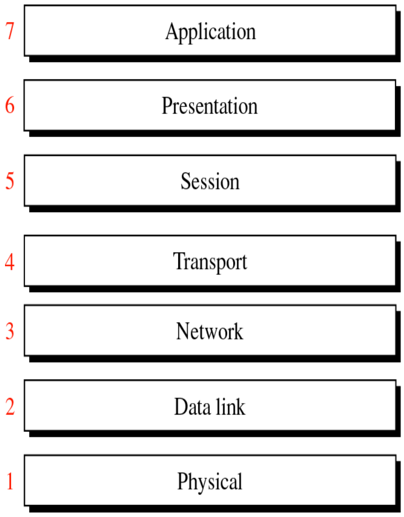
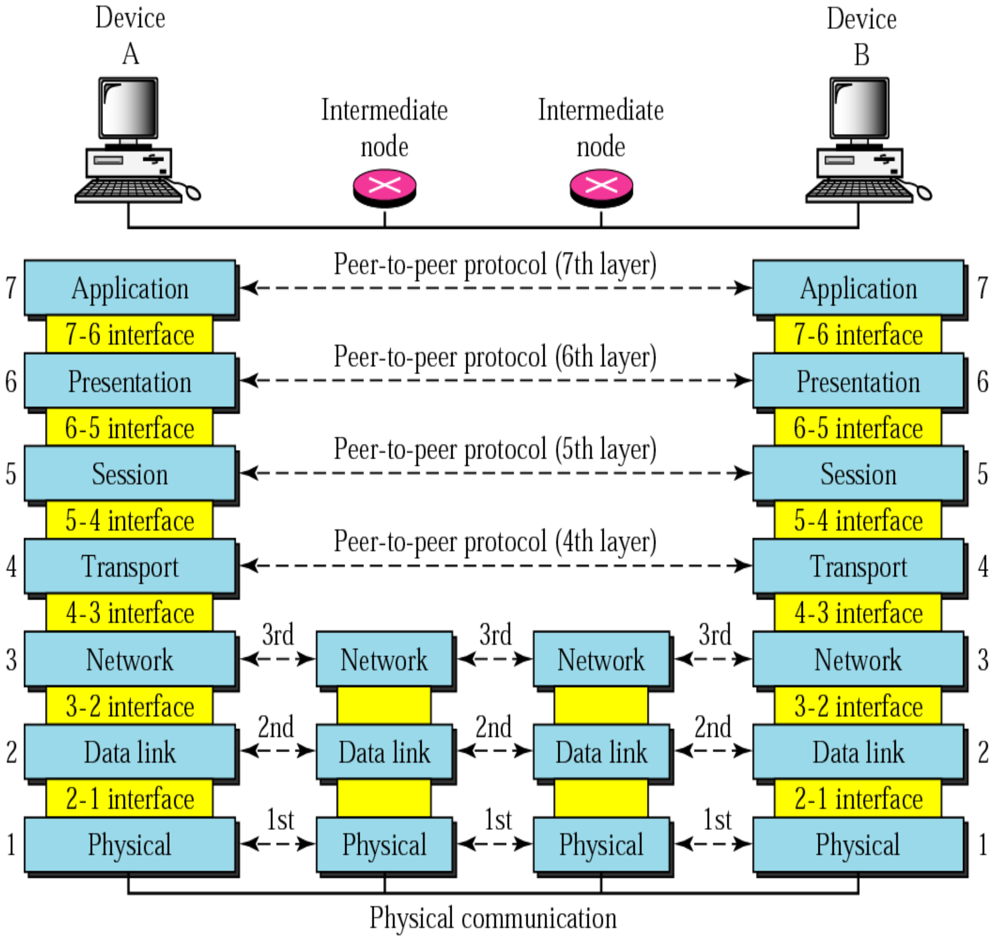
OSI (Open Systems Interconnected)

