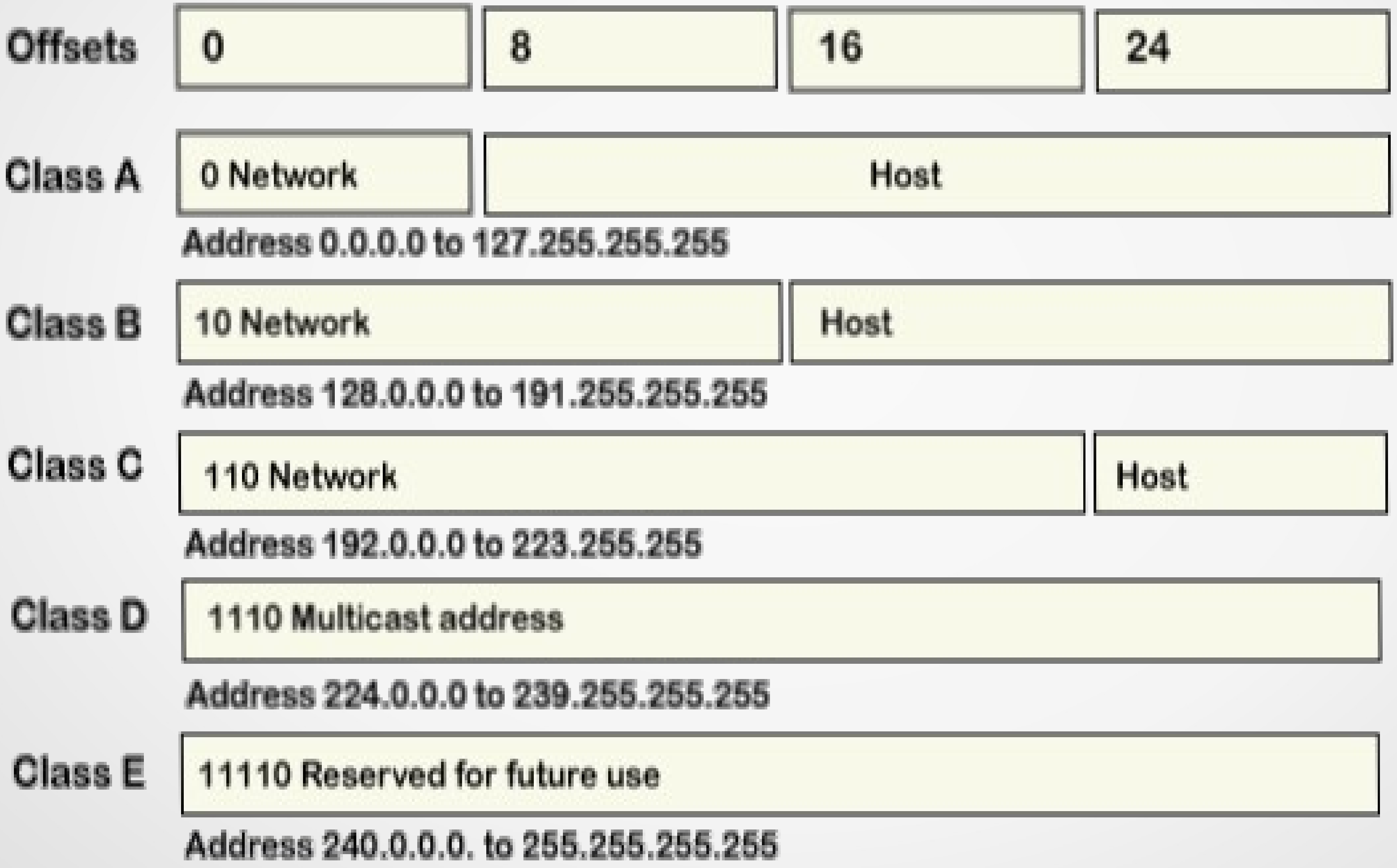
IP address

What is an IP Address?

- An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication.
- IP address act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source.
- IP address is an address having information about how to reach a specific host, especially outside the LAN.
- An IP address is a 32 bit unique address having an address space of 232.

- IP addresses were divided into five different categories called classes.
- These divided IP classes are class A, class B, class C, class D, and class E.
- classes A, B, and C are most important. Each address class defines a different number of bits for its network prefix (network address) and host number (host address).



