7.Application Layer => This is the top most layer of the OSI reference model. It is this layer where of the OSI reference model. It is this layer where the transmission of any data packet originates. This layer consists of all the applications which help in initiating the transmission. For e.g. TELNET, FTP or INTERNET explorer are used for initializing the transmission.All the above layers perform the job one after another and attach specific information of its functionality to the data packet and then forward it to the next layer.

Network Devices => There are several devices, which are used for transmitting the data from one location to another. Some devices can be used within a LAN, between two LAN's on similar protocols, between two LAN's with dissimilar protocols or to carry the data to longer distances through different path. Some of the devices with their working features are mentioned below;

1. Repeaters => This is one of the trivial use devices for linking two or more segments of a LAN. This device performs the job of amplification of the signals. So that it can be carried to longer distances .This device connects two segments of the same LAN keeping in view the attenuation

length of the media through which data transmission is made possible.

The drawbacks related to this device are of no filtration of data packets and at the dame time no error detection techniques are implemented. If a corrupted signal passes through the repeater its strength is increased .But the signal is not corrected.

2. HUB => This device is one of the most widely used devices in the network installation. It works as a control juncture for all the nodes in the network .Any transmission of data packet from one node to another is passed through this control device. It is because of this device that star topology is being implemented. There are three types of HUB available namely;

(a)Passive HUB => This is just like a repeater which is used for connecting the entire node in the Star topology.

(b)Active HUB => This device is the highly used device in today's world. This device broadcast the entire data to all the nodes in the network. It is not used for regenerating the signals. But for broadcasting the information in the network. The major drawback of this HUB is that of collision of data

packets in the network, if more then one user is transmitting the data. The other disadvantage related to this device is that of no filtration performed on the data packets. The entire network is recognized by a single domain name hence broadcasting in the obvious choice for transmission.

(c)Intelligent HUB (SWITCH) => This is the newly developed device for performing the transmission of data packets .This device removes the drawbacks of active HUB. This device divides the entire network into several sub domains. And each sub domain gives the information about a single node in the network. The concept of filtration is performed by this device on the basis of sub domains. Thus the collision of data packets is heavily reduced by this device. Whenever this device is used no broadcasting of data packets is performed.

Bridge HUB => This concept is implemented when the no of terminals in the network increases then the no. of ports available in a single HUB. In such scenario two Hub's are linked together to incorporate all the nodes in a single network. When the two devices (Hub's) are linked with each other it is referred as a bridge. Hence the name Bridge HUB.

The two HUBS allow the transmission of data packets in a single LAN combined.

Hierarchical HUB => There might be a scenarios that several no of nodes one attached in a single network and bridging hub's is not capable of allowing all the nodes in a single network .It is then the hierarchical hub concept is implemented to include all the nodes in a single LAN. Any transmission of data packet will always be performed by the parent HUB in the hierarchy. The two hubs at the same label can not communicate with each other directly. The transmission between the hubs is also allowed by their parent hub.

3. Bridge => This device is used to transfer the data packets from one network to another. Both the networks should work on the similar protocols so that the transmission can be performed between the networks. There are three types of bridges available namely;

(a) Transport Bridge => This was one of the trivial bridge device which was used for transmitting the data packets

from one network to another .As the name suggest “Transport” any of the node in any network is unaware of the bridge which is used for transmission. These categories of bridge have the information regarding all the nodes available in each of the networks (LAN). This entire information is stored in a table as a database an accordingly data is transmitted either within the network or from one network to another .The information stored in the table is manually entered and this updating is performed whenever any new node is attached with any of the network.

(b)Spanning Bridge => There was a problem when multiple local area networks (LAN) and multiple bridges were used for transmitting the data packets from one network to any of the other network. In such circumstances it was possible for any data packet to be traveling in an infinite loop and thus never reaches to the definition. To remove this problem an algorithm was designed on the concept of spanning tree. Here each node is connected to every other node in such a manner that a cyclic loop is not created. And thus the data packet will never be in an infinite loop. There are two ports which are used either for transmitting or blocking the transmission. It was referred as forwarding port and blocking

port. Whenever these were the chance of creating an infinite loop that particular port of the bridge was blocked.

(c)Source Routing Bridge => This is one of the newest bridging devices used in today's networks. It works in the similar manner when compared with spanning bridge. The major difference lies during the installation of a new network. In this case the data packets defines the bridges through which the transmission will be made and there by each bridge is capable of updating its information in the database regarding the network and as well as the name source routing. It also does not allow the movement of data packets in an infinite loop.

Working of Bridge => As this device is used for transmitting the data packets from one network to another and as well as within the same network. The concept is to transfer all the data packets to the bridge for the first time. It is then the bridge which finds the source node and the destination node in its database. If both the nodes are in the same network the data packets is transmitted back to the same network. Otherwise to the destination network where the node is available.

