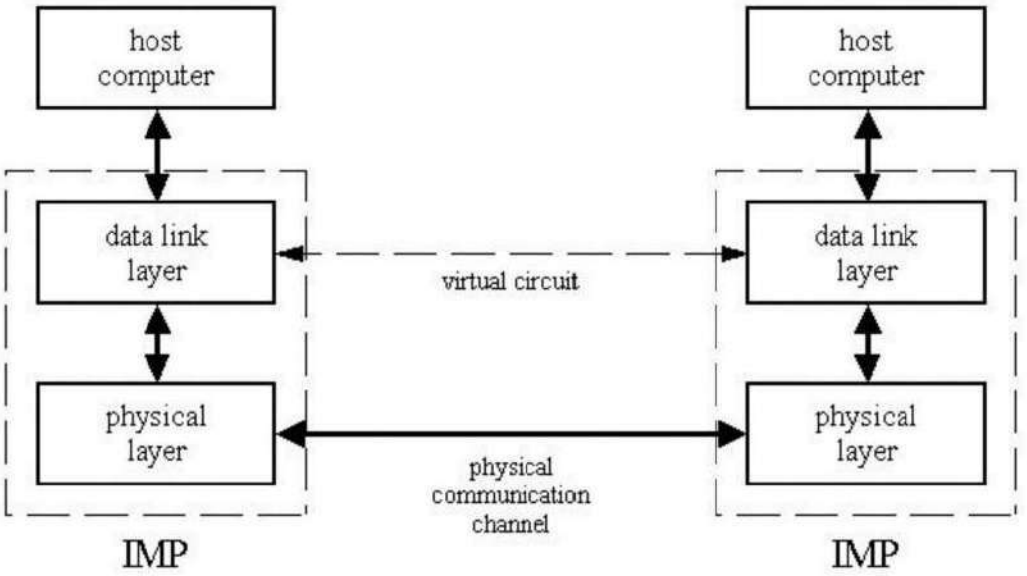
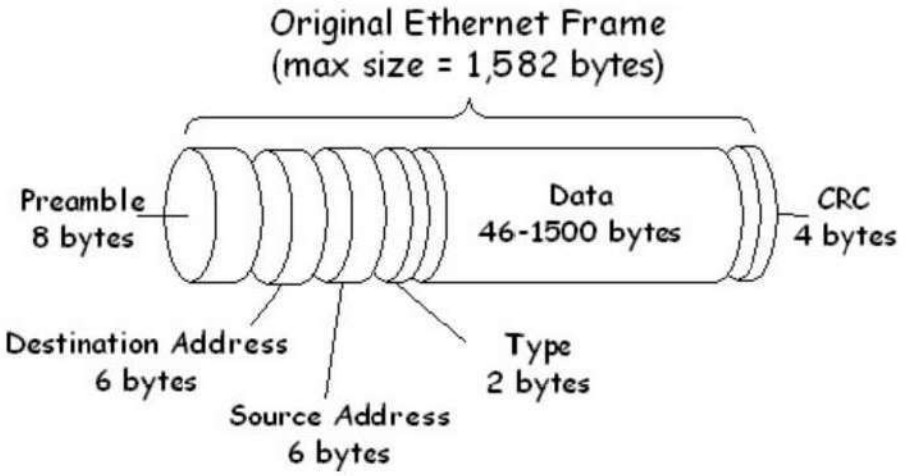
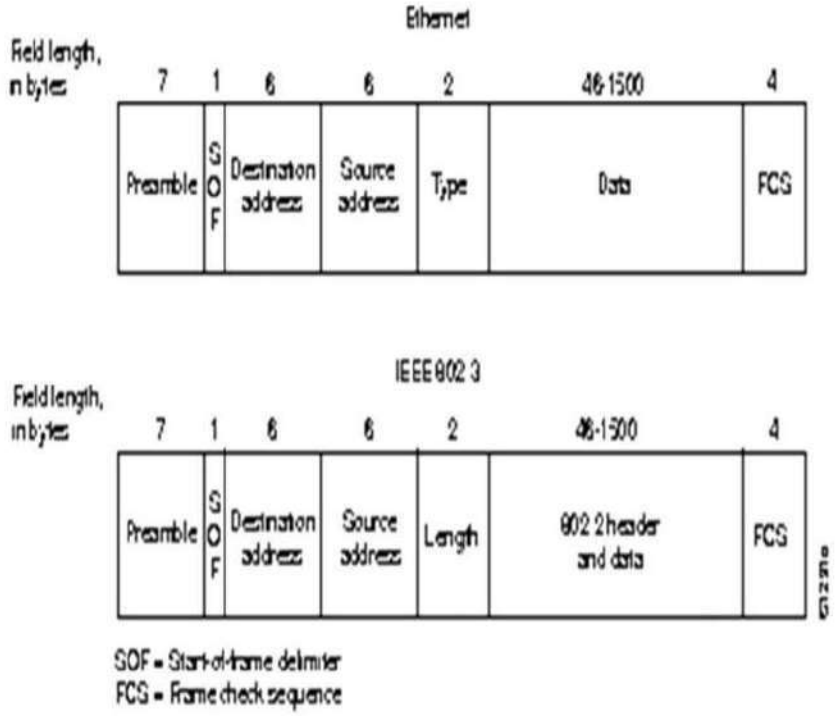
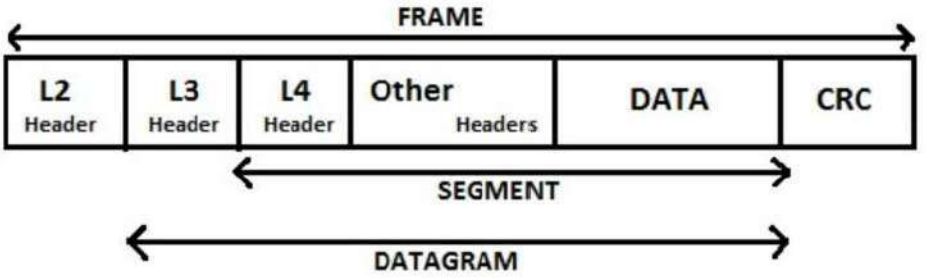

