Reference Models

THE OSI MODEL

- OSI Model was developed by the **International Organization for Standardization (ISO)**.
- The OSI Model consists of 7 layers and each layer has specific functions and responsibilities.
- This layered approach makes it easier for different devices and technologies to work together.
- OSI Model provides a clear structure for data transmission and managing network issues. The OSI Model is widely used as a reference to understand how network systems function.

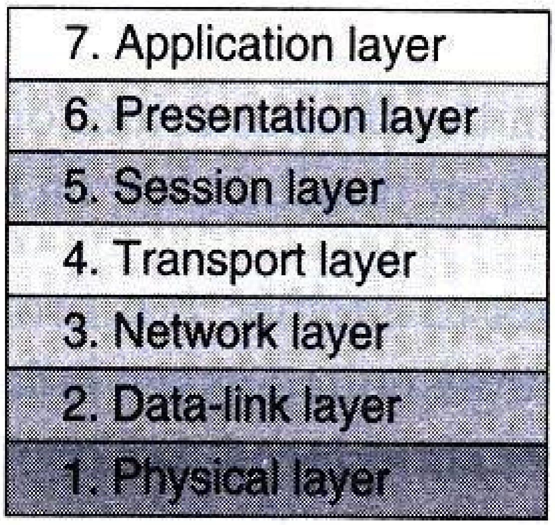


Figure 5.1 The seven- layer OSI model

Layered Architecture

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2),network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).

Layer 1 – Physical Layer

The lowest layer of the OSI reference model is the **Physical Layer**. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Layer 2 – Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame.

Layer 3 – Network Layer

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

Layer 4 – Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

Layer 5 – Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security.

Layer 6 – Presentation Layer

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Layer 7 – Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data 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.

Encapsulation

Figure 5.1 reveals another aspect of data communications in the OSI model: encapsulation. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

In other words, the data portion of a packet at level *N* - 1 carries the whole packet (data and header and maybe trailer) from level *N.* The concept is called *encapsulation;* level *N* - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level *N* - 1, the whole packet coming from level *N* is treated as one integral unit.

5.2 LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

1.Physical Layer

The **physical layer** coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission media. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Figure 5.3 shows the position of the physical layer with respect to the transmission media and the data link layer.

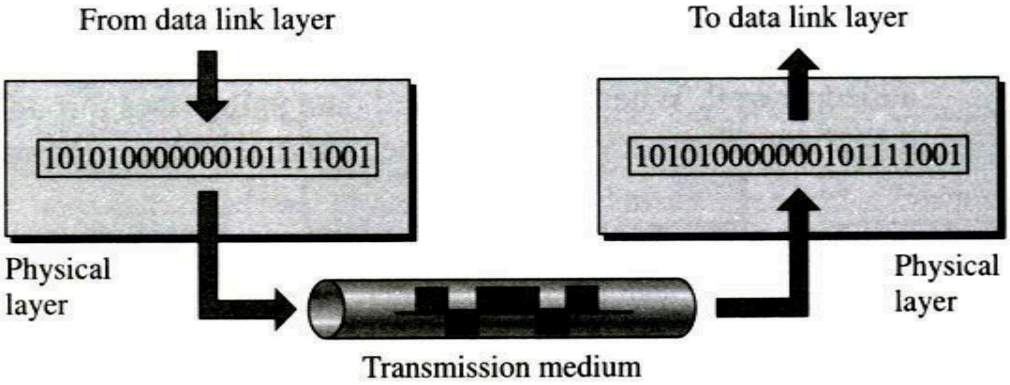


Figure 5.3*Physical layer*

The major duties of the physical layer are as follows:

1. **Physical characteristics of interfaces and media.** The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission medium.

2. **Representation of bits.** The physical layer data consists of a stream of bits (sequence of 0s or 1s) without any interpretation. To be transmitted, bits must be encoded into signals: electrical or optical. The physical layer defines the type of representation (how 0s and 1s are changed to signals).

3. **Data rate.** The **transmission rate-**The number of bits sent each second is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

4. **Synchronization of bits.** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

2.<u>Data Link Layer</u>

The **data link layer** transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error- free to the upper layer (network layer). Figure 5.4 shows the relationship of the data link layer to the network and physical layers.

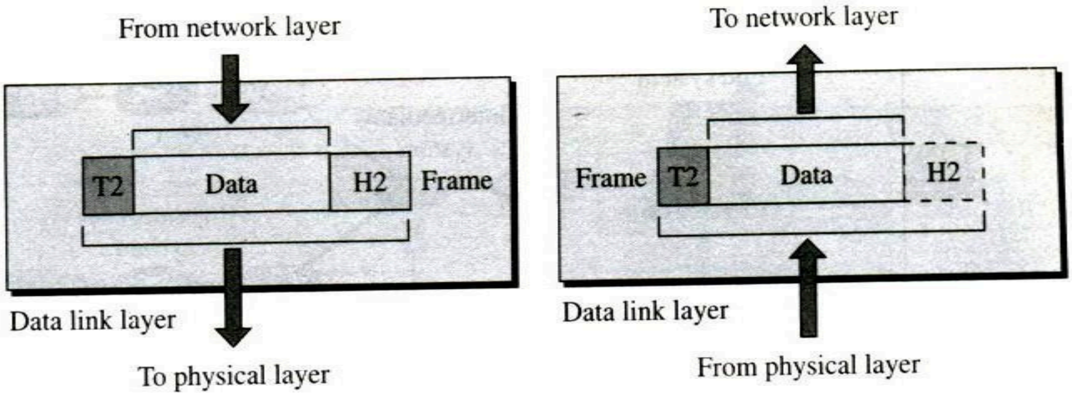


Figure 5.4 *Data link layer*

The data link layer is responsible for transmitting frames from one node to the next.

