Chapter-2
Reference Model

Network Criteria/Parameters

A network must be able to meet a certain number of criteria. Some of them are

1. Performance:

- Performance can be measured in many ways, including transit time (time required to travel message from one node to another) and response time(time required to get response after certain request).
- Performance of network depends upon the number of users, type of transmission medium, capabilities of network hardware and efficiency of the software.
- Performance is often evaluated using two metrics: throughput and delay.
- Large throughput and less delay is preferred but there is tradeoff i.e. if we try to increase throughput by sending more data to network, this will generate more traffic congestion to the network hence the delay is increased.

2. Reliability

- A network is reliable if there is accuracy of delivery.
- In addition to it, reliability is measured by the frequency of failure, the time it takes a link to recover from a failure etc.

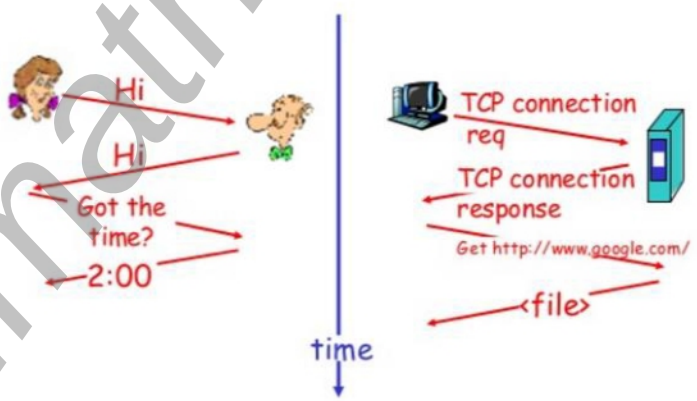
3. Security

- Security issues includes protecting data from unauthorized access, protecting data from being damage, implementing policies and procedures for recovery in case of data loss.

Protocols And Standards

- Protocols are the set of rules that govern all activity in the network that involves two or more communicating remote entities.
- Protocols are running everywhere in the network.
- Example: protocol in router determine a packet path from source to destination, error detection protocol could detect the transmission error etc.

a human protocol and a computer network protocol:



Protocol Stack , Interfaces and Services

- Protocols are the set of rules that govern all the activity in the network that involves two or more communication entities.
- **To reduce the design complexities, network designers organize the protocols, network hardware and software that implement the protocol in layers.**
- A protocol in one layer perform a certain set of operations on data, the data is then passed to the next layer where another protocol perform different set of operations. I.e. each layer provide certain services to upper layer.

