COMPUTER NETWORKS

TERM PAPER

SRIHARSHITHA BONDUGULA 20181111013

---

1) CLASSIFICATION OF NETWORKS

Classification criteria can be the technique (the technology behind the network), the scale or the geometrical arrangement of nodes.

Based on technique, networks can be classified into; *Broadcast networks(Figure 1) and Point to point networks(Figure 2).*

BROADCAST NETWORKS

In this type of network, one communication channel is shared by all the machines. One packet is sent to all the nodes. If it needs to be sent to a single recipient, the destination address (recipient node's address) is mentioned. Nodes reject the packet if the destination address mentioned is not theirs. There is a security risk in this kind of network. These networks facilitate unicasting (data is sent to all the nodes but only one node accepts based on the destination address mentioned), broadcasting (data is sent to all the nodes), multicasting (data is sent to all nodes by a sender but only a subset of nodes receive the sent data based on the mentioned addresses).

POINT TO POINT NETWORKS

In this type of network, there is a separate channel between all the nodes (pairwise connections). So if there are n nodes, there are ${}^{n}C_{2}$ channels. A packet sent by one node is received by only one intended node. Protocol becomes simpler making the hardware complex. This network facilitates unicasting, multicasting, and broadcasting.

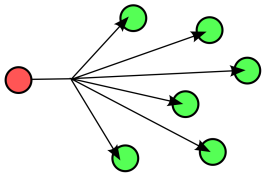


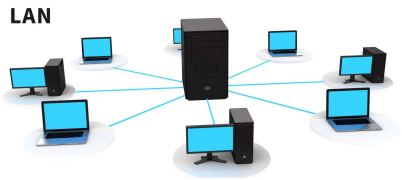
Figure 1

Figure 2

To make the hardware simpler (since connecting to all the nodes is practically impossible), an addressing scheme is used. The destination address is mentioned on each packet, each node passes the packet based on the mentioned address. Broadcasting does not need any addressing; the sender just sends the packet to all the nodes it is connected to. The receiver nodes further forward the packet to the nodes they are connected to. The packet thus will be sent to all the nodes in the network.

Based on the scale or size, networks can be classified into the following; *LAN, WAN, MAN, PAN, CAN.*

LOCAL AREA NETWORK (LAN)

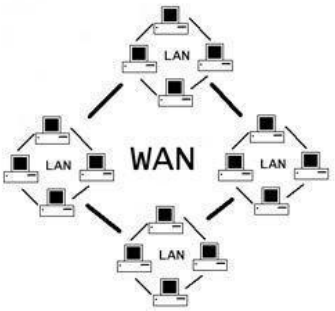


These include the networks that are usually privately owned (not shared) and are usually built over a small area like 2-3 km. These were traditionally built as broadcast networks with 10-20 nodes. But now, with an increased number of users and nodes, using a broadcast channel is difficult. And to deal with security issues point to point medium is being used instead. The data transmission rate is high (less delay) with less noise, errors, and fast acknowledgments. The data transmitted is usually text, files, etc, and not voice or video as it is over a small distance. Example: Campus network

METROPOLITAN AREA NETWORK (MAN)

These networks can be public and private, built over a distance <10 km. These are usually made up of interconnected LANs and are designed for small cities. All kinds of data are transmitted including voice and video with a high speed and low transmission time. It can be broadcast or point to point.

WIDE AREA NETWORK (WAN)



These networks extend over a large geographical area and are primarily public. Networking, routing, and transmission-related responsibilities are taken by communication subnet or network backbone. Most of these are serial in nature as installing so many wires and cables over a large area is not affordable and manageable. They are primarily point-to-point networks with lower speeds, higher delays, and a high cost of bandwidth. Example: Internet

PERSONAL AREA NETWORK (PAN)

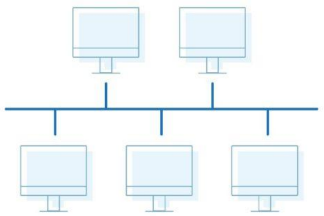
It is a network extending over a small area enabling communication between computer devices near a person. These can be wired (Headphones, USBs) or wireless (Bluetooth devices) with a range of a few meters and are very fast.

CAMPUS AREA NETWORK (CAN)

It includes a group of interconnected networks but within a smaller area than MAN. For example, Campus, school, apartnment, etc. Thus it is faster than MAN and slower than LAN.

