2... Network Models

Objectives...

- To learn about OSI and TCP/IP reference Models
- To study TCP/IP Protocol Suite
- To get information about IP addressing

2.1 NETWORK MODELS

- A Network Model reflects a design or architecture to accomplish communication between different systems. Network models are also referred to as network stacks or protocol suites. Examples of network models includes TCP/IP, Sequenced Packet Exchange/Internet Packet Exchange (SPX/ IPX) used by Novell Netware, the Network Basic Input Output System (Net-BIOS), which comprises the building blocks for most Microsoft networking and network applications; and AppleTalk, the network model for Apple Macintosh computers.
- A network model usually consists of layers. Each layer of a model represents specific functionality. Within the layers of a model, there are usually protocols specified to implement specific tasks. You may think of a protocol as a set of rules or a language. Thus, a layer is normally a collection of protocols.
- There are several different network models depending on what organization or company started them. The most important two models are:
  1. **OSI Network Model:** The International Standards Organization (ISO) has defined a standard called the International Organization for Standardization/Open System Interconnection Reference Model (ISO/ OSI-RM, or more simply, OSI-RM). This is a seven layer architecture explained in the next section. This model dominated data communication and networking literature before 1990. The OSI model was never fully implemented.
  2. **TCP/IP Model:** It is also called the Internet Model because TCP/IP is the protocol used on the internet. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet.

2.2 OSI REFERENCE MODEL (W-22, S-23)

- The International Organization for Standardization (ISO) is a worldwide body that promotes standards internationally. ISO-OSI describes the architecture, protocols and services that are needed to achieve this goal. There are multiple ISO-OSI standards. Some of these are complete, while others are still evolving.
- The term open system in ISO-OSI defines a computer system that can communicate with another computer system using the OSI protocol.

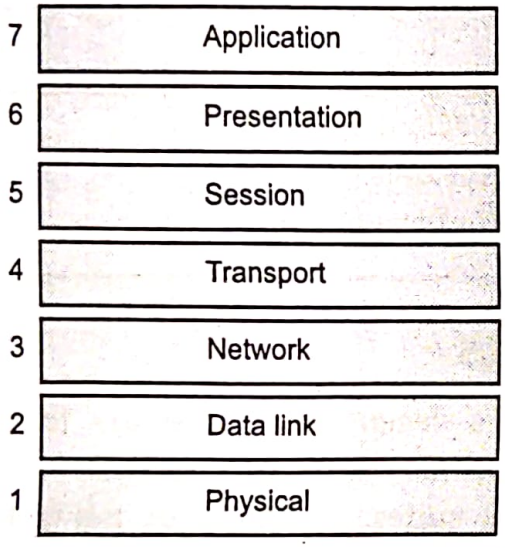


Fig. 2.1: The ISO-OSI Reference Model

- Each layer in the ISO-OSI Reference Model has a name, a number, protocols that provide specific functions, and defined services.
- Because the various intended uses of ISO-OSI are very broad, spanning terminals, personal computers, and very large mainframes, different services and protocol options are available at each layer. This range of support can accommodate different connection requirements and environments.
- Although there are many different architectures, standards and models the ISO-OSI Reference Model is mostly used to explain the different functions implemented in protocols from different layers and how these protocols work together.
- It is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- Seven layered model, higher layers have more complex tasks. Each layer provides services for the next higher layer. Each layer communicates logically with its associated layer on the other computer.
- Packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer. Each layer performs a unique, generic, and well-defined function.
- Layer boundaries are designed so that the amount of information flowing between any two adjacent layers is minimized. This is accomplished by having each layer within an open system use the services provided by the layer below. Conversely, each layer provides a sufficient number of services to the layer immediately above it.

2.2.1 Layers in the OSI Model

(S-18, S-19, W-18)

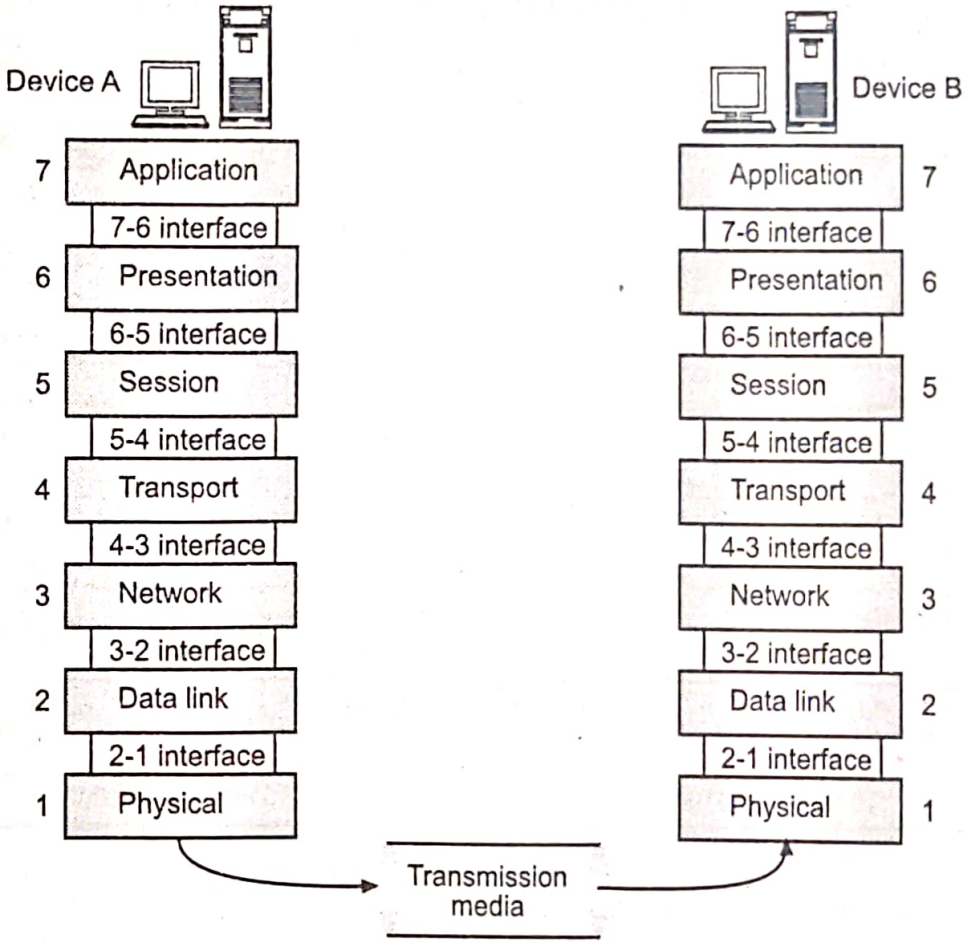


Fig. 2.2: Layered Architecture of the ISO-OSI Model

- Each interface defines what information and services a layer must provide for the layer above it. Layers 1, 2, and 3 are the network support layers; they deal with physical aspect of moving data from one device to another (such as electrical specification, physical connection). Layer 4 ensures end-to-end reliable data transmission. Layers 5, 6, and 7 are user support layers.
- The upper OSI layers are almost always implemented by software; lower layers are a combination of hardware and software, except physical layer, which is mostly hardware.
- This layered approach was selected as a basis for the OSI Reference Model to provide flexibility and open-ended capability through defined interfaces.
- The interfaces permit some layers to be changed while leaving other layers unchanged. In principle, as long as standard interfaces to the adjacent layers are adhered to, an implementation can still work.
- For example, a system implementation could use either HDLC or local area network protocols as the data link layer. Similarly, a particular layer such as the presentation layer can be implemented as a null layer for the time being.

- This means the layer is functionally empty, providing only the mandatory interfaces between the upper and lower layers (application and session layers respectively).

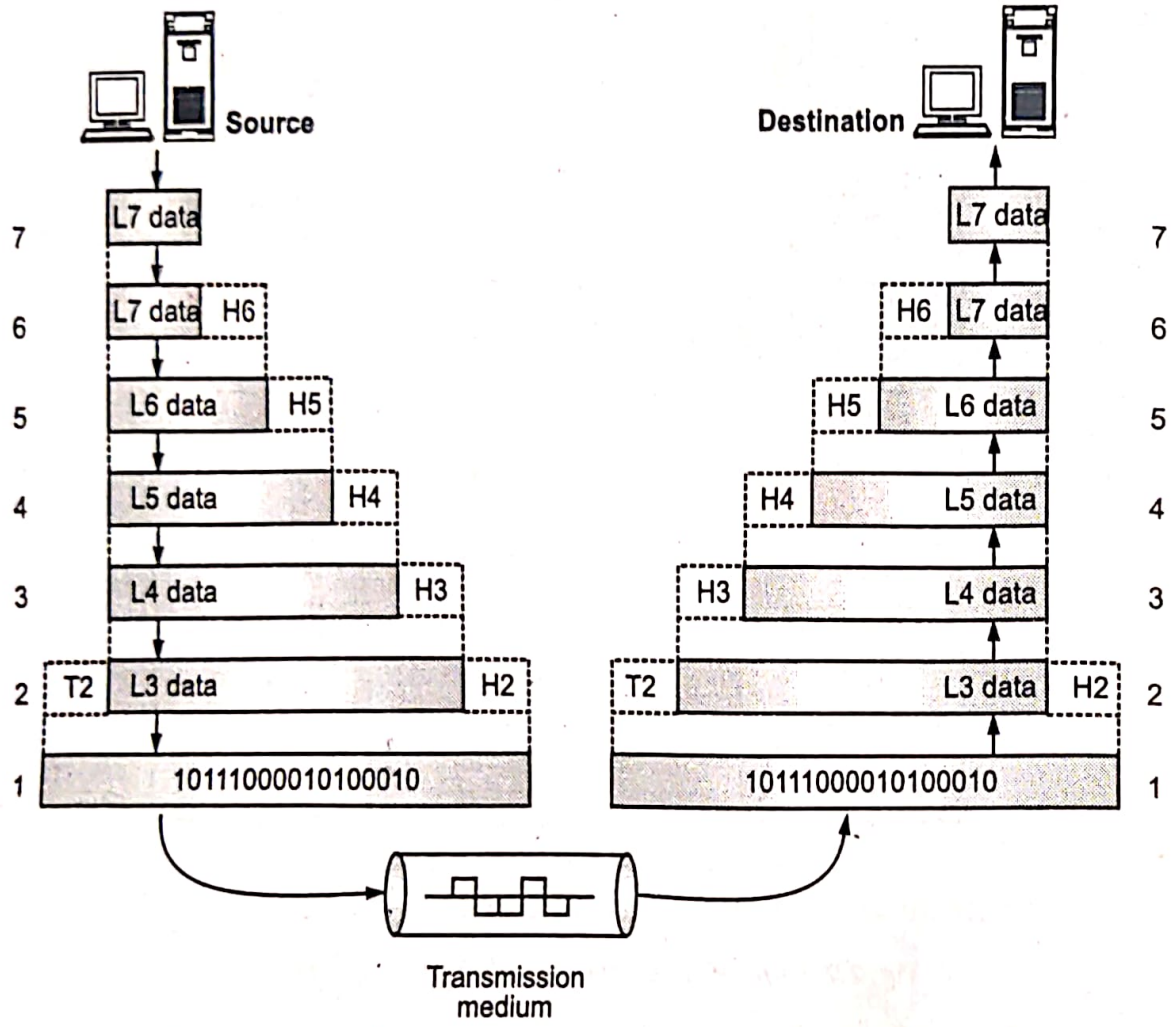


Fig. 2.3: Data Exchange using OSI Model

2.2.2 Functions of Each Layer (W-22)

- In this section, we will discuss the functions of each layer in the OSI model.