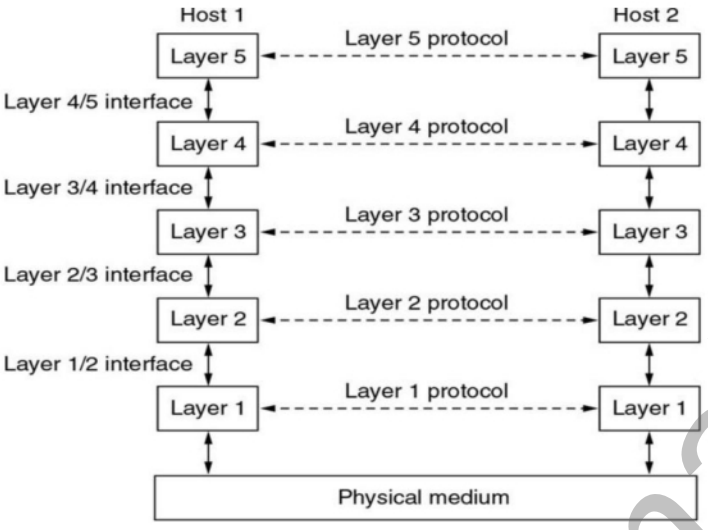


Fig 1: layer, services and interfaces

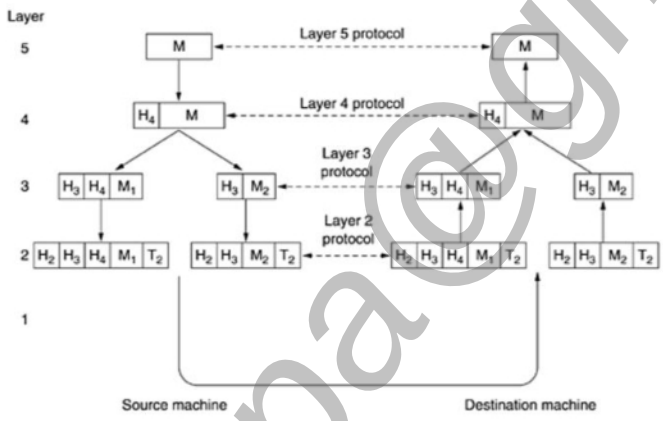


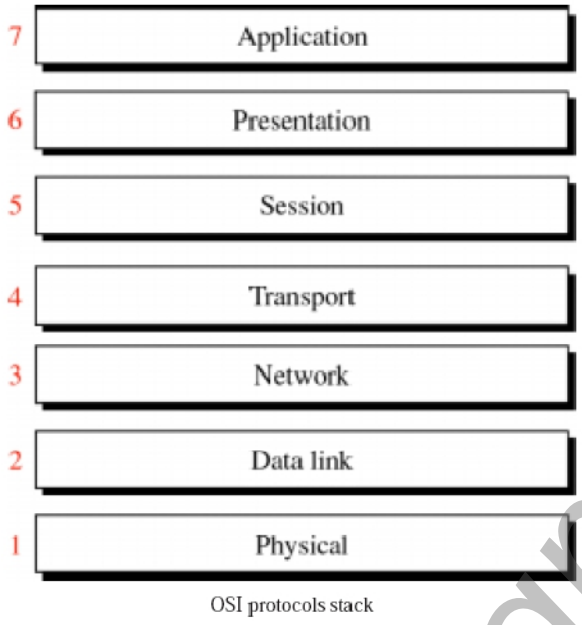
Fig 2: example information flow supporting virtual connection in layer 5

- The protocols at various layer are called protocol stack.
- The key concept of protocol stack is each n-1 layer provides service to upper layer n.
- These layers communicate with each other by exchanging n-message. These message are called layered-n protocol data unit or n-PDU.
- Between each pair of layer is an **interface** that define the **services** the lower layer provides to upper one.
- Example: The application-to-transport interface defines how application programs make use of the transport layers. For example, this interface level would define how a web browser program would talk to TCP/IP transport software
- In above figure 2, the source generates message in layer 5 and passed down to layer 4. This layer 4 put some header in front of message to obtain 4-PDU. Then this message is passed down to layer3. In layer 3, 4-PDU is divided into two parts M1 and M2 and additional header is appended in front of message. The header may include control information such as sequence number to allow **peer layer 3 on destination** to deliver message on right order. Simply header contains additional information needed by the sending and receiver side.
- The procedure continues in the source, adding more header at each layer until 1-PDU are sent to the destination over a physical link.
- At the other end, the destination host receive 1-PDU and direct them up the protocol stack. At each layer, the corresponding header is removed.
- Finally Message M is obtained from M1 and M2 and then passed to destinaiton applicaton.

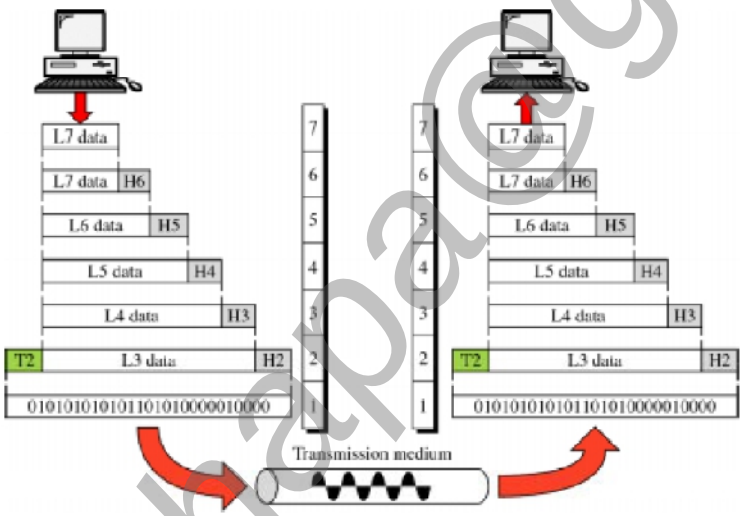
Drawback of Layer approach

1. Possibility of redundancy of functionality
2. Dependency of one layer to another violate the goal of separation of layers.

