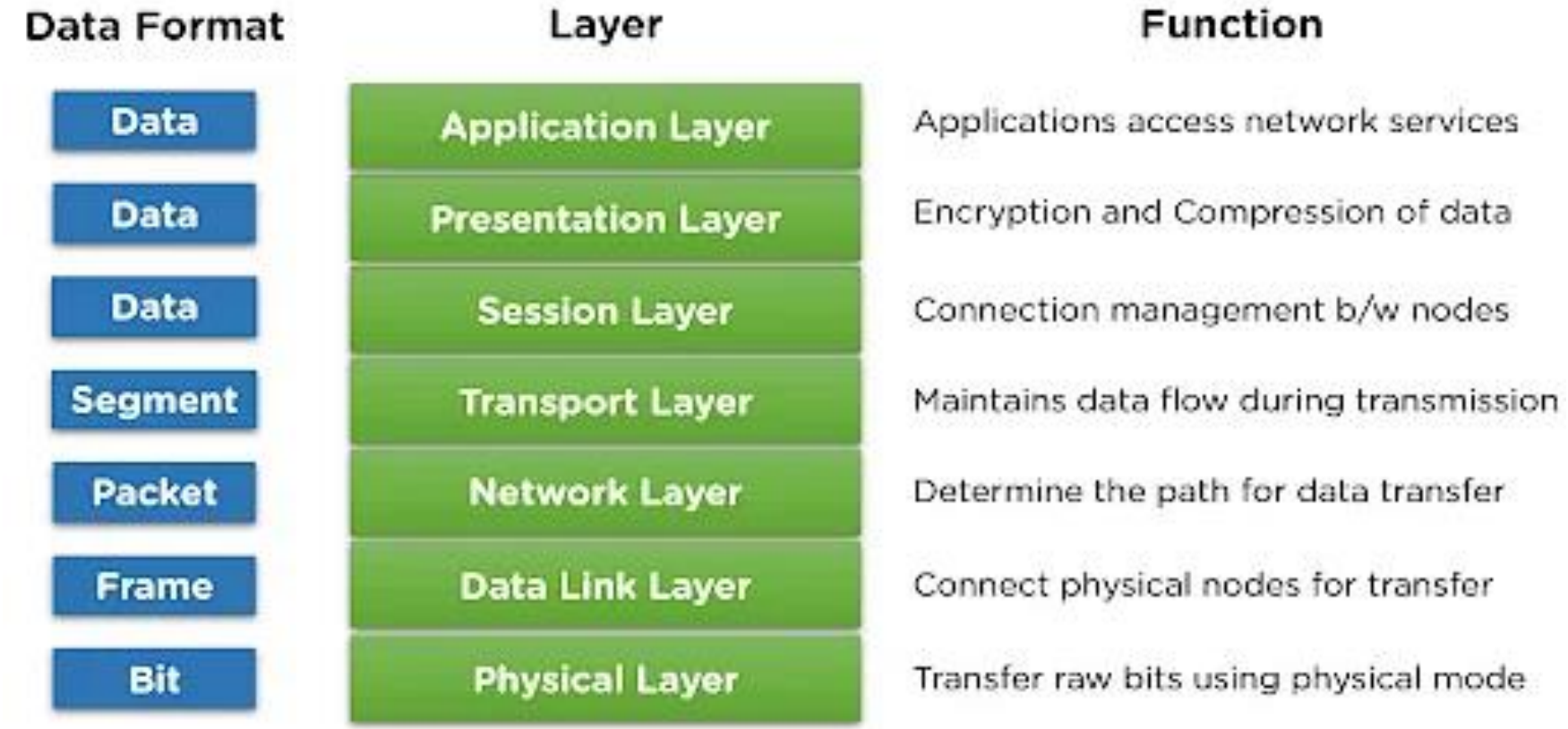
What Is the OSI Model

- 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, adopted by all major computer and telecommunication companies in the early 1980s

OSI Model



What Is the OSI Model



Data Format	Layer	Function
Data	Application Layer	Applications access network services
Data	Presentation Layer	Encryption and Compression of data
Data	Session Layer	Connection management b/w nodes
Segment	Transport Layer	Maintains data flow during transmission
Packet	Network Layer	Determine the path for data transfer
Frame	Data Link Layer	Connect physical nodes for transfer
Bit	Physical Layer	Transfer raw bits using physical mode