1. Physical Layer:

- The **Physical Layer** is the lowest layer (1st) of the OSI model.
- Physical layer deals with the mechanical and electrical specifications of the interface and transmission medium.
- Transmits the unstructured raw bit stream over a physical medium.
- Relates the electrical, optical mechanical and functional interfaces to the cable.
- Physical layer also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- Defines data encoding and bit synchronization.

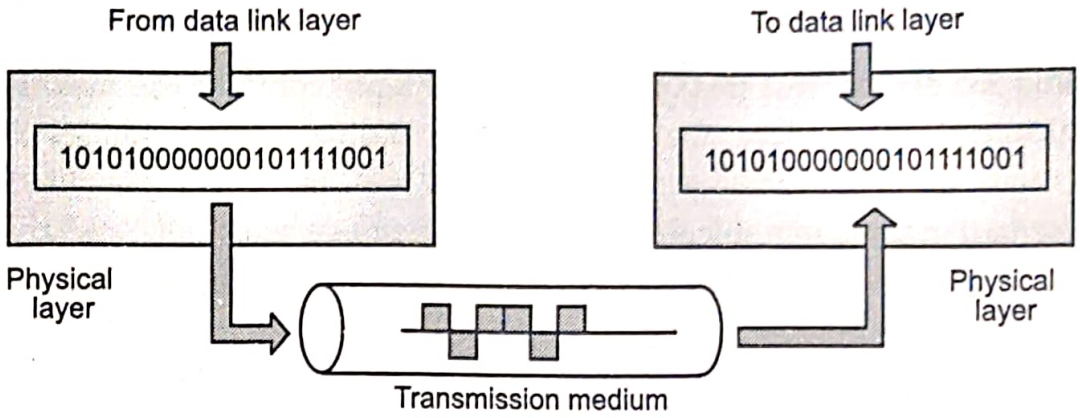


Fig. 2.4: Physical Layer

Responsibilities or functions of the Physical Layer:

(i) **Physical characteristics of Interfaces and Medium:** Physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

(ii) **Representation of Bits (Data Encoding):** Data consist of a stream of bits (0's and 1's). Any transmission medium doesn't understand about computer data i.e. 0 and 1, it understands only about signal. Physical layer converts binary data into signals and vice versa. To be transmitted, bits must be encoded into signals-electrical or optical. The physical layer defines the different types of encoding methods.

(iii) **Data rate:** The transmission rate i.e. the number of bits sent per second.

(iv) **Synchronization of bits:** The sender and receiver must use the same bit rate as well as must be synchronized at the bit level. The sender and receiver clocks must be synchronized.

(v) **Physical Topology:** It defines how devices are connected to make a network. For example, a *star topology* (devices are connected through a central device), a *ring topology* (every device is connected to the next).

(vi) **Transmission mode:** It 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.

2. Data Link Layer:

- The 2nd layer of the OSI model is the Data link layer.
- It makes the physical layer appear error free to the upper layer.
- Sends data frames from the Network layer to the Physical layer.
- Packages raw bits into frames for the Network layer at the receiving end.
- Responsible for providing error free transmission of frames through the Physical layer.

- This layer is often divided into two parts:

(i) **Media Access Control (MAC):** The MAC sub layer controls the means by which multiple devices share the same media channel. This includes contention methods and other media access details. The MAC layer also provides addressing information for communication between network devices.

(ii) **Logical Link Control (LLC):** The LLC sub layer establishes and maintains links between communicating devices.

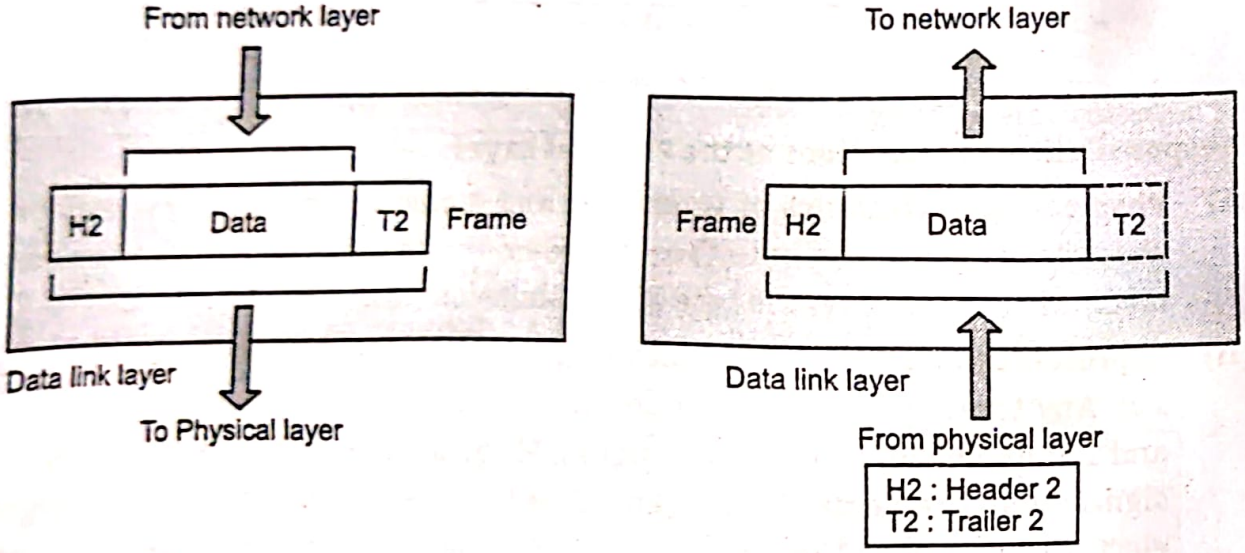


Fig. 2.5: Data Link Layer

Responsibilities or Functions of the Data Link Layer:

(i) **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames. Data link layer performs various framing functions like Frame Traffic Control, Frame Sequencing, Frame Delimiting and so on.

(ii) **Physical addressing:** If frames are distributed to different system on the network, the data link layer adds header to the frame to define the physical address of the sender (source address) and receiver address (destination address) of the frame. If the frame is intended for the system outside the sender's network, the receiver address is the address of device that connects one network to the next.

(iii) **Flow control:** Flow control is the traffic regulatory mechanism implemented by Data Link layer. If the rate at which the data are absorbed by receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism.

(iv) ***Error control:*** *It adds reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames. It also prevents duplication of frames.*

(v) **Access control:** When two or more devices are connected to the same link, data link layer protocols determine which device has control over the link at any given time.

3. Network Layer:

- The 3rd layer of the OSI model is the Network Layer.
- The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks (links). Whereas, the data link layer oversees the delivery of the packet between two systems on the same network (links). If two systems are connected to the same link, there is usually no need for a network layer.

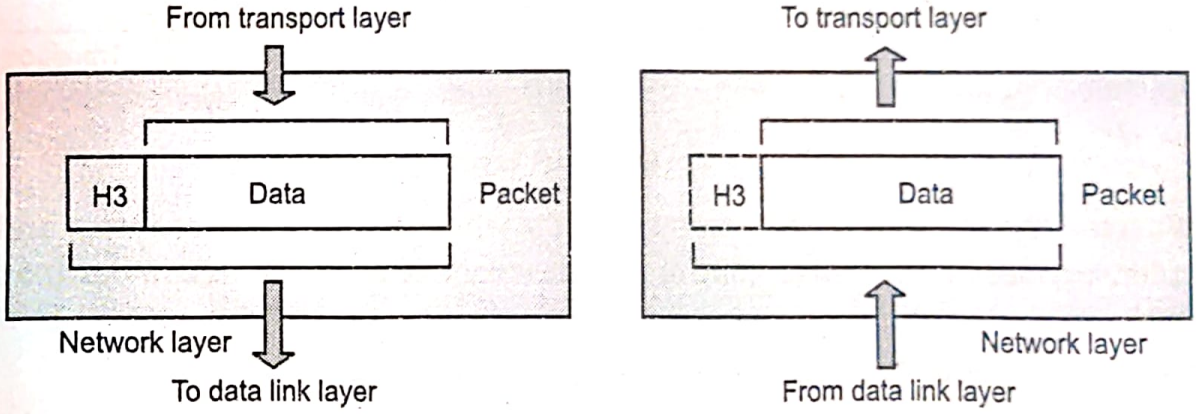


Fig. 2.6: Network Layer

Responsibilities or Functions of Network Layer:

(i) **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, then need of another addressing system to help to distinguish the source and destination systems.

(ii) **Routing:** When independent networks or links are connected together to create an internetwork (a network of networks), the connecting devices (called router or gateway) route the packets to their final destination.

(iii) **Congestion Control:** This layer is also responsible for handling the congestion problem at the node, when there are too many packets stored at the node to be forwarded to the next node.

(iv) **Internetworking:** One of the main responsibilities of network layer is to provide internetworking between different networks. It provides logical connection between different types of network.

4. Transport Layer:

- The 4th layer of the OSI model is the Transport Layer.
- The transport layer is responsible for source-to-destination, (end-to-end) delivery of the entire message.

- Network layer treats each packet independently, as though each packet belonged to a separate message, whether or not it does.

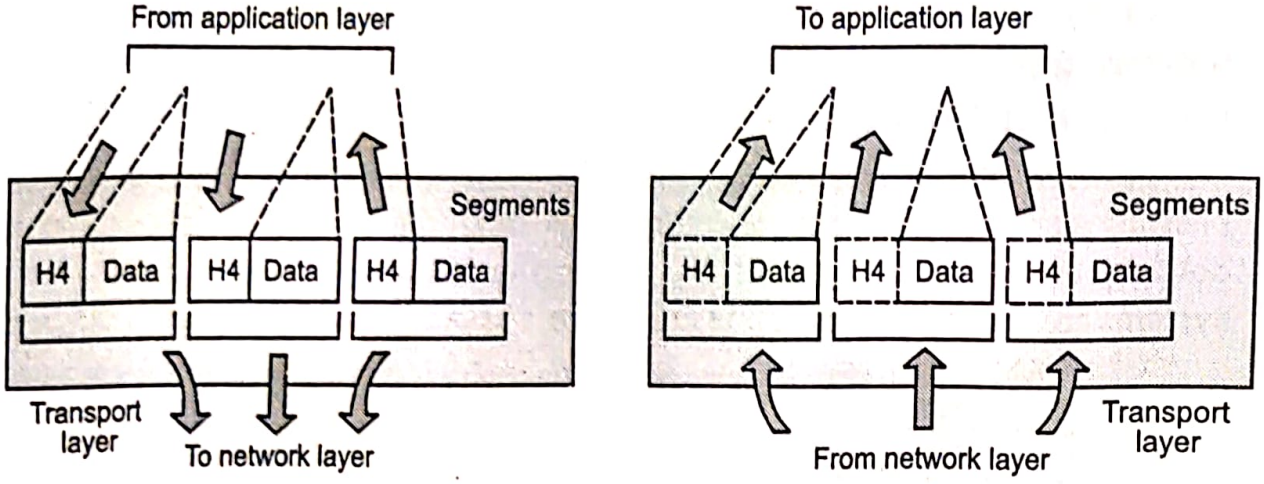


Fig. 2.7: Transport Layer

- Whereas, the transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the Source-to-destination level.