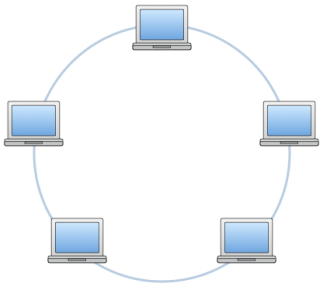
Based on the geometrical arrangement of wiring schema physically (the way actual cables are routed) or logically (the way network behaves), there exists another classification called *network topology*. Different network topologies possible are; *Bus, Ring, Star, Tree, Mesh*, etc.

BUS TOPOLOGY



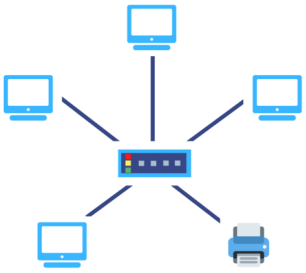
All the nodes in the network are connected to a single cable which is called a "backbone". If this cable is broken, the entire network fails. Data is transmitted in both directions. Signal reflection at the ends of the cable creates issues making termination of cables difficult. These networks are prone to data collisions making it slow. Initially, most LANs used bus topology, but it is rarely used now. It is easy to understand and cost-effective.

RING TOPOLOGY



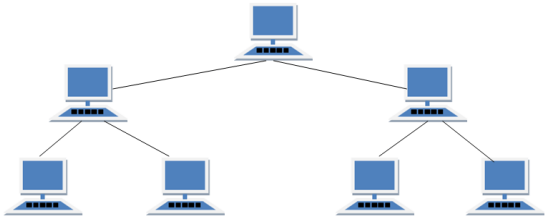
All the nodes in the network form a ring. Data is transmitted in a single direction, however, another ring can be added to make it bidirectional (Dual ring). The packet sent goes around and comes back to the sender node where it is pulled out and the next packet is sent. Thus, no terminator is needed. The transmission time depends on the distance from the sender node. Repeaters have to be used if there are a large number of nodes in the network. A double ring can be set up to deal with the delays. Higher technology nodes realize and the network can still function even after cable cuts. It is cheaper but troubleshooting is difficult and the network fails if one node fails.

STAR TOPOLOGY



Adding nodes disrupts the network in bus topology. To overcome this, star topology is introduced. In this topology, all the nodes in the network are connected to a central hub. Though it requires more cable, this topology makes adding and removing nodes easier. Network functions smoothly even if one node fails. Network fails only if the hub fails. It is expensive to install and use, but it is faster and easy to set up, modify and troubleshoot.

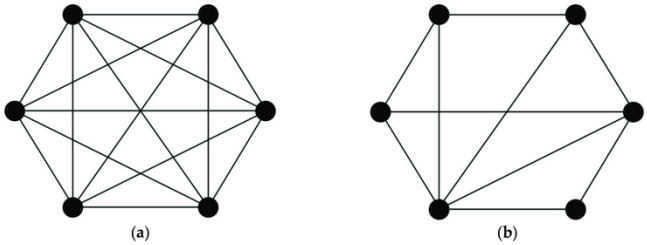
TREE TOPOLOGY

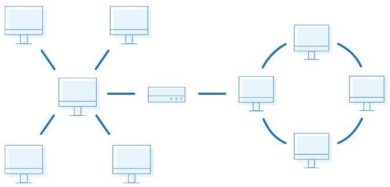


All nodes in the network are arranged in a hierarchical structure. It is an extended version of star and bus topology. It is used for networks with a very large number of nodes (especially WANs). It is logically a broadcast network with point-to-point links. It is expensive as it is heavily cabled. It is easy to maintain, expand and troubleshoot. Network fails only if the central hub/root node fails

MESH TOPOLOGY

All the nodes in the network are connected to each other. It is highly connected with n_{c_2} links in a network with n nodes. Thus it is heavily cabled. Unlike other topologies, there exists more than one path between 2 nodes in this topology. It is fast, robust, and provides security/privacy. Installation and configuration is difficult and costly.





A network can be a combination of topologies. Usually, a full mesh (fully connected - a) is used at the core of the network, partial mesh(only a subset of nodes are fully connected - b) in the middle, and a tree or star at the edges. This type of topology is called a hybrid topology. It can be configured based on the requirements.