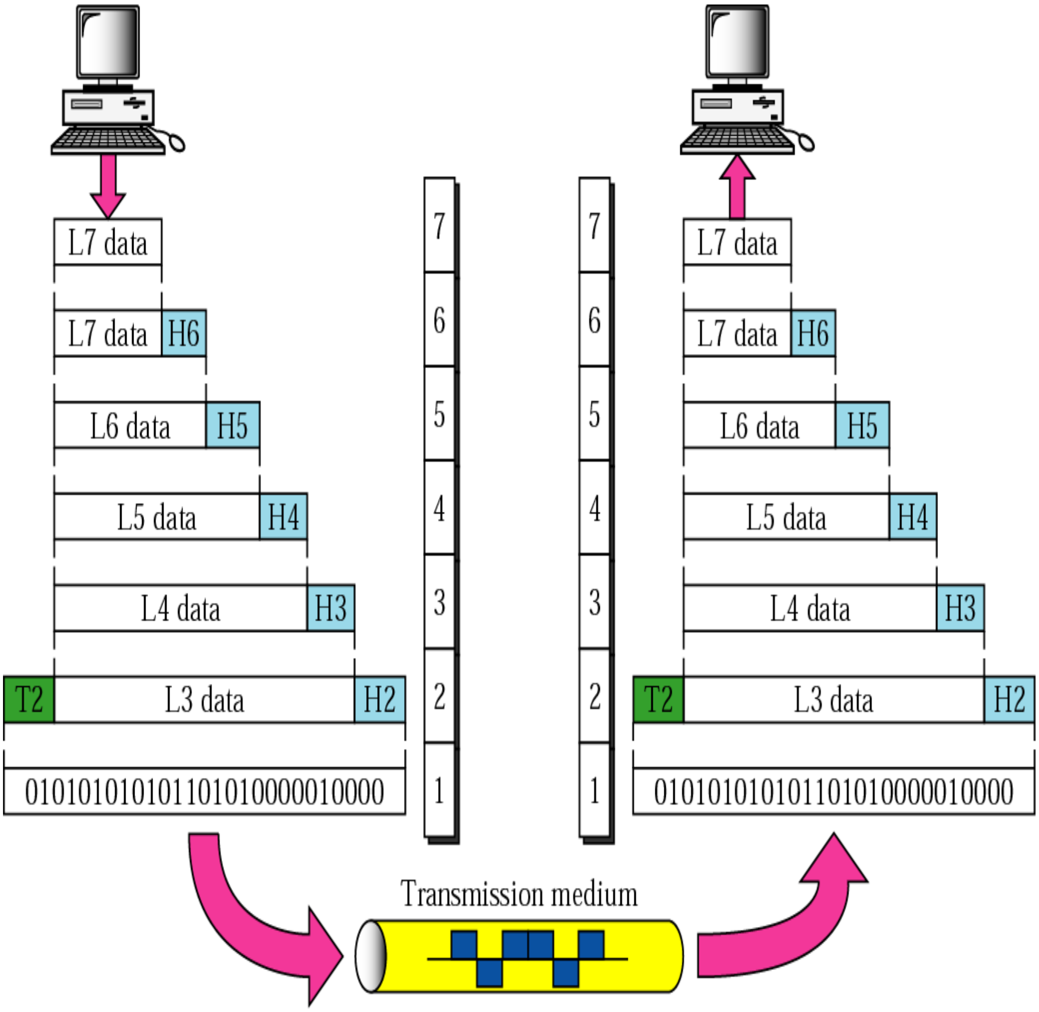
Reference Model

OSI reference model was developed by the international standards organization (ISO) at 1983. This model is called OSI because it deals with connectivity open systems (systems that are open for communication with other systems). The OSI model has seven layers.





An exchange using the OSI model:



Headers are added to the data at layers 6, 5, 4, 3, and 2. Trailers are usually added only at layer 2.

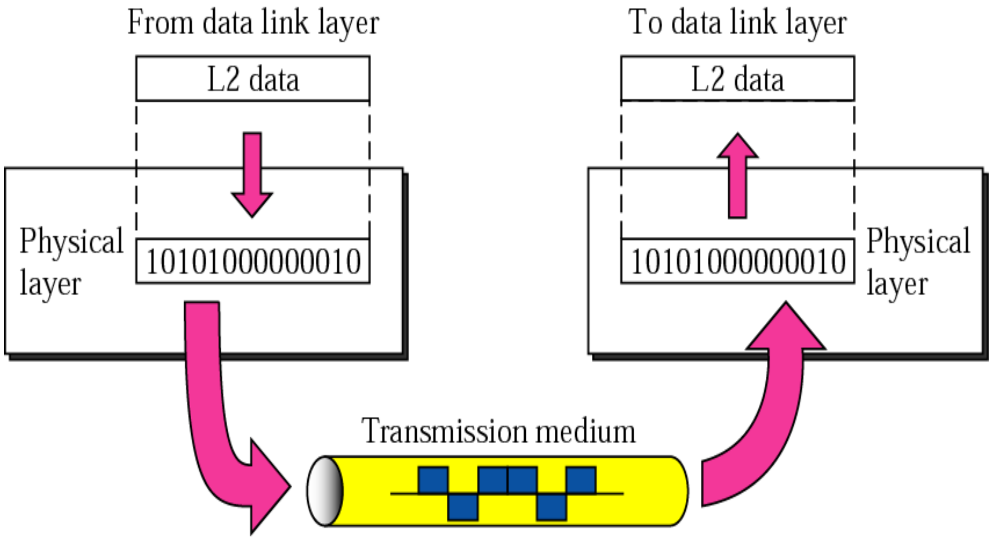
Layers in OSI Model:

Layer 1: Physical Layer

The first layer of the OSI model is the *Physical* layer, which specifies the electrical and mechanical requirements for transmitting data bits across the transmission medium (cable or airwaves). It involves sending and receiving the data stream on the carrier, whether that carrier uses electrical (cable),light (fiber optic), radio, infrared, or laser (wireless) signals.

The Physical layer specifications include: Voltage changes, The timing of voltage changes, Data rates, Maximum transmission distances, The physical connectors to the transmission medium (plug), and The topology or physical layout of the network.

Many complex issues are addressed at the Physical layer, including digital vs. analog signaling, baseband vs. broadband signaling, whether data is transmitted synchronously or asynchronously, and how signals are divided into channels (multiplexing). Devices that operate at the Physical layer deal with signaling (e.g., transceivers on the NIC), repeaters, basic hubs, and simple connectors that join segments of cable). The data handled by the Physical layer is in bits of 1s (ones) and 0s (zeros),which are represented by pulses of light or voltage changes of electricity, and by the state of those pulses (*on* generally representing *1* and *off* generally representing *0*). How these bits are arranged and managed is a function of the Data Link layer (layer 2) of the OSI model.