Responsibilities or Functions of the Transport Layer:

(i) Service-point Addressing (Port Addressing): Computers often run multiple programs at the same time.

- Source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on the other. The transport layer header therefore must include a type of address called a Service-point address (or port address).
- Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process on destination machine.

(ii) Segmentation and Reassembly: A message is divided into transmittable segments; each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in the transmission.

(iii) Connection control: It creates a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. The transport layer can provide connection oriented or connectionless services for connection control.

- A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination.
- A connection oriented transport layer makes a connection with destination transport layer first and then delivers data. After all data transfer is done, the connection is terminated.

(iv) **Flow control:** Transport layer makes sure that the sender and receiver communicate at the rate they both can handle. Flow control at this level is performed end to end rather than across a single link.

(v) **Error control:** Error control at this level is performed end to end. The transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss or duplication).

5. Session layer:

- The 5th layer of the OSI model is the Session Layer.
- Session layer has the primary responsibility of beginning, maintaining and ending the communication between two devices, which is called Session.
- It also provides for orderly communication between devices by regulating the flow of data.
- The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction between communicating systems.

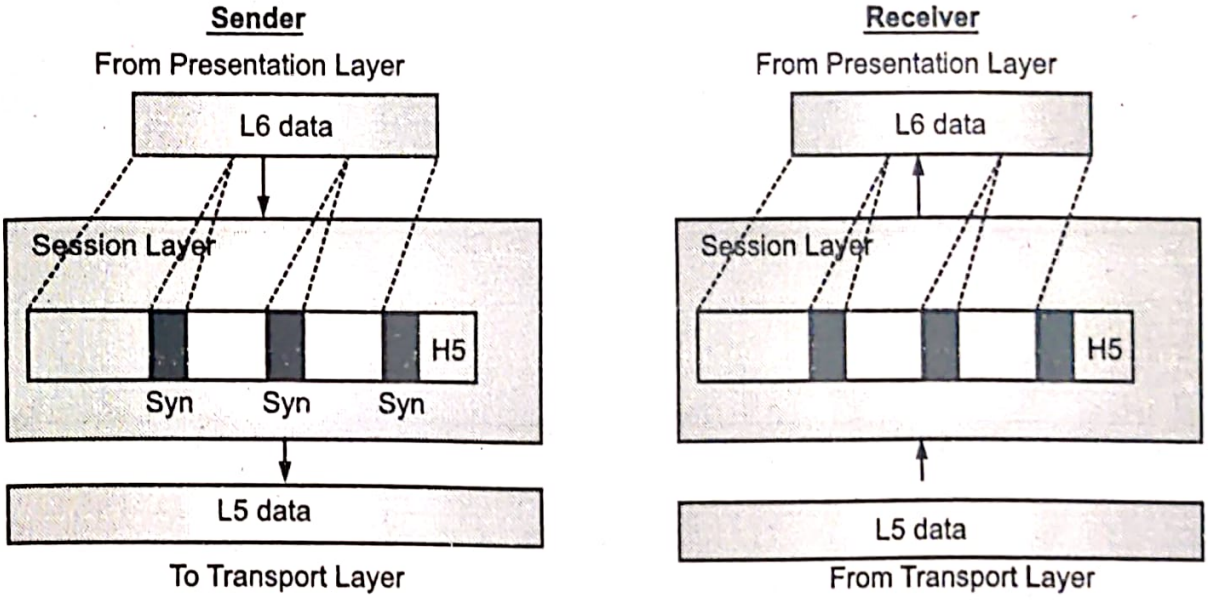


Fig. 2.8: Session Layer

- Above figure shows the relationship of the Session layer to the transport layer and presentation layer.

Responsibilities of the Session Layer:

(i) **Dialog control:** Dialog control is the function of session layer that determines which device will communicate first and the amount of data that will be sent. It also decides the communication between two processes to take place in either half duplex or full duplex mode.

(ii) **Token management:** Preventing two parties from attempting the same critical operation at the same time.

(iii) **Synchronization:** It allows a process to add checkpoints (synchronization points) into a stream of data. Use of checkpoints for long transmission allows them to continue from where they were after a crash.

For example, if a system sending a file of 2000 pages and process inserts checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. If crash happens during transmission of page 545, retransmission begins at page 501; pages 1 to 500 need not be retransmitted.

6. Presentation Layer:

- The 6th layer of the OSI model is the presentation layer. Presentation Layer is also called Translation layer.
- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The presentation layer is concerned with the representation of user or system data. This includes necessary conversions, (For example, printer control characters) and code translation (For example, ASCII to or EBCDIC).

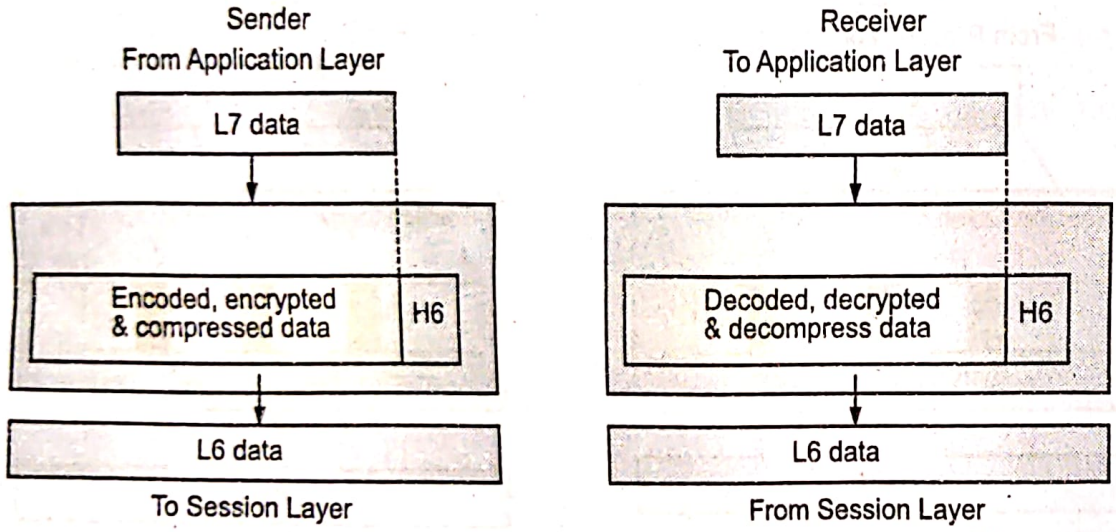


Fig. 2.9: Presentation Layer

Responsibilities or functions of the Presentation layer:

(i) **Translations:** Different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependant format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependant format.

(ii) **Encryption:** Converting computer data into non-readable form is encryption. It is required for important data transmission. Decryption reverses the original process to transform the message back to its original form.

(iii) **Compression:** Reduces the number of bits to be transmitted. Saves network bandwidth. Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.

7. Application Layer:

- The 7th layer of the OSI model is the Application Layer.
- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as e-mail, remote file access and transfer, shared database management and other types of distributed information services. Application layer is responsible for providing services to the user.

Services provided by the Application Layer:

(i) **Network Virtual Terminal (NVT):** A network virtual terminal is a software version of a physical terminal and it allows a user to log onto a remote host. The remote host believes it is communicating with one of its own terminal and allows the user to log on.

(ii) **File Transfer, Access and Management (FTAM):** This application layer protocol allows a user to access files in remote computer (to make changes or read data), to retrieve files from a remote computer and to manage or control files in a remote computer.

(iii) **Mail services:** This application provides the basis for e-mail forwarding and storage.

(iv) **HTTP (HyperText Transfer Protocol):** A standard Internet protocol that specifies the client/server interaction processes between Web browsers such as Microsoft Internet Explorer and Web servers such as Microsoft Internet Information Services (IIS).

2.2.3 Summary of ISO-OSI Layer Functions

Table 2.1: Summary of ISO-OSI Model Layers

OSI Layers	Functions
APPLICATION Message/data	Service advertisement, service availability. Manages communications between applications. (FPDAM) File, Print, Database, Application, and Messaging services. Allows applications to use the network. Handles network access, flow control and error recovery.

Contd...

PRESENTATION Message/data	Translation, compression, encryption, data conversion. Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression.
SESSION Message/data RPC (Remote Procedure calls) functions here.	Connection establishment, data transfer, connection release (Half-duplex, Full- duplex, Simplex). Allows applications on connecting systems to establish a session. Provides synchronization between communicating computers.
TRANSPORT Segments (or Datagrams)	Service addressing, segmentation and transport control, flow control, end-to-end data integrity. Responsible for packet handling. Ensures error-free delivery. Repackages messages, divides messages into smaller packets and controls error handling.
NETWORK Packets (or Datagrams)	Logical addressing, switching, routing, network control. Translates system names into addresses. Determines routes for sending data and manages network traffic problems, packet switching, routing, data congestion and reassembling data.
DATA LINK Frames	Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. LLC Layer (Logical Link Control): flow control and timing (802.2). Manages link control and defines SAPs (Service Access Points). MAC Layer (Media Access Control): framing and physical addressing (802.3, 802.4, 802.5, 802.12). Communicates with adapter card.
PHYSICAL Bits is concerned with definition of low level functions (voltage, media types)	Transmits data over a physical medium. Defines cables, cards and physical aspects as well as electrical properties, transmission media, transmission devices, physical topology, data signaling, data synchronization and data bandwidth. Manages data placement on and data removal from the network media.

2.3 TCP/IP REFERENCE MODEL (W-18)

- The TCP/IP Reference Model is sometimes called the *Internet Reference Model* or the *DoD Model*. The TCP/IP model or Internet Protocol Suite, describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network.

- TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers.

2.3.1 What is TCP/IP ?

- The name TCP/IP refers to a suite of data communication protocols. Its name comes from two of the more important protocols in the suite: the *Transmission Control Protocol (TCP)* and the *Internet Protocol (IP)*.
- TCP/IP originated out of the investigative research into networking protocols that the Department of Defense (DoD) initiated in 1969. In 1968, the DoD Advanced Research Projects Agency (ARPA) began researching the network technology that is now called *packet switching.*
- The original focus of this research was to facilitate communication among the DoD community. However, the network that was initially constructed as a result of this research then called ARPANET, gradually became known as the Internet.
- The TCP/IP protocols played an important role in the development of the Internet. In the early 1980s, the TCP/IP protocols were developed. In 1983, they became standard protocols for ARPANET.
- Because of the history of the TCP/IP protocol suite, it is often referred to as the **DoD protocol suite** or the **Internet Protocol Suite**.
- It is built into UNIX, and is available for most other operating systems.
- TCP/IP is not one protocol, but is a suite of many protocols. The protocols define applications, transport controls, networking, routing, and network management. It is today's most widely used multivendor interoperability protocol. (The other major multivendor interoperability protocol, OSI, is not yet completely defined and not widely used.)
- TCP/IP is a routable protocol that is suitable for connecting dissimilar systems (such as Microsoft Windows and UNIX) in heterogeneous networks, and it is the protocol of the worldwide network known as the Internet.