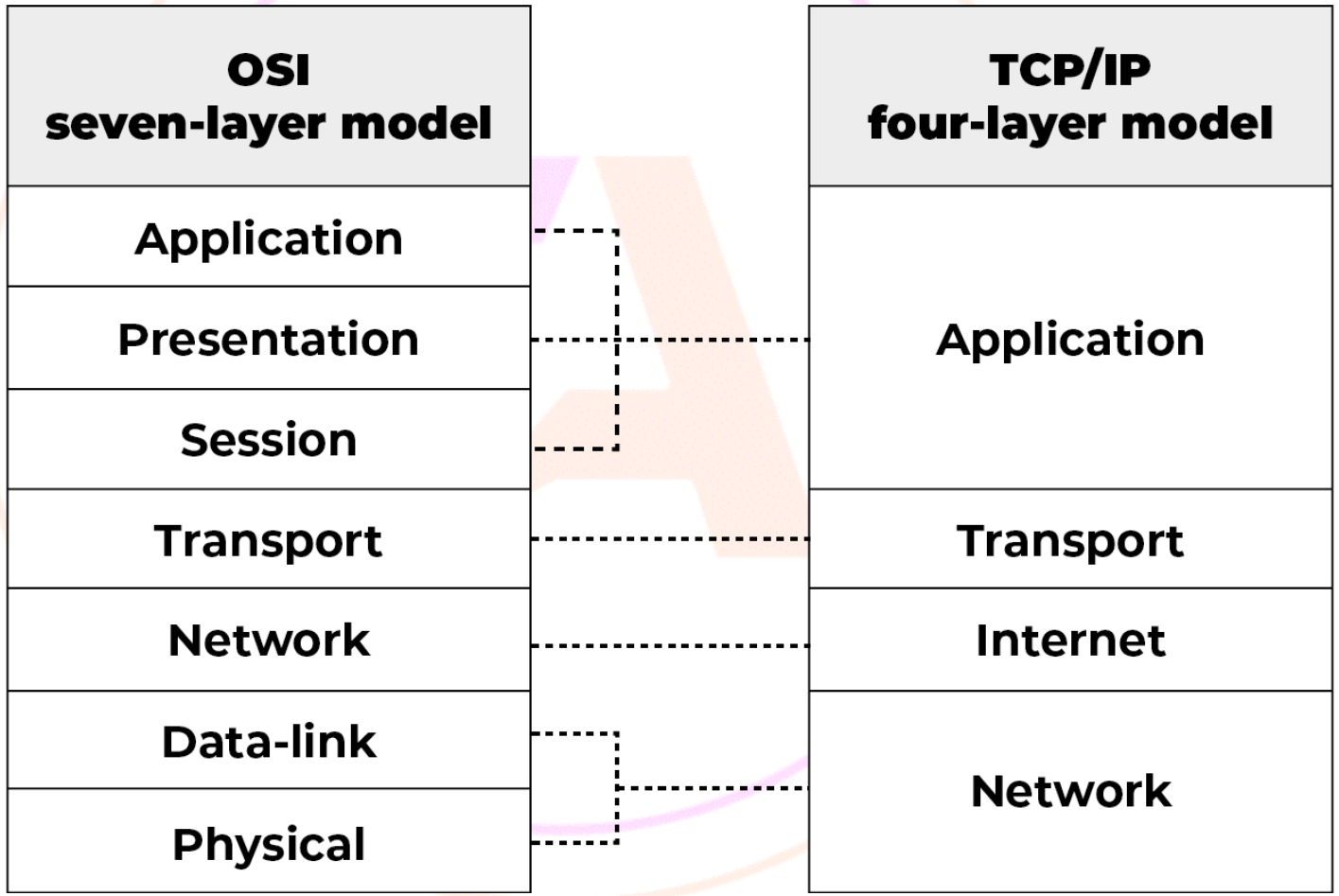
What Is the OSI Model

OSI model		
Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

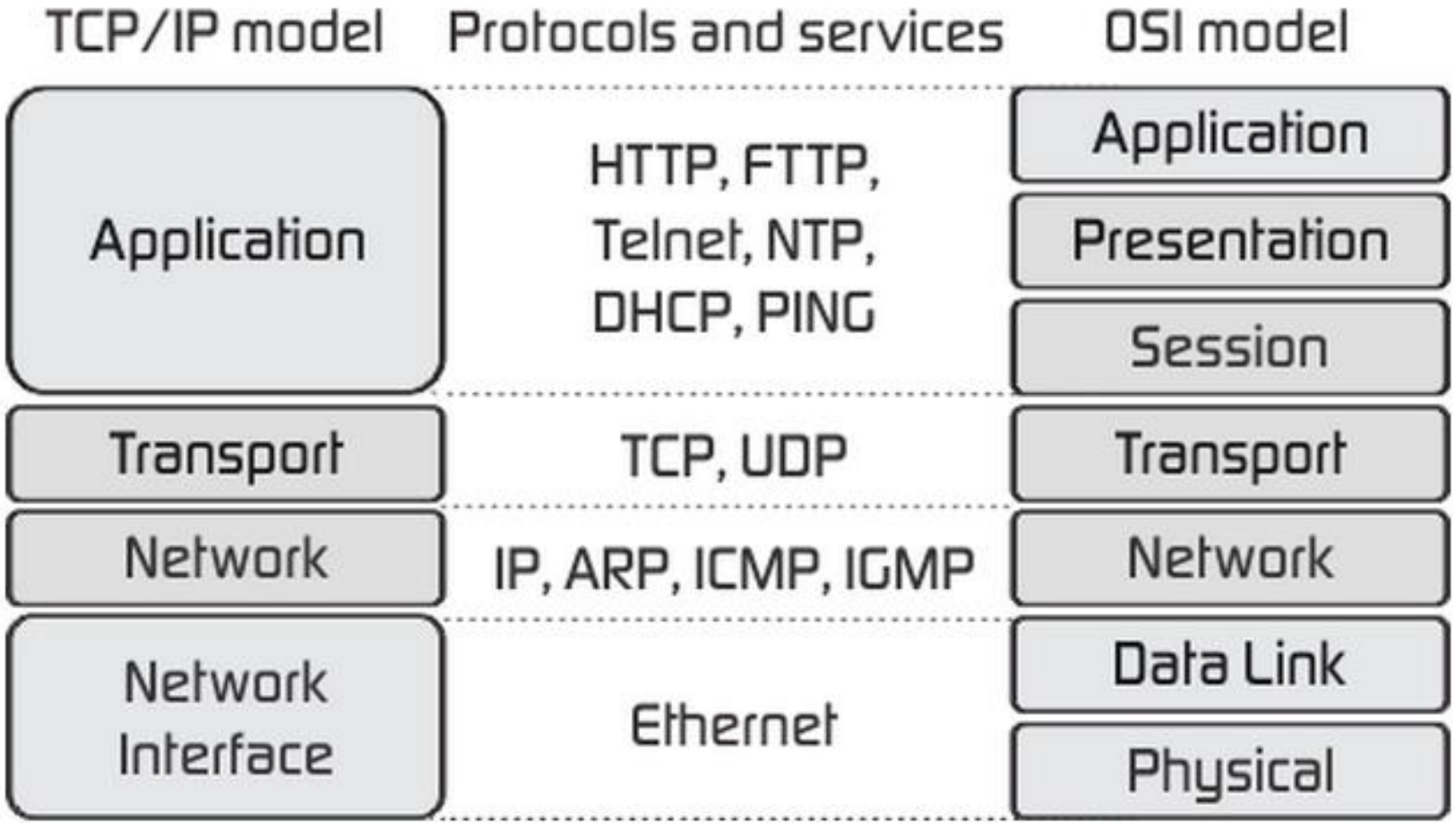
What Is the TCP/IP Model

- TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.
- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

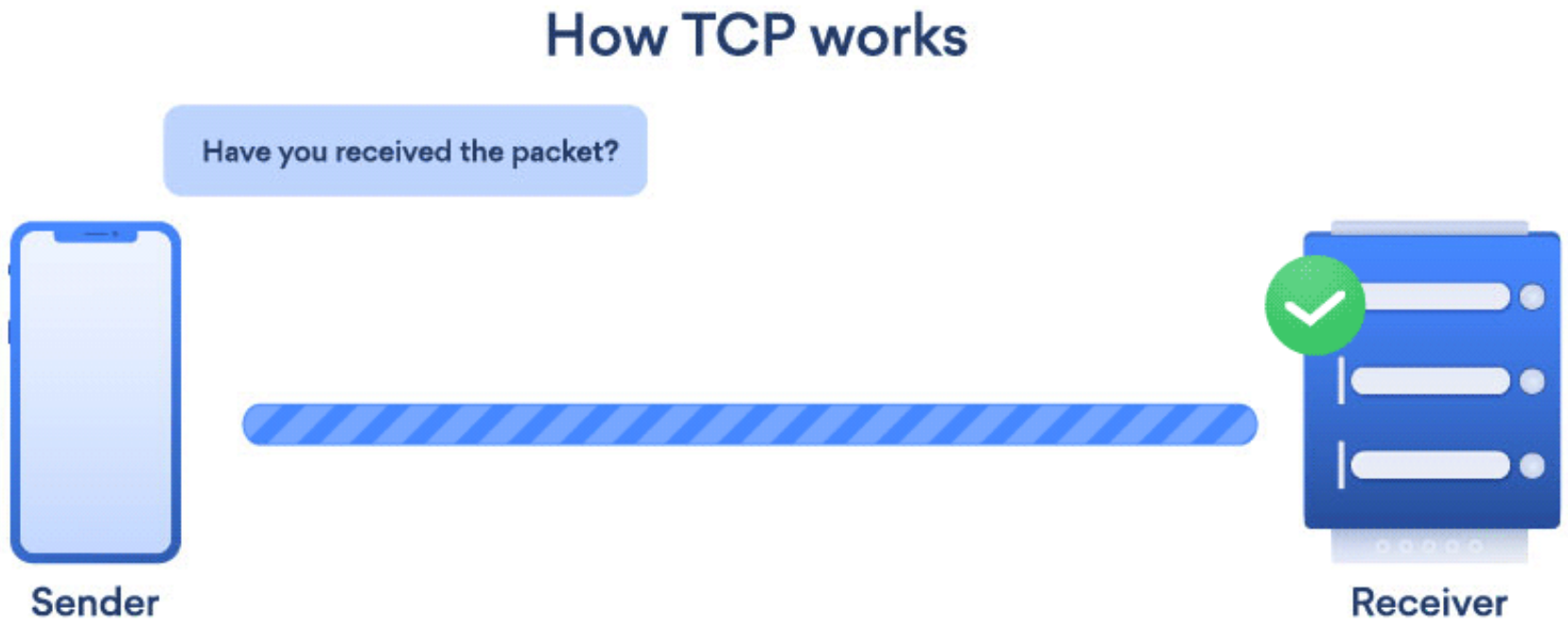
What Is the TCP/IP Model



What Is the TCP/IP Model



Working of Internet Protocol



TCP/IP(Transmission Control Protocol/ Internet Protocol)

- These are a set of standard rules that allows different types of computers to communicate with each other.

- TCP specifies how data is exchanged over the internet and how it should be broken into IP packets.

TCP/IP(Transmission Control Protocol/ Internet Protocol)

- It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.

- The TCP is also known as a connection-oriented protocol.

HTTP(Hyper Text Transfer Protocol)

- HTTP stands for HyperText Transfer Protocol. It is the primary protocol used to access the World Wide Web.
- Tim Berners-Lee led the development of HTTP at CERN in 1989 in collaboration with Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C).
- HTTP is a request-response (also called client-server) protocol that runs over TCP. The common use of HTTP is between a web browser (client) and a web server (server).

HTTP(Hyper Text Transfer Protocol)

- This protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer.
- This protocol defines how the information needs to be formatted and transmitted.
- And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page.

