MOTHER THERESA INSTITUTE OF COMPUTER APPLICATIONS
Melmoi village & post
Palamaner
Chittoor dist , A.P
Ph : 08579 258585,80

SNO	CONTENTS	Page NO

1. Routing Algorithms

Routing

Introduction

Routing is one of the most important features in a network that needs to connect with other networks. In this page we try to explain the difference between Routed and Routing protocols and explain different methods used to achieve the routing of protocols. The fact is that if routing of protocols was not possible, then we wouldn't be able to communicate using computers because there would be no way of getting the data across to the other end

Definition

Routing is used for taking a packet (data) from one device and sending it through the network to another device on a different network. If your network has no routers then you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know the following:

- Destination address
- Neighbor routers from which it can lean about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

Before we go on, I would like to define 3 networking terms:

Convergence: The process required for all routers in an internetwork to update their routing tables and create a consistent view of the network, using the best possible paths. No user data is passed during convergence.

Default Route: A "standard" route entry in a routing table which is used as a first option. Any packets sent by a device will be sent first to the default route. If that fails, it will try alternative routes.

Static Route: A permanent route entered manually into a routing table. This route will remain in the table, even if the link goes down. It can only be erased manually.

Dynamic Route: A route entry which is dynamically (automatically) updated as changes to the network occur. Dynamic routes are basically the opposite of static routes.

Shortest path routing algorithm

Shortest path routing algorithm is a simple and easy to understand technique. The basic idea of this technique is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line i.e., link. For finding a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph. The length of a path can be measured in a number of ways as on the basis of the number of hops, or on the basis of geographic distance etc.

There are a number of algorithms for computing the shortest path between two nodes of a graph. One of the most used algorithm is the Dijkstra algorithm. This is explained below:

In this algorithm, each node has a label which represents its distance from the source node along the best known path. On the basis of these labels, the algorithm divides the node into two sets i.e., tentative and permanent. As in the beginning no paths are known, so all labels are tentative. The Algorithm works in the following manner:

1) First mark source node as current node (T-node)

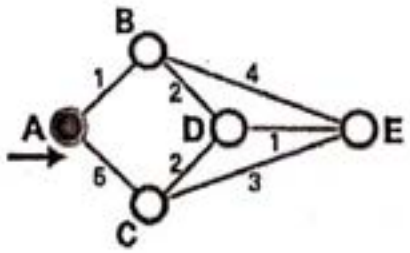
2) Find all the neighbors of the T-node and make them tentative.

3) Now examine all these neighbors.

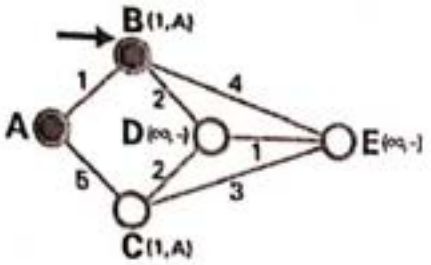
4) Then among these entire node, label one node as permanent (i.e., node with the lowest weight would be labeled as permanent) and mark it as the T-node.

5) If, the destination node is reached or tentative list is empty then stop, else go to step 2.An example of Dijkstra routing algorithm is explained in Figure 2: In this example, we want to find the best route between A and E. Here, we will show permanent nodes with filled circles and T-nodes with the --> symbol.

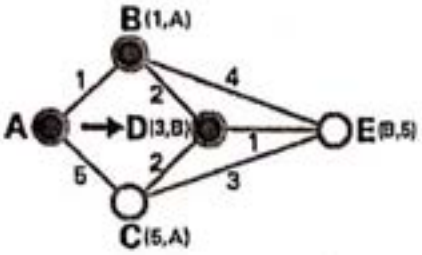
1) As shown in the Figure below, the source node (A) has been chosen as T-node, and so its label is permanent.



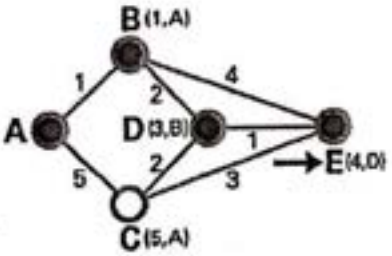
2) In this step, as you see B, C are the tentative nodes directly linked to T-node (A). Among these nodes, since B has less weight, it has been chosen as T-node and its label has changed to permanent.



3) In this step, as you see D, E are the tentative nodes directly linked to T-node(B). Among these nodes, since D has less weight, it has been chosen as T-node and its label has changed to permanent.



4) In this step, as you see C, E are the tentative nodes directly linked to T-node(D). Among these nodes, since E has less weight, it has been chosen as T-node and its label has changed to permanent.



5) E is the destination node. Now, since the destination node (E) has been, reached so, we stop here, and the shortest path is A –B –D –E.

DISTANCE VECTOR ROUTNIG

Nowadays, computer networks generally use dynamic routing algorithms rather than the static ones described above because; static algorithms do not take the current network load into account. Distance vector routing and link state routing are two main dynamic algorithms. In this section, we will go through the distance vector routing algorithm. It is also known as Belman-Ford routing algorithm.