2.3.2 Layers of TCP/IP Model (W-22, S-22)

- TCP/IP Model contains following Layers:

1. Application Layer:

- The top layer in the Internet reference model is the *application layer.* This layer provides functions for users or their programs, and it is highly specific to the application being performed.
- It provides the services that user applications use to communicate over the network, and it is the layer in which user-access network processes reside.

- These processes include all of those that users interact with directly, as well as other processes of which the users are not aware.
- This layer includes all applications protocols that use the host-to-host transport protocols to deliver data. Other functions that process user data, such as data encryption and decryption and compression and decompression, can also reside at the application layer.
- The application layer also manages the sessions, (connections) between cooperating applications.
- In the TCP/IP protocol hierarchy, sessions are not identifiable as a separate layer, and these functions are performed by the host-to-host transport layer.
- Instead of using the term "session," TCP/IP uses the terms "socket" and "port" to describe the path (or virtual circuit) over which cooperating applications communicate.
- Most of the application protocols in this layer provide user services, and new user services are added often.
- For cooperating applications to be able to exchange data, they must agree about how data is represented.
- The application layer is responsible for standardizing the presentation of data.

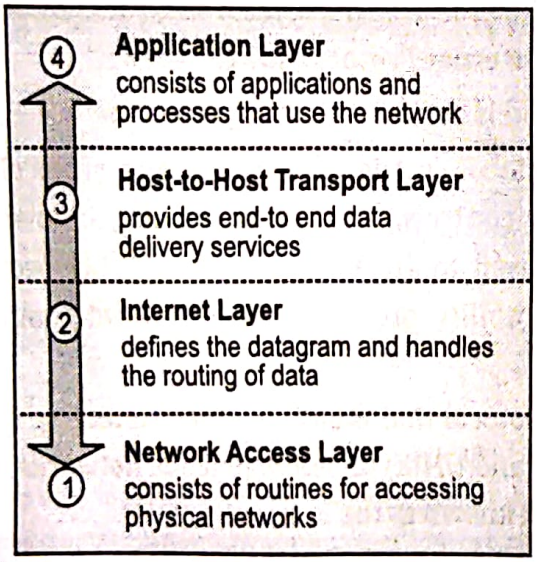


Fig. 2.10: Layers in the TCP/IP Protocol Architecture

2. Host-to-Host Transport Layer:

- The protocol layer just above the internet layer is the *host-to-host transport layer.* It is responsible for providing end-to-end data integrity and provides a highly reliable communication service for entities that want to carry out an extended two-way conversation.
- In addition to the usual transmit and receive functions, the host-to-host transport layer uses *open* and *close* commands to initiate and terminate the connection.

- This layer accepts information to be transmitted as a *stream* of characters, and it returns information to the recipient as a stream.
- The service employs the concept of a connection (or *virtual circuit). A connection is* the state of the Host-to-Host transport layer between the time that an open command is accepted by the receiving computer and the time that the close command is issued by either computer.

3. Internet Layer:

- In the Internet reference model, the layer above the network access layer is called the *internetwork layer.*
- This layer is responsible for routing messages through internetworks. Two types of devices are responsible for routing messages between networks.
- The first device is called a *gateway,* which is a computer that has two network adapter cards.
- This computer accepts network packets from one network on one network card and routes those packets to a different network via the second network adapter card. The second device is a *router,* which is a dedicated hardware device that passes packets from one network to a different network.
- The internetwork layer protocols provide a datagram network service. *Datagrams* are packets of information that comprise a header, data, and a trailer. The header contains information, such as the *destination address,* that the network needs to route the datagram.
- A header can also contain other information, such as the *source address* and *security labels.* Trailers typically contain a *checksum value,* which is used to ensure that the data is not modified in transit.
- The communicating entities which can be computers, operating systems, programs, processes or people that use the datagram services must specify the destination address (using control information) and the data for each message to be transmitted.
- The internetwork layer protocols package the message in a datagram and send it off. A datagram service does not support any concept of a session or connection.
- Once, a message is sent or received, the service retains no memory of the entity with which it was communicating. If such a memory is needed, the protocols in the Host-to-Host transport layer maintain it.
- The abilities to retransmit data and check it for errors are minimal or nonexistent in the datagram services. If the receiving datagram service detects a transmission error during transmission using the checksum value of the datagram, it simply ignores, (or drops) the datagram without notifying the receiving higher-layer entity.

4. Network Access Layer:

- The Network Access Layer is the lowest layer in the Internet reference model. This layer contains the protocols that the computer uses to deliver data to the other computers and devices that are attached to the network.
- The protocols at this layer perform three distinct functions:
  1. They define how to use the network to transmit a *frame*, which is the data unit passed across the physical connection.
  2. They exchange data between the computer and the physical network.
  3. They deliver data between two devices on the same network. To deliver data on the local network, the network access layer protocols use the physical addresses of the nodes on the network. A physical address is stored in the network adapter card of a computer or other device, and it is a value that is "hardcoded" into the adapter card by the manufacturer.
- Unlike higher level protocols, the network access layer protocols must understand the details of the underlying physical network, such as the packet structure, maximum frame size, and the physical address scheme that is used. Understanding the details and constraints of the physical network ensures that these protocols can format the data correctly so that it can be transmitted across the network.

2.4 TCP/IP PROTOCOL SUITE (S-22)

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers i.e. Host-to-Network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the Host-to-Network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer. So in this section, we assume that the TCP/IP protocol suite is made of five layers: Physical, Data Link, Network, Transport and Application.
- The first four layers provide physical standards, network interfaces, internetworking and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the Application Layer as shown in Fig. 2.11.
- TCP/IP is a hierarchical protocol made up of interactive modules with specific functionality. These modules are not interdependent. In OSI model, every layer is having predefined functions. The layers in TCP/IP protocol suite contain relatively

independent protocols that can be mixed and matched depending on the needs of the system. Every upper layer protocol is supported by one or more lower level protocols.

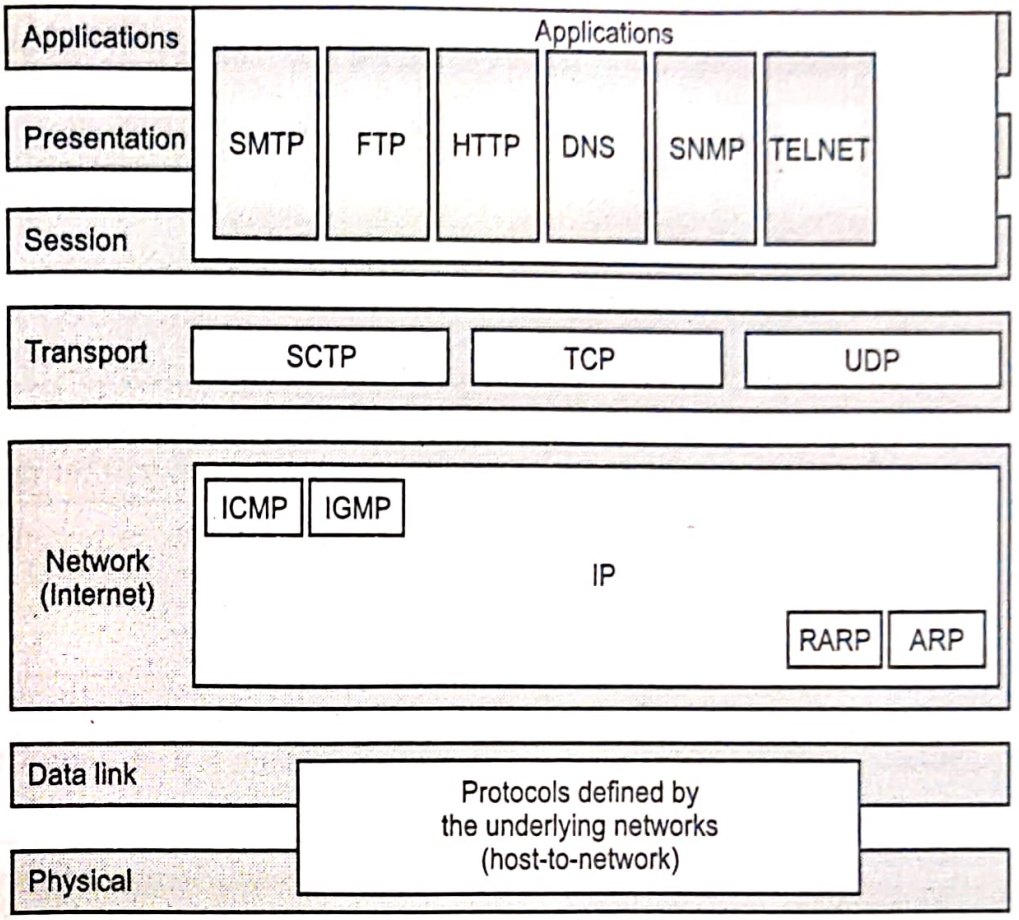


Fig. 2.11: TCP/IP and OSI Model

2.5 COMPARISON OF OSI & TCP/IP REFERENCE MODEL (S-19, W-22)

- The OSI and TCP/IP reference models have many things common. Both are based on concept of a stack of independent protocols.
- Functionality of the layers is almost same. The layers above transport are application oriented users of the transport service.
- Despite these fundamental similarities, the two models also have many differences as shown in following table.

Table 2.2: Comparison between ISO-OSI and TCP/IP model

Sr. No.	ISO-OSI Reference Model	TCP/IP Model
1.	7 layer model.	4 layer model.
2.	OSI model is useful in describing networks, but protocols are too general.	TCP/IP model is weak, but protocols are specific and widely used.

Contd....

3.	Model was conceptual, designers didn't know what functionality to put in the layers.	Model is practical, designers knows the functionality of each layer and used in real world network.
4.	Model is general, and easier to replace protocols.	Model is not general, and difficult to replace protocols.
5.	Model had to adjust when networks did not match the service specifications (wireless networks, internetworking).	Model need not require to adjust too much in this scenario.
6.	Model describes any type of network.	Model only describes TCP/IP which is not useful for describing any other networks.
7.	Network layer supports both Connection-oriented and connection-less service.	Network layer supports only connection-less service.
8.	Transport layers supports only connection-oriented service.	Transport layers supports both Connection oriented and connectionless service.

2.6 ADDRESSING (W-18, S-18, S-22, W-22, S-23)

- A network address serves as a unique identifier for a computer on a network.
- When set up correctly, computers can determine the addresses of other computers on the network and use these addresses to send messages to each other.