host computer
host computer
data link layer
data link layer
virtual circuit
physical layer
physical layer
physical communication channel
IMP
IMP


Original Ethernet Frame
(max size = 1,582 bytes)
Preamble
8 bytes
Data
46-1500 bytes
CRC
4 bytes
Destination Address
6 bytes
Source Address
6 bytes
Type
2 bytes

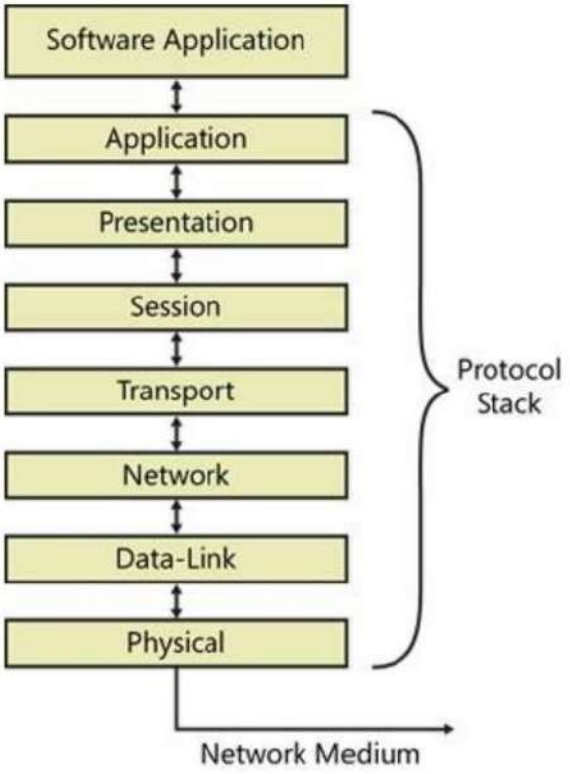


DATA PACKET



Packet at Layer 4 is called SEGMENT
Packet at Layer 3 is called DATAGRAM
Packet at Layer 2 is called FRAME

CISCOCHAMP.COM



The network layer:

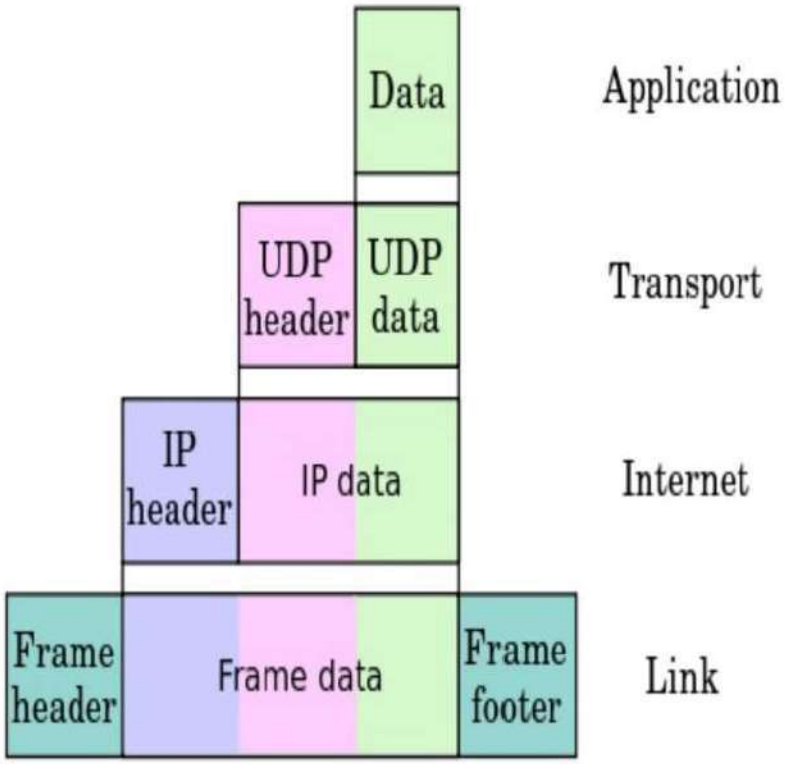
1. **The network layer, the third layer of the OSI model, is responsible for logical addressing and routing data packets across different networks.**
2. **It provides the necessary protocols and services to enable communication between devices on different networks, regardless of their physical connections.**
3. **One of the key functions of the network layer is to determine the optimal path for data packets to reach**

their destination by utilizing routing algorithms and maintaining routing tables.