Layer 2: Data Link Layer

Layer 2 is the Data Link layer, which is responsible for maintaining the data link between two computers, typically called hosts or nodes. It also defines and manages the ordering of bits to and from packets. Frames contain data arranged in an organized manner, which provides an orderly and consistent method of sending data bits across the medium. Without such control, the data would be sent in random sizes or configurations and the data on one end could not be decoded at the other end. The Data Link layer manages the physical addressing and synchronization of the data packets. It is also responsible for flow control and error notification on the Physical layer. Flow control is the process of managing the timing of sending and receiving data so that it doesn’t exceed the capacity (speed, memory, and so on) of the physical connection. Since the Physical layer is only responsible for physically moving the data onto and off of the network medium, the Data Link layer also receives and manages error messaging related to the physical delivery of packets.

Network devices that operate at this layer include layer 2 switches (switching hubs) and bridges. A layer 2 switch decreases network congestion by sending data out only on the port that the destination computer is attached to, instead of sending it out on all ports. Bridges provide a way to segment a network into two parts and filter traffic, by building tables that define which computers are located on which side of the bridge, based on their MAC addresses.

The Data Link layer is divided into two sublayers: the Logical Link Control (LLC) sublayer and the MAC sublayer.

The MAC Sublayer:

The MAC sublayer provides control for accessing the transmission medium. It is responsible for moving data packets from one NIC to another, across a shared transmission medium such as an Ethernet or fiber-optic cable.

Physical addressing is addressed at the MAC sublayer. Every NIC has a unique MAC address (also called the physical address) which identifies that specific NIC on the network. The MAC address of a NIC is usually burned into a read-only memory (ROM) chip on the NIC. Each manufacturer of network cards is provided a unique set of MAC addresses so that theoretically, every NIC that is manufactured has a unique MAC address. To avoid any confusion, MAC addresses are permanently burned into the NIC’s memory, which is sometimes referred to as the Burned-in Address (BIA).

NOTE:

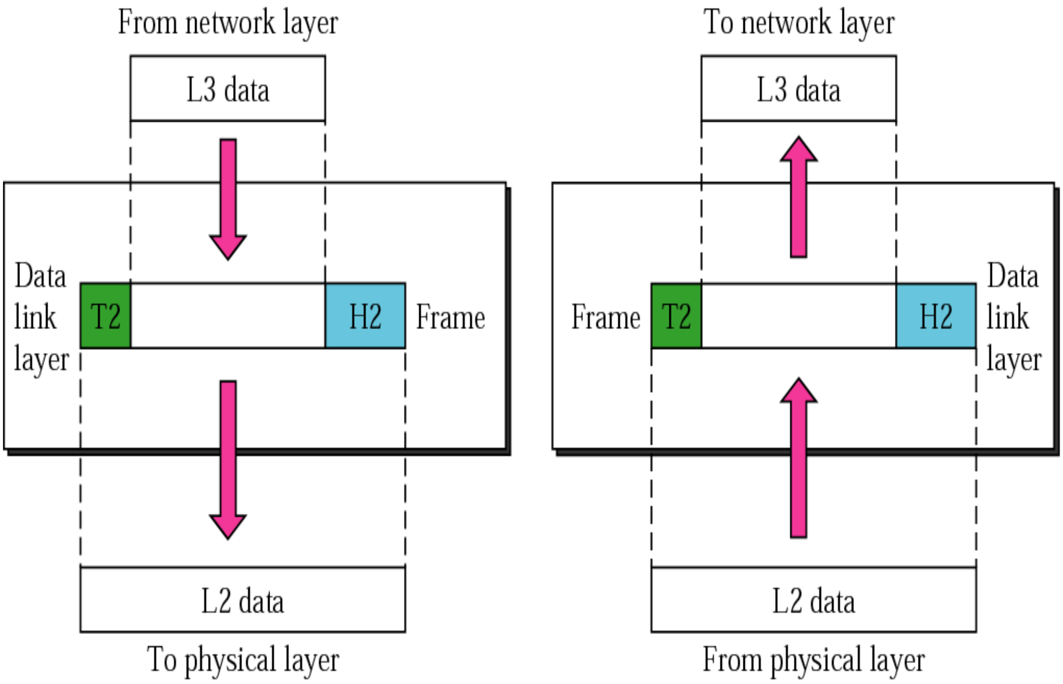
On Ethernet NICs, the physical or MAC address (also called the hardware address) is expressed as 12 hexadecimal digits arranged in pairs with colons between each pair (e.g., 12:3A:4D:66:3A:1C). The initial three sets of numbers represent the manufacturer, and the last three bits represent a unique NIC made by that manufacturer.

MAC refers to the method used to allocate network access to computers while preventing them from transmitting at the same time and causing data collisions.