Levels of Addresses used in TCP/IP protocol:

- In TCP/IP, different levels of addresses are used, (Ref. Fig. 2.12).
  1. Physical Address (Hardware Address or Link Address).
  2. Logical Address (IP Address).
  3. Port Address.
  4. Specific Address

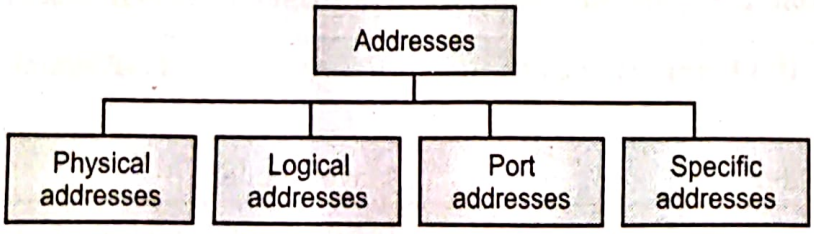


Fig. 2.12: Addresses in TCP/IP

- Physical address is basically a part of data link layer.
- Logical address is a part of network layer.

- Port address is a part of transport layer.
- Specific address is supported by application layer.
- Each address is related to a specific layer in the TCP/IP architecture, as shown in Fig. 2.13.

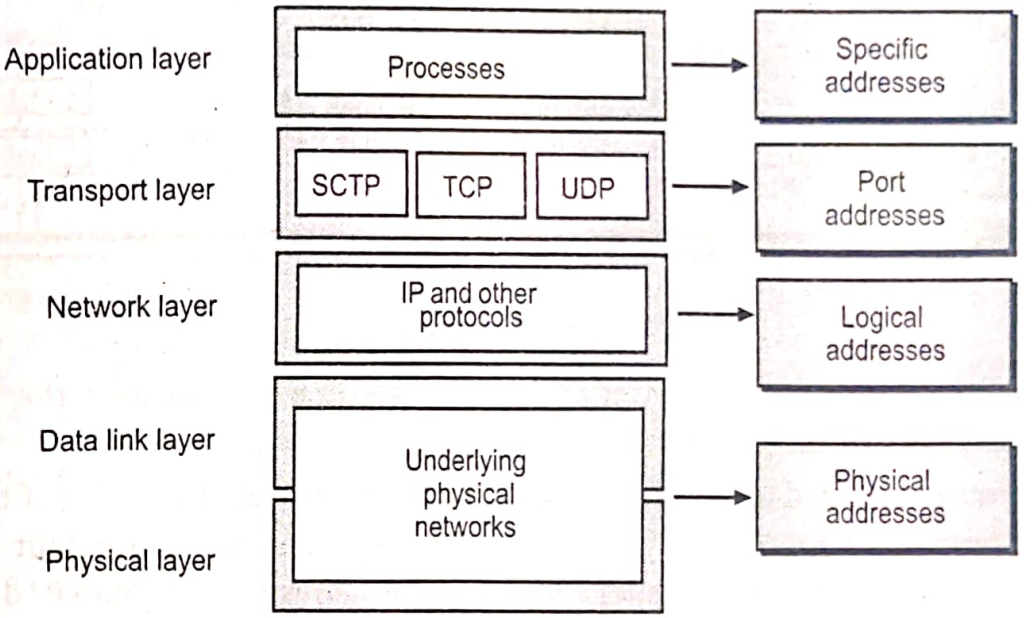


Fig. 2.13: Addresses related to layers in TCP/IP Architecture

2.6.1 Physical Addresses

- The physical addresses also known as the link address. This is the address of the node that defined by its LAN and WAN.
- Data link layer includes this address into data frame.
- Physical address is used when source and destination are from same network. It is lowest level address.
- The physical addresses have authority over the network i.e. LAN or WAN. The address size and format depend on the network.
- For example, Ethernet uses 6 byte (48 bit) physical address which is imprinted on the network interface card (LAN card).

Example:

- In Fig. 2.14, a node with physical address 10 sends a frame to a node with physical address 87, The two nodes are connected by a link i.e., bus topology LAN.
- At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection.
- Fig. 2.14 shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender

receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

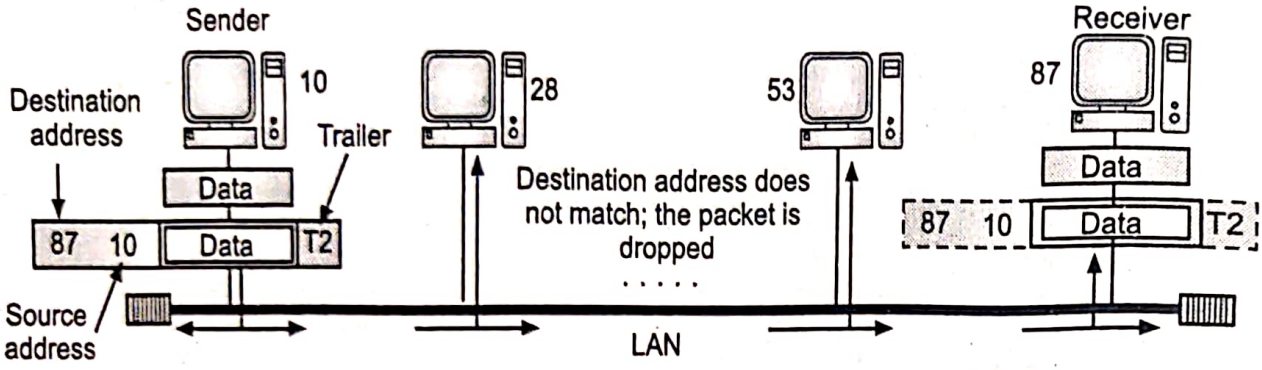


Fig. 2.14: Physical Addresses

- We have shown a bus topology for an isolated LAN. In a bus topology, the frame is propagated in both directions (left and right).
- The frame propagated to the left dies when it reaches the end of the cable if the cable end is terminated appropriately. The frame propagated to the right is sent to every station on the network. Each stations with physical addresses other than 87 drops the frame because the destination address in the frame does not match its own physical address.
- The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

Example of Physical Address:

- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

2.6.2 Logical Addresses

- The logical addresses also known as the IP address.
- When source and destination are from different networks or in on internetworking environment, physical addresses are not adequate where different networks can have different address format.
- A unique universal addressing system is needed in which every computer can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose.
- Logical addresses in a network model are necessary for universal communications that are independent of underlying physical networks.

- A logical address can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have same IP addresses. Logical addresses are necessary for universal communications.
- An IP addresses is 32 bit address usually written in dotted decimal format A.B.C.D. where each number is in the range 0 to 255. For example, 192.9.100.2.

Example:

- Fig. 2.15 shows a part of an Internet with two routers connecting three LANs.

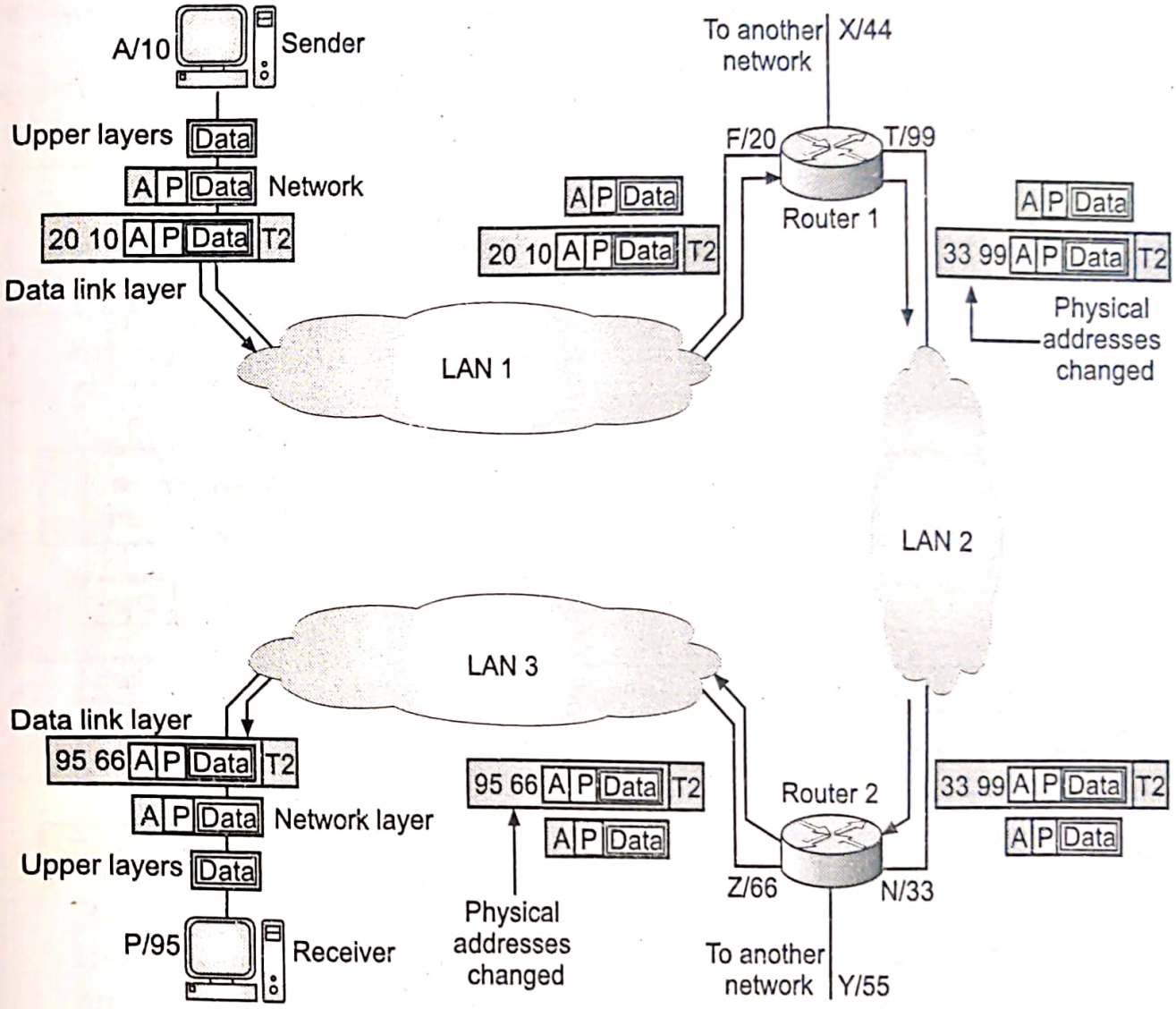


Fig. 2.15: Logical (IP) Addresses

- Each device/node like computer or router has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses.
- Each router, however, is connected to three network models for this reason each router has three pairs of addresses, one for each connection. Although it may obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection.

2.6.3 Port Addresses

- The IP address and the physical address in a network model are necessary for a quantity of data to travel from a source host to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- A system that sends nothing but data from one computer to another is not complete.
- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
- For example, computer x can communicate with computer z by using TELNET. At the same time, computer x communicates with computer y by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP network model architecture, the label assigned to a process is called a Port address.