Bellman-Ford Algorithm Routing Algorithms

The Bellman-Ford algorithm can be stated as follows: Find the shortest paths from a given source node subject keeping in mind the constraint that, the paths contain at most one link; then, find the shortest

paths, keeping in mind a constraint of paths of at most two links, and so on. This algorithm also proceeds in stages. The description of the algorithm is given below

s = source node

w(i, j) = link cost from node i to node j; $w(i, j) = \infty$ if the two nodes are not directly connected; $w(i, j) \geq 0$ if the two nodes are directly connected.

h = maximum number of links in a path at the current stage of the algorithm

Lh(n) = cost of the least-cost path from node s to node n under the constraint of no more than h links

1. [Initialisation]

$L_0(n) = \infty$, for all $n \neq s$

$L_h(s) = 0$, for all h

2. [Update]

For each successive $h \geq 0$:

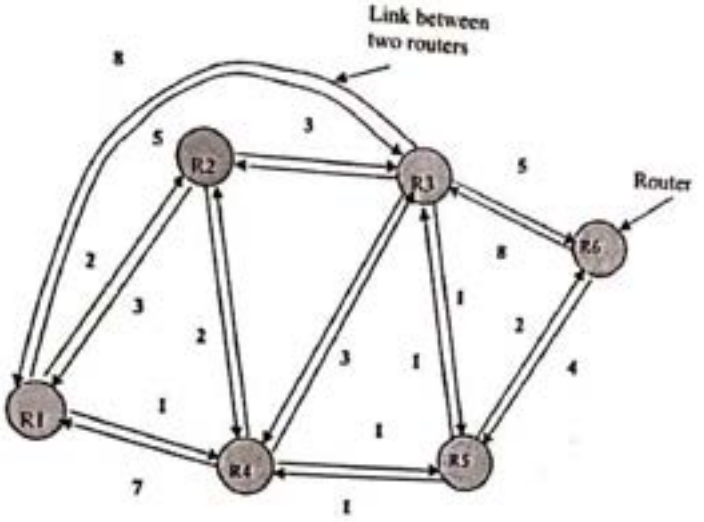
For each $n \neq s$, compute

$$L_{h+1}(n) = \min_j [L_h(j) = w(j, n)]$$

Connect n with the predecessor node j that achieves the minimum, and eliminate any connection of n with a different predecessor node formed during an earlier iteration. The path from s to n terminates with the link from j to n. For the iteration of step 2 with h = K, and for each destination node n, the algorithm compares potential paths from s to n of length K + 1 with the path that existed at theend of the previous iteration. If the previous, shorter path has less cost, then that path is retained. Otherwise a new path with length K + 1 is defined from s to n; this path consists of a path of length K from s to some node j, plus a direct hop from node j to node n. In this case, the path from s to j that is used is the K-hop path for j defined in the previous iteration.

Table 1 shows the result of applying this algorithm to a public switched network, using s = 1. At each step, the least-cost paths with a maximum number of links equal to h are found. After the final iteration, the least-cost path to each node and the cost of that path has been developed. The same procedure can be used with node 2 as the source node, and so on. Students should apply Dijkstra's algorithm to this subnet and observe that the result will eventually be the same.

(a)



Public switching newtwork

H	$L_4(2)$	Path	$L_4(3)$	Path	$L_4(4)$	Path	$L_4(5)$	Path	$L_4(6)$	Path
0	∞	—	∞	—	∞	—	∞	—	∞	—
1	2	1-2	5	1-3	1	1-4	∞	—	∞	—
2	2	1-2	4	1-4-3	1	1-4	2	1-4-5	10	1-3-6
3	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
4	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

LINK STATE ROUTING:

As explained above distance vector routing algorithm has a number of problems like count to infinity problem. For these reasons, it was replaced by a new algorithm, known as the link state routing. Link state routing protocols are like a road map. A link state router cannot be fooled as easily into making bad routing decisions, because it has a complete picture of the network. The reason is that, unlike approximation approach of distance vector, link state routers have first hand information from all their peer routers. Each router originates information about itself, its directly connected links, and the state of those links. This information is passed around from router to router, each router making a copy of it, but never changing it. Link-state involves each router building up the complete topology of the entire network (or at least of the partition on which the router is situated), thus, each router contains the same information. With this method, routers only send information to of all the other routers when there is a change in the 31topology of the network. The ultimate objective is that every router should have Routing Algorithms identical information about the network, and each router should be able to calculate its own best path independently. Independently calculate its own best paths. In contrast to the distance-vector routing protocol, which works by sharing its knowledge of the entire network with its neighbors', link-state routing works by having the routers inform every router in the network about its nearest neighbors.

The entire routing table is not distributed any router but, the part of the table containing its neighbors is: Link-state is also known as shortest path first.

Link State Packet

When a router floods the network with information about its neighborhood, it is said to be advertising. The basis of this advertising is a short packet called a link state packet (LSP). An LSP usually contains four fields: the ID of the advertiser, the ID of the destination network, the cost, and the ID of the neighbor router. The structure of a LSP is shown in Table 2.

Table 2: Link state packet (LSP)

Advertiser DD	Network DD	Cost	Neighbour DD
.....	.....	.....	.....
.....	.....	.....	.....

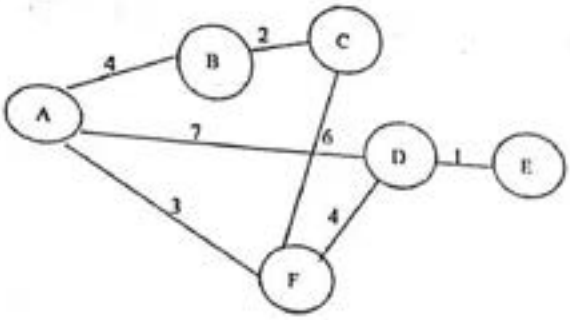
How Link State Routing Operates

The idea behind link state routing is simple and can be stated in five parts as suggested by Tanenbaum [Ref.1]. Each router must do the following:

1) Neighbour discovery : The Router has to discover its neighbors and learn their network addresses. As a router is booted, its first task is to learn who its neighbors are. The Router does this by sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send a reply disclosing its identity. These names must be globally unique. If two or more routers are connected by a LAN, the situation becomes slightly more complicated. One way of modeling the LAN is to consider it as a node itself. Please see reference [1] for further explanation through a diagram.