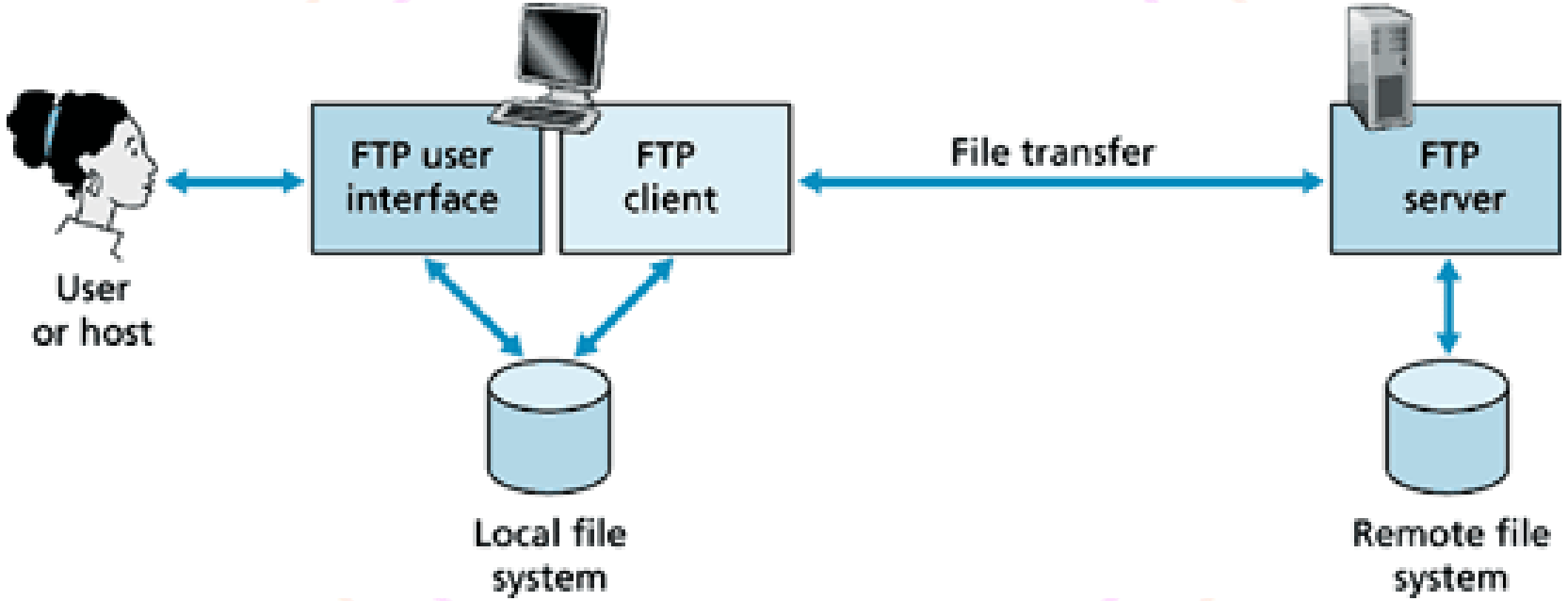
HTTP(Hyper Text Transfer Protocol)

- A web page is written using a markup language like HTML and is stored on a web server for access via its URL.
- Once a user opens a web browser and types in the URL of the intended web page, a logical communication link between the user machine (client) and the web server is created using HTTP.
- For example, whenever we enter the URL http//www.ncert.nic.in in a browser, it sends HTTP request to the web-server where ncert.nic.in is hosted. The HTTP response from the web-server fetches and sends the requested Web-page, which is displayed on your browse.

HTTPS (Hypertext Transfer Protocol Secure)

- HTTPS is an extension of the Hypertext Transfer Protocol (HTTP).
- It is used for secure communication over a computer network with the SSL/TLS protocol for encryption and authentication.
- So, generally, a website has an HTTP protocol but if the website is such that it receives some sensitive information such as credit card details, debit card details, OTP, etc then it requires an SSL certificate installed to make the website more secure. So, before entering any sensitive information on a website, we should check if the link is HTTPS or not.

FTP (File Transfer Protocol)



FTP (File Transfer Protocol)

- This protocol is used for transferring files from one system to the other.

- This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates each other using their ID and Password. And, the desired file transfer takes place between the machines.

FTP (File Transfer Protocol)

- When a user requests for a file transfer with another system, FTP sets up a connection between the two nodes for accessing the file. Optionally, the user can authenticate using user ID and password. The user then specifies the file name and location of the desired file. After that, another connection sets up and the file transfer happens directly between the two machines.

FTP (File Transfer Protocol)

- However, some servers provide FTP logins without authentication for accessing files.
- File transfer between two systems seems simple and straightforward because FTP takes care of issues between two communicating devices.

TELNET(TERMINAL NETWORK)

- TELNET is a standard TCP/IP protocol used for virtual terminal service given by ISO.
- This enables one local machine to connect with another.
- The computer which is being connected is called a remote computer and which is connecting is called the local computer.

Point to Point Protocol (PPP)

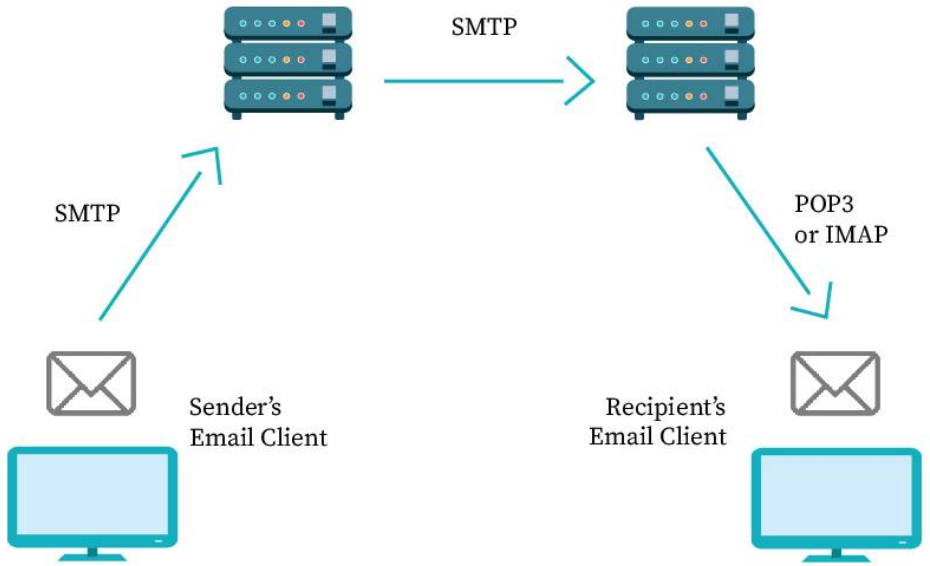
- PPP is a communication protocol which establishes a dedicated and direct connection between two communicating devices.
- This protocol defines how two devices will authenticate each other and establish a direct link between them to exchange data.

Point to Point Protocol (PPP)

- For example, two routers with direct connection communicate using PPP.
- The Internet users who connect their home computers to the server of an Internet Service Provider (ISP) through a modem also use PPP.

SMTP(Simple Mail Transfer Protocol)

- These protocols are important for sending and distributing outgoing emails.



Identifying Nodes in a Networked Communication

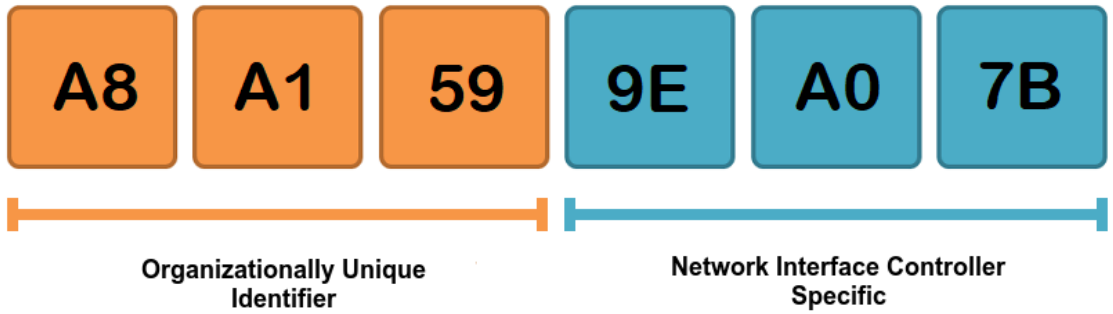
- Each node in a network should be uniquely identified so that a network device can identify the sender and receiver and decide a routing path to transmit data.

MAC Address

- MAC stands for Media Access Control. The MAC address, also known as the physical or hardware address, is a unique value associated with a network adapter called a NIC.
- The MAC address is engraved on NIC at the time of manufacturing and thus it is a permanent address and cannot be changed under any circumstances.
- The machine on which the NIC is attached, can be physically identified on the network using its MAC address.