The major duties of the data link layer are as follows:

1. **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called **frames.**

2. **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the connecting device that connects the network to the next one.

3. **Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

4. **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to prevent duplication of frames. Error control is normally achieved through a trailer added to the end of the frame.

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

- **Logical Link Control (LLC)** Establishing and terminating links, controlling frame traffic, sequencing frames, and acknowledging frames

- **Media Access Control (MAC)** Managing media access, delimiting frames, checking frame errors, and recognizing frame addresses

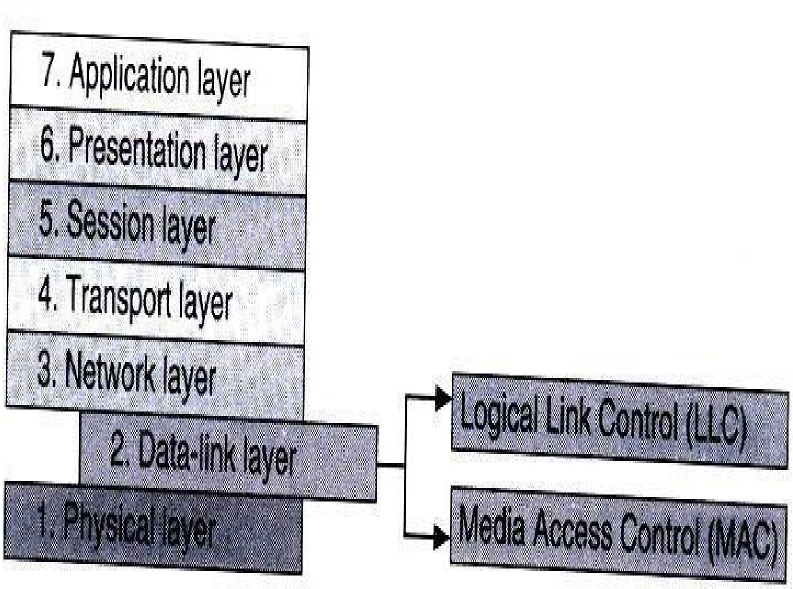


Figure 5.5 Project 802 LLC and MAC sublayers

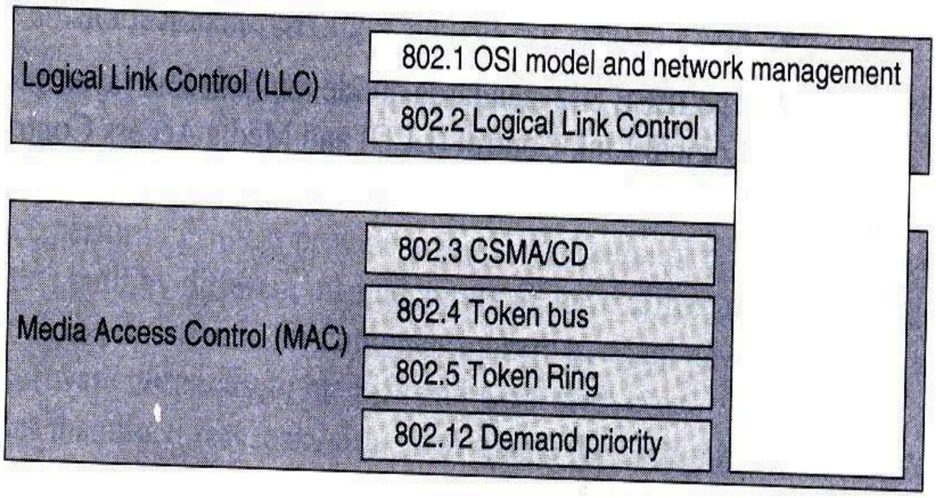
Logical Link Control (LLC) Sublayer

The LLC sub-layer manages data-link communication and defines the use of logical interface points called *service access points* (SAP), Other computers can refer to and use SAPs to transfer information from the LLC sub-layer to the upper OSI layers. Category 802.2 defines these standards.

Media Access Control (MAC) Sublayer

MAC sublayer is the lower of the two sublayers, providing shared access to the physical layer for the computers' NICs. The MAC layer communicates directly with the NIC and is responsible for delivering errorfree data between two computers on the network.

Categories 802.3, 802.4, 802.5, and 802.12 define standards for this sublayer and OSI layer 1, the physical layer.


Logical Link Control (LLC)
802.1 OSI model and network management
802.2 Logical Link Control
Media Access Control (MAC)
802.3 CSMA/CD
802.4 Token bus
802.5 Token Ring
802.12 Demand priority

LLC and MAC Standard

3.__Network Layer__

The **network layer** is responsible for the **source-to-destination delivery** of a packet possibly across multiple networks. Whereas the data link layer oversees the delivery of the packet between two systems on the same network, the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks with connecting devices between the networks, there is often a need for the network layer to accomplish source-to-destination delivery. Figure 5.6 shows the relationship of the network layer to the data link and transport layers.