References:

1) Lecture notes and slides
2) https://www.studytonight.com/computer-networks/network-topology-types

---

2) MEDIUM ACCESS ALGORITHMS/PROTOCOLS

In the case of a broadcast channel, multiple users use a single channel as explained in previous section. How to allocate this channel to individual nodes? It can be done through 2 approaches;

a) Static allocation
- Divide the channel into n slots and assign each slot to each individual node.
- FDM (Frequency division multiplexing) - split the assigned bandwidth assign different bandwidths to different nodes
- TDM (Time division multiplexing) - split the assigned time frame into smaller time frames and allocate them to different nodes. Each node is assigned the whole bandwidth in the allocated time frame.
- As the slots are predetermined, it is simple to implement. Bandwidth allocation may get wasted and is not efficent. It is not suitable in case of bursty traffic.
- Example: Television broadcast (One way transmission)

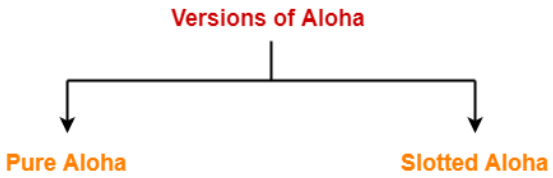
b) Dynamic allocation
- Channel is allocated to a node based on the requirement.
- Allocations are not permanent and are flexible.
- Allocation is done either by a central manager or by the nodes themselves.

- Thus wastage is less and is efficient and suitable for bursty traffic.

Any of the above approaches can be used based on the requirement.
Popular protocols or Algorithms that are used for channel allocation in a broadcast channel environment are discussed here. These are the random access protocols where all the nodes accessing the channel are given the same priority. They can send data whenever the channel is free.

1) ALOHA

ALOHA is an access protocol for transmission of data via a shared network channel. It is the simplest of all random access protocols. There are 2 versions of ALOHA.



a) PURE ALOHA

In this protocol, there are no restrictions on the nodes. All the nodes compete to access the channel and to transmit their respective dataframes. There is no coordination between the nodes. Each node continues to transmit without checking whether the channel is free or not. If the channel is idle, data frame is transmitted successfully otherwise collision occurs and the frames in the channel are discarded. Receivers are always in listening mode as they can receive data at any time. As the channel is prone to collision, there is a necessity of checking whether the frame is polluted or not. If a collision is detected, the frame is sent again (retransmitted) after some random time.

There is no guarantee of the transmission of the frame as it is prone to collision. Thus it is a best effort mechanism protocol. Thus, as the channel is always in contention, this protocol is not suitable for loaded or busy channels. It is suitable for lightly loaded channels where nodes rarely have something to transmit. For example, Satellite communication. The wait time for each node to transmit when it is ready is less, i.e zero delay as it can transmit whenever it wants to which is an advantage for lightly loaded networks. Theoretical efficiency of this protocol is 18% which might go down with the increase in the number of nodes.

b) SLOTTED ALOHA

To bring some order to the chaos seen in pure aloha, slotted aloha was introduced. Transmission in shared channel is done in discrete time slots. Transmission of data is allowed only at the beginning of these time slots. If a node misses this time, it should wait till next slow. Nodes compete at the start of time slot only. Until the time slot ends and until the transmission of the node is done, another node cannot start transmitting. Nodes cannot start transmitting whenever they are ready as in pure

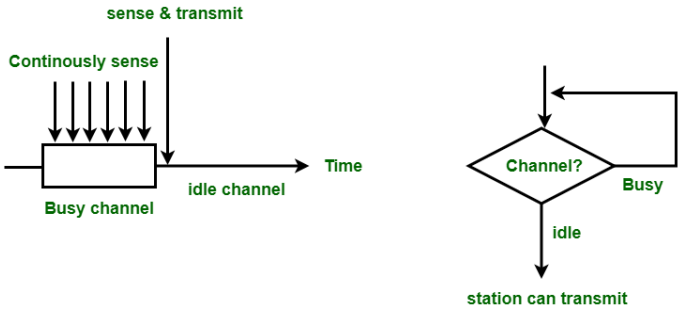
aloha. This reduces the chance/probability for collision as collisions are now confined only to the start of the slot.
Collisions occur only if more than one node try to transmit at the beginning of the slot. Thus, with decreased chance of collision, it is considered as an improvement of pure aloha and its efficiency is 37%. This might go down with increase in the number of nodes in the network.

