***Bandwidth* is defined as the amount of information that can flow through a network connection in a given period of time**.

10BASE-T refers to the speed of transmission at 10Mbps. The type of transmission is baseband, or digitally interpreted. The T stands for twisted pair.

A packet is a logically grouped unit of information that moves between computer systems

Fiber Single-mode fiber consists of the same parts as multimode. The outer jacket of single-mode fiber is usually yellow. The major difference between multimode and single-mode fiber is that single-mode **allows only one mode of light to propagate through the smaller, fiber-optic core**. The single-mode core is eight to ten microns in diameter

***x* KB / *y* Mbps** = *x*(1024) B / *y* Mbps

= *x*(1024)(8) b / *y* Mbps

= 8192 *x* b / *y* Mbps

= .00819 *x* Mb / *y* Mbps

= .00819 *x* / (*y*/sec)

= .00819 ((*x*/1) / (*y*/sec))

= .00819 ((*x*/1) * (sec/*y*))

= .00819 (*x*/*y*) sec

= **8.29 (*x*/*y*) ms**

advantages: RING

1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Each device incorporates a repeater.
5. Relatively easy to install and reconfigure.
6. Fault isolation is simplified.

Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.

Unidirectional traffic.

Advantages: MESH

1. The use of dedicated (link carries traffic only between the two device it connects) links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. It is robust, if one link becomes unusable, it does not incapacitate (affect) the entire system.
3. Privacy and Security (every message sent travels along a dedicated line; only the intended recipient sees it).
4. Point-to-point links makes fault identification and fault isolation easy.

Disadvantages:

1. Large amount of cabling required.
2. Large amount of I/O ports required.
3. Installation and reconfiguration are difficult.
4. The sheer bulk of the wiring can be greater than the available space (in the walls, ceiling, or floors) can accommodate.
5. The hardware required to connect each link (I/O ports and cables) can be prohibitively expensive.

Peer To Peer	Client/Server
Does not required special SW	Required
Lower cost Implementation	Higher cost
Easy Installation	Difficult Installation
Does not require administration	Required
Does not provide a single point of Failure	Provide a single point of failure

Low security	High security
Un centralized	High control of administration & management
Suitable for small nets	Suitable for large nets

- BNC : Coax
- RJ-45 : UTP & STP
- RJ-11 : Phone , VSAT

Light

electromagnetic interference

UTP

1-

2- DNS

3-

4- **data link layer**

5- transport layer

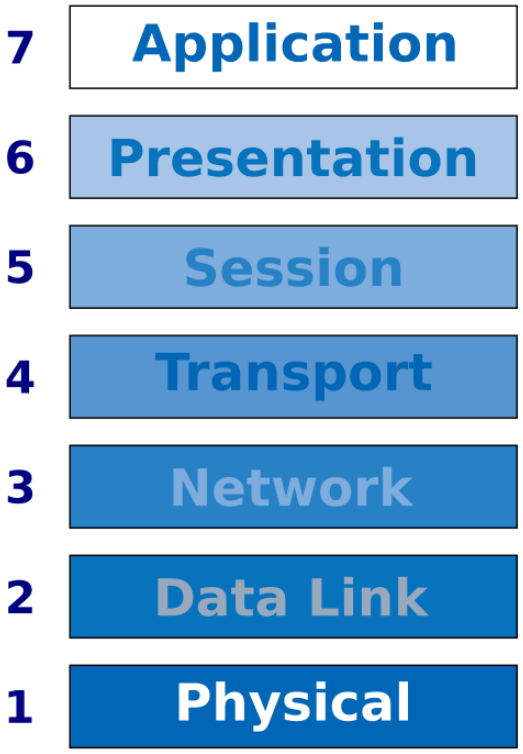
6- physical layer

7-

8- network layer

9- 4

10- application layer



- Reduce Complexity.
- Standardizes Interfaces.
- Facilitates Modular Engineering.
- Ensures Interoperable Technology.
- Accelerates Evolution.

Memorize name & no of layers

Simplifies Teaching and Learning

Similarities include:

1. Both have layers.
2. Both have application layers, though they include very different services.
3. Both have comparable transport and network layers.
4. Both models need to be known by networking professionals.
5. Both assume packets are switched. This means that individual packets mat take different paths to reach the same destination. This is contrasted with circuit-switched networks where all the packets take the same path.

Differences include:

1. TCP/IP combines the presentation and session layer issues into its application layer.
2. TCP/IP combines the OSI data link and physical layers into the network access layer.
3. TCP/IP appears simpler because it has fewer layers.
4. TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, networks are not usually built on the OSI protocol, even though the OSI model is used as a guide.

1- **Build the data (application layer):** As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.

2- **Package the data for end-to-end transport (transport layer):** The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.

3- **Append (add) the network address to the header (network layer):** The data is put into a packet or datagram that contains a network header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.

4- **Append (add) the local address to the data link header (data link layer):** Each network device must put the packet into a frame. The frame allows connection to the next directly-connected network device on the link. Each device in the chosen network path requires framing in order for it to connect to the next device.

5- **Convert to bits for transmission (physical layer):** The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium (usually a wire). A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN. Headers and trailers are added as data moves down though the layers of the OSI model.