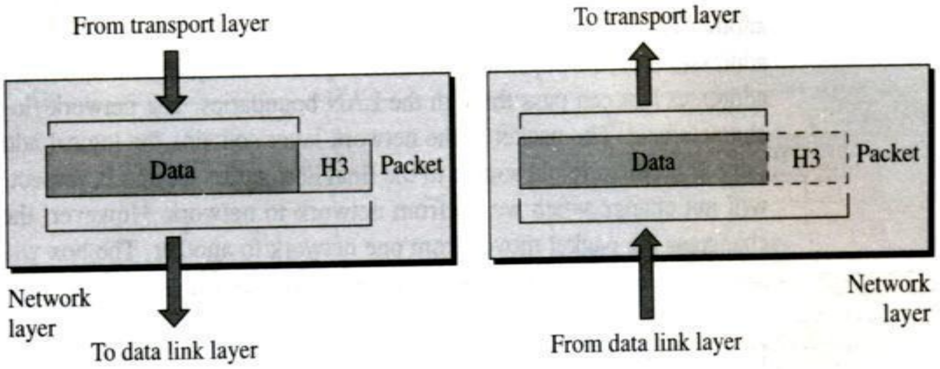


Figure 5.6*Network layer*

The major duties of the network layer are as follows:

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

layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

2. **Routing.** When independent networks or links are connected to create an **internetwork** (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

***4.**Transport Layer*

The **transport layer** is responsible for **process-to-process delivery** of the entire message. Whereas the network layer oversees host-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the process-to-process level. Figure 5.7 shows the relationship of the transport layer to the network and session layers.

From Session layer To Session layer

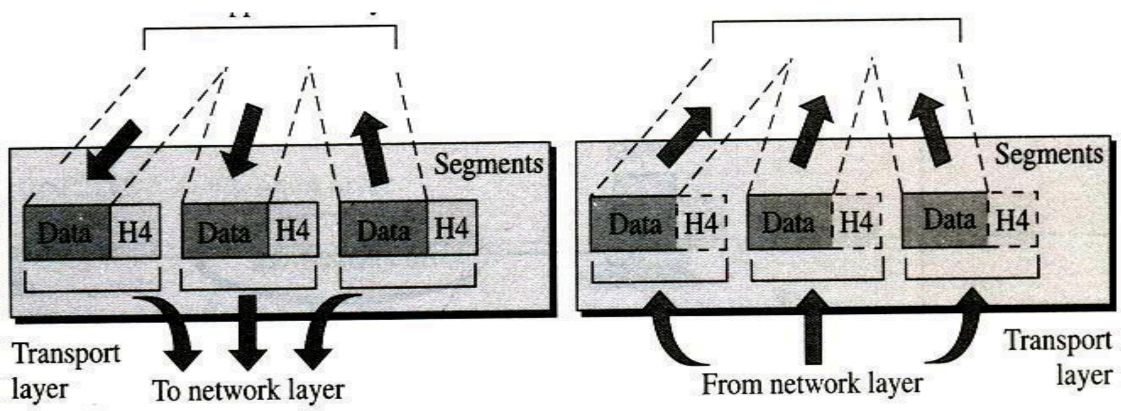


Figure 5.7 Transport layer

The transport layer is responsible for delivery of a message from one process to another.

The major duties of the transport layer are as follows:

1. **Port addressing.** Computers often run several processes (running programs) at the same time. For this reason, process-to-process delivery means delivery not only from one computer to the next but also from a specific process on one computer to specific process on the other. The transport layer header must therefore include type of address called a **port address.** The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

2. **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 arrival at the destination and to identify and replace packets that were lost in the transmission.

3. **Connection control.** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated,

4. **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

5. **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed end to end rather than across a single link.

5.Session Layer

The **session layer** is the network dialog *controller.* It establishes, maintains, and

syn- chronizes the interaction between communicating systems. Specific responsibilities of the session layer include the following:

1. **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode. For example, the dialog between a terminal connected to a mainframe can be half-duplex.

2. **Synchronization.** The session layer allows a process to add checkpoints **(synchronization points)** into a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100 page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure 5.8 illustrates the relationship of the session layer to the transport and presentation layers.

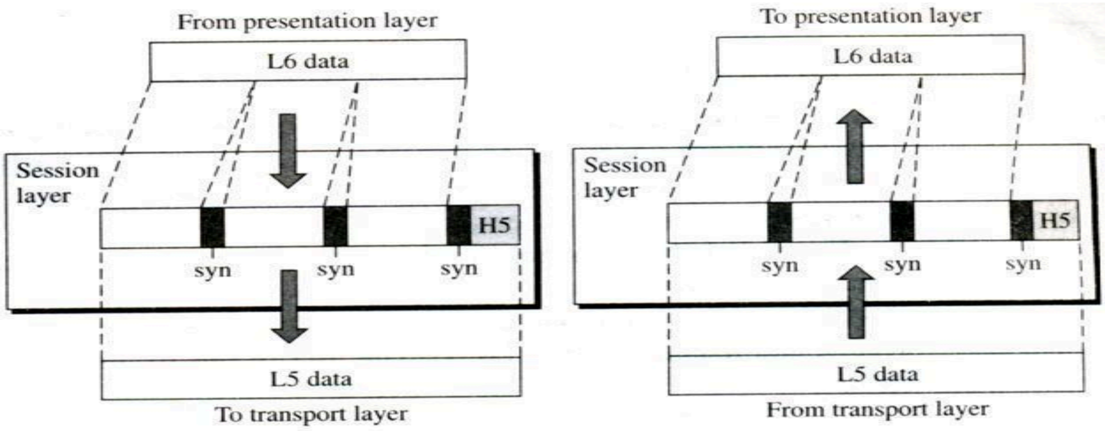


Figure 5.8*Session layer*

6.__Presentation Layer__

The **presentation layer** is concerned with the syntax and semantics of the information exchanged between two systems. Figure 5.9 shows the relationship between the presentation layer and the application and session layers.