2) CSMA -> Carrier Sense Multiple Access protocol

This protocol ensures that collision does not occur. In Aloha, node does not care to listen to the channel, it just tries to transmit whenever it is ready which leads to collision. To avoid such situation, every node listens to the carrier and transmits only if the channel is free else it waits until channel becomes free. Once the channel becomes free, they compete to capture it. Thus as everybody backsoff when channel is busy, collision probability is reduced and efficiency increases. There are various ways of sensing the carrier, i.e how long the node waits to sense the carrier when the channel is busy. Different protocols these decisions lead to are;

a) PERSISTENT CSMA or 1-PERSISTANT CSMA

If a node is ready to transmit, it continuously listens to the carrier, i.e waits until the channel becomes free. Once channel becomes free, it transmits. There is an increased chance for the node to capture the channel if it waits persistently. On the other side, if more than one node wait persistently, say 2 nodes, then there is a problem. When both the nodes detect that the channel is free, they try to transmit simultaneously which causes collision. This is called propagation delay. So, both the chance for collision and chance for capturing the channel are high and the efficiency depends on the load or concurrency factor of the channel.

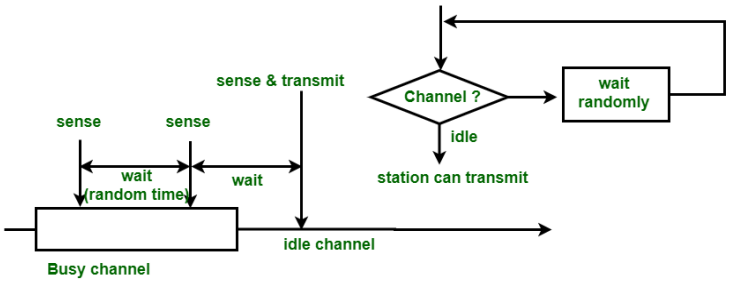


It is efficient than slotted aloha and pure aloha as if channel is busy it won't result into collision. Because collision now takes place only if >1 node are ready to transmit at exactly the same time and chances of that occurring is less making this protocol efficient.

b) NON-PERSISTANT CSMA

Channel is not sensed continuously. If the node finds the channel busy, it waits for sometime (random) and comes back to sense the channel again. Unlike in persistent CSMA, nodes do not listen continuously until the channel becomes free. So with this introduced randomness, the chance for propagation delay that causes collisions is further reduced. Thus with increased randomness, chance for collision is reduced and efficiency is increased. It works efficiently even when the load is high. But, as the nodes wait to capture the channel and

transmit the data, delay is increased. At times, nodes keep waiting even when the channel is free.



Non persistent CSMA and persistent CSMA are 2 extreme cases. There are other protocols based on the probability with which a node continues to listen to a channel after finding it busy. Say p is that probability, then the protocol is called as **p-persistent CSMA**. Lower the value of p, closer the protocol is to Non-persistent CSMA (better it is for loaded network) and higher the value of p closer the protocol is to persistent CSMA. Another version of the same is **0-persistent CSMA**. Superiority of nodes is decided before hand and each node waits in order until it gets a chance to send.

3) CSMA-CD -> Carrier Sense Multiple Access protocol - Collision detection

It is similar to CSMA. There is some variation when a collision occurs. In CSMA, there is no dependency between detection of collision and transmission. The node continues to transmit the data even after the collision. This does not make sense as it is just waste of time because transmission is not meaningful after collision. CSMA-CD is capable of terminating the transition immediately after detection of collision unlike CSMA. Remaining time period is thus saved. It is an unreliable protocol, i.e there is no acknowledgement built into it and there is not guarantee of delivery. It does better than ALOHA and persistent CSMA. It is used in Ethernet protocol with a slight variation.

CSMA-CA (Collision avoidance) is another variation of CSMA protocol.