The OSI Reference Model



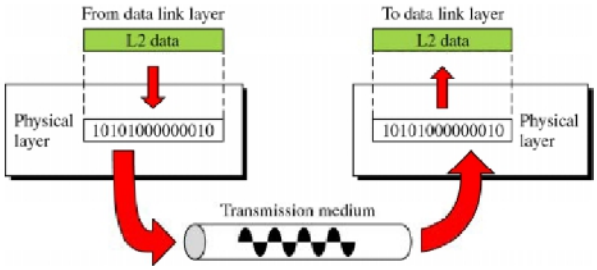
OSI protocols stack



- Appeared after TCP/IP model.
- The international organization for standardization (ISO) has developed OSI (open system interconnection) model in 1977.
- A open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- In order for computer communicate, there must be some rules, followed by the computer for transferring information from one computer to another.
- OSI model, simple define which task need to be done and which protocol will handle those tasks at each of the seven layers of the model. These all layers are present in each computer logically; all the information before transferring has to be processed under the seven layers.
- At each layer (except layer 7 and 1) in the sender side, a header is added to the data unit received from the upper layer. At the layer 2, a trailer is added as well.
- As each block of data reaches the next higher layer in receiving end, the header and trailer attached to it at the corresponding layer at the sending device are removed, and actions appropriate to that layer are taken.

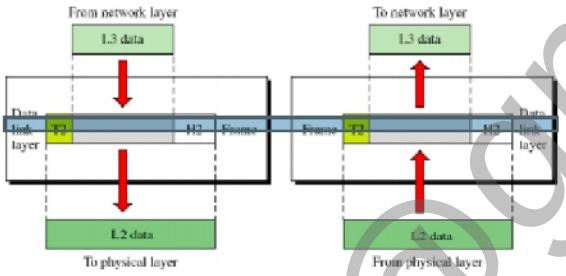
Layers in OSI model

1. **Physical Layer**



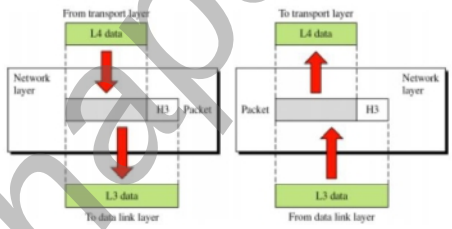
This layer is used for sending bits 1's or 0's from one computer to another computer. It also deals with the physical connection between the computers. It mainly transmits and receives the signal.

2. **Data Link Layer**



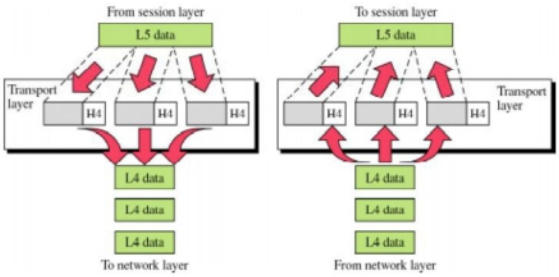
The data link layer provides for the delivery of data over a single link from one device to another in the route and device decided by the network layer. The data link layer is responsible for correcting transmission errors induced during transmission. This is achieved by the data link layer by performing the tasks like framing(encapsulation), flow control, error control, access control, and physical addressing.

3. **Network Layer**



The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks. So the network layer is responsible for deciding route and forwarding the packets to a particular device. For this it uses two protocol i.e. IP and routing protocol. IP for translating logical network address to physical machine address. Routing protocols are used to determine the path for the packet if there are several ways a packet can get to its destination.

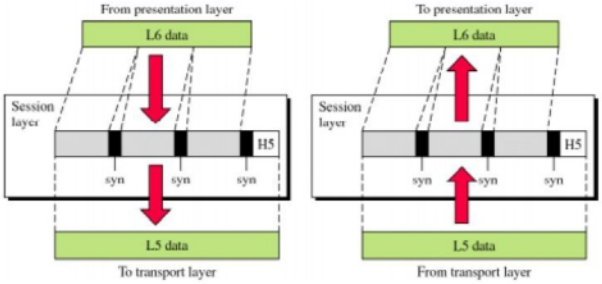
4. **Transport Layer**



This layer is responsible for delivering error free data to destination computer. This layer breaks the large message into small packets and then sends these packets to the destination computer. The transport layer also sends acknowledgement to the sender that message has been sent successfully i.e. the transport layer ensures data is successfully sent and received between two end systems. If data is sent incorrectly, this layer has the responsibility to ask for retransmission of the data. Also it ensures data are passed onto the upper layers in the same order in which they were sent. It also provides multiplexing/DE multiplexing for combining data from several source for transmission over a single data path. Congestion control is also provided by this layer.