4. The network layer encapsulates the data received from the transport layer into packets, adding necessary header information such as source and destination IP addresses.
5. It also performs fragmentation and reassembly of packets if the data is too large to fit within a single packet, ensuring efficient transmission across the network.
6. Network layer protocols, such as Internet Protocol (IP), enable the identification and addressing of devices by assigning unique IP addresses to each device on a network.
7. The network layer is responsible for delivering packets from the source device to the destination device, even if the devices are on different networks.
8. It handles issues such as packet loss, congestion control, and quality of service (QoS) to ensure reliable

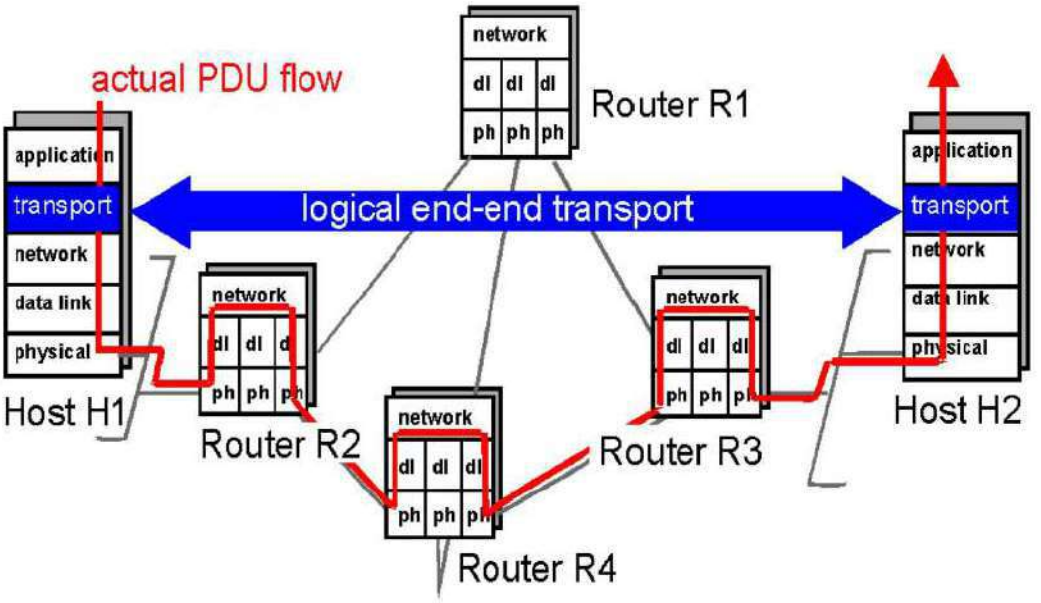
and efficient data transmission.

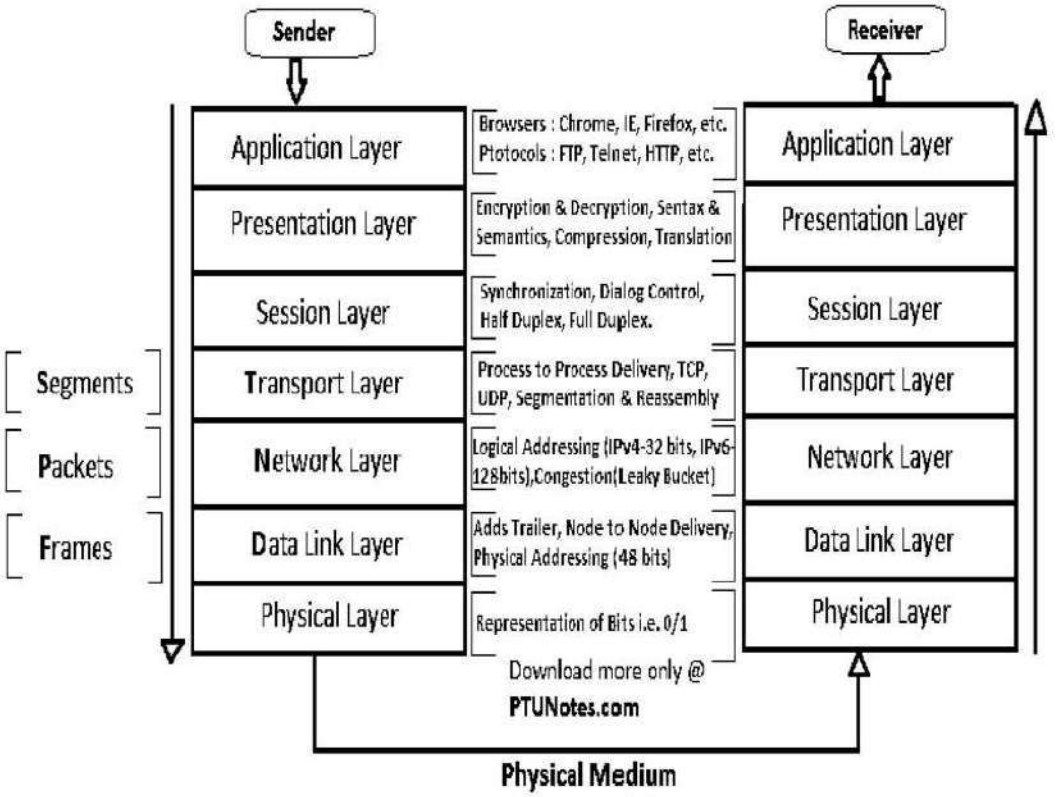
9. Network layer devices, such as routers, operate at this layer and make forwarding decisions based on the destination IP address of the packets.
10. The network layer plays a crucial role in the overall functioning of the Internet, allowing for interconnectivity and global communication between networks and devices.