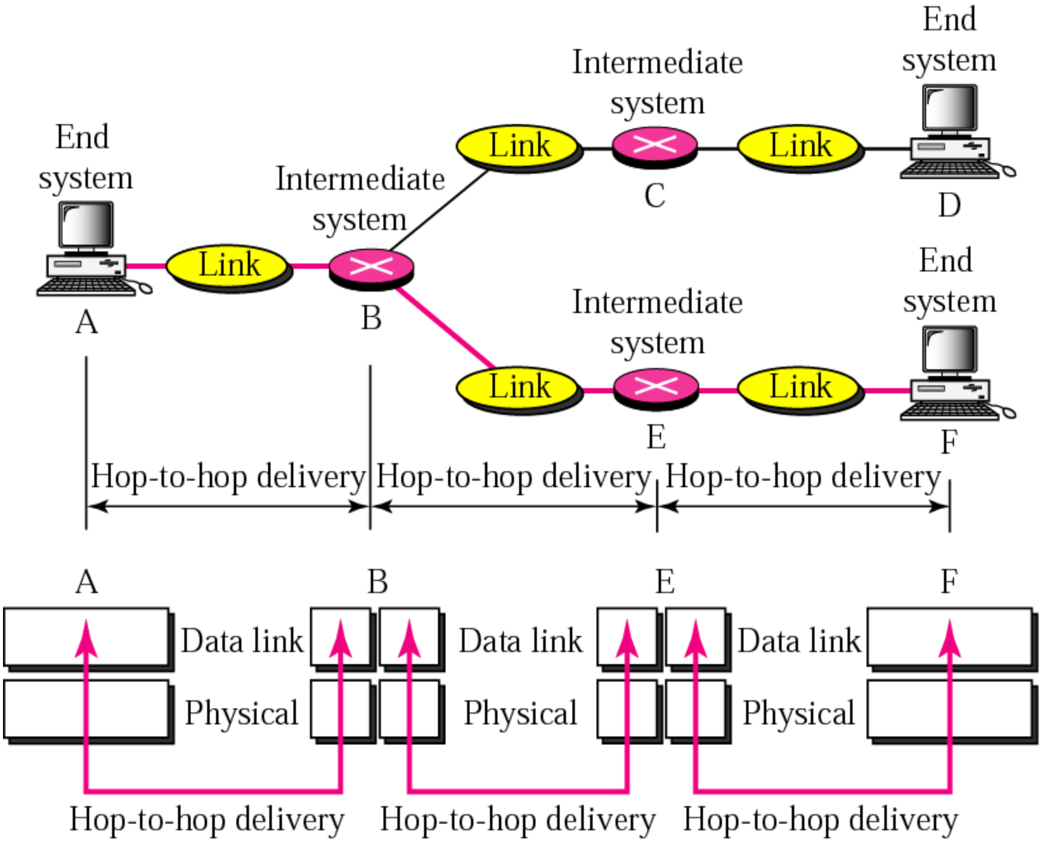
The LLC Sublayer:

The LLC sublayer provides the logic for the data link;thus it controls the synchro-nization, flow control, and error-checking functions of the Data Link layer. This layer manages connection-oriented transmissions; however, connectionless service can also be provided by this layer. Connectionless operations are known as Class I LLC, whereas Class II can handle either connectionless or connection-oriented operations. With connection-oriented communication, each LLC frame sent is acknowledged. The LLC sublayer at the receiving end keeps up with the LLC frames it receives (also called Protocol Data Units [PDUs]); therefore, if it detects that a frame has been lost during transmission, it can send a request to the sending computer to start the transmission over again, beginning with the PDU that never arrived.

The LLC sublayer sits above the MAC sublayer, and acts as a liaison between the upper layers and the protocols that operate at the MAC sublayer (e.g., Ethernet, Token Ring, and so on).The LLC sublayer is defined by Institute of Electrical &Electronics Engineers (IEEE) 802.2. Link addressing, sequencing, and definition of Service Access Points (SAPs) also take place at this layer.



Node-to-node delivery:



Layer 3: Network Layer

The next layer is the *Network* layer (layer 3),which is where packets are sequenced and logical addressing is assigned. Logical addresses are nonpermanent, software assigned addresses that can only be changed by administrators. The IP addresses used by the TCP/IP protocols on the Internet, and the Internet Package Exchange (IPX) addresses used by the IPX/Sequenced Packet Exchange (SPX) protocols on NetWare networks are examples of logical addresses. These protocol stacks are referred to as *routable* because they include addressing schemes that identify the network or subnet and the particular client on that network or subnet.

NOTE:

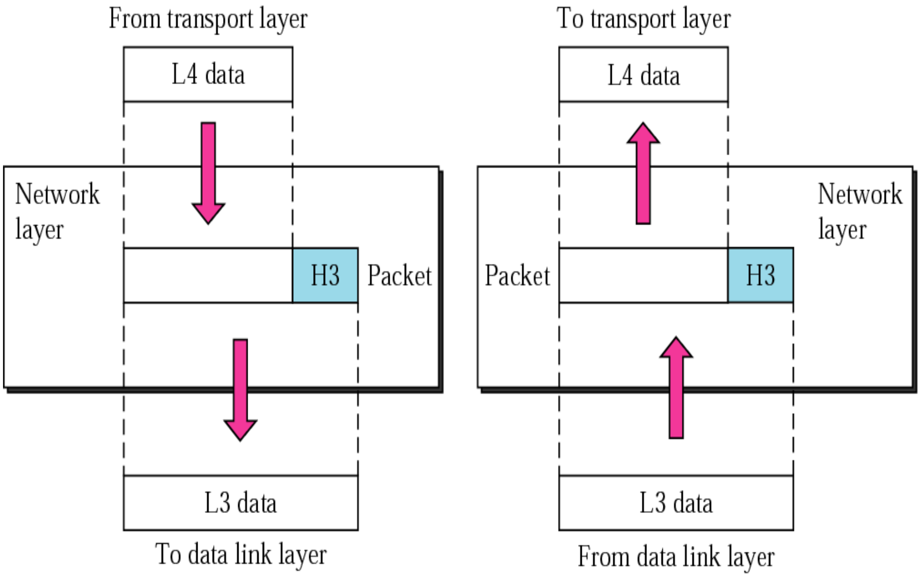
To understand the difference between physical and logical addresses, consider this analogy: A house has a physical address that identifies exactly where it is located. This is similar to the MAC address on a NIC.