Offsets 0 8 16 24

Class A 0 Network Host

Address 0.0.0.0 to 127.255.255.255

Class B 10 Network Host

Address 128.0.0.0 to 191.255.255.255

Class C 110 Network Host

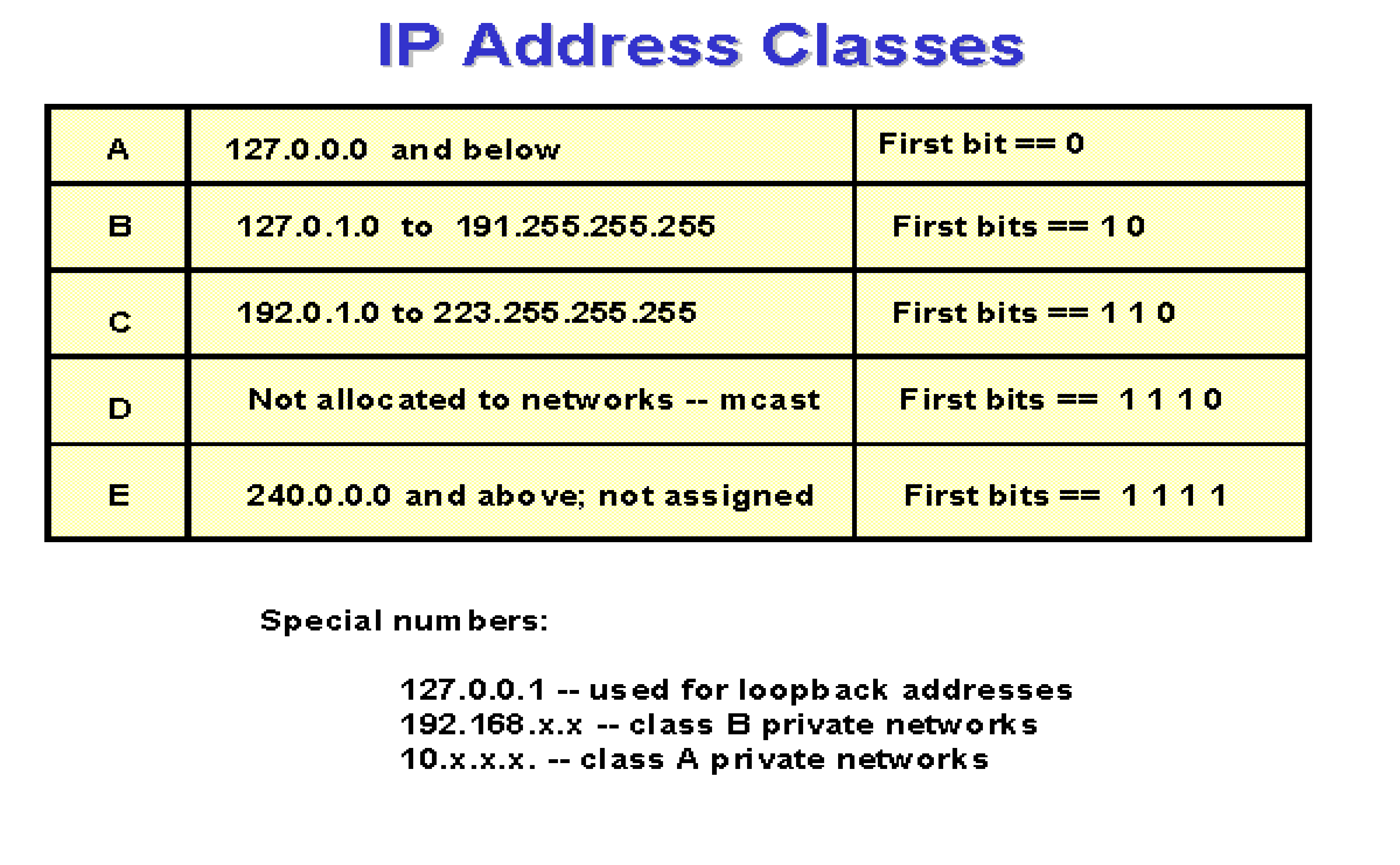
Address 192.0.0.0 to 223.255.255

Class D 1110 Multicast address

Address 224.0.0.0 to 239.255.255.255

Class E 11110 Reserved for future use

Address 240.0.0.0. to 255.255.255.255

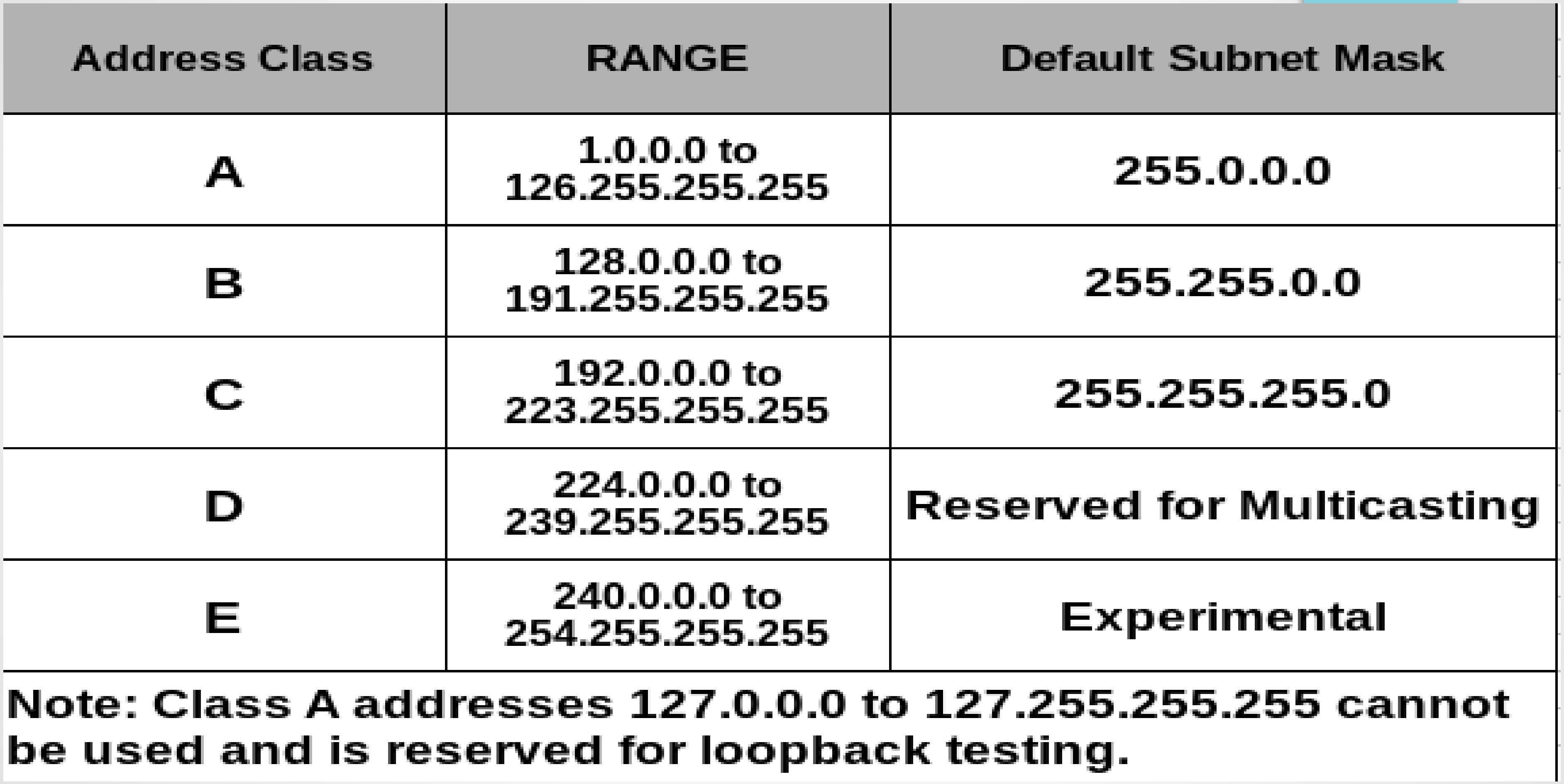


IP Address Classes

A	127.0.0.0 and below	First bit == 0
B	127.0.1.0 to 191.255.255.255	First bits == 1 0
C	192.0.1.0 to 223.255.255.255	First bits == 1 1 0
D	Not allocated to networks -- mcast	First bits == 1 1 1 0
E	240.0.0.0 and above; not assigned	First bits == 1 1 1 1

Special numbers:

127.0.0.1 -- used for loopback addresses
192.168.x.x -- class B private networks
10.x.x.x. -- class A private networks



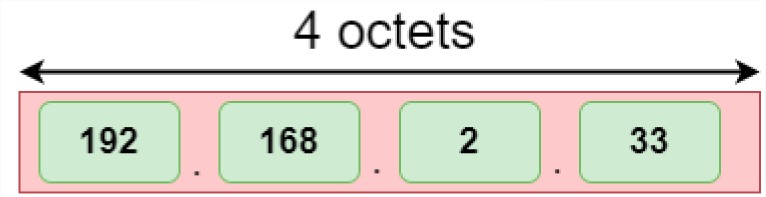
Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