The transport layers.

1. The transport layer, the fourth layer of the OSI model, is responsible for the reliable delivery and end-to-end communication of data between hosts on a network.
2. It provides services such as segmentation, reassembly, and error checking to ensure data is transmitted correctly and efficiently.
3. The transport layer establishes connections between applications running on different hosts using protocols like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
4. TCP, a connection-oriented protocol, guarantees data delivery by establishing a reliable connection, managing flow control, and performing error recovery.
5. UDP, a connectionless protocol, offers a lightweight alternative to TCP, providing a best-effort delivery mechanism without the overhead of establishing a connection or performing extensive error recovery.


actual PDU flow
application
transport
network
data link
physical
Host H1
network
dl dl dl
ph ph ph
Router R1
logical end-end transport
Router R2
Router R3
Router R4
Host H2

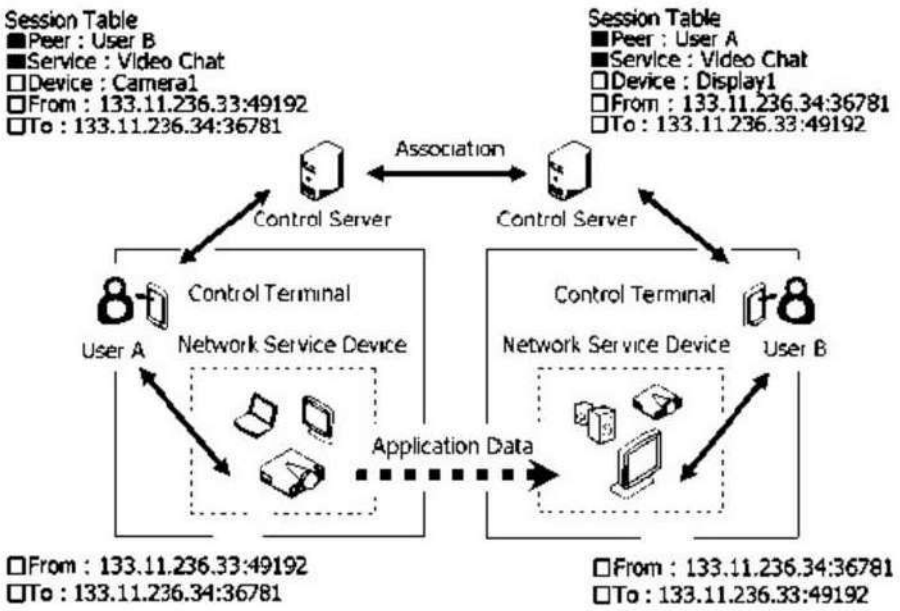

Sender
Receiver
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Segments
Packets
Frames
Browsers : Chrome, IE, Firefox, etc.
Ptotocols : FTP, Telnet, HTTP, etc.
Encryption & Decryption, Sentax & Semantics, Compression, Translation
Synchronization, Dialog Control, Half Duplex, Full Duplex.
Process to Process Delivery, TCP, UDP, Segmentation & Reassembly
Logical Addressing (IPv4-32 bits, IPv6-128bits),Congestion(Leaky Bucket)
Adds Trailer, Node to Node Delivery, Physical Addressing (48 bits)
Representation of Bits i.e. 0/1
Download more only @
PTUNotes.com
Physical Medium

Session layer:

1. The session layer, the fifth layer of the OSI model, is responsible for establishing, managing, and terminating sessions or connections between applications running on different network devices.
2. It provides services that allow applications to communicate and exchange data reliably, including session establishment, maintenance, and synchronization.
3. The session layer handles session control protocols, which manage the dialogue and coordination between communicating applications, ensuring that data is transmitted in an organized and synchronized manner.
4. It also handles session checkpointing and recovery, allowing for the resumption of interrupted sessions in case of network failures or disruptions.
5. The session layer provides authentication, authorization, and accounting (AAA) mechanisms to

ensure secure and controlled access to network resources during session establishment.