2) Measure delay : Another job that a router needs to perform is to measure the delay or cost to each of its neighbors. The most common way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. For even better results, the test can be conducted several times and the average used. This method implicitly assumes that delays are symmetric, which may not always be the case.

3) Building link state packets: After collecting the information needed for the exchange, the next step for each router is to build a link state packet containing all the data. This packet starts with the identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbor, the delay to that neighbor is given. As an example, let's consider the subnet given in Figure 5 with delays shown as labels on the lines. For this network, the corresponding link state packets for all six routers are shown in the Table 3.



The link state packets for the subnet in fig

Table 3: The link state packets (LSPs) for the subnet in figure

A	
Seq.	
Age	
B	4
D	7
F	3

B	
Seq.	
Age	
C	2
A	4

C	
Seq.	
Age	
B	2
F	6

D	
Seq.	
Age	
A	7
E	1
F	4

E	
Seq.	
Age	
D	1

F	
Seq.	
Age	
A	3
C	4
D	6

Building the link state packets is easy. The hard part is determining when to build them. One possibility, is to build them periodically, that is, at regular intervals. Another possibility is to build them when some significant event occurs, such as a line or neighbour going down or coming back up again or changing its properties appreciably.

4) Distribute the packets : Let us describe the basic algorithm in distributing the link state packet. The fundamental concept here is flooding to distribute the packets. But to keep the number of packets flowing in the subnet under control, each packet contains a sequence number that is incremented for each new packet delivered. When a new link state packet arrives, it is checked against the list of packets already scene by a router. It is discarded in case the packet is old; otherwise it is forwarded on all lines except the one it arrived on. A router discards an obsolete packet (i.e., with a lower sequence) in case it has seen the packet with a highest sequence number. The age of a data packet is used to prevent corruption of the sequence number fromcausing valid data to be ignored. The age field is decremented once per second by the routers which forward the packet. When it hits zero it is discarded. How often should data be exchanged?

5) Compute shortest path tree : After accumulating all link state packets, a router can construct the entire subnet graph because every link is represented. In fact, every link is represented twice, once for each direction. The two values can be averaged or used separately.Now, an algorithm like Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations. The results of this algorithm can be installed in the routing tables, and normal operation resumed. Problems in Link State RoutingIn link state protocol, the memory required to store the data is proportional to k * n, for n

routers each with k neighbors and the time required to compute can also be large. In it bad data e.g., data from routers in error will corrupt the computation.

HIERARCHICAL ROUTING:

As you see, in both link state and distance vector algorithms, every router has to save some information about other routers. When the network size grows, the number of routers in the network increases. Consequently, the size of routing tables increases, as well, and routers cannot handle network traffic as efficiently. We use hierarchical routing to overcome this problem. Let's examine this subject with an example:

We use distance vector algorithms to find best routers between nodes. In the situation depicted below in Figure 6, every node of the network has to save a routing table with 17 records.

Here is a typical graph and routing table (Table 4) for A:

Table 4: A's Routing Table

Destination	Line	Weight
A	—	—
B	B	1
C	C	1
D	B	2
E	B	3
F	B	3
G	B	4
H	B	5
I	C	5
J	C	6
K	C	5
L	C	4
M	C	4
N	C	3
O	C	4
P	C	2
Q	C	3

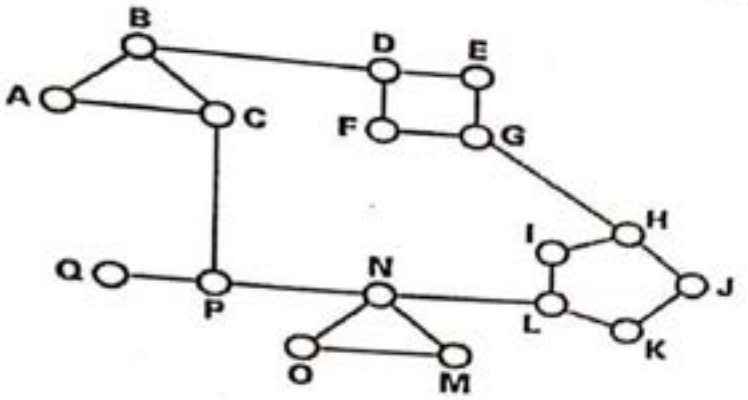


Figure 6: Network graph

In hierarchical routing, routers are classified in groups known as regions (Figure 7). Each router has only the information about the routers in its own region and has no information about routers in other regions. So routers just save one record in their table for every other region. In this example, we have classified our network into five regions as shown below

Table 5: A's Routing table for Hierarchical routing

Destination	Line	Weight
A	—	---
B	B	1
C	C	1
Region 2	B	2
Region 3	C	2
Region 4	C	3