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

- IPv4 (Internet Protocol version 4)
- IPv6 (Internet Protocol version 6)

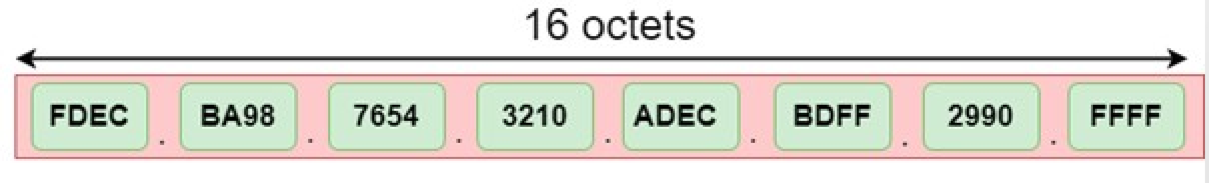
What is IPv4?

- IPv4 is version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by a dot (.), i.e., periods. This address is unique for each device



What is IPv6?

- IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong.
- IPv6 is the next generation of IP addresses.
- The main difference between IPv4 and IPv6 is the address size of IP addresses.
- The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address.
- IPv6 provides a large address space, and it contains a simple header as compared to IPv4.



Introduction to CIDR

- **CIDR (Classless Inter-Domain Routing or supernetting)** is a method of assigning IP addresses that improves the efficiency of address distribution and replaces the previous system based on Class A, Class B and Class C networks.
- CIDR IP addresses consist of two groups of numbers, which are also referred to as groups of bits.
- The most important of these groups is the network address, and it is used to identify a network or a sub-network (subnet).
- In contrast to classful routing, which categorizes addresses into one of three blocks, CIDR allows for blocks of IP addresses to be allocated to internet service providers.

Domain Name System

- The Domain Name System (DNS) is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks.
- It associates various information with domain names assigned to each of the associated entities.
- DNS is a core internet technology that translates human-friendly domain names into machine-usable IP addresses.

  Example : 128.66.111.102 – Exam Moodle

- The DNS operates as a distributed database, where different types of DNS servers are responsible for different parts of the DNS name space.