References:

1) Lecture notes and slides
2) https://www.tutorialspoint.com/aloha-protocol-in-computer-network
3) https://www.geeksforgeeks.org/multiple-access-protocols-in-computer-network/

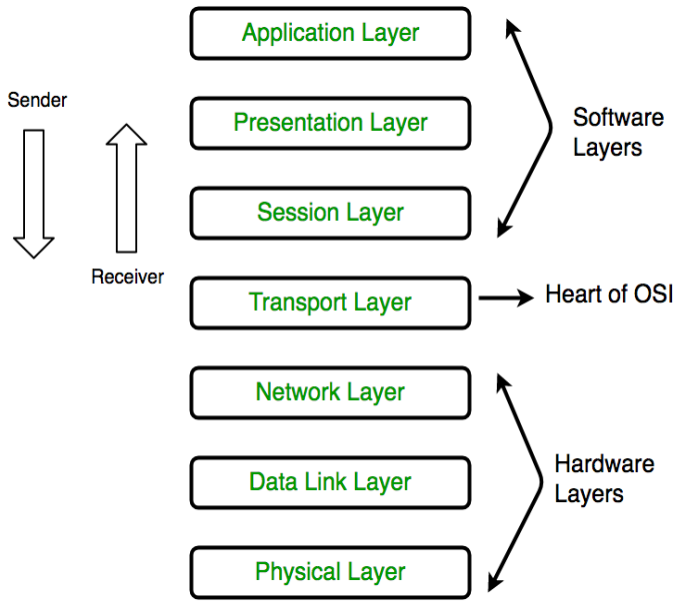
---

3) OSI REFERENCE MODEL

Networks are organised as stack of layers built one above the other. Function of each layer is different and lower layer hides some details and provides services/ useful information to the higher layers. This type of layered model or design simplifies the design, increases the modularity and makes it easily understandable. It standardises the interfaces and reduces the complexity. There are different kinds of network reference models. Some examples of such models that are layered are; OSI, TCP/IP (Most popular), IBM SNA, DECNet (Previous generation models).

Most of the implementations (for example; campus network) use TCP-ICP model and not OSI reference model. OSI model is used in aviation, control, manufacturing, telecom companies etc. OSI stands for **Open system Interconnect**. 'Open' because, standards before these were closed, i.e we need to buy them or they aren't revealed to others. For example, IBM SNA, DECNet built and sold systems. Others could not use their design to build products which are compatible with them.

OSI was developed by ISO (International Organization of Standardization), which is under UN charter in 1984. It has a 7 layer architecture with each layer having specific functionality to perform. It does not give implementation details. It does not specify any working protocol like TCP or IP or UDP or HTTP. This model just gives us the details of what needs to be done and what function needs to be performed by a given layer. It had several layers influenced by IBM SNA. They give a rough model and anybody can build protocols or systems using this model. Thus it was called 'Open'. Any company, or any start up can buy OSI standard and build a model around it and sell it in the market certified. There will be a certification agency to check whether it is OSI compliant. ISO, as an organization, developed some protocols around OSI model too.



BASIS OF LAYERS AND ARCHITECTURE:

- Model is configured with seperate layers of proper abstraction
- Each layer in the architecture performs some well defined function
- Layered model is chosen so that there will be no confusion and people can create different layers over the given model.

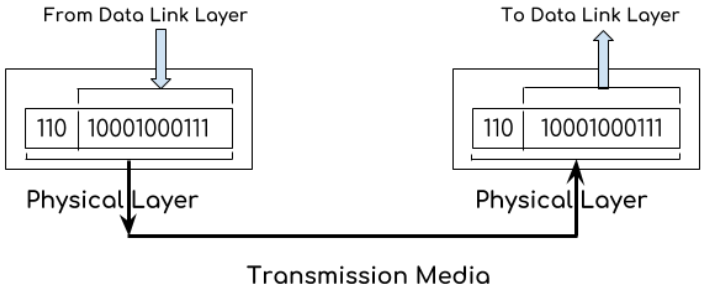
- Layers are designed in such a way that the information flow between 2 adjacent layers in interface is minima so that there is optimal use of resources i.e., ISI control information should be minimised.
- It makes sure that there is optimal control information for the peer layer on the other side.
- Architecture is designed in such a way that it is not too small or too large

Following are the 7 layers of the OSI reference model,

1. PHYSICAL LAYER

This is the lowest layer of the architecture that provides physical communication channel between network devices.It contains information in the form of raw bits(101010) only(not even ASCI character). These 1 or 0 are be expressed in physical form i.e, voltage or current or frequency. Thus, this layers receives the signal, converts it into bits and send it to the next layer (Data link layer). This layer also defines the duration of signals or transmission rate (larger the duration of signal, lower is the speed). It also determines the transmission mode and physical topology of the network.