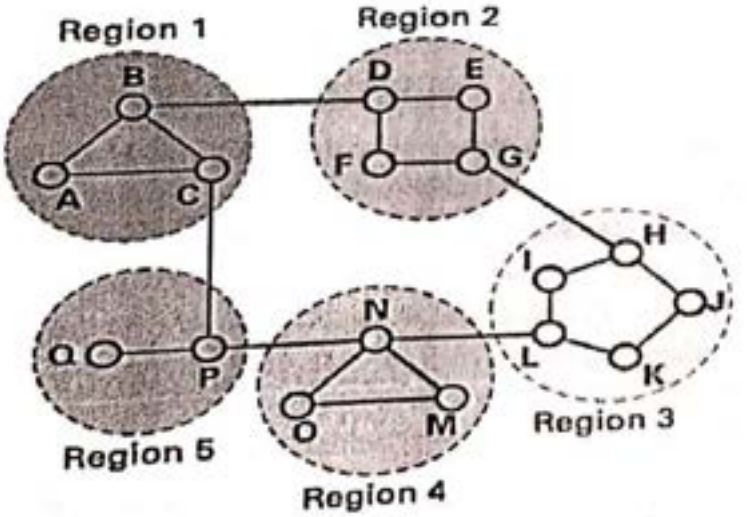


Figure 7: Hierarchical routing

If A wants to send packets to any router in region 2 (D, E, F or G), it sends them to B, and so on. As you can see, in this type of routing, the tables sizes are reduced so, network efficiency improves. The above example shows two-level hierarchical routing. We can also use three or four level hierarchical routing as well. In three-level hierarchical routing, the network is classified into a number of clusters. Each cluster is made up of a number of regions, and each region contains a number of routers. Hierarchical routing is widely used in Internet routing and makes use of several routing protocols.

BROADCAST ROUTING

Up to now we were discussing about sending message from a source to a destination. Sometimes a host needs to send messages all other hosts. This type of transmission i.e., to send a message to all destinations simultaneously is known as broadcasting. There are a no. of methods These are for broadcasting.

• Send a distinct packet to each destination

This is a very simple method, in which a source sends a distinct packet to each destination. Major disadvantages of this method are:

a) It wastes bandwidth.

b) In this method source needs to have a complete list of all destinations. Because of this reason this method is the least desirable of the other methods.

• Flooding

This is also a very simple method of broadcasting. In this method every incoming packet is sent out on every outgoing line except the line from which it arrived. Thisalgorithm is very simple to implement. But the major disadvantage of this algorithm isthat it generates lots of redundant packets, thus consumes too much bandwidth.

• Multidestination routing

In this method each packet contains either a list of destinations or a bit map indicating the desired destinations. When a packet arrives at a router, router determines the set of output lines that would be required by checking all the destinations. Router only chooses those output lines which are the best route to at least one of the destinations. After this router creates a new copy of the packet for each output line to be used and 36Network Layer in each packet it includes only those destinations that are to use the line. Therefore, the destination set is partitioned among the output lines. In this, after a sufficient number of hops, each packet will carry only one destination and can be treated as a normal packet.

• Using a spanning tree

A spanning tree is a subset of graph that includes all the nodes (of graph) but contains no loops. This method uses the spanning tree, therefore, each router knows which of its lines belong to the spanning

tree. When a packet arrives at a router, it copies onto all the spanning tree lines except the one it arrived on. Advantage of this method is that it makes excellent use of bandwidth and generates only the minimum number of packets required to do the job.

In this method each router must have knowledge of some spanning tree. Sometimes this information is available (e.g., with link state routing) but sometimes it is not (e.g., with distance vector routing), this is the major disadvantage of this method.

• Reverse path forwarding

Our last broadcast algorithm is an attempt to approximate the behaviour of the previous one, even when the routers do not know anything at all about spanning trees. The idea, called reverse path forwarding, is remarkably simple once it has been pointed out. In this method, when a broadcast packet arrives at a router, the router checks whether the packet arrived on the line that is normally used for sending packets to the source of the broadcast or not.

If the packet arrived on the line that is normally used for sending packets to the source of the broadcast then Router forwards copies of it onto all lines except the one it arrived on.

Else (i.e., packet arrived on a line other than the preferred one for reaching the source) Router discards the packet as a likely duplicate.

MULTICAST ROUTING

In many cases, you need to send same data to multiple clients at the same time. In this case, if, we use unicasting then the server will connect to each of its clients again and again, but each time it will send an identical data stream to each client. This is a waste of both server and network capacity. If, we use broadcasting in this case, it would be inefficient because sometimes receivers are not interested in the message but they receive it nonetheless, or sometimes they are interested but are not supposed to see the message.

In such cases i.e., for sending a message to a group of users (clients), we use another technique known as multicasting. The routing algorithm used for multicasting, is called multicast routing.

Group management is the heart of multicasting. For group management, we require some methods to create and destroy a group and to allow processes to join and leave a group. When a router joins a group, it informs its host of this fact. For routing, routersmainly want to know which of their hosts belong to which group. For this, either the Routing Algorithmshost must inform their router about changes in the group membership, or routers must query their hosts periodically. On receiving this information, routers tell their neighbours, so the informations propagated through the subnet.