MAC Address

- Each MAC address is a 12-digit hexadecimal numbers (48 bits in length), of which the first six digits (24 bits)contain the manufacturer's ID called Organisational Unique Identifier (OUI) and the later six digits (24 bits) represents the serial number assigned to the card by the manufacturer. A sample MAC address looks like.



MAC Address

- The MAC address belongs to the data link layer of the Open Systems Interconnection (OSI) model, which encapsulates the MAC address of the source and destination in the header of each data frame to ensure node-to-node communication.

INTERNET PROTOCOL

- An IP stands for internet protocol.
- An IP address is assigned to each device connected to a network.
- Each device uses an IP address for communication.
- It also behaves as an identifier as this address is used to identify the device on a network.

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

INTERNET PROTOCOL

- IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN).

Internet Protocol

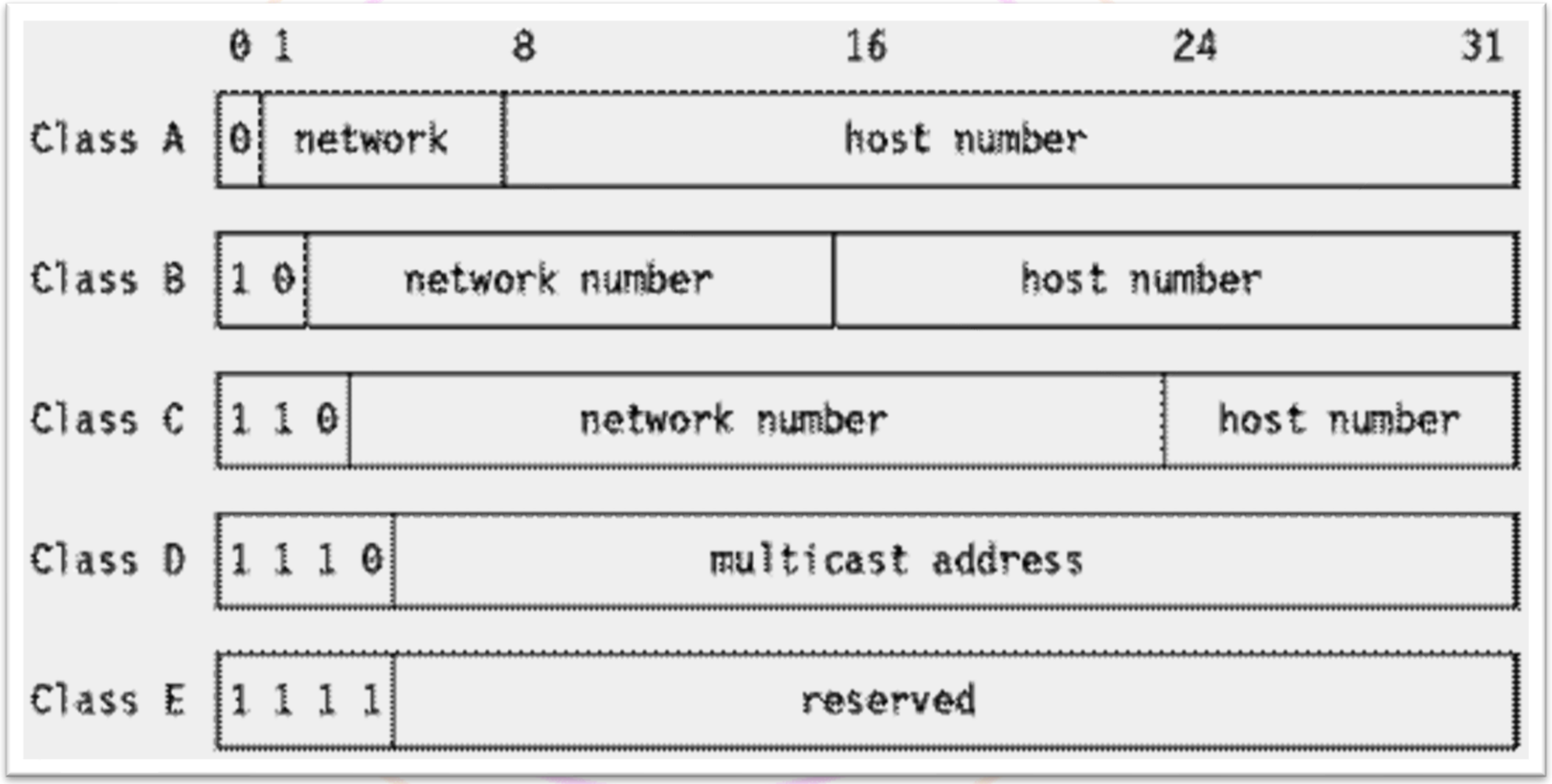
IPv4	vs.	IPv6
Deployed 1981		Deployed 1998
32-bit IP address		128-bit IP address
4.3 billion addresses Addresses must be reused and masked		$7.9x10^{28}$ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18		Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration		Supports autoconfiguration

INTERNET PROTOCOL

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

INTERNET PROTOCOL



INTERNET PROTOCOL

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Serial No	IP address	Port Number
01.	Internet Protocol address (IP address) used to identify a host in network.	Port number is used to identify an processes/services on your system
02.	IPv4 is of 32 bits (4 bytes) size and for IPv6 is 128 bits (16 bytes).	The Port number is 16 bits numbers.
03.	IP address is the address of the layer-3 IP protocol.	Port number is the address of the layer-4 protocols.
04.	IP address is provided by admin of system or network administrator.	Port number for application is provided by kernel of Operating System.
05.	ipconfig command can be used to find IP address .	netstat command can be used to find Network Statistics Including Available TCP Ports.
06.	IP address identify a host/computer on a computer network.	Port numbers are logical interfaces used by communication protocols.
07.	192.168.0.2, 172.16.0.2 are some of IP address examples.	80 for HTTP, 123 for NTP, 67 and 68 for DHCP traffic, 22 for SSH etc.

The World Wide Web (WWW)

- The World Wide Web (WWW) or web in short, is an ocean of information, stored in the form of trillions of interlinked web pages and web resources.
- The resources on the web can be shared or accessed through the Internet.
- Earlier, to access files residing in different computers, one had to login individually to each computer through the Internet.

THE WORLD WIDE WEB (WWW)

- Besides, files in different computers were sometimes in different formats, and it was difficult to understand each other's files and documents.

- Sir Tim Berners-Lee — a British computer scientist invented the revolutionary World Wide Web in 1990 by defining three fundamental technologies that lead to creation of web:

THE WORLD WIDE WEB (WWW)

- HTML – HyperText Markup Language. It is a language which is used to design standardised Web Pages so that the Web contents can be read and understood from any computer.

- Basic structure of every webpage is designed using HTML.

THE WORLD WIDE WEB (WWW)

- URL – Uniform Resource Identifier. It is a unique address or path for each resource located on the web.
- It is also known as Uniform Resource Locator (URL). Every page on the web has a unique URL.
- Examples are: https://www.mhrd.gov.in
- URL is sometimes also called web address.
- However, a URL is not only the domain name.

DOMAIN NAME SYSTEM

- The Internet is a vast ocean where information is available in the form of millions of websites. Each website is stored on a server which is connected to the Internet, which means each server has an IP address.

- Every device connected to the Internet has an IP address. To access a website, we need to enter its IP address on our web browser.

- But it is very difficult to remember the IP addresses of different websites as they are in terms of numbers or strings.

DOMAIN NAME SYSTEM

- However, it is easier to remember names, and therefore, each computer server hosting a website or web resource is given a name against its IP address.
- These names are called the Domain names or hostnames corresponding to unique IP addresses assigned to each server.
- For easy understanding, it can be considered as the phonebook where instead of remembering each person's phone number, we assign names to their numbers.

DNS Server

Instead of remembering IP addresses, we assign a domain name to each IP.

But, to access a web resource, a browser needs to find out the IP address corresponding to the domain name entered.

Conversion of the domain name of each web server to its corresponding IP address is called domain name resolution. It is done through a server called DNS server.

DNS Server

Thus, when we enter a URL on a web browser, the HTTP protocol approaches a computer server called DNS server to obtain the IP address corresponding to that domain name.

After getting the IP address, the HTTP protocol retrieves the information and loads it in our browser.