6. It enables session data encryption and decryption, protecting the confidentiality and integrity of data transmitted between applications.



If this session is with a database server, this layer has checkpoints at various locations so that if the connection is interrupted and restored.

The transition is executed in the database is not lost even if the user has not committed. This activity is called synchronization.

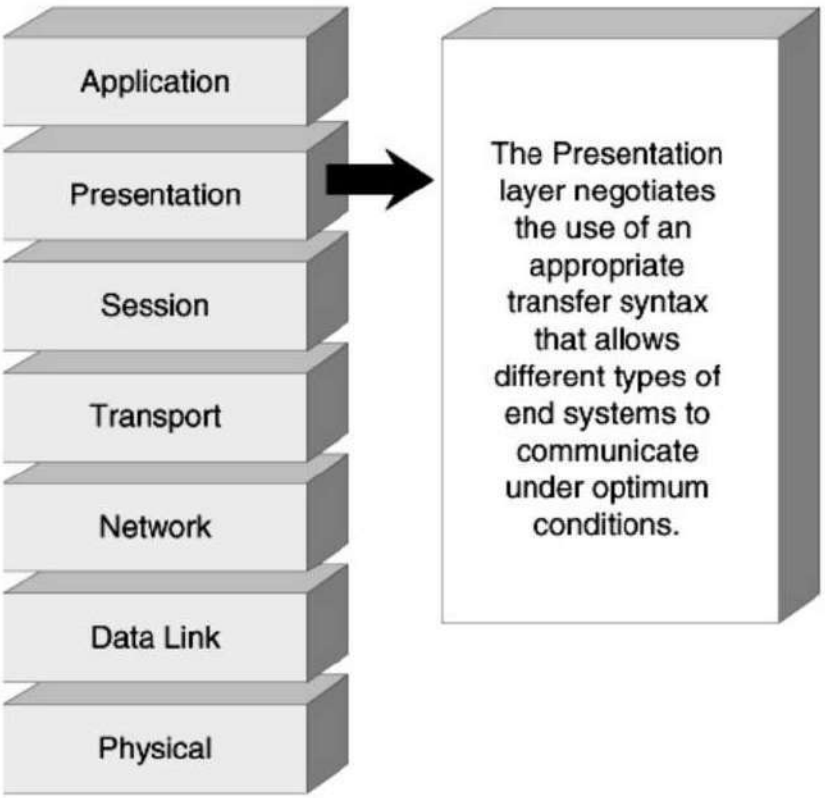
Another function of this layer is the control unit that

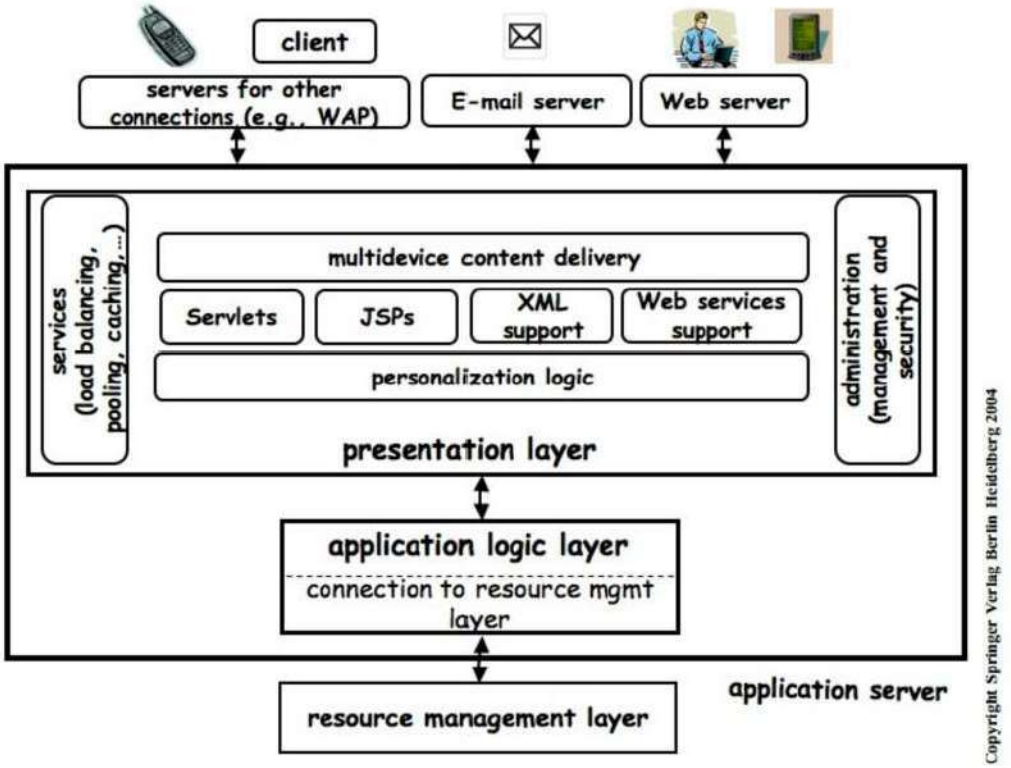
determines who gets to speak at a meeting. That is very useful for video conferencing.