Now, we will learn the working of multicasting through an example. In our example (as shown in Figure 8), we have taken a network containing two groups i.e., group 1 and 2. Here, some routers are attached to hosts that belong to only one of these groups and some routers are attached to hosts that belong to both of these groups

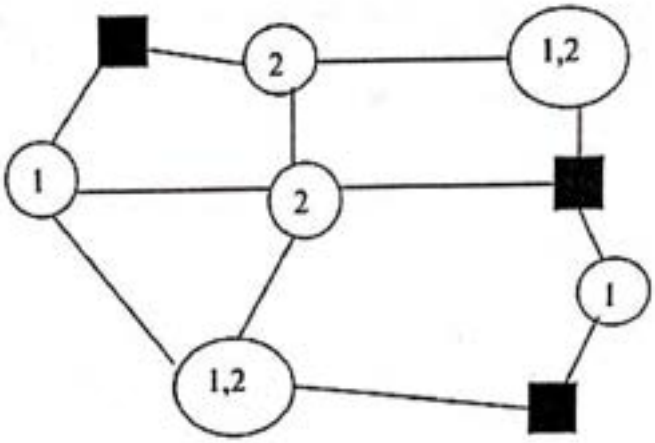


Figure 8: Network containing two groups i.e., 1 and 2

To do multicast routing, first, each router computes a spanning tree covering all other routers. For example, Figure 9 shows spanning tree for the leftmost router.

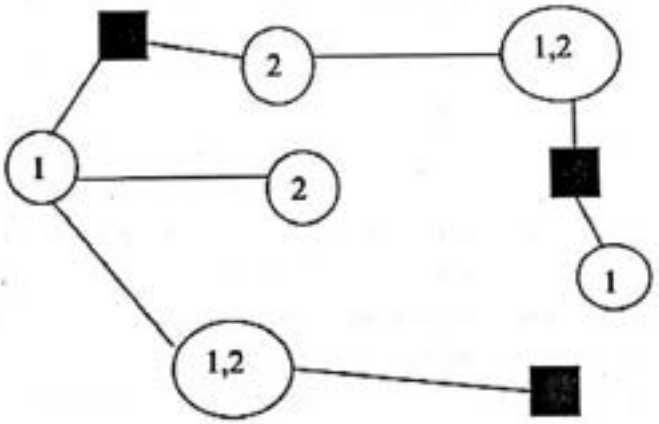


Figure 9: Spanning tree for the leftmost router

Now, when a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it. Pruning is the task of removing all lines that do not lead to hosts that are members of the group. For example, Fig. 10 shows the pruned spanning tree for group 1 and Fig. 11 shows the pruned spanning tree for group 2. There are a number of ways of pruning the spanning tree. One of the simplest ones that can be used, if link state routing is used and each router is aware of the complete topology, including the hosts that belong to those groups. Then, the spanning tree can be pruned, starting at the end of each path, working toward the root, and removing all routers that do not belong to the group under consideration. With distance vector routing, a different pruning strategy can be followed. The basic algorithm is reverse path forwarding. However, whenever a router with no hosts interested in a particular group and no connections to other routers, receives a multicast message for that group,

it responds with a PRUNE message, thus, telling the sender not to send it any more multicasts for that group. When a router with no group members among its own hosts has received such a message on its lines, it, too, can respond with a PRUNE message. In this way, the subnet is recursively pruned.

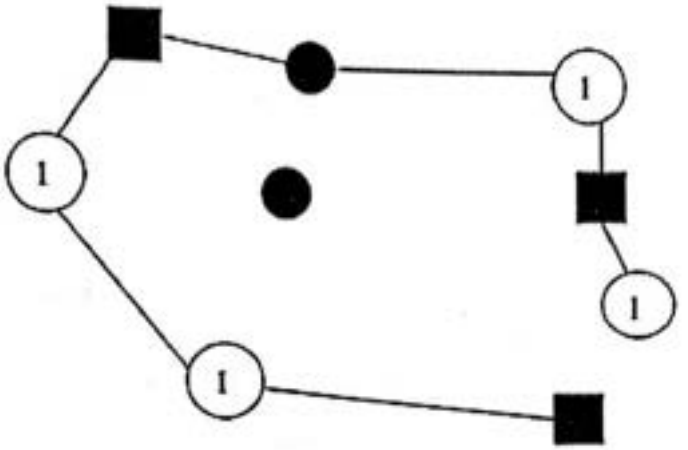


Figure 10: A pruned spanning multicast tree for group 1

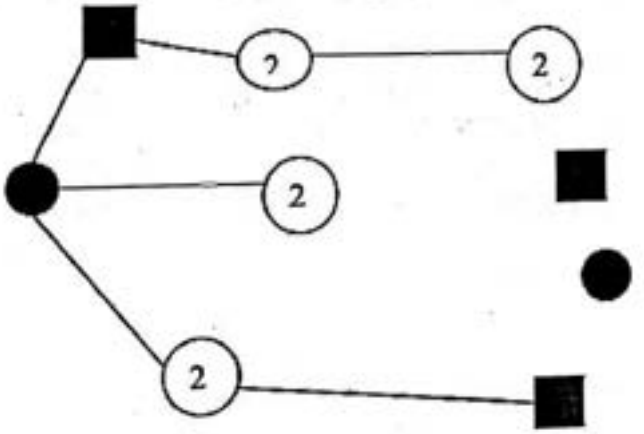
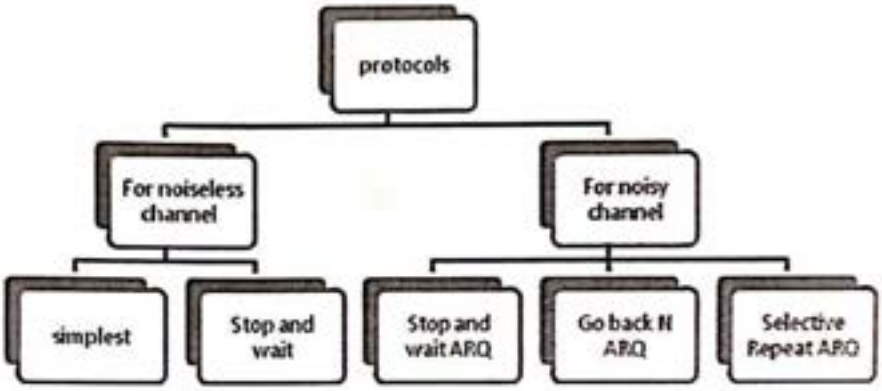