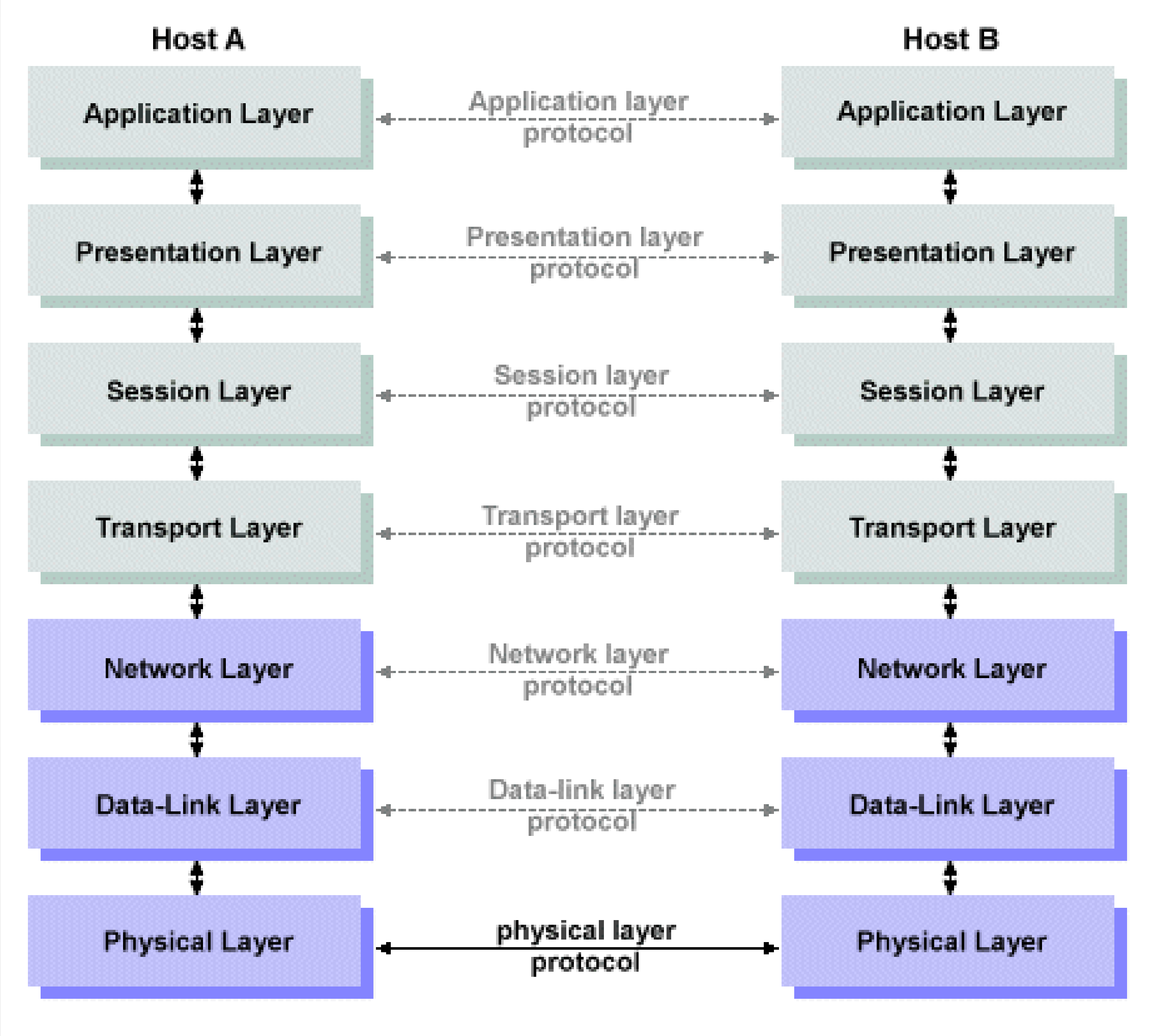
OSI Model

- The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.

- OSI model has seven layers.and each layer performs a particular network function.

- The layers may be listed in a top-to-bottom or bottom to top order.
- 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 model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.


Host A
Host B
Application Layer
Application layer protocol
Application Layer
Presentation Layer
Presentation layer protocol
Presentation Layer
Session Layer
Session layer protocol
Session Layer
Transport Layer
Transport layer protocol
Transport Layer
Network Layer
Network layer protocol
Network Layer
Data-Link Layer
Data-link layer protocol
Data-Link Layer
Physical Layer
physical layer protocol
Physical Layer

1) 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 bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

2) Data Link Layer

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

3) Network Layer

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

4) Transport Layer

Segmentation : This layer accepts the message from the (session) layer, and breaks the message into smaller units.The transport layer at the destination station reassembles the message.

- **Service Point Addressing :** In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address

5) Session Layer

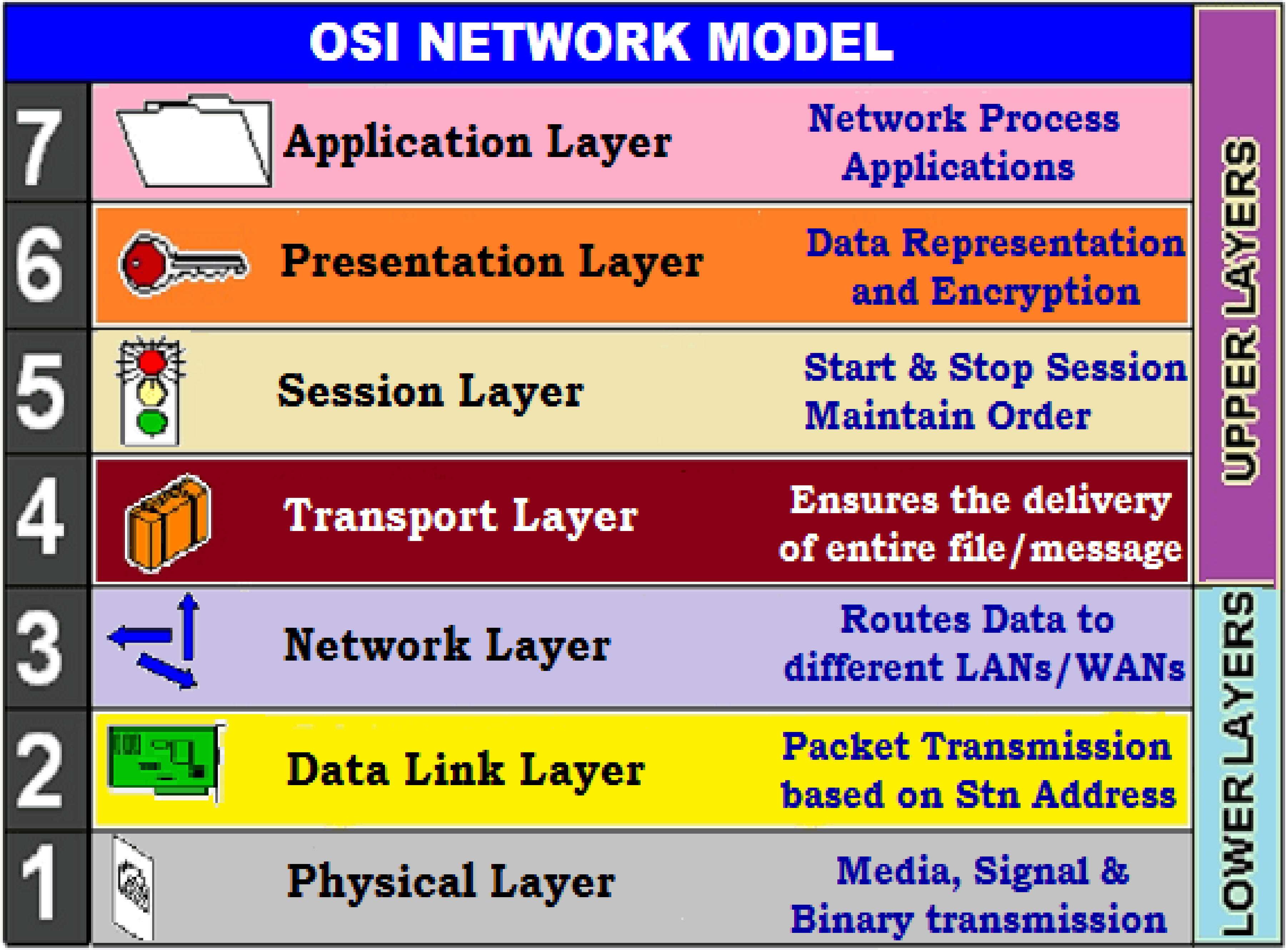
- Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into the data.
- These synchronization points help 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.