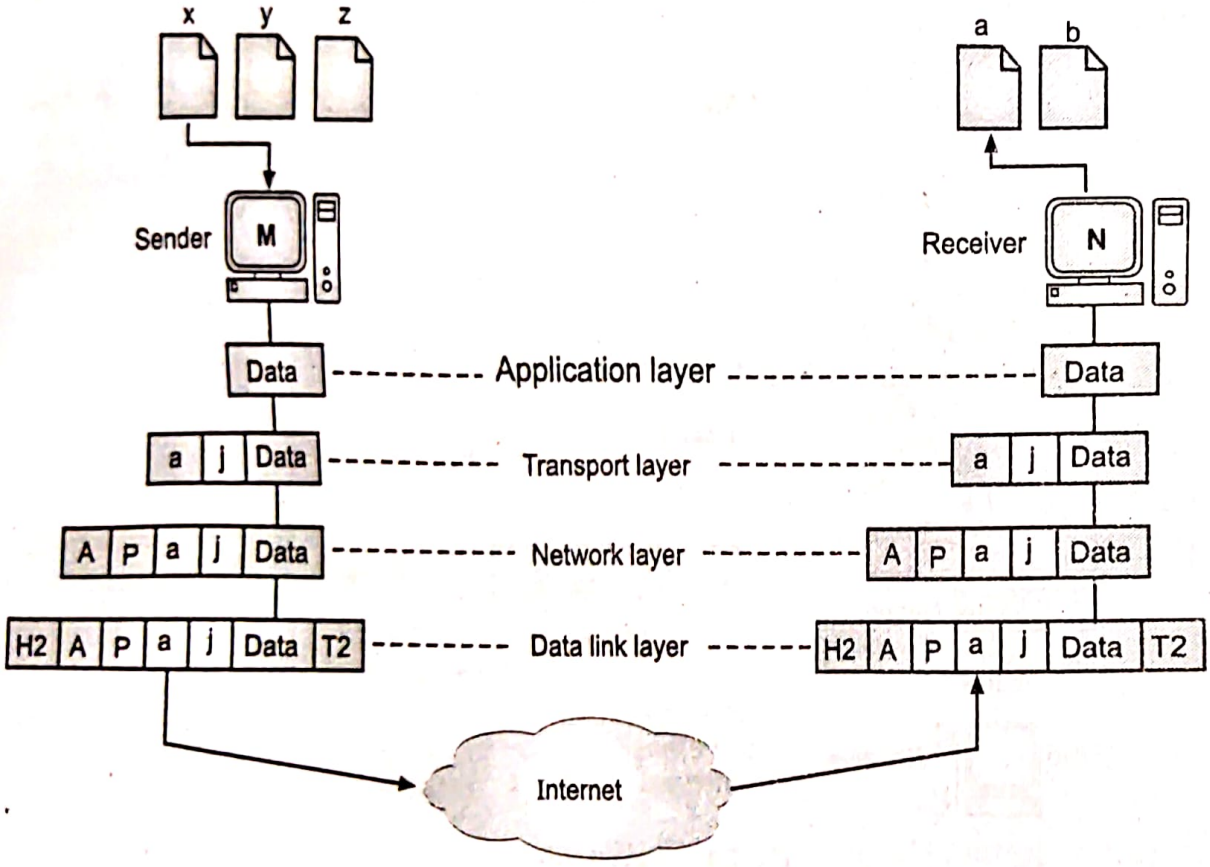


Fig. 2.16: Port Addresses

- A port address in TCP/IP network model is 16 bits in length. For example, A port address is a 16-bit address represented by one decimal number as 753.
- IANA (Internet Assigned Numbers Authority) has divided port numbers into three ranges:

(i) **Well Known Ports:** Ports ranging from 0 to 1023 are assigned and controlled by IANA.

(ii) **Registered Ports:** Ports from 1024 to 49,151 can be registered with IANA to prevent duplication.

(iii) **Dynamic Ports:** Ports from 49,152 to 65,535. They can be used by any process.

- In Fig. 2.16, two computers are communicating via Internet are shown. The sender is running three processes with port addresses x, y and z.
- The receiver is running two processes with port addresses a and b. Process 'x' wants to communicate with process 'a'. Both computers are using the same application. Process x's data must be delivered to process a and not b.
- For this, transport layer encapsulates data from the application layer in a packet and adds two port addresses x and a, as source port and destination port addresses.
- The packet is then given to network layer with adds logical addresses M and N and then data link layer adds physical addresses of the next hop. Although physical addresses change from hop to hop, logical and port addresses remain the same.

2.6.4 Specific Addresses

- Addresses are user friendly addresses and are called specific addresses.
- Some applications use friendly addresses that are designed for that specific address. However, this address gets changed according to the required logical and port addresses sent from the sender computer.
- For example, e-mail address and URL, for example: iamheremg@gmail.com, www.educationindia.edu and so on.

2.7 IP ADDRESSING

- An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network.
- There are two kinds of IP addresses, public (also called globally unique IP addresses) and private.

1. **Public IP addresses** are assigned by the Internet Assigned Numbers Authority (IANA). The addresses are guaranteed to be globally unique and reachable on the Internet. This assures that multiple computers do not have the same IP address. An Internet service provider (ISP) obtains a range of public IP addresses from IANA, and then the ISP assigns the addresses to customers to use when they connect to the Internet through the ISP.

- Public IP addresses are routable on the Internet, which means that a computer with a public IP address is visible to other computers on the Internet.

2. **Private IP addresses** cannot be used on the Internet. IANA has set aside three blocks of IP addresses that cannot be used on the global Internet. These three blocks of addresses are private IP addresses, and they are used for networks that do not directly connect to the Internet.

- A private IP address is within one of the following blocks or range of addresses:
  - 192.168.0.0/16: This block allows valid IP addresses within the range 192.168.0.1 to 192.168.255.254.
  - 172.16.0.0/12: This block allows valid IP addresses within the range 172.16.0.1 to 172.31.255.254.
  - 10.0.0.0/8: This block allows valid IP addresses within the range 10.0.0.1 to 10.255.255.254.
- Network ID is used to identify the subnet upon which the host resides. The host ID is used to identify the host itself within the given subnet.

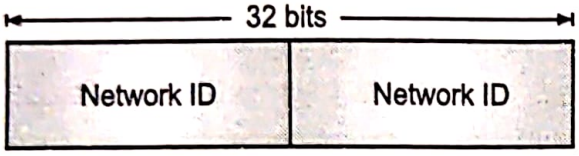


Fig. 2.17: IDs of IP Address

Parts of an IP Address:

- Any TCP/IP network will require a unique network number and every host on a TCP/IP network will require a unique IP address. Let us understand how IP addresses are constructed.
- An IP address is a 32-bit number that uniquely identifies a network interface on a machine. IP addresses are typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IP address. This form of representing the bytes of an IP address is often referred to as the dotted-decimal format.
- The bytes of an IP address can be further classified into two parts: the **Network part** and the **Host part**. The example below shows the components of the Class B network 192.168.1.100.

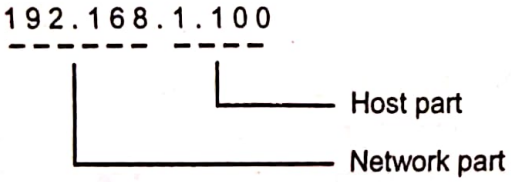


Fig. 2.18: Parts of an IP Address

1. **Network Part:**

   This part specifies the unique number assigned to your particular network. It is also the part that identifies the class of network assigned. In the above example, the network part takes up two bytes of the IP address, namely 192.168.

2. **Host Part:**

- This is the part of the IP address that you assign to each host, and uniquely identifies each host on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

- IP addresses can be displayed in three typical formats:
  - **Binary notation:** Binary notation is the format that systems on the network use to process the address. An example of binary notation is 11000000.10101000.00000001.01100100.
  - **Hexadecimal notation:** Hexadecimal notation is the format typically used when identifying IPv6 addresses. An example of hexadecimal notation of an IPv4 address is C0.A8.01.64
  - **Dotted-decimal notation:** Dotted-decimal notation is the format that is typically used for displaying the IP address in a human-readable format. An example of dotted-decimal notation is 192.168.1.100.
- The IP addressing scheme is integral to the process of routing IP datagrams through an internetwork.

2.7.1 Classful Addresses

- Classful addressing is a concept that divides the available address space of IPv4 into five classes namely A, B, C, D & E. Nowadays, this concept has become obsolete and has been replaced with classless addressing.
- The most complicated part of an IP address is that the division between the network identifier and the host identifier is not always in the same place.
- A hardware address, for example, consists of 3 bytes assigned to the manufacturer of the network adapter and 3 bytes that the manufacturer itself assigns to each card.
- IP addresses can have various numbers of bits assigned to the network identifier, depending on the size of the network.
- The IANA defines several different classes of IP addresses, which provide support for networks of different sizes, as shown in Fig. 2.19 (a).

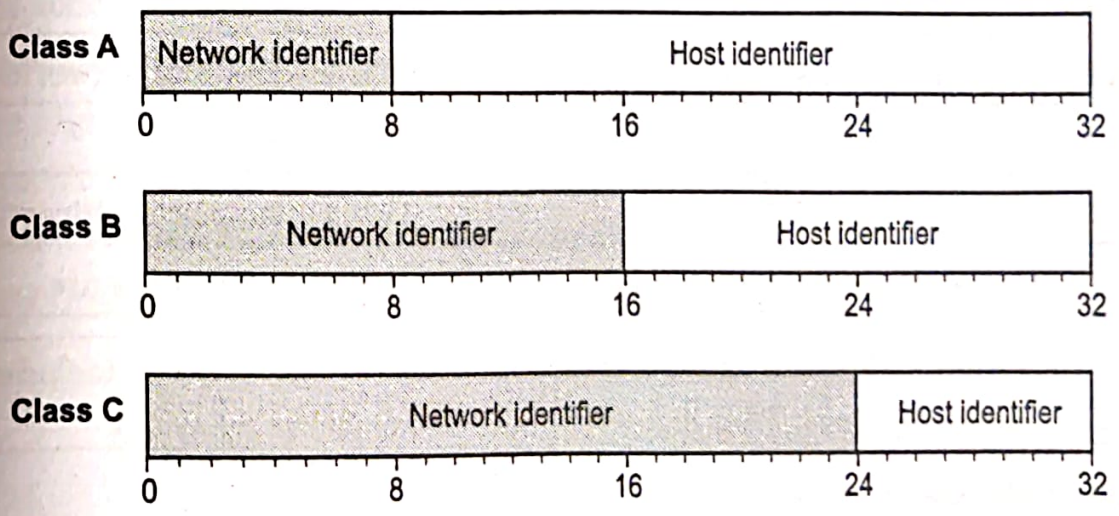


Fig. 2.19 (a): Three Classes of IP addresses with different sized network and host identifiers

Network Addressing and IP Address Classes:

- IP addresses are broken into 4 octets (IPv4) separated by dots called dotted decimal notation. An octet is a byte consisting of 8 bits. The IPv4 addresses are in the following form:

  192.168.10.1

- There are two parts of an IP address:
  - Network ID
  - Host ID
- The various classes of networks specify additional or fewer octets to designate the network ID versus the host ID.