Figure 11: A pruned spanning multicast tree for group 2

After pruning, multicast packets are forwarded only along the appropriate spanning tree. This algorithm needs to store separate pruned spanning tree for each member of each group. Therefore, this would not be good for large networks.

2.THE DATA LINK LAYER

The data link layer can combine framing, flow control and error control to achieve the delivery of data from one node to another. The protocols are normally implemented in software by using one of the common programming languages. To make our discussion language free, we have written in pseudo code a version of each protocol that concentrates mostly on the procedure instead of delving into those that can be used for noiseless channels and those that can be used for noisy channels. The protocols in the first category cannot be used in real life, but they serve as a basis for understanding the protocols of noisy channels.



In a real life network, the data link protocols are implemented as bidirectional; data flow in both directions. In these protocols the fow and error control information such as acknowledgement(ACK) and negative acknowledgement(NAK) is included in the data frames in a technique called piggy backing. Because bidirectional protocols are more complex than unidirectional ones, we chose thelatter for our discussion. If they are understood, they can be extended to bidirectional protocols.

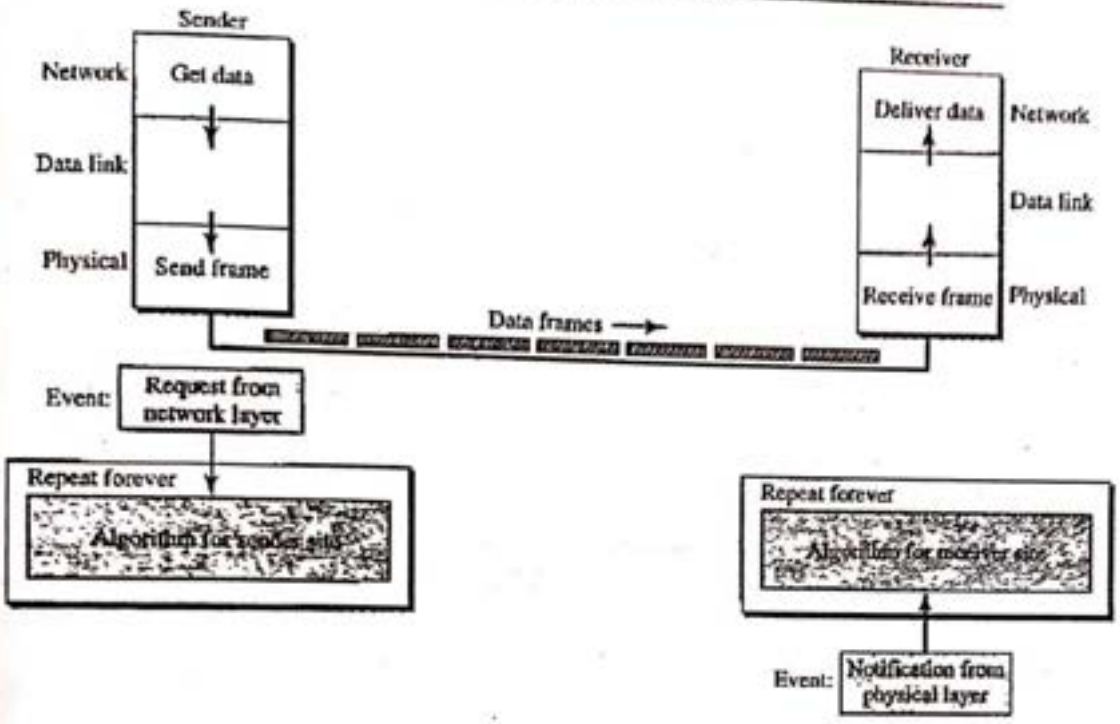
Protocols for Noiseless channels:

Simplest protocol:

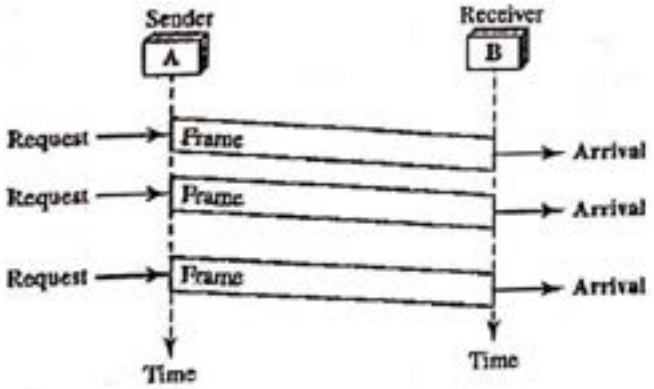
The first protocol which we call the simplest protocol for lack of any other name, is one that has no flow or error control. It is a unidirectional protocol in which data frames are traveling in only one direction from the sender to receiver. We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be neglible. The data link layer of the receiver immediately removes the beaded from the frame and hands the data packet to its network layer, which can also accept the packet immediately. In other words the receiver can never be overwhelmed with incoming frames.