A house also has a logical address assigned to it by the post office that consists of a street name and number. The post office occasionally changes the names of streets or renumbers the houses located on them This is similar to the IP address assigned to a network interface.

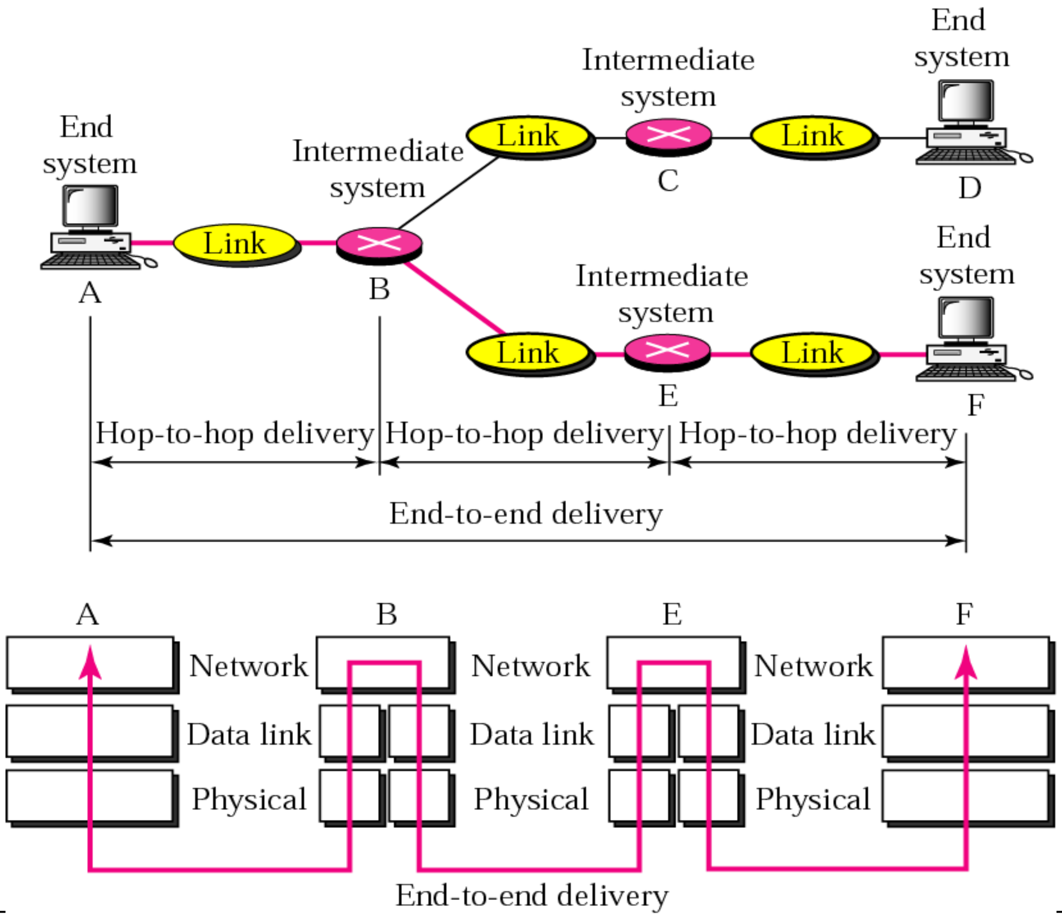
The Network layer is also responsible for creating a virtual circuit (i.e., a logical connection, not a physical connection) between points or nodes. A node is a device that has a MAC address, which typically includes computers, printers, and routers. This layer is also responsible for routing, layer 3 switching, and forwarding packets.

Routing refers to forwarding packets from one network or subnet to another. Without routing, computers can only communicate with computers on the same network. Routing is the key to the global Internet, and is one of the most important duties of the Network layer.

Finally, the Network layer provides additional levels of flow control and error control. As mentioned earlier, from this point on, the primary methods of implementing the OSI model architecture involve software rather than hardware. Devices that operate at this layer include routers and layer 3 switches



End-to-end delivery:



Layer 4: Transport Layer

The transport layer is the heart of the whole protocol hierarchy. Its task is to provide reliable, cost-effective data transport from the source machine to destination machine, independent of the physical network.