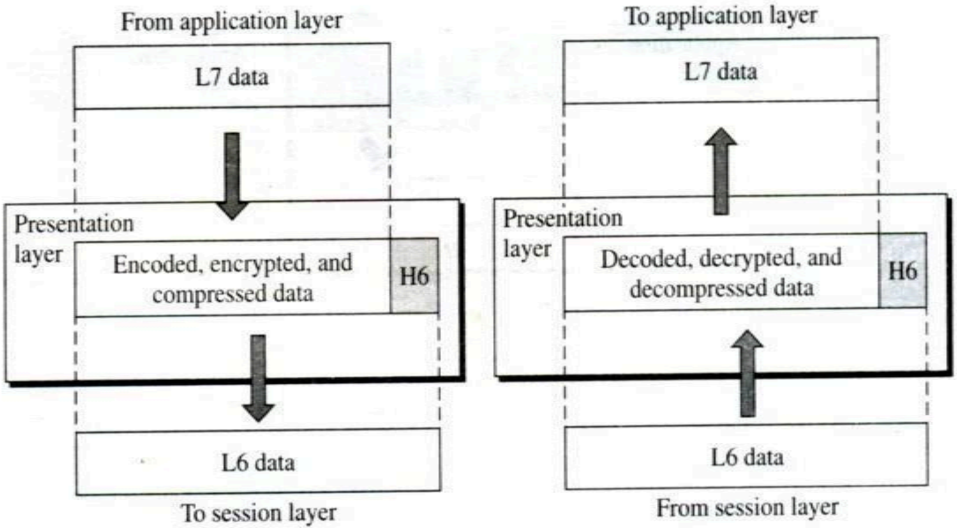


Figure 5.9*Presentation layer*

Specific responsibilities of the presentation layer include the following:

1. **Translation.** The processes (running programs) in two Systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because 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- dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver- dependent format.

2. **Encryption.** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

3. **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7.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 electronic mail remote file access and transfer, shared database management, and other types of distributed information services.

Figure 5.10 shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: X.400 (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example uses X.400 to send an email message.

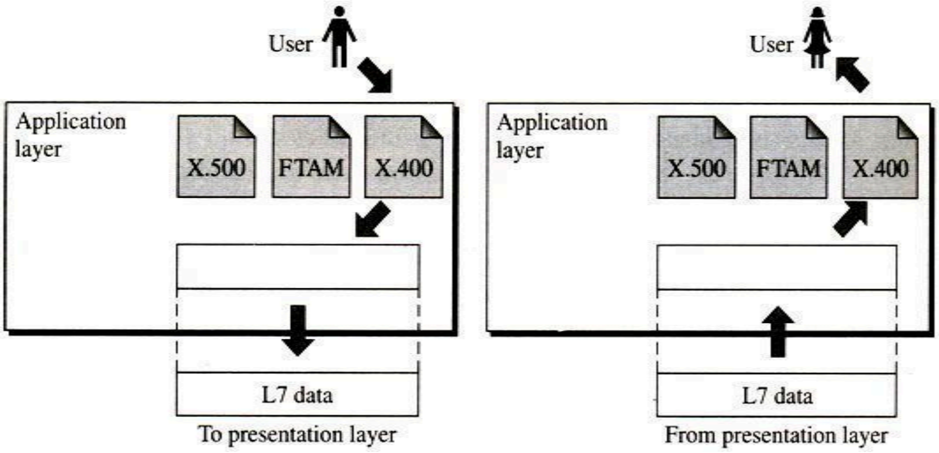


Figure 5.10 Application layer

Specific services provided by the application layer include the following:

1. **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows you to log on.

2. **File transfer, access, and management (FTAM).** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

3. **Mail services.** This application provides the basis for email forwarding and storage.

4. **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

Protocols associated **with** application layer of OSI model are as follows:

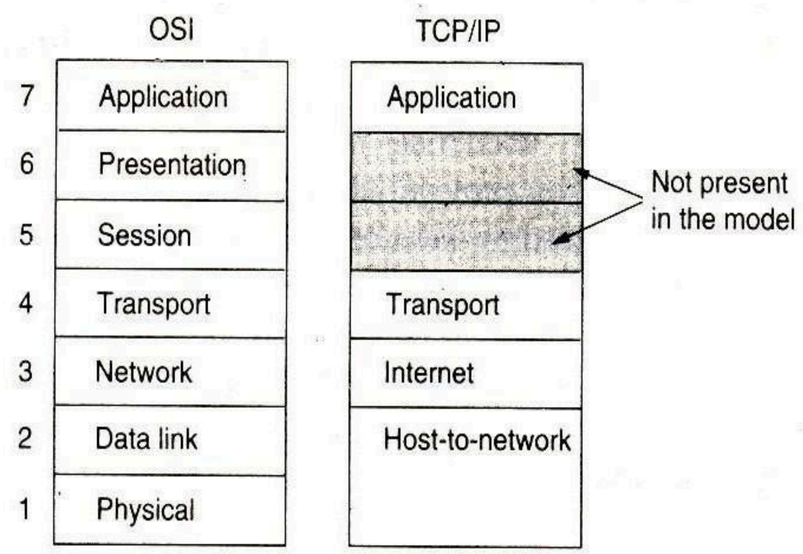
1. TELNET
2. File Transfer Protocol (FTP)
3. Simple Mail Transfer Protocol (SMTP)
4. Domain Name System (DNS)
5. Hypertext Transfer Protocol (HTTP)

5.2 TCP/IP PROTOCOL SUITE

- The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense).