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the receiver site receives a frame from its physical layer, extracts datafrom the frame and delivers the data to its network layer. The data link layers of the sender and receiver provide transmission services for their network layers. The data link layers use the services provided by their physical layers

The design of the simplest protocol with no flow or error control



The bellow fig shows an example of communication using this protocol. It is very simple. The sender sends a sequence of frames without even thinking about the receiver. To send three frames, three events occur at the sender site and three events at the receiver site. Note that the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.

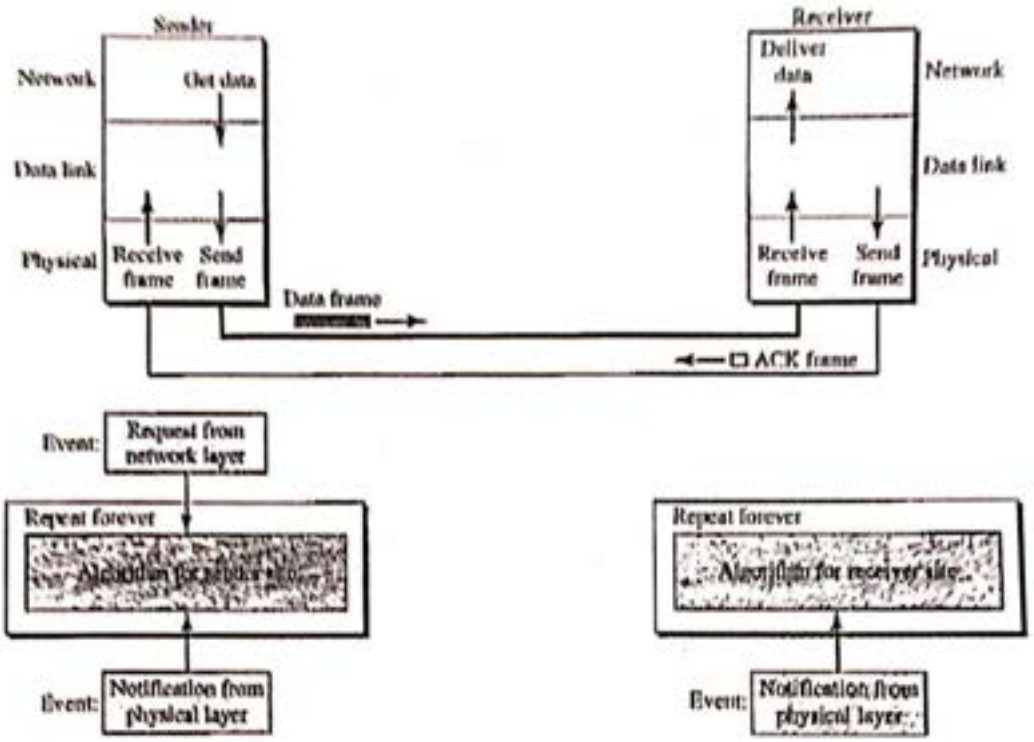


Stop and wait protocol:

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally the receiver does not have enough storage space especially if it is receiveing data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming over whelmed with frames, we somehow need to tell the sender to slow down. There must be feedback from the receiver to the sender.

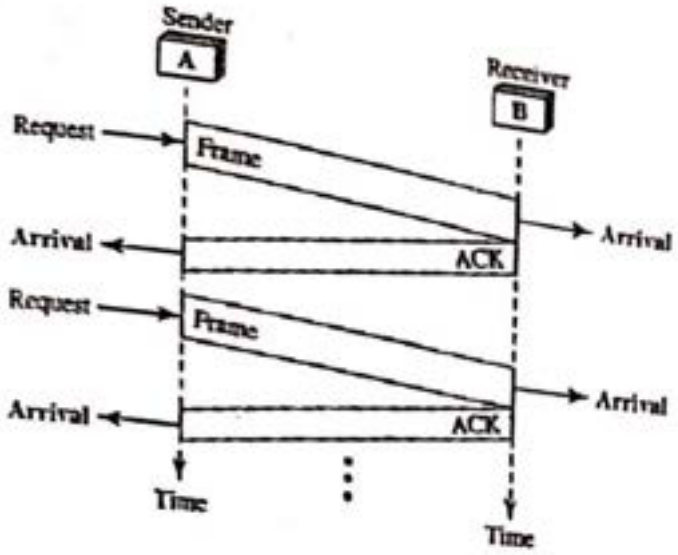
The protocol we discuss now is called the stop and wait protocol because the sender sends one frame stops, until it receives confirmation from the receiver, and then sends the next frame. We still have unidirectional communication for data frames, but auxiliary ACK frames travel from the other direction we add flow control to our previous protocol.

Figure 11.8 *Design of Stop-and-Wait Protocol*



The above figure illustrates the mechanism. When we observe we can see the traffic on the forward channel and the reverse channel. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel; we therefore need a half duplex link.

The bellow fig shows an example of communication using this protocol. It is still very simple. The sender sends one frame and waits from feedback from the receiver. Ehen the ACK arrives, the sender sends the next frame. Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.



Protocols for Noisy channels :

Although the stop and wait protocol gives us an idea of how to add flow control to its predecessor noiseless channels are nonexistent. We can ignore the error or we need to add error control to our protocols. We discuss three protocols in this section that use error control.