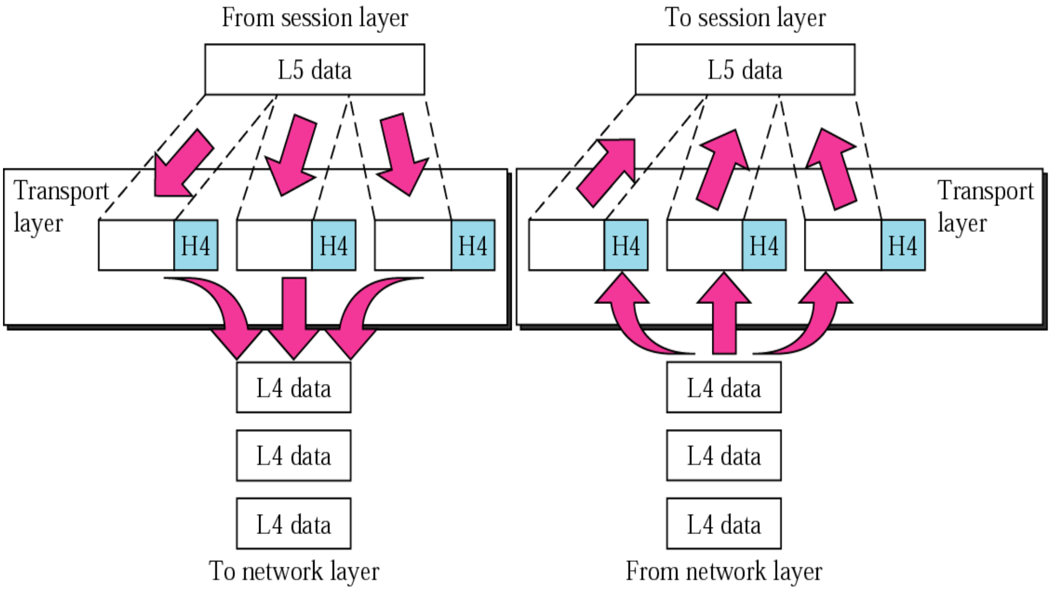
The primary function of transport layer is enhancing the Quality of Service (QoS) provided by the network layer. The QoS parameters are:

1- Connection establishment delay.
2- Connection establishment failure probability.
3- Throughput (number of bits/sec).
4- Residual error ratio (number of lost messages per total sent).
5- Protection.
6- Priority.
7- Resilience (Probability of transport layer terminating a connection due to internal problems).

The QoS are specified by transport layer when a connection is requested.

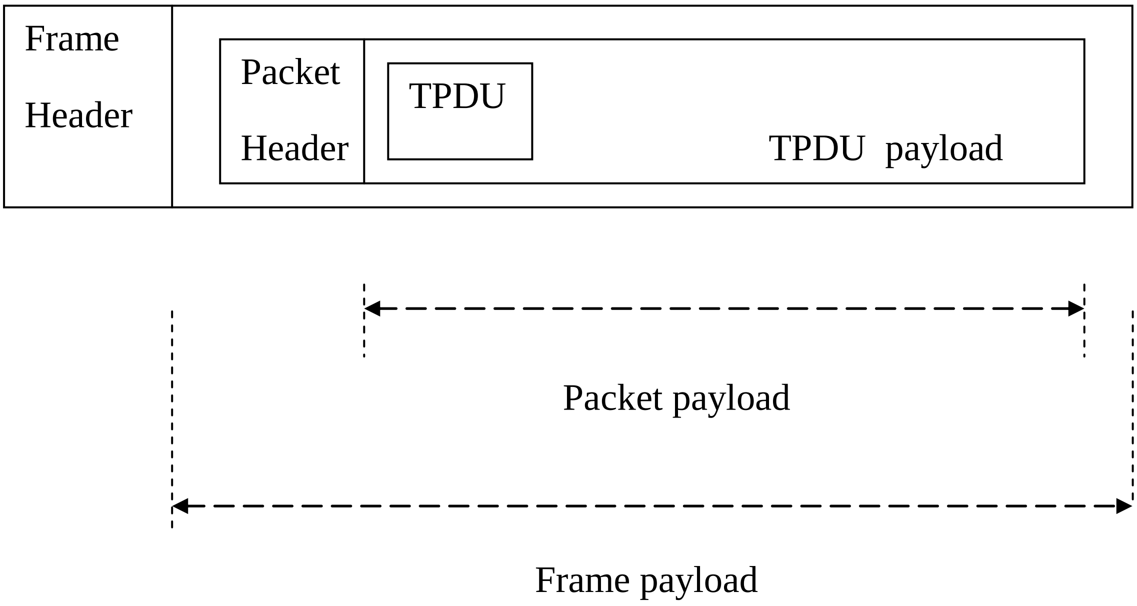
Other tasks of transport layer are:

1- Accept data from the session layer, split it up to the smaller units if needed, pass these to the network layer and ensure that all pieces arrive correctly at the other end.
2- Determines what type of service to provide the session layer (connection oriented or connectionless).
3- Multiplexing several message streams onto one channel.
4- Take care of establishing and deleting connections across the network.
5- The option negotiation such as about the speed or the throughput.



Note:

Transport protocol data (TPDU) sent from transport entity in source machine to transport entity in destination machine. The TPDUs exchanged by the transport layer are contained in packets (exchanged by the network layer). The packets are contained in frames (exchanged by the data link layer) as shown in figure below:



NOTE:

What's the difference between a connection-oriented protocol and a connectionless protocol? A connection-oriented protocol (e.g., TCP) creates a connection between two computers before sending the data, and then verifies that the data has reached its destination by using acknowledgements (ACKs) (i.e., messages sent back to the sending computer from the receiving computer that acknowledge receipt). Connectionless protocols send the data and trust that it will reach the proper destination or that the application will handle retransmission and data verification.

Consider this analogy: You need to send an important letter to a business associate that contains valuable papers. You call him before e-mailing the letter, to let him know that he or she should expect it (establishing the connection). A few days later your friend calls to let you know that he received the letter, or you receive the return receipt (ACK).

This is how connection-oriented communication works. When mailing a postcard to a friend, you drop it in the mailbox and hope it gets to the addressee. You don’t expect or require any acknowledgement. This is how connectionless communication works.