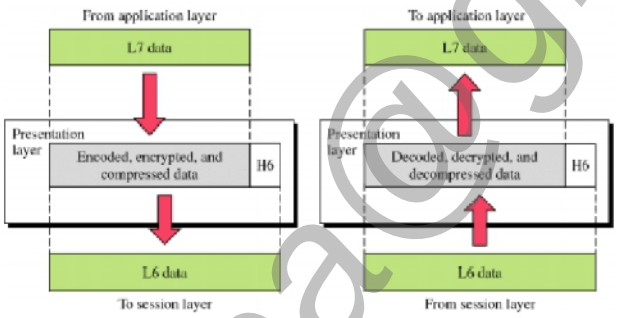
The Transmission Control Protocol (TCP) of the TCP/IP protocol suite resides at the transport layer.

5. Session Layer



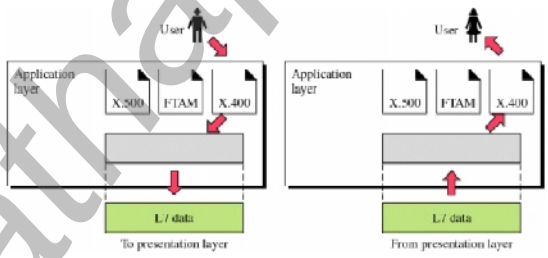
It is responsible for the session between computers to be established and terminated. It provides two system into a dialog to find each other and provide a common link. Also, the session layer organizes and synchronizes the exchange of data between application processes. It works with the application layer to provide simple data sets called synchronization points that let an application know how the transmission and reception of data are progressing. In simplified terms, the session layer can be thought of as a timing and flow control layer.

6. Presentation Layer



This layers translates the information between the format the network require and the format the computer expects. The presentation layer is responsible for task like data translation, compressions, encryption etc.

7. Application Layer



The application layer is the topmost layer of OSI model. It provides services that directly user application such as webpage, email, file transfer etc. it uses many protocols including HTTP to support web, SMTP to support email, FTP to support file transfer, DNS etc.

Summary

Summary:
Physical Layer: How to transmit bits.
Data Link Layer: How to transmits frames
Network: How to route packets to the node.
Transport: How to send packets to the applications.
Session: Manage connections.
Presentation: Encode/Decode messages, security.
Application: Everything else.

Benefits of OSI model

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.

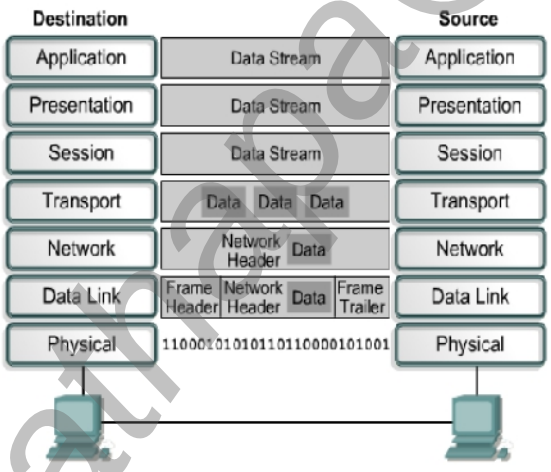
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

Protocols in TCP/IP and OSE

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Data Encapsulation

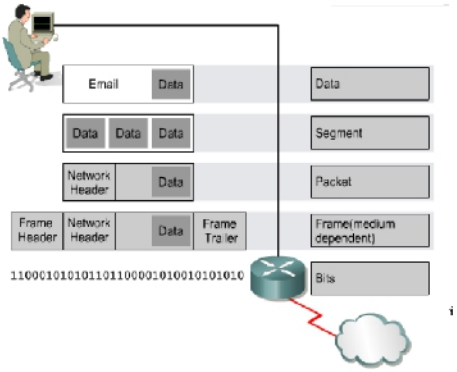
All communications on a network originate at a source, and are sent to a destination. The information sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another computer (host B), the data must first be packaged through a process called encapsulation. Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information.