VoIP

- Voice over Internet Protocol or VoIP, allows us to have voice call (telephone service) over the Internet, i.e., the voice transmission over a computer network rather than through the regular telephone network.

- It is also known as Internet Telephony or Broadband Telephony.

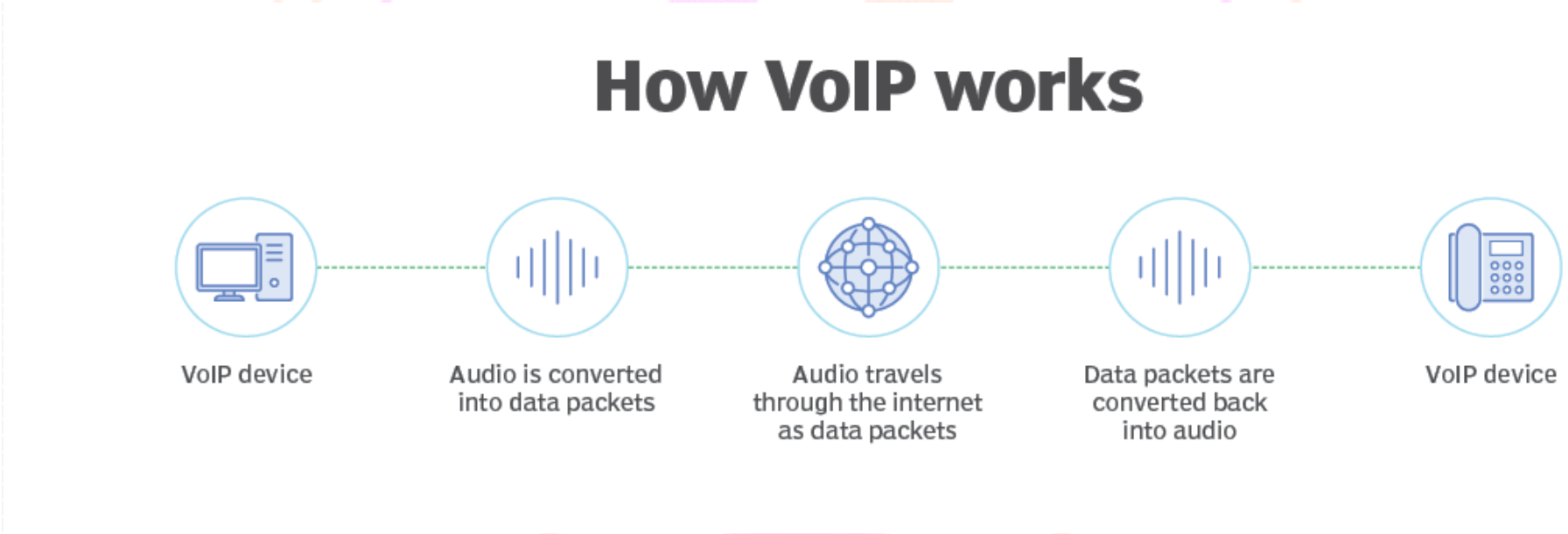
VoIP

- The process works similarly to a regular phone, but VoIP uses an internet connection instead of a telephone company's wiring. VoIP is enabled by a group of technologies and methodologies used to deliver voice communications over the internet, including enterprise local area networks or wide area networks.

- A VoIP service will convert a user's voice from audio signals to digital data, then send that data through the internet. If another user is calling from a regular phone number, the signal is converted back to a telephone signal before it reaches that user.

VoIP

- VoIP can also perform routing of incoming and outgoing calls through existing telephone networks



Basic of Email

Electronic mail is a method of exchanging messages between people using electronic devices. Invented by Ray Tomlinson, email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email.

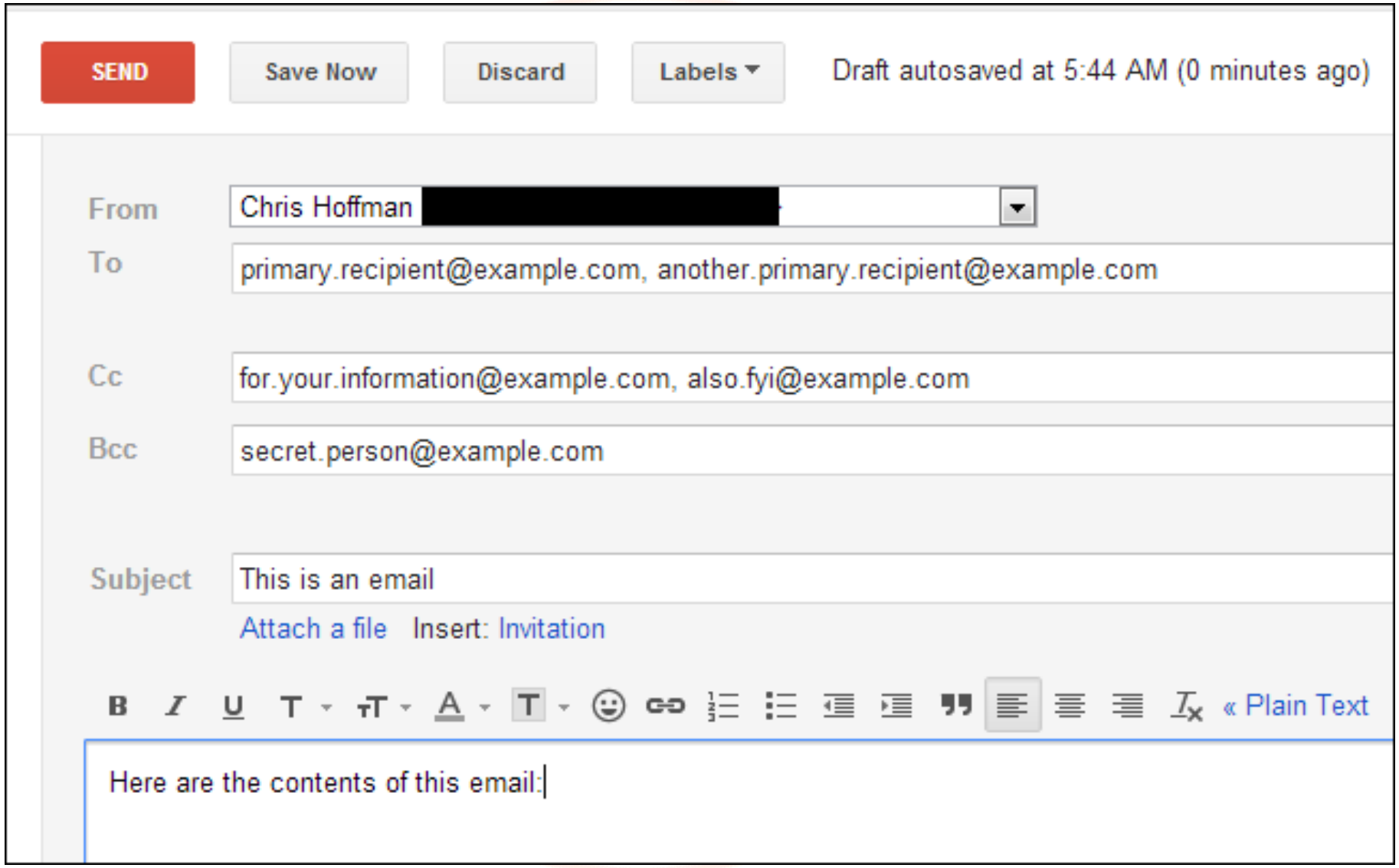
Email, short for Electronic Mail, consists of messages which are sent and received using the Internet. There are many different email services available that allow you to create an email account and send and receive email and attachments, many of which are free.

Today, the top webmail providers are Yahoo!, Microsoft's Outlook.com (previously Hotmail), and Google's Gmail.

The first five lines of an E-mail message is called E-mail header.

The header part comprises of following fields:

- From
- Date
- To
- Subject
- CC
- BCC



- **Bcc Stands for "Blind Carbon Copy."** When you send an e-mail to only one person, you type the recipient's address in the "To:" field. When you send a message to more than one person, you have the option to enter addresses in the "Cc:" and "Bcc:" fields. "Cc" stands for "Carbon Copy," while "Bcc" stands for "Blind Carbon Copy."