6) Presentation Layer

- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

7) Application Layer

- Application Layer is also called Desktop Layer.
- These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- Example: Application – Browsers, Skype Messenger, etc.



OSI NETWORK MODEL

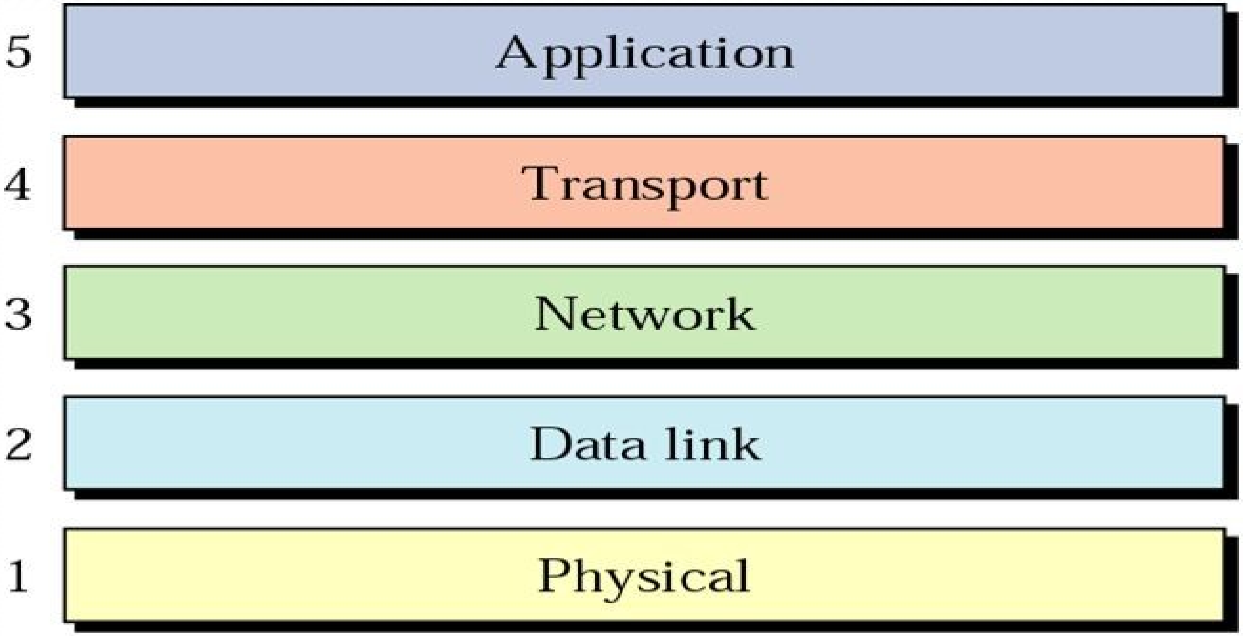
7	Application Layer	Network Process Applications	UPPER LAYERS
6	Presentation Layer	Data Representation and Encryption	
5	Session Layer	Start & Stop Session Maintain Order	
4	Transport Layer	Ensures the delivery of entire file/message	
3	Network Layer	Routes Data to different LANs/WANs	LOWER LAYERS
2	Data Link Layer	Packet Transmission based on Stn Address	
1	Physical Layer	Media, Signal & Binary transmission	