Example:

Perform the following five conversion steps in order to encapsulate the data.

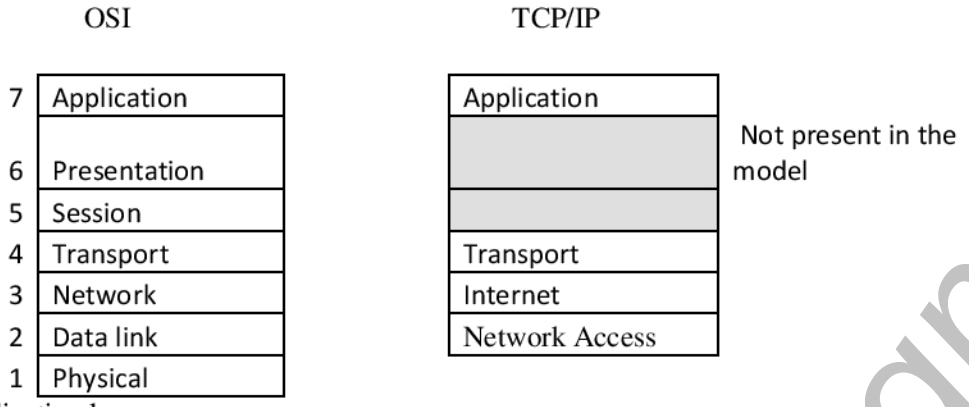
1. Build the data.
2. Package the data for end-to-end transport.
3. Add the network IP address to the header.
4. Add the data link layer header and trailer.
5. Convert to bits for transmission.



TCP/IP Reference Model

The ARPANET was a research network sponsored by the DOD (U.S Department Of Defense). It had connected hundreds of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble inter working with them, so new reference architecture was needed. Thus, the ability to connect multiple networks together without facing any problem was one of the major design goals from the very beginning. This architecture later became known as TCP/IP Reference Model, after its two primary protocols.

This model basically consists of four main layers as describe in figure.



1. Application layer:

On top the transport layer is the application layer. TCP/IP combines the OSI application, presentation, and session layers into its application layer. The application layer handles high-level protocols, representation, encoding, and dialog control. The TCP/IP protocol suite combines all application related issues into one layer. It ensures that the data is properly packaged before it is passed on to the next layer. TCP/IP has protocols to support file transfer i.e. FTP, e-mail i.e. SMTP, DNS, and remote login etc.

2. Transport Layer:

The transport layer ensures that packets are delivered error free, in sequence and with no losses or duplication. The transport layer break large message from the upper layer application into packet to be sent to the destination computer and again on receiving site resembles packet into the message to be presented to the applicaton layer. The transport layer typically sent an acknowledgement to the originator for message received. Two end to end protocols have been defined here. The first one, TCP (Transmission Control Protocol) is a reliable connection oriented protocol that allows a byte stream originated on one machine to be delivered without error on any other machine in the internet. The second protocol in this layer, UDP (User Datagram Protocol), is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server type request reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

3.Internet Layer

The main job of this layer is to inject packet into any network and have them travel independently to the destination. The main protocol that function at this layer is IP. Best path determination and packet switching occurs at this layer. Other protocols that operate at this layer are ARP, RARP etc.

4. Network Access:

The network access layer allows an IP packet to make a physical link to the network media. It includes all the detail include in OSI data link and physical layer. Drivers for software applications, modem cards, and other devices operate at the network access layer. The network access layer defines the procedures used to interface with the network hardware and access the transmission medium.

Comparison of OSI Model and TCP/IP Model:

The OSI and TCP/IP models have many similarities:

- Both are based on layers' concept.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.
- Networking professionals need to know both models.

Here are some differences of the OSI and TCP/IP models:

- TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- TCP/IP combines the OSI data link and physical layers into its network access layer.
- TCP/IP appears simpler because it has fewer layers.
- When the TCP/IP transport layer uses UDP it does not provide reliable delivery of packets. The transport layer in the OSI model always does.