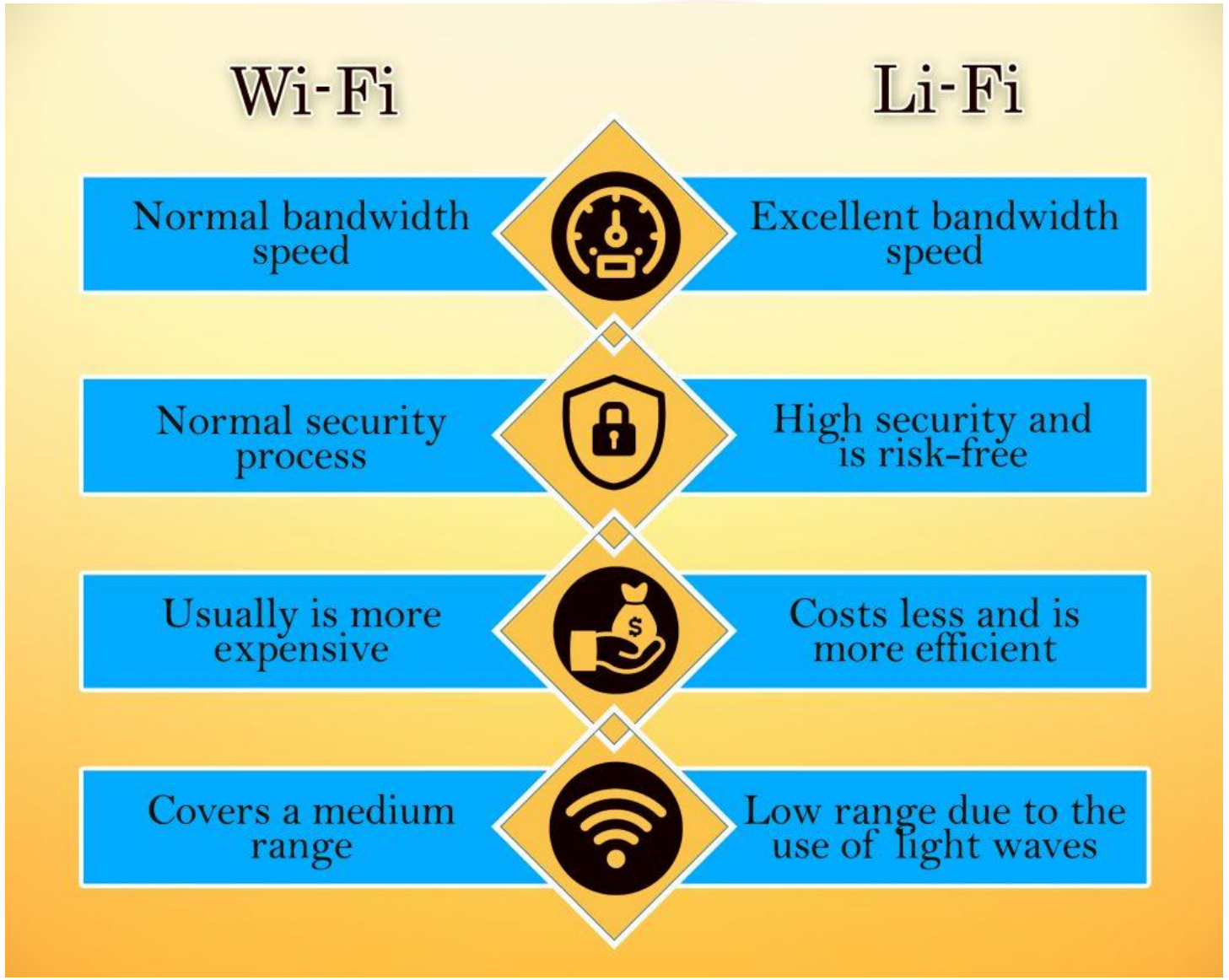
- **A Carbon Copy, or "Cc'd"** message is an e-mail that is copied to one or more recipients. Both the main recipient (whose address is in the "To:" field) and the Cc'd recipients can see all the addresses the message was sent to. When a message is blind carbon copied, neither the main recipient nor the Bcc'd recipients can see the addresses in the "Bcc:" field.

- **Blind carbon copying** is a useful way to let others see an e-mail you sent without the main recipient knowing. It is faster than sending the original message and then forwarding the sent message to the other recipients.

Q. Which of the following statement is correct about Wi-Fi and Li-Fi?

I. Wi-Fi uses light emitting diodes for data transmission.
II. Li- Fi works very well in dense environment.
III. In Li-Fi, data transfer speed is about 1 Gbps.

A. I
B. II
C. I and II
D. II and III



Q. With reference to 'LiFi' recently in the news, which of the following statements is/are correct?

1. It uses light as the medium for high-speed data transmission.
2. It is a wireless technology and is several times faster than 'WiFi'.

Select the correct answer using the code given below

A. 1 only
B. 2 only
C. Both 1 and 2
D. Neither 1 nor 2

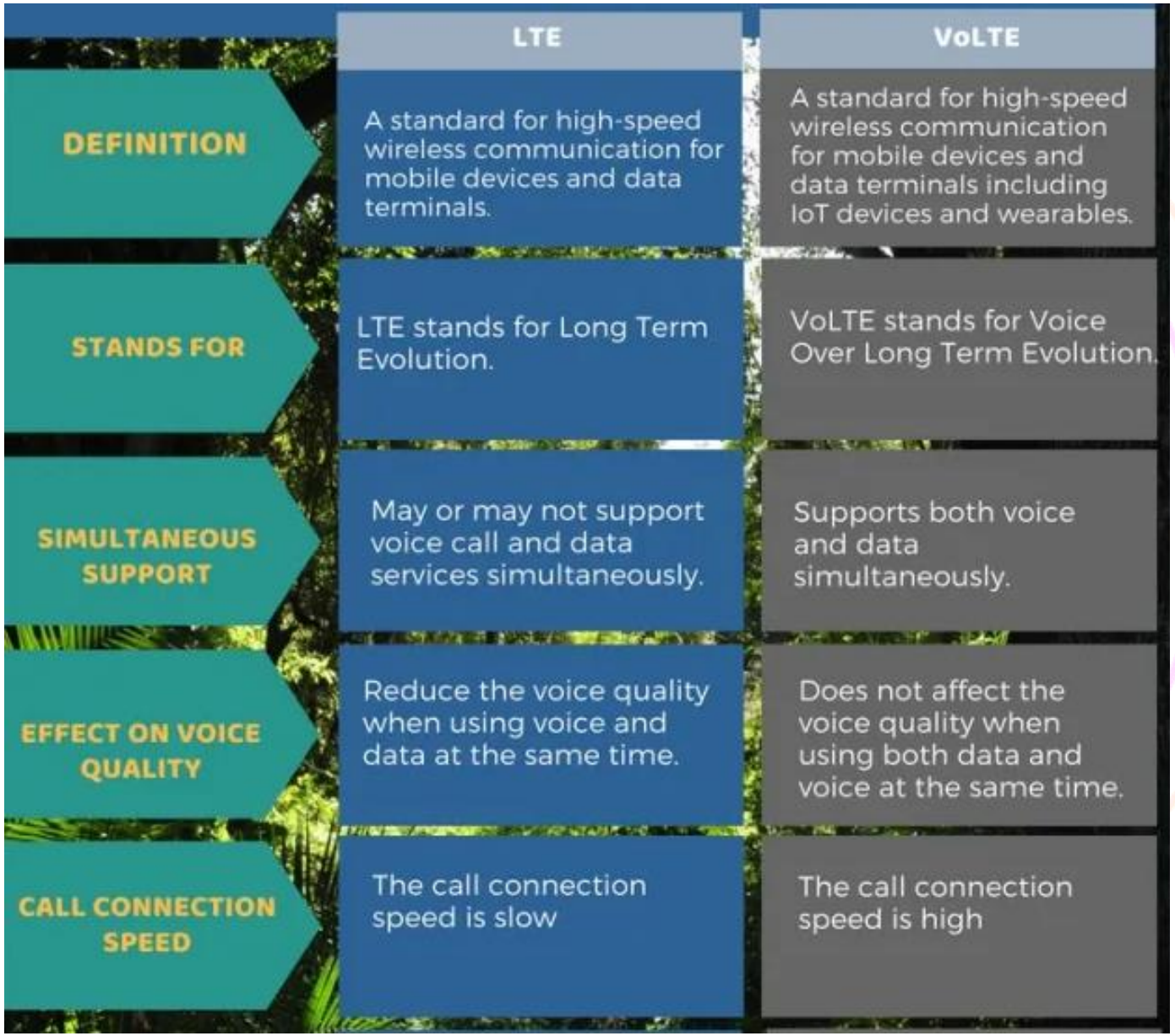
SrNo.	Comparison Basis	LIFI	WIFI
1.	Full Form	Light fidelity	Wireless fidelity
2.	Operation	Transmits data using bits with help of light from LED bulbs.	Transmits data with help of radio waves with help of WIFI router
3.	Security	Secured (cannot be hacked) as light is blocked by walls.	Not secured (can be hacked) as for RF signal dry walls are transparent
4.	Interference	Do not have any interference issue similar to radio waves.	Has interference issue from nearby access points (routers)
5.	Spectrum	The Spectrum range is 10000times than Wi-Fi	It has radio spectrum range.
6.	Frequency	The frequency band is 100 times of Tera HZ	The frequency band is 2.4GHz,4.9GHzand 5GHz
7.	Speed	Fast speed internet (greater than 1- 3.5Gbps)	Comparatively slow speed (54-250 Mbps)
8.	Where To Use	Anywhere, where light source is present.	Inside a building. typically Within a array of WLAN communications , habitually inside a structure.
9.	Cost	Cheap as LED lamps are used.	Quiet expensive.
10.	Data transmission rate	Very high rate of data transmission due to visible light spectrum.	Transmission rate is slow as compared to Li-Fi as RF is used to communicate.
11.	System components	Lamp drivers, LED bulbs and light detectors will form complete Li-Fi system.	Routers have to be to be installed, devices like laptops, PDAs, desktops are called as stations.