All electrochemical definitions and offboard cable connectors are defined at physical layer. Different types of connectors are used at this layer, for example, RJ45 connector(8 pins). Example of physical layer devices are Hub, Repeater, Modem, Cables etc.



2. DATA LINK LAYER:

This layer is responsible for node to node delivery of the information. It converts raw bits into frames so that the information is ordered and meaningful (Framing). Only then, instructions, control messages can be passed and words and characters can be defined. This layers includes error handling mechanics. It is responsible for flow control, i.e with the speed at which data is being transmitted. Who will transmit? Only one person can transmit for meaningful communication so who will take turn? Who will control the channel during a particular period? etc.., i.e access control will be defined in this layer. This layer is also responsible for physical addressing, i.e after creation of frames, it adds physical addresses (MAC address) of sender and/or receiver in the header of each frame and transmits it to the receiver node. Examples of Data link layer devices are switch and bridge.

3. NETWORK LAYER:

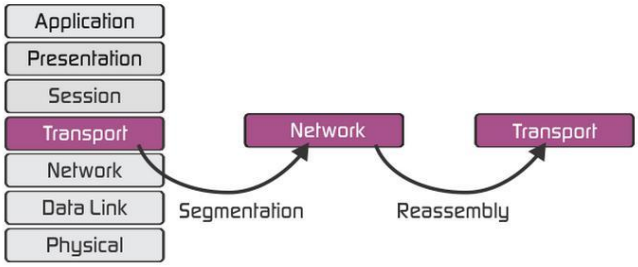
Multiple nodes or networks together form a subnet. Transmission between nodes that belong to different subnets or networks is controlled by the network layer.As there are multiple networks, to make hopping easier from one network to the other, packet routing is

necessary, i.e selection of the shortest path to transmit the packet, from the number of routes available. This can be fixed or dynamic. Addressing and packet size come into play in this layer. It adds IP addresses of host and receiver to the header of the data packet.

Delay means time taken for data to travel from source to destination and jitter means variation in delay. This layer deals with congestion control and quality of service(delay or jitter). It is responsible for interconnection of heterogenous networks and for handling variations in network technologies because there might be different type of technologies, different cables, connectivity links connected at different parts of network and all of them have to work together for the data to reach the destination. Routers are the network layer devices.
These 3 layers form the crux of networking and are called as lower layers or hardware layers.

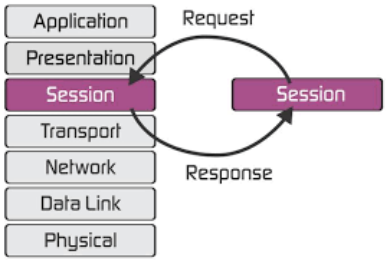
4. TRANSPORT LAYER

This layer divides or segregates network infrastructure with operation system stack users in the system. The data in this layer is referred to as segment. This layer seperates users from the details of the network and ensures the order of delivery of the packets before passing on to the higher layers for further processing. It ensures end to end communication, establishes connection. It is responsible for segmenation at the sender node and reassembly at the receiver node. This layer is called as Heart of the OSI model.



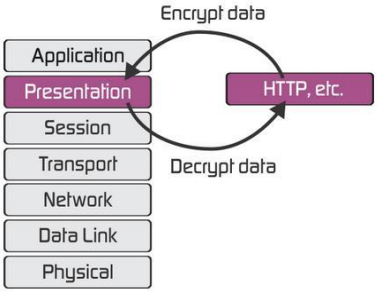
5. SESSION LAYER

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.It is responsible for controlling dialogue between 2 systems. This layer also deals with the loss of data and recovery after crashes.



6. PRESENTATION LAYER

It is also called as translation layer. Data received form application layer is manipulated in the format according to the requirement and transmitted over the network. Syntax and semantics of formats and codes, data structures etc are handled in this layer. It is responsible for data compression and cryptography.



7. APPLICATION LAYER:

This is the topmost layer which is implemented by network applications. Some examples of user applications include HTTP, SMTP and Telnet.

Physical, data link and network layer are actually a part of network infrastructure backbone(switches, routers) and are hence called as hardware layers. Transport, Session, presentation and application layers are found in end systems and nodes (Mobile phones, proxy machines etc). Last 3 layers are called as upper layers or software layers.

References:

1) Lecture notes and slides
2) https://www.geeksforgeeks.org/layers-of-osi-model/