OSI MODEL	TCP/IP MODEL
Contains 7 Layers	Contains 4 Layers
Uses Strict Layering resulting in vertical layers.	Uses Loose Layering resulting in horizontal layers.
Supports both connectionless & connection-oriented communication in the Network layer, but only connection-oriented communication in Transport Layer	Supports only connectionless communication in the Network layer, but both connectionless & connection-oriented communication in Transport Layer
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguish between Service, Interface and Protocol.
Protocols are better hidden and can be replaced relatively easily as technology changes (No transparency)	Protocols are not hidden and thus cannot be replaced easily. (Transparency) Replacing IP by a substantially different protocol would be virtually impossible
OSI reference model was devised before the corresponding protocols were designed.	The protocols came first and the model was a description of the existing protocols

The Internet was developed based on the standards of the TCP/IP protocols. The TCP/IP model gains credibility because of its protocols. The OSI model is not generally used to build networks. The OSI model is used as a guide to help students understand the communication process.

Connection oriented and connection less service

The end system exchange message with each other according to an application level protocol in order to accomplish some task. The TCP/IP network provides two types of services to its application.

1. Connectionless service
2. Connection oriented service

1. Connectionless service

In connectionless service, when one side of an application wants to send packets to another side of an application, the sending application simply sends the packets without handshaking. Since there is no handshaking process prior to the transmission of packets, data can be delivered faster but there is no acknowledgement either, so a source never knows for sure which packets arrive in the destination. This service also has no provision for flow control and congestion control. The network connectionless service is provided by **UDP** (User datagram protocol).

2. Connection oriented service

When an application uses connection oriented service, the client and the server residing at different end system send control packet to each other before sending packets with real data. The procedure of sending control packet is also called as handshaking that alert client and server to be ready for transmission of packets. Once handshaking procedure is finished between, a connection is established between two end system hence called as connection oriented. The

connection oriented service also provides other services like reliable data transfer, flow control, congestion control. The connection oriented service is provided by **TCP** (Transmission control protocol).
Note:

- By **reliable data transfer**, we mean that an application can rely on the connection to deliver all of its data without error and in proper order. Reliability is achieved through the use of acknowledgement and retransmission. Example: consider an application that has established a connection between end system A and B. when end system B receives a packets from A, it sends an acknowledgement. When end system A receives the acknowledgement, it knows that the corresponding packet has definitely been received. But when end system A doesn't receive an acknowledgement, it assume that the packet it send was not received by B so it retransmits the packet after certain time.
- **Flow control** makes sure that neither side of a connection over whelms the other side by sending too many packets too fast. The flow control service forces the sending end system to reduce its rate whenever there is such risk.
- **Congestion control** service helps to prevent the network from entering into a state of grid lock. If every pair of communication end system continue to pump packets into the network as fast as they can, grid lock set in and few packets are delivered to destination because packets loss occur as router buffer overflows. So in order to avoid this problem the congestion control service forces end system to reduce the rate at which they send packet into the network during the period of congestion.

Networking Hardware:

NIC

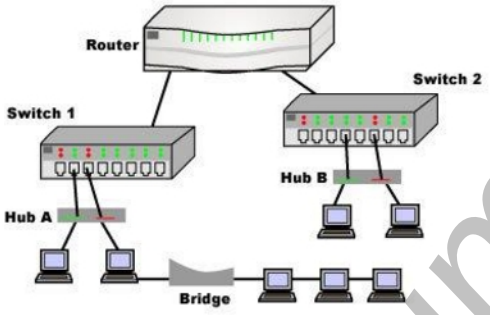
- A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface) is a computer hardware component that connects a computer to a computer network.
- A network adapter prepares data for transmission, sends and receives the data, and translates the data back into a computer readable form.
- Different types of component can function as network adapter. Example, we might use a MODEM to dial a phone line to connect our workstation to internet.
- Early network interface controllers were commonly implemented on expansion cards that plugged into a computer bus
- The NIC contains the electronic circuitry required to communicate using a wired connection (e.g., Ethernet) or a wireless connection (e.g.,WiFi).
- The network controller implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet, Fibre Channel, Wi-Fi or Token Ring.
- The NIC may use one or more of the following techniques to indicate the availability of packets to transfer:
  1. **Polling** is where the CPU examines the status of the peripheral under program control.
  2. **Interrupt-driven I/O** is where the peripheral alerts the CPU that it is ready to transfer data.
- Also, NICs may use one or more of the following techniques to transfer packet data:
  1. **Programmed input/output** is where the CPU moves the data to or from the designated peripheral to memory.
  2. **Direct memory access** is where an intelligent peripheral assumes control of the system bus to access memory directly. This removes load from the CPU but requires more logic on the card. In addition, a packet buffer on the NIC may not be required and latency can be reduced.