Which of the following statements are correct regarding VoLTE?

(A) VoLTE stands for 'Voice over Long Term Evalution'.
(B) It is a digital packet voice service delivery over IP via an LTE access network.
(C) Provides more efficient use of spectrum than traditional voice.
(D) Eliminates the need to have voice on one network and data on another network.

Choose the correct answer from the options given below:

1. A, B, C and D Only
2. B, C and D Only
3. A, B and C Only
4. A, C and D Only



- **Light-Fidelity (Li-Fi) is a wireless optical networking technology that uses light-emitting diodes (LEDs) for data transmission.**
- **Wireless-Fidelity (Wi-Fi) is a wireless optical networking technology that uses routers, modems and access point for data transmission.**
- **Wi-Fi work in less dense environment due to interference related issues while Li-Fi is unrestricted by radio interference.**
- **In Li-Fi, data transfer speed is about 1 Gbps while data transfer speed in Wi-Fi ranges from 150Mbps to maximum of 2 Gbps.**

Q. For which type of connection WPA security used?

A. Ethernet
B. Bluetooth
C. Wi-Fi
D. Infrared

- ✓ For Wi-Fi connection WPA security used.
- ✓ WPA stands for Wi-Fi Protected Access.
- ✓ Wi-Fi Protected Access (WPA) is a security standard for users of computing devices equipped with wireless internet connections.
- ✓ WPA2 stands for Wi-Fi Protected Access II.
- ✓ The Wi-Fi Alliance announced WPA3 as a replacement to WPA2 in 2018.
- ✓ Bluetooth is a wireless technology used for exchanging data between fixed and mobile devices over short distances.
- ✓ The IEEE standardized Bluetooth as IEEE 802.15.1

Q. Which among the following network topologies has the highest transmission speed?

A) LAN
B) WAN
C) MAN
D) Both LAN and WAN have equal transmission speeds.

Q. Which of the following internet service is appropriate to access the computer of your office from home?

A. WWW
B. IRC
C. FTP
D. Telnet

- ✓ Any application that empowers users to remotely access another computer(no matter how far away) is called remote access.
- ✓ Telnet is an application protocol that uses a virtual terminal connection to offer bidirectional interactive text-oriented communication over the Internet.
- ✓ Telnet facilitates remote login on a computer.
- ✓ It also facilitates terminal emulation purposes.
- ✓ Telnet was developed in 1969.
- ✓ Telnet allows users to execute various application programmes on a distant site and then transport the results back to their local computer.

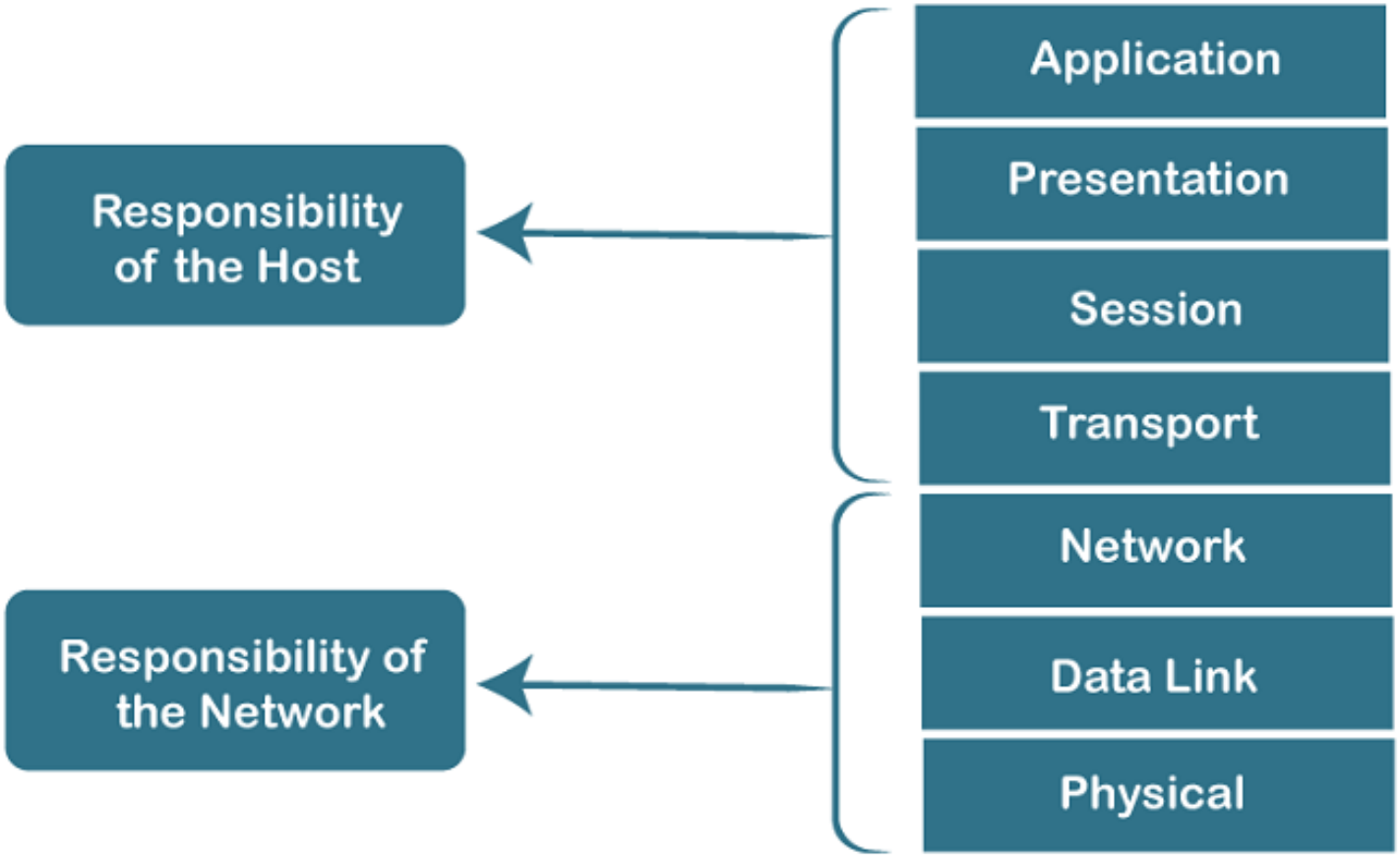
- ✓ **Real-Time Protocol (RTP)** is a protocol designed to handle real-time traffic (like audio and video) of the Internet.