- Thus, the ability to connect multiple networks in a seamless way was one of the major design goals from the very beginning.

- This architecture later became known as the **TCP/IP Reference Model,** after its two primary protocols. It was first defined in (Cerf and Kahn, 1974).



- 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: 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.

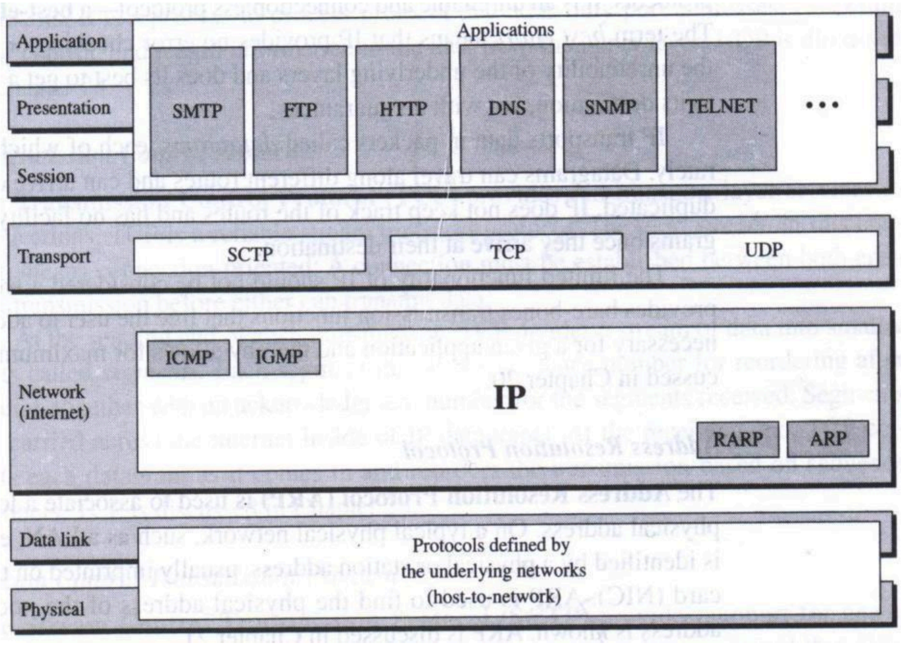


Figure 5.11 TCP/IP and OSI model

Physical and Data Link Layers

At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking.

IP transports data in packet called datagram, each of which is transported separately. Datagram can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagram once they arrive at their destination.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol

The User Datagram Protocol (UDP) is the simpler of the two standard TCPIIP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagram. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

The application layer in TCPIIP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer. Communication at the network layer is host-to-host (computer-to-computer); a computer somewhere in the world needs to communicate with another computer somewhere else in the world. Usually, computers communicate through the Internet. The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer. For this level of communication, we need a global addressing scheme; we called this as logical addressing. Today, we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite.

The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses if there is no confusion. The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPv6 (IP version 6).In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation. These addresses are referred to as IPv6 (IP version 6) addresses.

Address mapping:

Internet Protocol (IP) as the main protocol at the network layer. IP was designed as a best-effort delivery protocol, but it lacks some features such as flow control and error control. It is a host-to-host protocol using logical addressing. To make IP more responsive to some requirements in today's internetworking, we need the help of other protocols.

We need protocols to create a mapping between physical and logical addresses. IP packets use logical (host-to-host) addresses. These packets, however, need to be encapsulated in a frame, which needs physical addresses (node-to-node). We will see that a protocol called ARP, the Address Resolution Protocol, is designed for this purpose. We sometimes need reverse mapping-mapping a physical address to a logical address. For example, when booting a diskless network or leasing an IP address to a host. Three protocols are designed for this purpose: RARP, BOOTP, and DHCP. Lack of flow and error control in the Internet Protocol has resulted in another protocol, ICMP that provides alerts. It reports congestion and some types of errors in the network or destination host.

IP was originally designed for unicast delivery, one source to one destination. As the Internet has evolved, the need for multicast delivery, one source to many destinations, has increased tremendously. IGMP gives IP a multicast capability.

Mapping Logical to Physical Address: ARP

Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver. The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network (see Figure 5.12).

Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.