Presentation layer:

1. *The presentation layer, the sixth layer of the OSI model, focuses on the formatting, encryption, and compression of data to ensure its compatibility and secure transmission between different systems.*
2. *It handles data translation from the application layer into a format the receiving system can understand and vice versa through data encoding and decoding.*
3. *The presentation layer is responsible for data compression techniques, reducing data size for efficient transmission over the network and decompressing it at the receiving end for proper interpretation.*
4. *It also handles data encryption and decryption, providing security for sensitive information during transmission and ensuring confidentiality and integrity.*

5. *The presentation layer defines a common language or syntax that allows different systems to communicate and interpret data correctly, regardless of their underlying hardware or software differences.*
6. *It deals with the conversion of data formats, such as converting text files from one character encoding scheme to another, to ensure seamless interoperability between systems with different encoding standards.*
7. *The presentation layer plays a vital role in ensuring the seamless and accurate transfer of data between applications, while also providing security and data manipulation capabilities to enhance the overall communication process.*


Application
Presentation
Session
Transport
Network
Data Link
Physical
The Presentation layer negotiates the use of an appropriate transfer syntax that allows different types of end systems to communicate under optimum conditions.


client
servers for other connections (e.g., WAP)
E-mail server
Web server
services (load balancing, pooling, caching, ...)
multidevice content delivery
Servlets
JSPs
XML support
Web services support
personalization logic
administration (management and security)
presentation layer
application logic layer
connection to resource mgmt layer
application server
resource management layer
Copyright Springer Verlag Berlin Heidelberg 2004

Functions of the presentation layer:

- **Translation:**

  The networks can deal with different types of computers, such as Macintosh, PC, Unix, and Mainframe systems, which can all be presented to the same network.

  These systems have many features and represent the data differently; different character sets can be used. The presentation layer manages the group to hide the differences between machines.

- **Compression:**

  It is the responsibility layer of compression.

- **Encryption:** encryption and decryption can be prepared at the presentation layer.

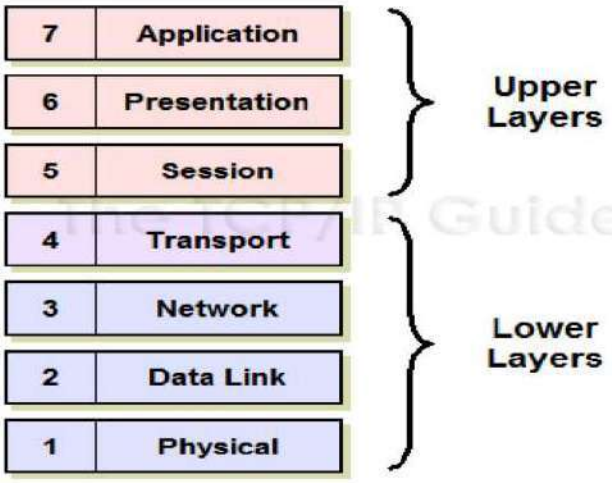
The application layer:

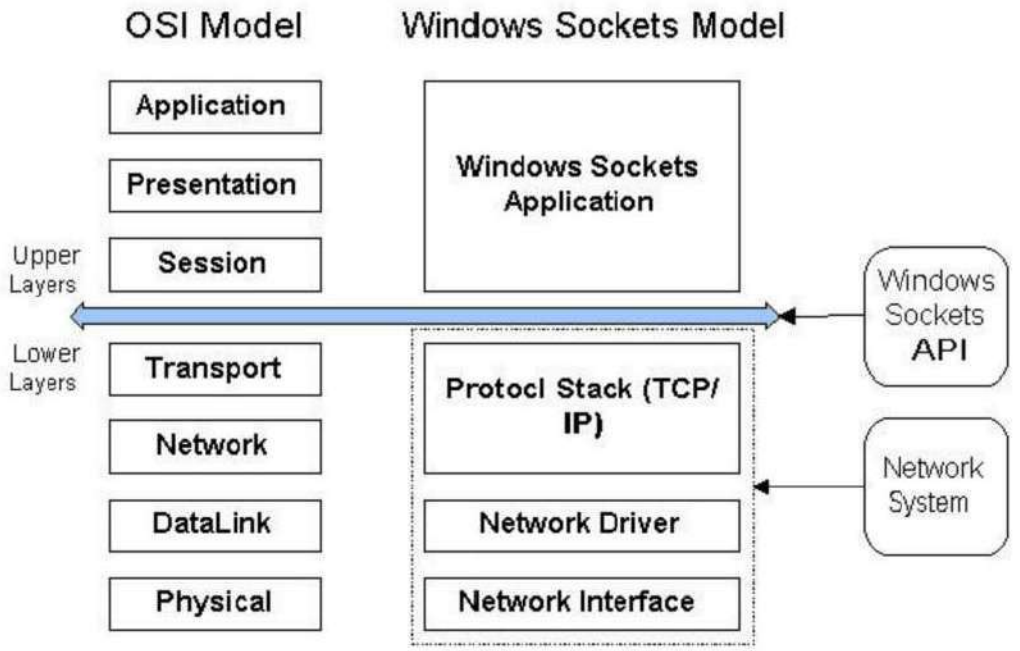
An application layer is a layer of abstraction that specifies the protocols and methods of common interface used by