Source routing bridge and spanning bridge generates the database automatically by gathering the information from the header of the data packet whereas Transport Bridge needs manual feeding of the information.

4. Routers => This device is used for transmitting the data packets in wide area networks. Routers are capable of storing large amount of data about the network and as well as the nodes or the hops available in any network .Routers is used for transmitting the data packets in a cost effective manner. There are several algorithms which are being implemented in order to calculate the cost for transmission. At a time any one of the algorithm is implemented in the device and accordingly the entire database about the network is generated.

There are three basic types over which the cost is calculated. Firstly the length i.e. the distance to be covered between the source and the destination, secondly the no of intermediate nodes (Hops) between the source and the destination and thirdly the type of service available wireless or wire.

5. Gateways => This device is used to transfer the data packets between two or more network working on dissimilar protocols. It is because of this device which helps in communicating between different types of network available in today's world. This device nearly converts the arrival of data packets in such format which is easily accessible by the destination network.

Error => When any data packet is transmitted it should reach to the destination in the correct manner. There can be some circumstances due to which error can be generated in the data. In digital terms error is defined as conversion of 0 to 1 and vice versa.

There are two approaches which are followed for error control mechanisms.

(a)Error Detection => Error detection methods are suppose to detect any error which might be generated during the transmission.

(b)Error Correction => Error correction implements such methods which are helpful in performing error detection in the first stage and after that the corrupted data is corrected

in the second phase. In networking this concept is rarely used.

Types of Error => There are two categories of errors which are generated in the data packets;
(

a)**Single Bit Error =>** In this category just one bit value is converted i.e. either 0 is converted to 1 or 1 is converted to 0. This conversion takes place at a single location in the entire data packet.

(b)**Burst Error =>** In this type of error multiple bits values are converted which can be either consecutive or dispersed on several locations in the data packet.

Error Detection Techniques => There are several techniques which are implemented in order to detect any error which might have generated in the data packet. Some of the methods are mention below;

(i) Parity Bit => Parity bit is referred as the most significant bit of the data. In this concept the data packet is of 7bits and one additional bit is attached in order to perform the error detection. This particular bit is referred as Parity bit.
There are two approaches which are following in Parity bit error detection technique:

(a)Even Parity => In this mechanism the no of 1's are counted in the entire data and then an additional bit is attached depending upon the no of 1's are even or not. If it is not even then 1 bit is attached and if already even then 0 bit is attached.

(b)Odd Parity => In this mechanism the no of 1's are suppose to be in odd no. and accordingly one bit or 0 bit is attached.

(ii)Two Dimensional Parity => In this mechanism of error detection multiple data sets are collected together and arranged 1 below another. After this arrangement the row wise parity of each individual is performed in the first cycle. After the completion of the first cycle the column wise parity is performed on the entire data sets. This task is performed

in the second cycle, after this the entire data set with the newly created parity check is transmitted. At the receiving end this parity check data is used for cross checking the validation of the data.

Disadvantage => The above described two methods have one common disadvantage. These error detection techniques can only be used for single bit errors not for burst errors.

C.R.C: -

Algo for CRC (Sender) =>

(

a)Get the Data on which error detection is to be performed.

(b) Attach n – 1 zeroes to the data for the division of n- bits.

(c) Perform Binary Division (XOR) on the newly created Data.

(d) The Remainder Availability is the CRC.

(e) Send the Data by eliminating the no of zeroes and Attaching the CRC.

Algo for CRC (Receiver) =>

(a) Receive the Data with the Header.

(b) Retrieve the CRC from Header and attach it to Data.

(c) Perform Binary Division (XOR) on the newly data.

(d) If the Remainder is all zeroes then the Data is correct.

Else

The Data is Incorrect.

(e) Send +ve/ - ve Acknowledgment accordingly.

CHECKSUM =>

Working (Sender) –

(a) Arrange the Data and perform addition (Binary Addition).

(b) Take the 1's compliment of the result after addition.

(c) The complimented value is the checksum.

(d) Data sets with the complimented value is transmitted.

Working (Receiver) –

(a) Collect the datasets from the data section and checksum for header section.

(b) Perform addition on the data sets.

(c) Again perform addition with resulted value and the checksum value.

(d) Take the 1's compliment of the newly result obtained.

(e) If the result is all zeros then data is correct

Else

Corrupted Data.

Checksum is the most widely used error detection technique and is performed only on the transport layer of the OSI – Reference model this mechanism uses the concept of binary addition with its 1's complement technique. On the basis of the binary addition and the 1's compliment technique error detection can be easily performed. The basic concept is to divide the entire length of data into equal sizes. And then perform the binary addition. The algorithms perform or followed at the sender and the receiver end is give above.