TCP/IP Model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

Internet layers

- The TCP/IP protocol suite is made of 5 layers



5 Application

4 Transport

3 Network

2 Data link

1 Physical

- **Layer**
  - **A grouping of related tasks involving the transfer of information .**
  - **Each layer addresses an essential networking tasks**

Protocols

- A protocol is a set of rules and guidelines for communicating data.
- Rules are defined for each step and process during communication between two or more computers.
- Networks have to follow these rules to successfully transmit data

Application Layer protocols

Telnet :

- 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.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer.
- 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. Telnet is an abbreviation for Terminal Network.
- Two types of login possible : Local Login And Remote Login
-

- 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. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform.

- They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

- **HTTP**
- **HTTP stands for HyperText Transfer Protocol.**
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

- **FTP**
- File Transfer Protocol (FTP) is an application layer protocol that is used to transfer the files between the local devices (PC, smartphone, etc.) to a server. It transfers both text and binary files over the Internet.
- FTP opens two connections between the computers − one for the commands and replies (control connection) and a second one for data transfers (data connection).
- FTP is built on a client-server model architecture using the control connection and data connection between the client and server.

- **TFTP**
- The benefit of using TFTP is that it enables bootstrapping code to use the similar underlying TCP/IP protocols that the operating framework uses once it starts execution. Thus it is the possibility for a device to bootstrap from a server on another physical network.
- **The main features of TFTP are as follows**−
- TFTP is based on the client-server principle and uses well-known UDP port number 69 for the TFTP server.
- TFTP is an unsecured protocol and does not support authentication.
- TFTP incorporates idle − RQ (stop and wait) error recovery mechanism.
- Every TFTP data unit bears a sequence number.
- Each data unit is separately acknowledged. After taking the acknowledgement, the next data unit is transmitted.
- Error recovery is by retransmission after timeout. TFTP uses adaptive timeout with an exponential back-off algorithm.

- **FTP**
- File Transfer Protocol (FTP) is an application layer protocol that is used to transfer the files between the local devices (PC, smartphone, etc.) to a server.
- It transfers both text and binary files over the Internet.

  FTP opens two connections between the computers − one for the commands and replies (control connection) and a second one for data transfers (data connection).
- FTP is built on a client-server model architecture using the control connection and data connection between the client and server.

IEEE standards

- The IEEE standards in computer networks ensure communication between various devices; it also helps to make sure that the network service.
- IEEE 802 LAN/MAN Standards Committee. ...
- IEEE 802.1 Higher Layer LAN Protocols Working Group. ...
- IEEE 802.3 Ethernet Working Group. ...
- IEEE 802.11 Wireless LAN Working Group. ...
- IEEE 802.15 Working Group for Wireless Specialty Networks. ...