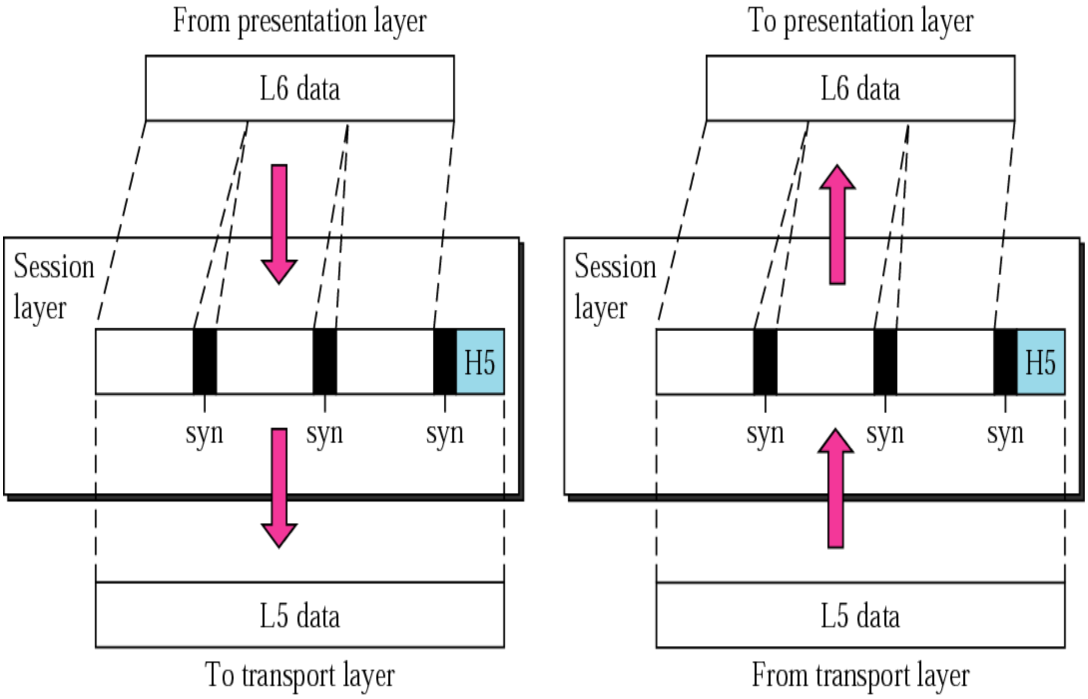
Layer 5: Session Layer

After the Transport layer establishes a virtual connection, a communication session is made between two processes on two different computers. The Session layer (layer 5) is responsible for establishing, monitoring, and terminating sessions, using the virtual circuits established by the Transport layer. The Session layer is also responsible for putting header information into data packets that indicates where a message begins and ends. Once header information is attached to the data packets, the Session layer performs synchronization between the sender’s Session layer and the receiver’s Session layer. The use of ACKs helps coordinate the transfer of data at the Session-layer level.

Another important function of the Session layer is controlling whether the communications within a session are sent as full-duplex or half-duplex messages. Half-duplex communication goes in both directions between the communicating computers, but information can only travel in one direction at a time (e.g., radio communications where you hold down the microphone button to transmit, but cannot hear the person on the other end).With full-duplex communication, information can be sent in both directions at the same time (e.g., a telephone conversation, where both parties can talk and hear one another at the same time).

Whereas the Transport layer establishes a connection between two machines, the Session layer establishes a connection between two processes. An application can run many processes simultaneously to accomplish the work of the application.

After the Transport layer establishes the connection between the two machines, the Session layer sets up the connection between the application process on one computer and the application process on another computer.