FLOW CONTROL => Flow control technique is used to perform the transmission in a specified manner between a sender and a receiver. There are several techniques which are used for maintaining the flow of data packets between the sender and the receiver. This technique is implemented at the data link layer and transport layer of the OSI-Reference model. It is performed in order to restrict a fast sender to over run a slow receiver.

There are basically three types of Flow Control techniques;

1. STOP & WAIT => This is one of the earliest technique which is used for controlling the flow of data. As the term suggest, when the data is transmitted the transmission is stopped. Hence the name “STOPS” and after that the sender waits for the acknowledgment from the receiver, hence the term “WAIT”. If the sender does not receive the acknowledgment it never transmits the data packet until the duration specified is over. This mechanism of transmission control has several flows in it.

Drawback => Firstly the transmission is unidirectional i.e. only sender can transmit the data the receiver can not. Secondly there is wastage of bandwidth during the entire interval when the sender waits for the acknowledgment.

The only Merit associated in this technique is the guaranteed information of data packet whether transmitted or not.

Problems during Transmission =>

(1) Data is Lost

(2) Acknowledgment is Lost

(3) Data is Delayed

(4) Acknowledgment is Delayed.

In all of the above cases the timer works as the most important tool for finding out the duration in which data

packet is to be transmitted is over or not. And accordingly retransmission of the same data packet or transmission of new data packet is dependent.

2. PIGGY BACKING => This mechanism removes the drawback of STOP & WAIT flow control mechanism. In this technique sender is also transmitting the data and as well as acknowledgment and also the receiver transmits the data and acknowledgment after receiving the data. Thus the uses of bandwidth are increased as compared with STOP & WAIT flow control. There is a restriction on the receiver side that the data will be transmitted only when the acknowledgment is to be send.

3. SLIDING WINDOW => This is a new concept which has evolved to remove the drawbacks of STOP & WAIT and Piggy Backing flow control techniques. In this new mechanism a fixed size of window is designed which consist of fixed no of data packets. This entire data packet within a frame is referred as a window. There are several windows dependent upon the amount of data being transmitted are created. Whenever any data packet of a particular window is transmitted it moves to the next segment and covers the first packet of that segment. This process is referred as Sliding and this process continues until all the data packets are

transmitted. Hence the name of the mechanism Sliding Window.

There are two types of mechanism implemented through Sliding Window concept. They are,

(a) GO BACK N => In this technique of transmission multiple data packets are transmitted simultaneously depending upon the size of the window. In this technique whenever any single data packet is lost or delayed then form that packet to the last transmitted packet all the data packets are retransmitted. Here ‘N’ suggests the packet no. which has not reached to the receiver due to any reason.

Disadvantage => In this flow control mechanism the major drawback is of retransmitting all the data packets when a single data packet is corrupted or loosed. Thus redundant data packets are present in the network.

(b) Selective Repeat => In this flow control mechanism the drawback of GO BACK N strategies is removed. Here a new concept of negative acknowledgment is designed. In these strategies the concept of sliding window is implemented. Thus multiple packets are transmitted simultaneously. Whenever any data packet is received a positive

acknowledgment is transmitted. And if the data packet is loosed due to any reason then a negative acknowledgment is transmitted by the receiver. Thus only the data packets of which negative acknowledgment are received by the sender, those data packets are only retransmitted by the sender.

Advantage : -

(1) This mechanism nearly performs the optimum utilization of the bandwidth.
(2) There are no redundant data packets available in the network because of the negative acknowledgment strategies.
(3) The sender does not have to wait before transmitting the new data packets.

Disadvantage-

The only disadvantage related to this control technique is the complexity involved for the implementation of –ve acknowledgment.

SWITCHING TECHNIQUES => There are several types of techniques implemented for transmitting the data from a sender to a receiver. All the categories are with some merits and demerits. Some of them are listed below;

1. Circuit Switching => This switching technique establishes a permanent connection between the source and the destination .The foremost concept in this switching technique is that of established the link before any data is transmitted. If the link is not established then the data transmission is not performed. The advantage of using such switching technique is of guaranteed link between the source and the destination from the start to the end of the communication. The disadvantage is related with the wastage of bandwidth because no other use can access the same link for transmission.

2. Message Switching => In this switching technique the permanent link between the sender and the receiver is not established. The entire data is decomposed into several sieges of message and then it was transmitted through all the paths available for transmission. This switching technique has the major drawback of not having the defined

size of the data packets (message packets). In this case any user can transmit the data with variable sieges. Thus a standard siege was not defined in the switching technique.

3. Packet Switching => This is the most widely used switching technique in today's world. In this switching technique a siege of the data was fixed according to the network through which transmission is to be performed. The data packets where transmitted along all the free routs available for the destination.