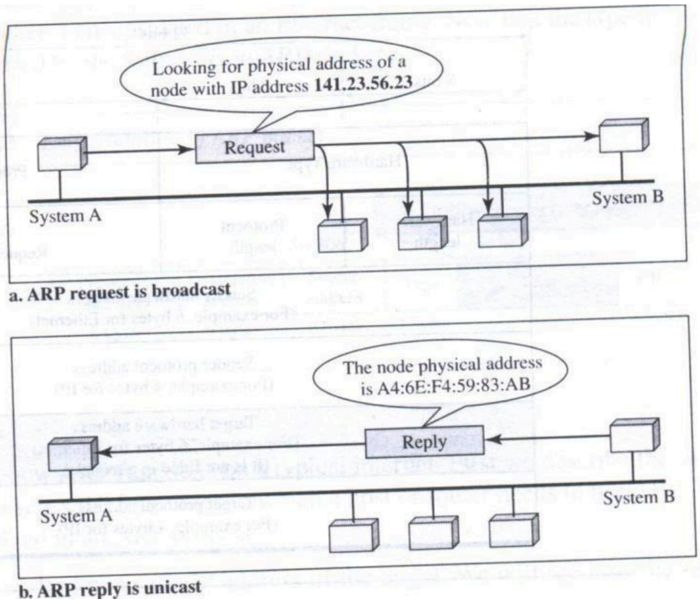

Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
a. ARP request is broadcast
The node physical address is A4:6E:F4:59:83:AB
Reply
System A
System B
b. ARP reply is unicast

Figure 5.12 ARP operation

In Figure 5.12 a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IF address of 141.23.56.23.

This packet is received by every system on the physical network, but only system B will answer it. Now system A can send all the packets it has for this destination by using the physical address it received.

Operation

Let us see how ARP functions on a typical internet. First we describe the steps involved. we discuss the four cases in which a host or router needs to use ARP. These are the steps involved in an ARP process:

1. The sender knows the IP address of the target. We will see how the sender obtains this shortly.

2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with Os.

3. The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as the source address and the physical broadcast address as the destination address.

4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes its IP address.

5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.

6. The sender receives the reply message. It now knows the physical address of the target machine.

7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

Mapping Physical to Logical Address: RARP, BOOTP, and DHCP

There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

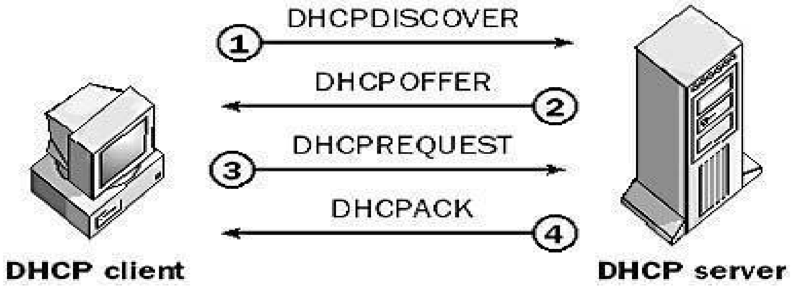
RARP

Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical(IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses.

DHCP (Dynamic Host Configuration Protocol)

- DHCP stands for Dynamic Host Configuration Protocol.
- Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network.

DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server



Process of DHCP server configuration

DHCP (Dynamic Host Configuration Protocol) is a client-server protocol that uses DHCP servers and DHCP clients. A DHCP server is a machine that runs a service that can lease out IP addresses and other TCP/IP information to any client that requests them. The DHCP server typically has a pool of IP addresses that it is allowed distribute to clients, and these clients leasean IP address from the pool for a specific period of time, usually several days. Once the lease is ready to expire, the client contacts the server to arrange for renewal. DHCP clients are client machines that run special DHCP clients of to communicate with DHCP server.

DHCP DISCOVER: The client broadcasts a request for a DHCP server.

DHCPOFFER: DHCP servers on the network offer an address to the client.

DHCPREQUEST: The client broadcasts a request to lease an address from one of the offering DHCP servers.

DHCPACK: The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.

5.3 IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.IPv4 addresses is unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time. We will see later that, by using some strategies, an address may be assigned to a device for a time period and then taken away and assigned to another device.

On the other hand, if a device operating at the network layer has m connections to the Internet, it needs to have m addresses. We will see later that a router is such a device.

The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

Notations

There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a4-byte address. The following is an example of an IPv4 address in binary notation:

0111010110010101 0001110100000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address:

117.149.29.2

Figure 5.13 shows an IPv4 address in both binary and dotted-decimal notation.

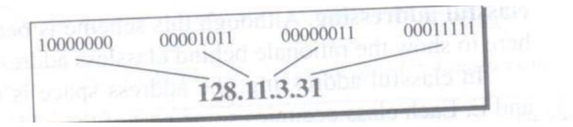


Figure 5.13 Dotted-decimal notation and binary notation of an IPv4 address

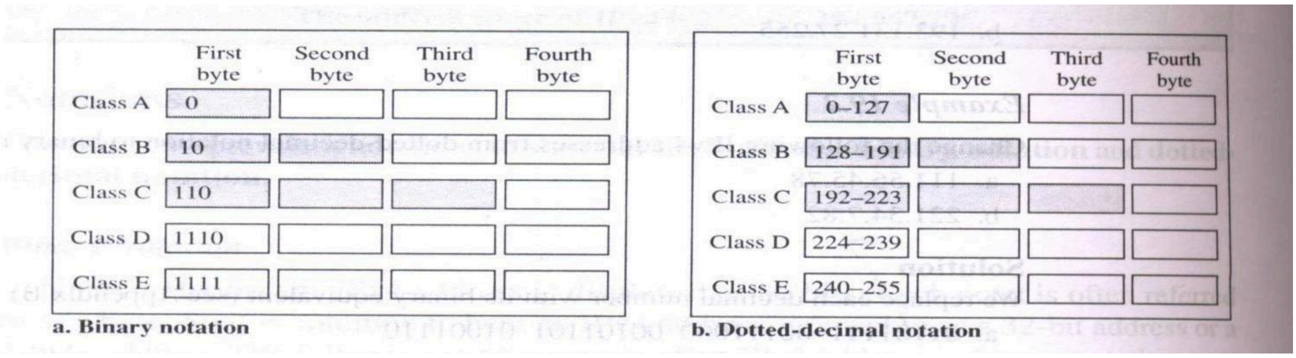
Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show the rationale behind classless addressing.