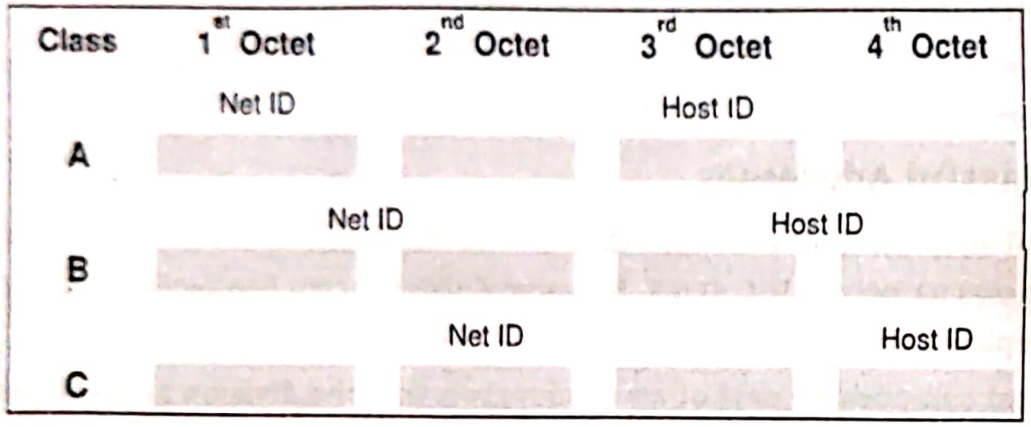


Fig. 2.19 (b): Octets in Classes

- Network address is an address that defines the network itself.
- The addressing scheme for class A through E networks is shown below.

Table 2.3: Addressing Scheme for Classes

Network Type	Address Range	Normal Netmask	Comments
Class A	001.x.x.x to 126.x.x.x	255.0.0.0	For very large networks
Class B	128.1.x.x to 191.254.x.x	255.255.0.0	For medium size networks
Class C	192.0.1.x to 223.255.254.x	255.255.255.0	For small networks
Class D	224.x.x.x to 239.255.255.255		Used to support multicasting
Class E	240.x.x.x to 247.255.255.255		Reserved for future use

Note: We use the 'x' character here to denote 'don't care situations' which includes all possible numbers at the location. It is many times used to denote networks.

1. Class A Addressing:

- First byte specifies the network portion (8 bits).
- Remaining bytes specify the host portion (24 bits).

- The highest order bit of the network byte is always 0.
- Network values of 0 and 127 are reserved.
- This class is used for large addressing networks.
- There are 126 Class A networks.
- There are more than 16 million host values for each Class A network.

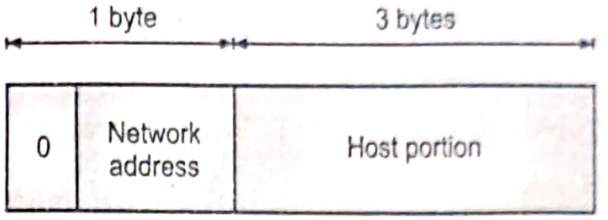


Fig. 2.20: Class A Addressing

2. Class B Addressing:

- The first two bytes specify the network portion (16 bits).
- The last two bytes specify the host portion (16 bits).
- The highest order bits 6 and 7 of the network portion are 10.
- This class is used for medium sized addressing networks.
- There are more than 16 thousand Class B networks.
- There are 65 thousand nodes in each Class B network.

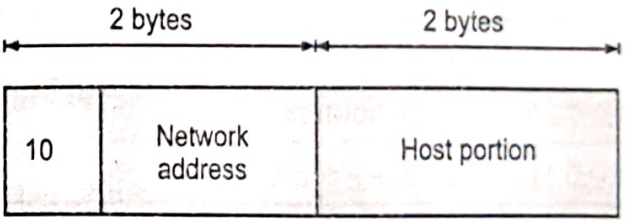


Fig. 2.21: Class B Addressing

3. Class C Addressing:

- The first three bytes specify the network portion (24 bits).
- The last byte specifies the host portion (8 bits).
- The highest order bits 5, 6 and 7 of the network portion are 110.
- This class is used for addressing small sized networks.
- There are more than 2 million Class C networks.
- There are 254 nodes in each Class C network.

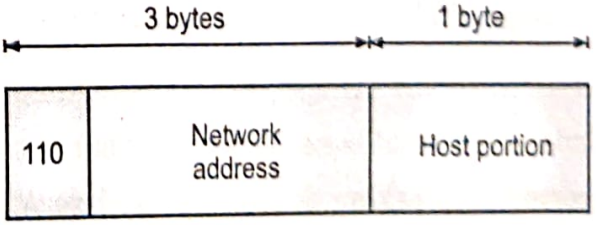


Fig. 2.22: Class C Addressing

4. Class D Addressing:

- Class D address defines a group-ID and used for multicasting.
- Internet authorities have designated some multicast addresses to specific groups.

Fig. 2.23: Class D Addressing

Table 2.4: Categories of Class D addresses.

Address	Group
224.0.0.0	Reserved
224.0.0.1	ALL SYSTEMS on this SUBNET
224.0.0.2	ALL ROUTERS on this SUBNET
224.0.0.4	DVMRP ROUTERS
224.0.0.5	OFPFIGP ALL ROUTERS
224.0.0.6	OSPFIGP Designated ROUTERS
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IGRP Routers
224.0.0.11	Mobile Agents

5. Class E Addressing:

- Fig. 2.24 shows address format of class E addressing.
- This format begins with 1110 that shows it is reversed for the future use.

Fig. 2.24: Class E addressing

Subnetting and Supernetting:

- To overcome the flaws of classful addressing, these two solutions were introduced to compensate for the wastage of addresses. Let us discuss them one by one.

Subnetting:

- IP networks can be divided into smaller networks called subnetworks (or subnets).
- Subnetting is the process of breaking down a main class A, B, or C network into subnets for routing purposes.

- A subnet mask is the same basic thing as a netmask with the only real difference being that you are breaking a larger organizational network into smaller parts, and each smaller section will use a different set of address numbers.
- This will allow network packets to be routed between subnetworks. When subnetting, the number of bits in the subnet mask determines the number of available subnets.
- Two to the power of the number of bits minus two is the number of available subnets.

Number of available subnets = $2^n - 2$ Where, n: Number of bits

- When setting up subnets the following must be determined:
  - Number of segments
  - Hosts per segment.
- Subnetting provides the following advantages:
  - **Network traffic isolation:** There is less network traffic on each subnet.
  - **Simplified Administration:** Networks may be managed independently.
  - **Improved security:** Subnets can isolate internal networks so they are not visible from external networks.

Subnet Masks:

- A 14 bit subnet mask on a class B network only allows 2 node addresses for WAN links. A routing algorithm like OSPF (Open Shortest Path First) must be used for this approach.
- These protocols allow the Variable Length Subnet Masks (VLSM). RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol) don't support this. Subnet mask information must be transmitted on the update packets for dynamic routing protocols for this to work.
- The router subnet mask is different than the WAN interface subnet mask.
- One network ID is required by each of:
  - Subnet
  - WAN connection.
- One host ID is required by each of:
  - Each NIC on each host.
  - Each router interface.

Types of Subnet Masks:

- **Default:** Fits into a Class A, B, or C network category.
- **Custom:** Used to break a default network such as a Class A, B, or C network into subnets.

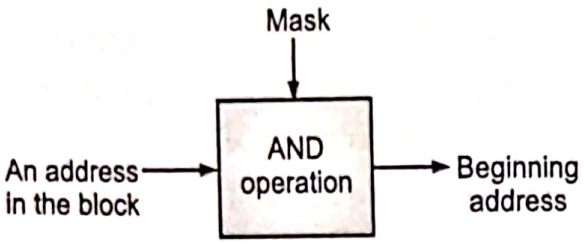


Fig. 2.25: Masking Concept

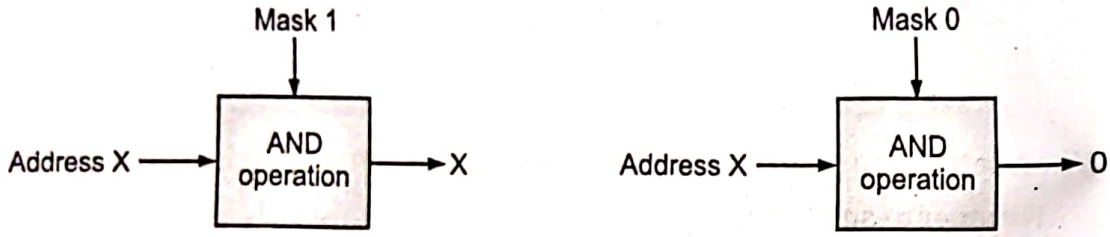
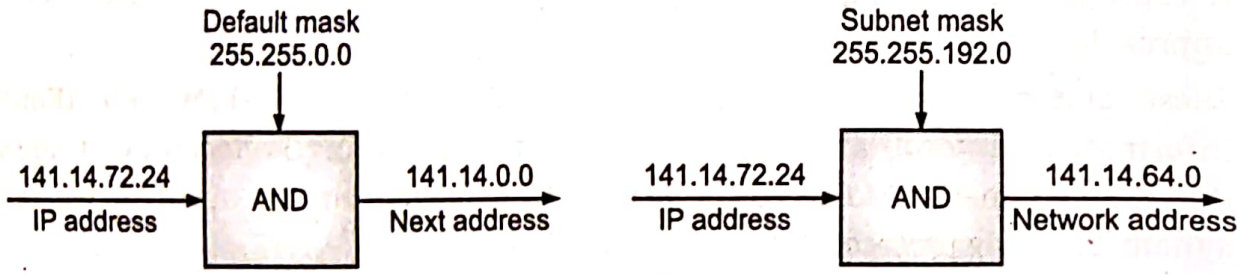


Fig. 2.26: AND Operation

Table 2.5: Default Masks

Class	Mask in Binary	Mask in dotted-decimal
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0