the computer in a communication network. The abstraction Layer application is used for both standard models of computer networks: the Internet protocol suite (TCP/IP) and the reference model for Open Systems Interconnection (OSI). Although both models use the same term for its highest respective layer, detailed definitions and functions differ.

Characteristics of the 7 OSI MODEL LAYERS

Layers 7-4 are responsible for end-to-end communications between the sender and the destination. Layers 3-1 are responsible for the communications between network devices.





The top layer is the application layer closest to the end user application. The lower layer is the transport layer. It handles the data. The physical layer and the data link layer deal with hardware and software.

The bottom layer, the physical layer, is closest to the physical network transmission media cable,

Chapter 5

PROTOCOLS

NETWORK PROTOCOL

A protocol is a set of rules for communication between computers on a network. These rules are guidelines that regulate and govern the following characteristics of a network.

- Allowed physical topologies

-Access method,

-Cables type

The essential elements of a protocol are semantics, syntax, and timing.

Syntax:

It refers to syntax, data structure, or format, which is the order in which they occur. For example, a simple protocol might expect the first eight bits of data to be the sender's address, the second eight bits, the destination address, and the rest of the stream to be the message itself.

Semantics

It refers to the semantic meaning of each bit section.

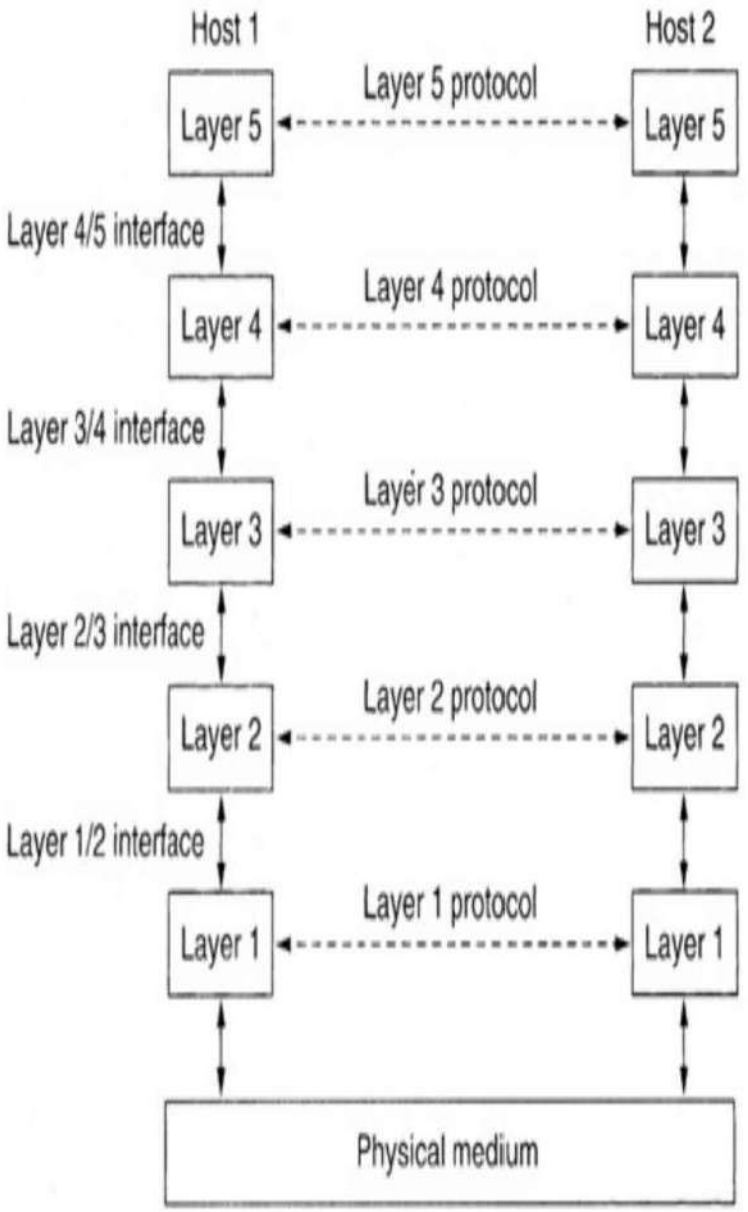
How a pattern is interpreted and the actions to take based on that interpretation. For example, is an address to identify the way forward or the message's final destination?