In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Figure 5.14



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

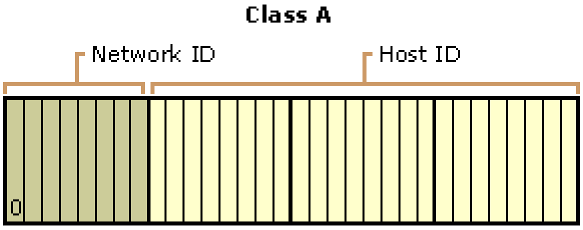
b. Dotted-decimal notation

Figure 5.14 IPv4 Classes

The Internet community originally defined five *address classes* to accommodate networks of varying sizes. Microsoft TCP/IP supports class A, B, and C addresses assigned to hosts. The class of address defines which bits are used for the network ID and which bits are used for the host ID. It also defines the possible number of networks and the number of hosts per network.

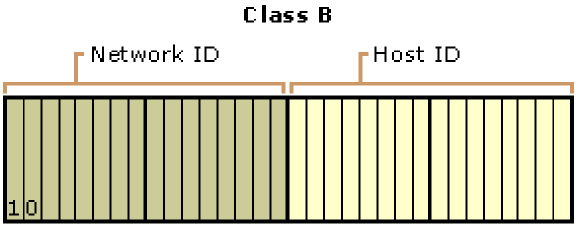
1) Class A

Class A addresses are assigned to networks with a very large number of hosts. The high-order bit in a class A address is always set to zero. The next seven bits complete the network ID. The remaining 24 bits (the last three octets) represent the host ID. This allows for 126 networks and 16,777,214 hosts per network. Figure illustrates the structure of class A addresses.



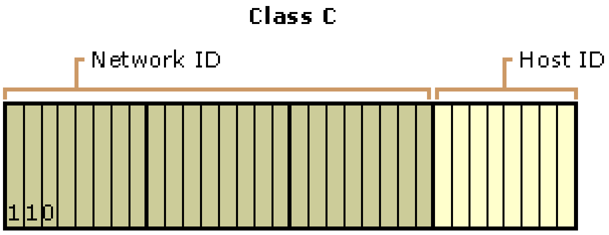
2) Class B

Class B addresses are assigned to medium-sized to large-sized networks. The two high-order bits in a class B address are always set to binary 1 0. The next 14 bits complete the network ID. The remaining 16 bits represent the host ID. This allows for 16,384 networks and 65,534 hosts per network. Figure illustrates the structure of class B addresses.



3) Class C

Class C addresses are used for small networks. The three high-order bits in a class C address are always set to binary 1 1 0. The next 21 bits complete the network ID. The remaining 8 bits (last octet) represent the host ID. This allows for 2,097,152 networks and 254 hosts per network. Figure illustrates the structure of class C addresses.



4) Class D

Class D addresses are reserved for IP multicast addresses. The four high-order bits in a class D address are always set to binary 1 1 1 0. The remaining bits are for the address that interested hosts recognize. Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.

5) Class E

Class E is an experimental address that is reserved for future use. The high-order bits in a class E address are set to 1111.

Example Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is O. This is a class A address.

b. The first 2 bits are 1; the third bit is O. This is a class C address.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

List any four IP functions.

1. **Addressing:** In order to perform the job of delivering datagrams, IP must know where to deliver them to. For this reason, IP includes a mechanism for host addressing. Furthermore, since IP operates over internetworks, its system is designed to allow unique addressing of devices across arbitrarily large networks. It also contains a structure to facilitate the routing of datagrams to distant networks if that is required.

2. **Data Encapsulation and Formatting/Packaging:** IP accepts data from the transport layer protocols UDP and TCP. It then encapsulates this data into an IP datagram using a special format prior to transmission.

3. **Fragmentation and Reassembly:** IP datagrams are passed down to the data link layer for transmission on the local network. However, the maximum frame size of each physical/data-link network using IP may be different. For this reason, IP includes the ability to *fragment* IP datagrams into pieces so they can each be carried on the local network. The receiving device uses the reassembly function to recreate the whole IP datagram again.

4. **Routing / Indirect Delivery:** When an IP datagram must be sent to a destination on the same local network, this can be done easily using the network's underlying LAN/WLAN/WAN protocol using what is sometimes called *direct delivery*. However, in many (if not most cases) the final destination is on a distant network not directly attached to the source. In this situation the datagram must be delivered *indirectly*. This is accomplished by routing the datagram through intermediate devices.

IPv4	IPv6
1. Source and destination addressesare32 bits (4 bytes) in length.	1. Source and destination addresses are 128 bits(16 bytes)in length.
2. Uses broadcast addresses to send traffic to all nodes on a subnet.	2. There arenoIPv6 broadcast addresses. Instead, multicast scoped addresses are used.
3. Fragmentation is supported at Originating hosts and intermediate routers.	3. Fragmentation is not supported at routers. It is only supported at the originating host.
4. IP header includes a checksum.	4. IP header does not include a checksum.
5. IP header includes options.	5. All optional data is moved toIPv6 extension headers.
6.IPsec support is optional	6.IPsec support Is required in a fullIPv6 implementation.
7. No identification of payload for QoS Handling by routers is present within the IPv4 header.	7. Payload identification for QoS handling By routers is included in theIPv6 header using the Flow Label field.