(a) Without Subnetting **(b) With Subnetting**

Fig. 2.27: Default mask and Subnet mask

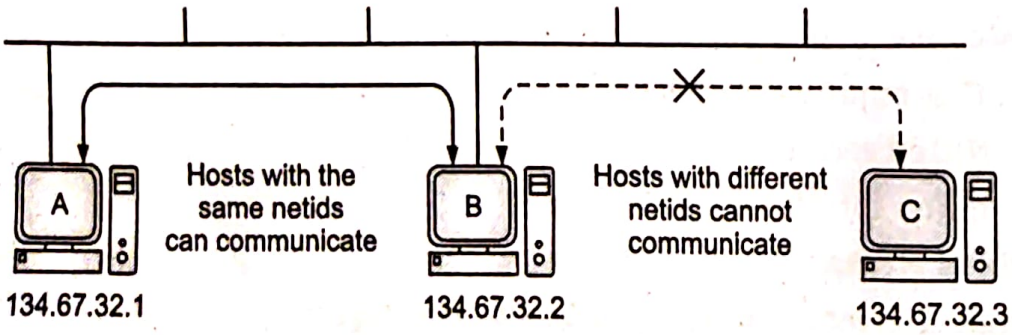


Fig. 2.28: Host Communication on a Local Network

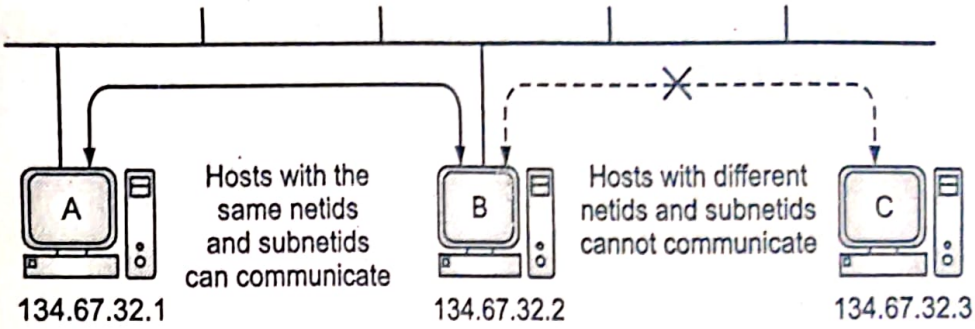


Fig. 2.29: Host Communication with Subnetting

- A subnet is defined by applying a bitmask, the subnet mask, to the IP address. If a bit is on the mask, the equivalent bit in the address is interpreted as a network bit.
- If the bit in the mask is off, the bit belongs to the host part of the address. The subnet is only known locally. To the rest of the Internet, the address is still interpreted as a standard IP address.

Supernetting:

- As the blocks in class A and B were almost consumed so, new organizations consider class C. But, the block of class C is too small then the requirement of the organization. In this case, the solution which came out is supernetting which grants to join the blocks of class C to form a larger block which satisfies the address requirement of the organization.

2.7.2 Classless Addresses (S-23)

- Classless addressing is a concept of addressing the IPv4 addresses. It was adopted after the failure of classful addressing. The classful addressing leads to wastage of addresses as it assigns a fixed-size block of addresses to the customer. But, the classless addressing assigns a block of addresses to the customer according to its requirement which prevents the wastage of addresses.
- Classless addressing is also called **Classless Inter-Domain Routing (CIDR)**. This addressing type helps to allocate IP addresses more efficiently. When the user requires a particular number of IP addresses, this method assigns a block of IP addresses concerning certain rules. And, this block is called a CIDR block and has the required number of IP addresses.

Properties:

1. Addresses in a block must be in contiguous form.
2. The number of address in a block must be the power of 2 i.e. 2, 4, 8, 16, ...
3. The first address must be evenly divisible by the number of addresses.

Representation:

- In Classless addressing a block, IP address is given like 192.168.10.1/28 (after "/" number of the mask bit is given).
- We can find a mask for the whole block by putting the given after bits out of 32 as 1 and rest of the bits as 0.

- Here, we have 28 bits. So, we need to put 28 bits out of 32 bits as 1 and rest of bits as 0 will give us the mask for the IP address block.

  11111111.11111111.11111111.11100000

  255. 255. 255. 240

  Mask is 255.255.255.240

Important points:

1. To get the first IP address of the block set the rightmost (32 - n) bits to 0s.
2. Last IP address of the block can be found by setting the rightmost bits to 1s.
3. Number of IP addresses of the given block can be found by 232 - n.

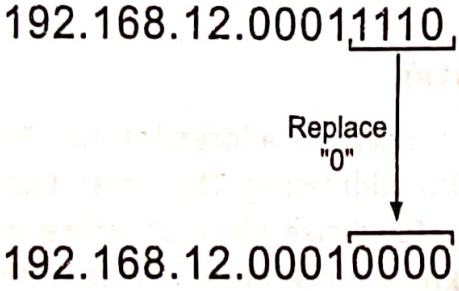
Example:

192.168.12.30/28

Mask value : 255.255.255.240

- In the above example, if we want to find the first address of the given blocks then have to put 0 to set a rightmost bit of the given IP.
- To make it is easy to convert only the last octet into binary and then set 1 or 0 accordingly and rest will remain the same.

  Binary of 30 = 11110



- Hence, the first IP address of the block is 192.168.12.16 (Satisfying Property no. 3).
- Again, to get the last IP address of the block we have to replace all the rightmost bit to 1,
- 192.168.12.00011110
- After replacing all the rightmost bits to 1 we obtain 192.168.12.00011111 i.e. 192.168.12.31.

Table 2.6: Difference between Classful and Classless Addressing

Sr. No	Classful Addressing	Classless Addressing
1.	This alloctes IP addresses according to five major classess.	It is designed to replace classful addressing. It minimizes the rapid exhaustion of IP addresses.
2.	The network ID and host ID changes depending on the classes	There is no boundary on network ID and host ID
3.	Less Practical and useful	More practical and useful

Summary

- A Network Model is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network model to another. The software consists of instruction sets that make possible the services that we expect from a network model.
- A reference model is a conceptual framework for understanding relationships.
- The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model.
- OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing.
- 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.
- The ISO-OSI model consists of seven layers i.e. Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, and Application Layer.
- Physical layer activates, maintain and deactivate the physical connection. It converts the digital bits into electrical signal.
- Data link layer synchronizes the information which is to be transmitted over the data it also provides error and flow controlling.
- The Network Layer routes the signal through different channels to the other end.
- Transport Layer decides if data transmission should be on parallel path or single path. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.
- Session layer manages and synchronize the conversation between two different applications.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems.
- Manipulation of data (information) in various ways is done in Application Layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer.
- TCP/IP is also called as Internet Model. It has four layers.
- The TCP/IP (Transmission Control Protocol and Internet Protocol) is a set of protocols, or a protocol suite, that defines how all transmission are exchanged across the Internet.
- TCP/IP protocol suite uses four different types of addresses i.e. Physical addresses (also known as the link address, is the address of the node as defined by its LAN and WAN), Logical Addresses (also called as IP address, is a unique universal addressing system is needed in which every computer can be identified uniquely, regardless of

the underlying physical network), Port addresses (a port address is a 16-bit address represented by one decimal number), Specific addresses (user friendly addresses).

- A network address is an identifier for a node or network interface of a computer network. A network address is simply a code used by computers as a means of identification.
- Addressing is the mechanism for identifying senders and receivers, on the network.
- IP address is an address having information about how to reach a specific host, especially outside the LAN.
- Classful and classless addressing are two IP addressing types. The main difference between classful and classless addressing is that classless addressing allows allocating IP addresses more efficiently than classful addressing.

Check Your Understanding

1. Which layer of the OSI reference model corresponds to the IP protocol of the TCP/IP protocol stack ?
   (a) Transport (b) Network
   (c) Internet (d) Data link
2. The entities in the same layer on different machines are called _____.
   (a) hosts (b) peers
   (c) protocols (d) IMP's
3. As the data packet moves from the lower to the upper layers, headers are _____.
   (a) Added (b) Rearranged
   (c) Modified (d) Subtracted
4. Which of the following is a TCP/IP transport layer protocol ?
   (a) IP (b) FTP
   (c) UDP (d) ICMP
5. What is the main function of the transport layer ?
   (a) Process-to-process delivery
   (b) Note-to-node delivery
   (c) Synchronization
   (d) Updating and maintenance of routing tables
6. Which of the following device operates at the network layer of the OSI model ?
   (a) repeater (b) router
   (c) bridge (d) hub
7. The length of an IP address if IPv4 is _____ bits.
   (a) 46 (b) 32
   (c) 16 (d) 64
8. Which of the following is a NOT an Internet layer protocol in the TCP/IP stack ?
   (a) IP (b) UDP
   (c) ARP (d) ICMP
9. The OSI model has ___ layers.
   (a) 4 (b) 5
   (c) 6 (d) 7

10. TCP/IP model does not have _____ layer but OSI model have this layer.
    (a) session layer (b) presentation layer
    (c) application layer (d) both (a) and (b)
11. Which layer links the network support layers and user support layers
    (a) session layer (b) data link layer
    (c) transport layer (d) network layer
12. Which address is used in an internet employing the TCP/IP protocols?
    (a) physical address and logical address
    (b) port address
    (c) specific address
    (d) all of the mentioned
13. TCP/IP model was developed _____ the OSI model.
    (a) prior to (b) after
    (c) simultaneous to (d) none of the mentioned
14. Which layer is responsible for process to process delivery?
    (a) network layer (b) transport layer
    (c) session layer (d) data link layer
15. Which address identifies a process on a host?
    (a) physical address (b) logical address
    (c) port address (d) specific address
16. Which layer provides the services to user?
    (a) application layer (b) session layer
    (c) presentation layer (d) none of the mentioned
17. Transmission data rate is decided by _____.
    (a) network layer (b) physical layer
    (c) data link layer (d) transport layer
18. The physical layer concerns with _____.
    (a) bit-by-bit delivery
    (b) process to process delivery
    (c) application to application delivery
    (d) none of the mentioned

ANSWERS

1. (b)	2. (b)	3. (d)	4. (c)	5. (a)	6. (b)
7. (b)	8. (b)	9. (d)	10. (d)	11. (c)	12. (d)
13. (a)	14. (b)	15. (c)	16. (a)	17. (b)	18. (a)

Practice Questions

Q.I Answer the following questions in short.

1. What is network model?
2. Write name of addresses used in TCP/IP protocol.

3. Differentiate between physical address and logical address.
4. Which device operates at the network layer of the OSI model?
5. What is subnetting?

Q.II Answer the following questions.

1. Explain functions of each layer ISO-OSI reference model.
2. What is addressing? Explain logical addressing in network.
3. Explain the functions of Transport Layer in OSI-Reference Model.
4. Draw TCP/IP model and state the functions of each layer.
5. Compare OSI and TCP/IP reference Model.
6. Describe protocol hierarchy in brief.
7. What are the similarities available in TCP/IP and OSI model?
8. Explain classful addressing of TCP/IP model in detail.
9. Explain IP address in detail.

Q.III Define the following terms:

1. Physical address
2. Broadcast address
3. Port address
4. HTTP
5. Framing

Previous Exams Questions

Summer 2018

1. Explain functions of each layer of ISO-OSI reference model. **[5 M]**

Ans. Please refer to section 2.2.1.

2. Explain different types of addresses. **[5 M]**

Ans. Please refer to section 2.6.

Winter 2018

1. Explain functions of each layer ISO-OSI reference model. **[5 M]**

Ans. Please refer to section 2.2.1.

2. Explain different types of addresses. **[5 M]**

Ans. Please refer to section 2.6.

3. Explain TCP/IP protocol in detail. **[5 M]**

Ans. Please refer to section 2.3.

Summer 2019

1. Draw TCP/IP model and state the functions of each layer. **[5 M]**

Ans. Please refer to section 2.2.1.

2. Compare ISO/OSI reference model and TCP/IP. **[5 M]**

Ans. Please refer to section 2.5.