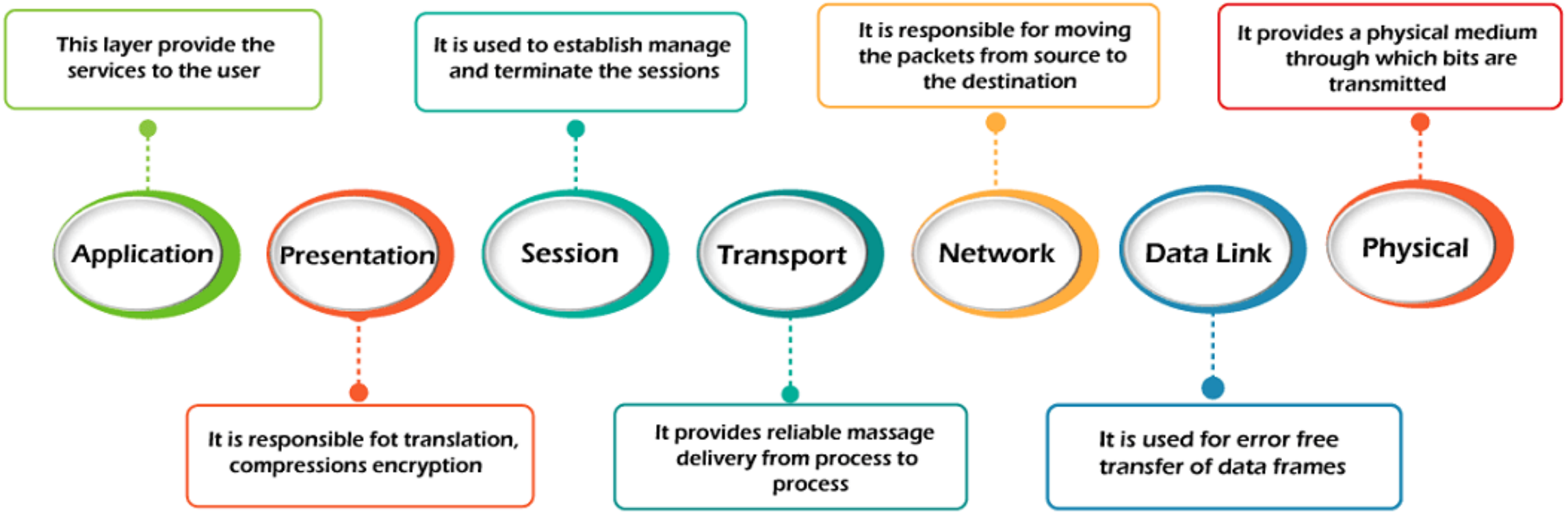
- ✓ **File Transfer Protocol** is a set of rules that govern how computers transfer files from one system to another over the internet

Q. The design issue of Datalink Layer in OSI Reference Model is

A. Framing
B. Representation of bits
C. Synchronization of bits
D. Connection control

Characteristics of OSI Model





Functions of a Physical layer:

- ✓ **Line Configuration:** It defines the way how two or more devices can be connected physically.
- ✓ **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ✓ **Topology:** It defines the way how network devices are arranged.
- ✓ **Signals:** It determines the type of the signal used for transmitting the information.

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.

Functions of the Data-link layer

- ✓ **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.

Functions of the Data-link layer

- ✓ **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.

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).

Functions of Transport Layer:

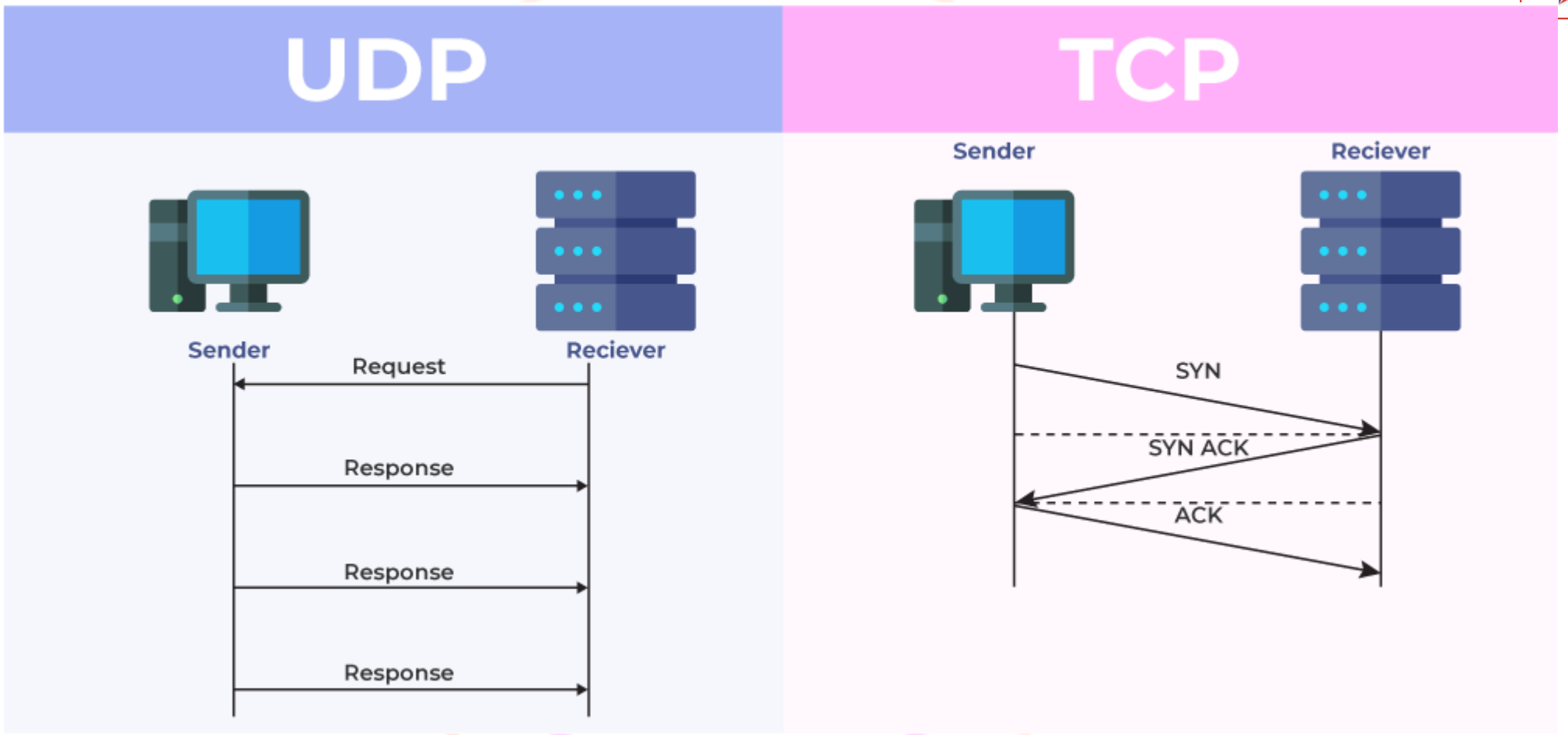
- ✓ **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the 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.

Functions of Transport Layer:

- ✓ **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.

Functions of Transport Layer:

- ✓ **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.



Protocol	TCP	UDP
Connection	connection-oriented	connectionless
Usage	high reliability, critical-less transmission time	fast, efficient transmission, small queries, huge numbers of clients
Ordering of data packets	rearranges packets in order	no inherent order
Reliability	yes	no
Streaming of data	read as a byte stream	sent and read individually
Error checking	error checking and recovery	simply error checking, no error recovery
Acknowledgement	acknowledgement segments	no acknowledgment

Functions of Transport Layer:

- ✓ **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.

Functions of Session layer:

- ✓ **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- ✓ **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

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.

Functions of Presentation layer:

- ✓ **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.

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.

Q. Coaxial cables are categorized by Radio Government rating are adapted for specialized functions. Category RG-59 with impedance 75Ω used for

a. Cable TV
b. Ethernet
c. Thin Ethernet
d. Thick Ethernet

Q. Match the following :

List – I	List – II
a. Application layer	1. TCP
b. Transport layer	2. HDLC
c. Network layer	3. HTTP
d. Data link layer	4. BGP

Codes : a b c d

a. 2 1 4 3

b. 3 4 1 2

c. 3 1 4 2

d. 2 4 1 3

Q. Which layer of OSI reference model is responsible for decomposition of messages and generation of sequence numbers to 'ensure correct re-composition from end to end of the network?‘

a. Physical
b. Data-link
c. Transport
d. Application

Q. The period of a signal is 10 ms. What is its frequency in Hertz?

a. 10
b. 100
c. 1000
d. 10000