8.Address must be configured either manually or through DHCP	8.Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCP, or manually configured.
9. *IP* address represented in decimal number system	*9. IP* address is represented in hexadecimal number system
10. *‘.’*used as separator.	10. ‘ *:’* used as separator.

Connectionless Versus Connection-Oriented Service

A transport layer protocol can either be connectionless or connection-oriented.

Connectionless Service

In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release. The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either. We will see shortly that one of the transport layer protocols in the Internet model, UDP, is connectionless.

Connection-Oriented Service

In a connection-oriented service, a connection is first established between the sender and the receiver. Data are transferred. At the end, the connection is released. We will see shortly that TCP and SCTP are connection-oriented protocols.

Reliable Versus Unreliable

The transport layer service can be reliable or unreliable. If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service. On the other hand, if the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.

Compare UDP and TCP

TCP	UDP
1. TCP is connection oriented protocol	1. UDP is connection less protocol
2. It provides reliable delivery of messages	2. It provides unreliable delivery of messages
3. It assigns datagram size dynamically for efficiency.	3. Every datagram segment is of the same size.
4. TCP has flow control	4. UDP has no flow control
5. Overhead is low	5. Overhead is very low.
6. Transmission speed is high	6. Transmission speed is very high

Connectionless and connection oriented protocol.

Connection less protocol: These protocols do not establish a connection between devices. It is manually achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there or if it is prepared to receive the information.

Connection-oriented protocol: It means that when devices communication they perform hand sharing to set up on end to end connection. Usually one device begins by sending a request to open a connection, and the other responds.

Connectionless protocols: 1) IP 2) ICMP 3) UDP

1. IP

IP is internet Protocol.

It is unreliable protocol because it does not provide any error control and flow control.

Packets in IP are called "Datagram"

2. ICMP

It is internet control message protocol.

It reports error and sends control messages.

Error reporting messages include – destination unreachable, source quench, time exceed, parameter problem, redirection etc.

Query message includes –echo request and reply, time stamp request and reply, router solicitation and advertisement etc.

3. UDP

UDP is user datagram protocol.

It is connectionless protocol because data is sent without establishing a connection between sender and receiver before sending the data.

UDP is unreliable because data is delivered without acknowledgement.

UDP does not perform Auto retransmission.

UDP does not use flow control.

UDP has high transmission speed.

Connection oriented protocol:

1) TCP 2) SLIP 3) PPP 4) SMTP

1) TCP

TCP is transmission control protocol.

It is connection oriented protocol because connection must be established prior to transmission of data.

TCP is reliable protocol because data is delivered with acknowledgement.

TCP perform Auto Retransmission if the data is lost.

TCP use flow control.

TCP has low speed of transmission.

2. SLIP

SLIP is serial line internet protocol

SLIP does not perform error detection and correction.

SLIP does not provide any authentication.

SLIP is not approved internet standard.

SLIP supports only Internet protocol (IP)

SLIP supports static IP address assignment

3. PPP

PPP is point to point protocol.

PPP perform error detection

PPP provides authentication and security.

PPP is approved internet standard.

PPP supports IP and other protocols.

PPP supports Dynamic IP address assignment

4. SMTP

SMTP is simple mail transfer protocol.

It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection.

SMTP is standard application layer protocol for delivery of email over TCP/IP network.

SMTP establishes a TCP connection between sender and port number 25 of receiver.

OSI reference model	TCP/IP network model
1)It has 7 layers	1)It has 4 layers
2)Transport layer guarantees delivery of packets	2)Transport layer does not guarantees delivery of packets
3)Horizontal approach	3)Vertical approach
4)Separate presentation layer	4)No session layer, characteristics are provided by transport layer
5)Separate session layer	5)No presentation layer, characteristics are provided by application layer
6)Network layer provides both connectionless and connection oriented services	6)Network layer provides only connection less services
7)It defines the services, interfaces and protocols very clearly and makes a clear distinction between them	7)It does not clearly distinguishes between service interface and protocols
8)The protocol are better hidden and can be easily replaced as the technology changes	8)It is not easy to replace the protocols
9)OSI truly is a general model	9)TCP/IP cannot be used for any other application
10)It has a problem of protocol filtering into a model	10)The model does not fit any protocol stack.

Addressing:

- The addresses can be of different types such as physical address and logical address
- In an internet employing the TCP/IP protocols, four level of addresses are used by computer
- When the computer wish to communicate with one another, they need to know the address of each other each computer has its own address.

- Physical Address
- Logical Address
- Port Address
- Specific Address

- **Physical Address (MAC Address):**
  - ✔ The packet from source to destination hosts pass through physical network.
  - ✔ At the physical level the IP address is not useful but the hosts and router are recognized by their MAC addresses.
  - ✔ A MAC address is the local address.it is unique locally but it is not unique universally.
- **Logical Address (IP Address):**
  - ✔ Logical address are required to facilitate universal communications in which different types of physical network can be involved.
  - ✔ The logical address is also called as the IP Address

- **Port Address**
  - ✔ Port is a logical address of a 16-bit unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.

- **Specific Address**

  - ✔ Some applications have user-friendly addresses that are designed for that specific application.
  - ✔ Examples include the e-mail address and the Universal Resource Locator (URL) .