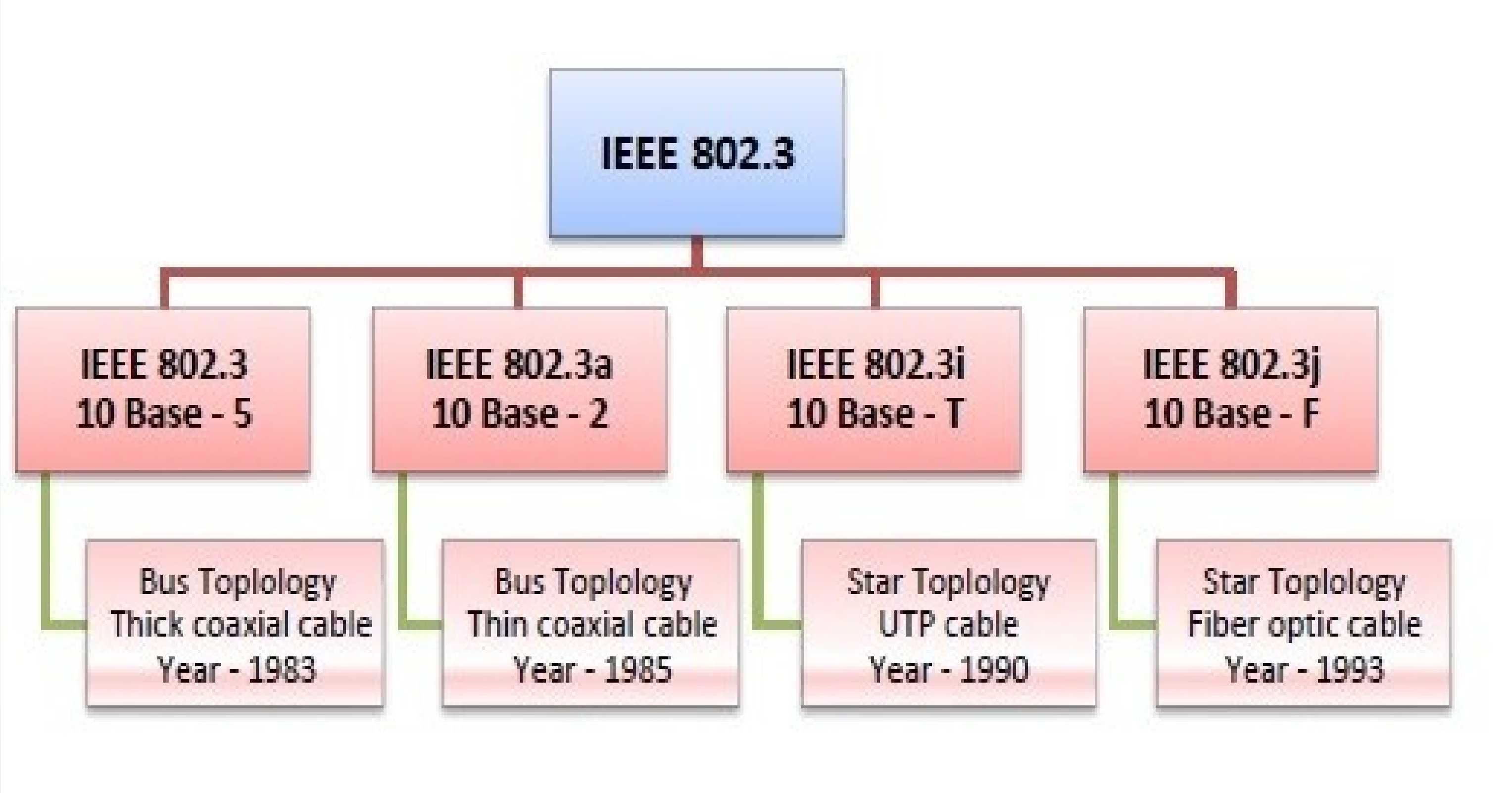
802.1

- IEEE 802.1 handles the architecture, security, management and internetworking of local area networks (LAN), metropolitan area networks (MAN) and wide area area networks (WAN) standardized by IEEE 802.
- **The following are key IEEE 802.1 tasks:**

  Designs and implements standards that regulate network management practices
- Provides services, including LAN/MAN management, media access control (MAC) bridging, data encryption/encoding and network traffic management.
- IEEE 802.1 is comprised of four groups that focus on different standards and policies in the following areas:
- Internetworking
- Audio/video (A/V) bridging
- Data center bridging
- Security

802.3

- IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks.
- Ethernet Technology used in LANs, MANs.
- IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.
- **There are a number of versions of IEEE 802.3 protocol. The most popular ones are.**
- IEEE 802.3: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core.
- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors.
- IEEE 802.3i: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.
-



IEEE 802.3

IEEE 802.3
10 Base - 5

Bus Toplology
Thick coaxial cable
Year - 1983

IEEE 802.3a
10 Base - 2

Bus Toplology
Thin coaxial cable
Year - 1985

IEEE 802.3i
10 Base - T

Star Toplology
UTP cable
Year - 1990

IEEE 802.3j
10 Base - F

Star Toplology
Fiber optic cable
Year - 1993

802.11

- 802.11 is an IEEE standard which defines Wireless Local Area Network (WLAN) or WiFi.
- It covers all WLAN series of products. It is optimized for nearly 100 meters.
- It does not provide the service throughout the coverage area to enable continuous connectivity.
- This 802.11 standard provides less scalability in usability point of view.

802.16

- 802.16 is an IEEE standard which defines Wireless Inter-operability for Microwave Access (WiMAX) technology products.
- It covers all WiMAX series of products. It is optimized for 50 km.
- It provides the service throughout the coverage area to enable continuous connectivity.
- This 802.16 standard provides more scalability in usability point of view.