Protocol stack

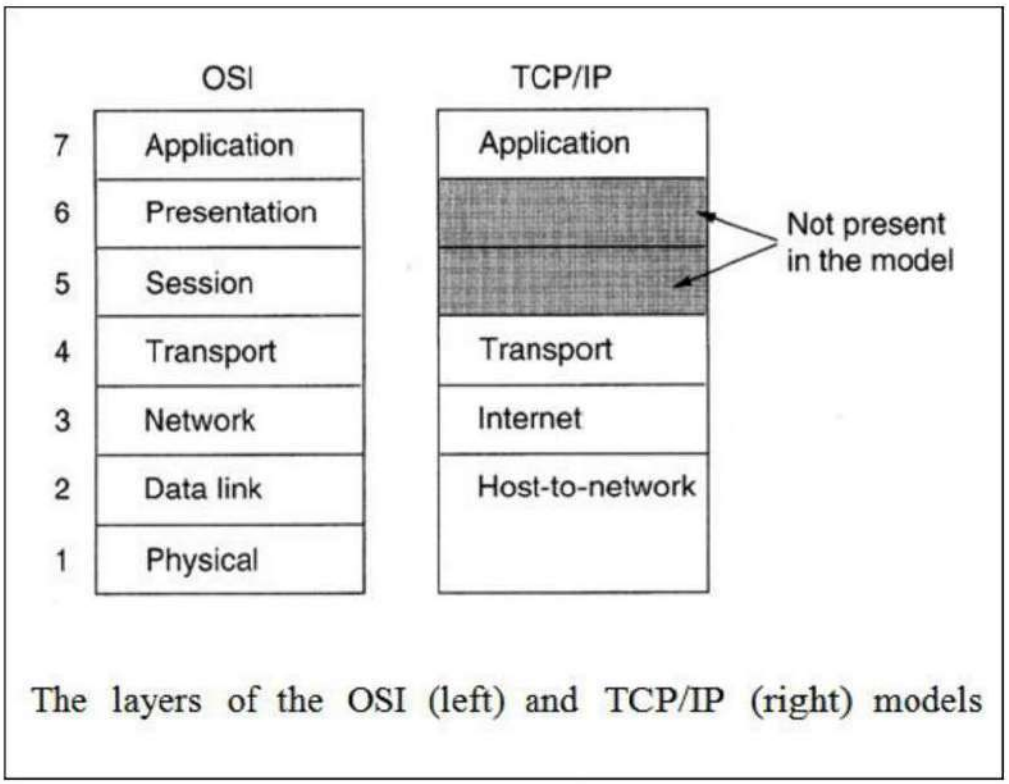
Hosts connected to network utility programs provide users with applications such as email, file transfer, and access to web applications. These application programs, in turn, invoke standard software libraries network to access the network.

This network software creates and receives network traffic: construction and issuing packets, etc., and the hardware level, including establishing voltages.

A protocol stack is a collection of protocols defining the various interfaces between all the layers.



Layers, protocols and interfaces in network software



The layers of the OSI (left) and TCP/IP (right) models

• Types of Protocols

There are many standard protocols. Standard protocols have their advantages and disadvantages. Some are reliable, and some are faster and easier than others. From the user's perspective, the only exciting aspect of the protocols, if the user wants to communicate with other computers, is that their computer or device must support the right. Protocols are implemented in either hardware or

software.

Popular protocols:

Address Resolution Protocol

- Data packets travel through different physical networks to reach the destination.
- - On the physical level, routers and hosts are identified by their physical address, which is a local address. The physical address can meet the target for communication with the same network.
- Communication between different networks requires both physical address (MAC) and logical (IP). The user should be able to assign a logical address corresponding to a physical address and vice versa.
- Two protocols are used:
- ARP maps the logical address to a physical address.
- RARP assigns the physical address to a logical

address.

1- Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) contacts a physical address with its IP address.

-Each time a server (router) needs to determine the physical address of another host (router) on the network, It broadcasts an ARP query packet containing the physical address of the IP receiver network.

-All devices on the network and routers receive packet checks for IP addresses.

-The recipient buried identifies the IP address and responds with an ARP response packet, which includes its IP and physical address.

- The sender can send all packets ordained for this receiver.

2. Reverse Address Resolution Protocol (RARP)

- All devices and routers are assigned a single logical address, which is required to create the IP datagram.
- This address is usually stored in a configuration file, which is stored on the hard disk.
- This reverse address resolution protocol (RARP) determines the logical address when the physical address is known.
- A device started first, getting the physical address of the NIC.
- The device creates an RARP request packet and transmits it over the network.
- Another device on the network works as a server and has all the IP addresses that respond with a RARP response packet. This package includes the sender's IP address.

Internet Control Message Protocol (ICMP)

ICMP is an extension of the Internet Protocol that supports

packets containing error messages, control, and information. A method used for communicating error messages and other information transmission. There are two types of messages: ICMP request messages and error reporting.