Repeater

- Every network architecture specification includes a maximum supported cable lengths for different media types because of problem of attenuation-the weakening of signal over distance.
- So we can extend the distance of communication by using repeater.
- A repeater connects two segments of your network cable.
- It receives and regenerates the signals to proper amplitudes and sends them to the other segments.
- When talking about, Ethernet topology, you are probably talking about using a hub as a repeater.
- Repeaters require a small amount of time to regenerate the signal.

- This can cause a propagation delay which can affect network communication when there are several repeaters in a row.
- Many network architectures limit the number of repeaters that can be used in a row.
- Repeaters work only at the physical layer of the OSI network model. Hub, switches, router also act as repeater.

Hub, Bridge, Switch, Router



Hub

- Also called as multiport repeater
- A hub is just used to connect network segments together.
- Provide half duplex communication.
- Work at physical layer of network.
- A Hub is the simplest of these devices. In general, a hub is the central part of a wheel where the spokes come together.
- Hubs cannot filter data so data packets are sent to all connected devices/computers and do not have intelligence to find out best path for data packets.
- This leads to inefficiencies, wastage bandwidth and insecure.
- Hubs are used on small. A hub contains multiple ports.
- When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
- Almost replaced by switches.

There are many types of hub

1. Active hub: don't require power and are simple splitter or combiners that group workstations into a single segment.
2. Passive hub: require power and include a repeater function and are thus capable of supporting many more connections.

Bridge

- Is smarter networking tool than hub.
- Bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol.
- Having a single incoming and outgoing port and filters traffic on the LAN by looking at the MAC address, bridge is more complex than hub.
- Bridge looks at the destination of the packet before forwarding unlike a hub.
- When a frame arrives at the bridge, it extracts the destination address from the frame and looks it up in a table to see where the frame is to be sent.
- It restricts transmission on other LAN segment if destination is not found.
- A bridge works at the data-link level of a network, copying a data frame from one network to the next network along the communications path.
- The main advantage of bridge is that it restrict flow of unnecessary traffic between network segments.
- Almost replaced by switches.
- Work at Data link layer of OSI model.

Switch

- A switch when compared to bridge is a fast, intelligent multiport bridge that increases the network speed and throughput.
- Switches can perform error checking before forwarding data, which are very efficient by not forwarding packets that error-end out or forwarding good packets selectively to correct devices only.
- Usually large networks use switches instead of hubs to connect computers within the same subnet.

- The main difference between bridge and switch is that, a switch is most often used to connect individual computer so when one host want to send a frame to another host in the same LAN, the bridge gets the frame but just discard it while switch must actively forward the frame between the two hosts.
- The switch maintain a table, MAC address table for each port corresponding to the MAC address learnt when a host connected at a port transmits data.
- The switch forwards data based on MAC address table.
- Work at datalink layer of OSI model.
- More expensive than bridge.

Router

- A router, like a switch forwards packets based on address.
- It is an internetworking device that can intelligently use a network address information to decide the best path for the data to take to its destination
- They operate at the network layer of OSI model, router can connect two different network.
- Usually, routers use the IP address to forward packets, which allows the network to go across different protocols.
- Routers try to learn the addresses of all the different network segments in the internetwork, so router maintain a routing table.
- For static router, we will have to manually enter the routing information in the routing table and modify it whenever the network topology changes.
- A dynamic router can use the information on the network packet to builds it routing table dynamically.
- Routers forward packets based on software while a switch forwards using hardware.
- Routers support different WAN technologies but switches do not. Besides, wireless routers have access point built in.
- The most common home use for routers is to share a broadband internet connection.
- As the router has a public IP address which is shared with the network, when data comes through the router, it is forwarded to the correct computer.

Assignment:

1. **What are lack of OSI model's success?**
   (see DCCN, Forouzen page no 45)