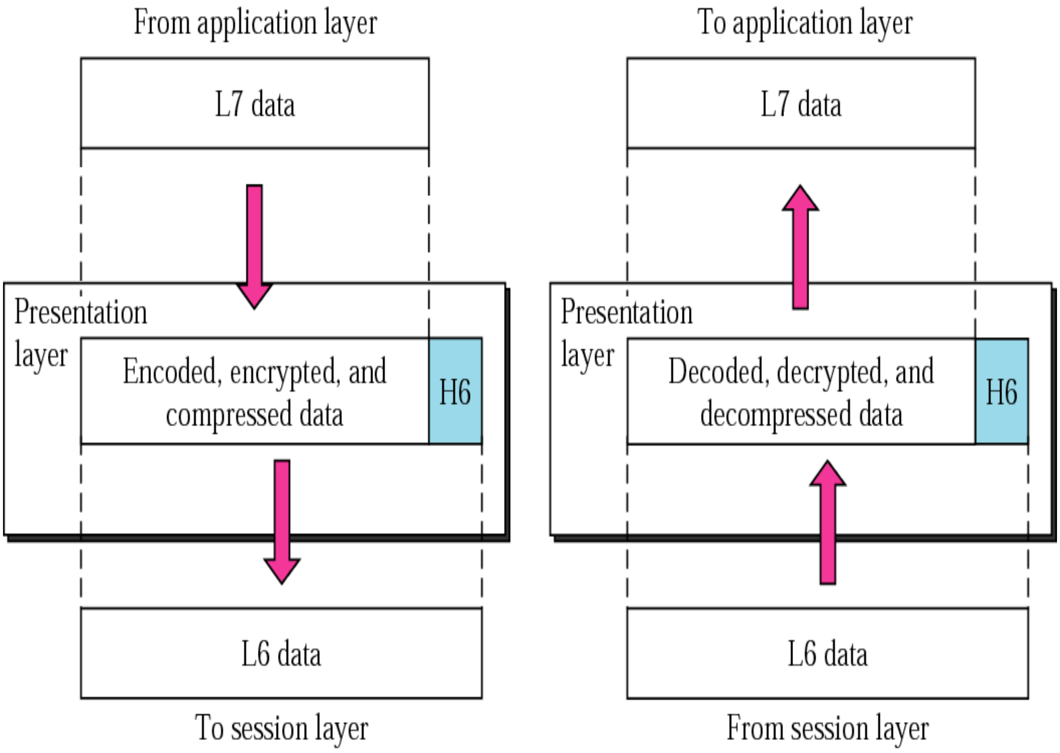


Layer 6: Presentation Layer

Data translation is the primary activity of the Presentation layer (layer 6).When data is sent from a sender to a receiver, it is translated at the Presentation layer (i.e., the sender's application passes data down to the Presentation layer, where it is changed into a common format).When the data is received on the other end, the Presentation layer changes it from the common format back into a format that is useable by the application. Protocol translation (i.e., the conversion of data from one protocol to another so that it can be exchanged between computers using different platforms) takes place here.

The Presentation layer is also where gateway services operate. Gateways are connection points between networks that use different platforms or applications (e.g., e-mail gateways, Systems Network Architecture (SNA) gateways, and gateways that cross platforms or file systems). Gateways are usually implemented via software such as the Gateway Services for NetWare (GSNW). Software redirectors also operate at this layer.

This layer is also where data compression takes place, which minimizes the number of bits that must be transmitted on the network media to the receiver. Data encryption and decryption also take place in the Presentation layer.

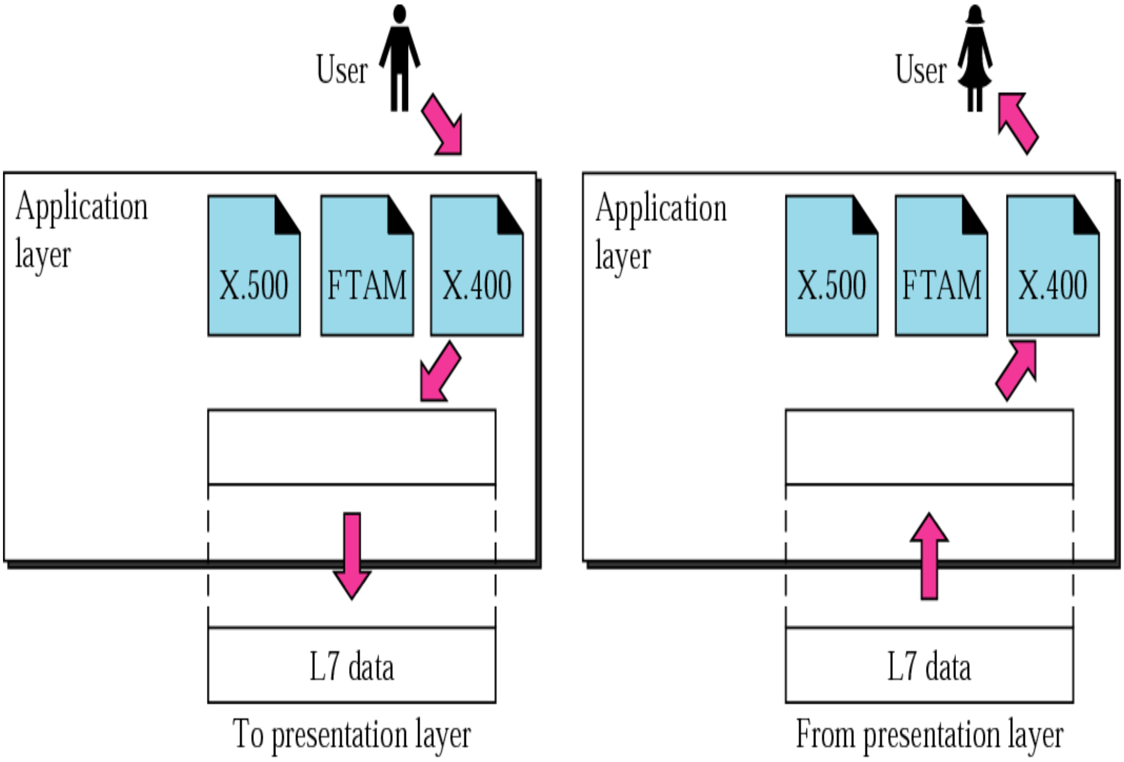


Layer 7: Application Layer

The *Application* layer is the point at which the user application program interacts with the network. Don't confuse the networking model with the application itself. Application processes (e.g., file transfers or e-mail) are initiated within a user application (e.g., an e-mail program).Then the data created by that process is handed to the Application layer of the networking software. Everything that occurs at this level is application-specific (e.g., file sharing, remote printer access, network monitoring and management, remote procedure calls, and all forms of electronic messaging).

You have to distinguish between the protocols mentioned and the applications that might bear the same names, because there are many different FTP programs made by different software vendors that use the FTP to transfer files.

The OSI model is generic and can be used to explain all network protocols. Various protocol suites are often mapped against the OSI model for this purpose. A solid understanding of the OSI model aids in network analysis, comparison, and troubleshooting. However, it is important to remember that not all protocols map well to the OSI model (e.g.,TCP/IP was designed to map to the U.S. Department of Defense (DoD) model).


User
User
Application layer
X.500
FTAM
X.400
Application layer
X.500
FTAM
X.400
L7 data
To presentation layer
L7 data
From presentation layer