Stop and wait automatic repeat request:

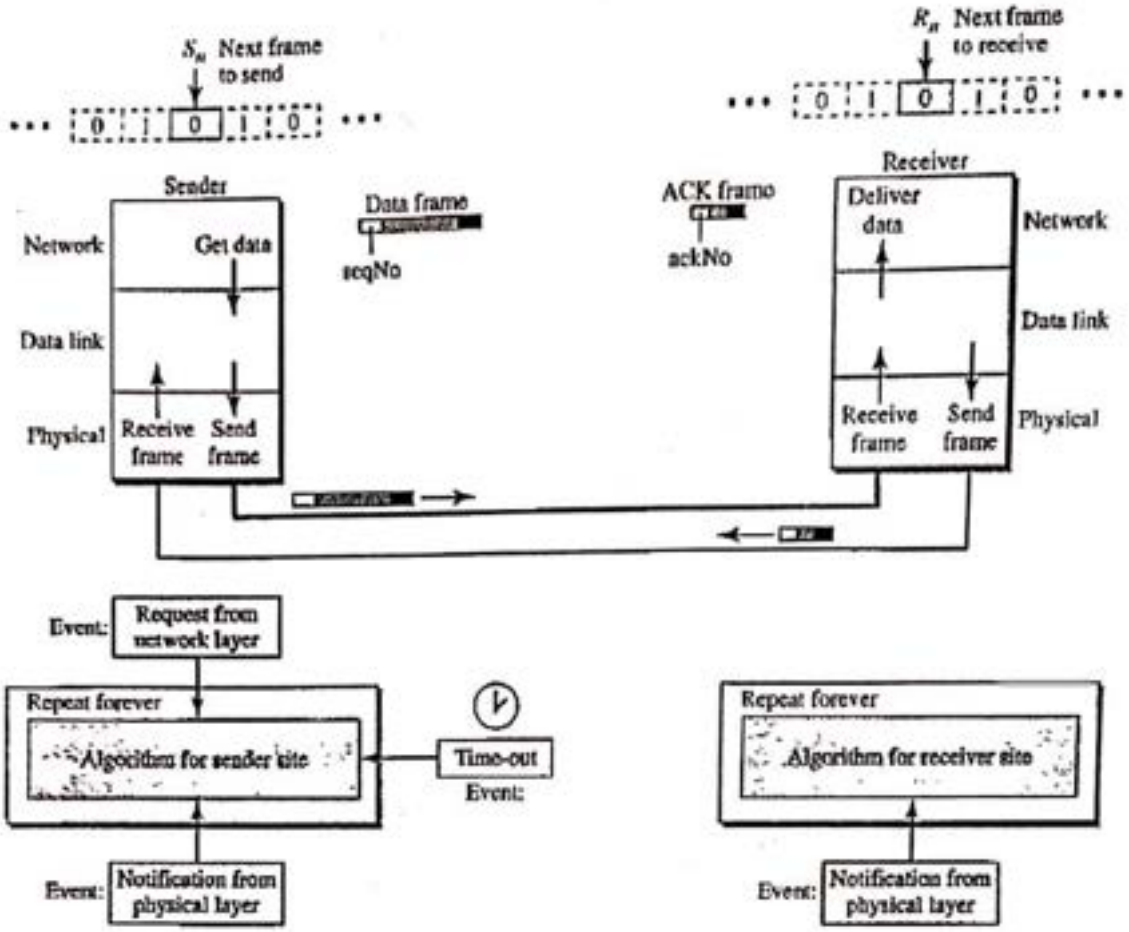
Our first protocol called the stop and wait automatic repeat request adds a simple error control mechanism to the stop and wait protocol. Let us see how this protocol detects and corrects errors.

To detect and correct corrupted frames we need to add redundancy bits to our data frame when the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver.

Lost frames are more difficult to chandle than corrupted ones. In our previous protocols there was no way to identify a frame. The received frame could be the correct one or a duplicate, or a frame out of order. The solution in to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.

The corrupted and lost frames need to be resent in this protocol. If the receiver does not respond when there is an error, how can the sender know which frame ro resend? To remedy this problem the sender keeps a copy of the sen frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted. Since the protocol uses the stop and wait mechanism there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.

Since an ACK frame can also be corrupted and lost it too needs redundancy bits and a sequence number. The ACK frame for this protocol has a sequence number field. In this protocol, the sender simply discards a corrupted ACK frame or ignores an out of order one.



The bellow fig shows the design of the stop and waits ARQ protocol. The sending device keeps a copy of the last frame transmitted unitl it receives an acknowledgement for that frame. A data frames uses a seqNo; an ACK frame uses an ackNo. The sender has a control variable, which we call S_n (sender next frame to send) that holds the sequence number for the next frame to be sent (0 or 1).

The receiver has a control variable, which we call Rn(receiver, next frame expected) that holds the number of the next frame expected. When a frame is sent the value of sn is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa. Three events can happen at the sender site; one event can happen at the receiver site. Variable sn points to the slot that matches the sequence number of the frame that has been sent, but not acknowledged; rn points to the slot that matches the sequence number of the expected frame.

Efficiency:

The stop and wait ARQ discussed in the previous section is very inefficient if our channel is thick and long. By thick, we mean that our channel has a large bandwidth; by long, we mean the round-trip delay is long. The product of these two is called the bandwidth delay product. We can think of the channel as a pipe. The bandwidth delay product then is the volume pipe in bits. The pipe is always there. If we do not use it, we are inefficient. The bandwidth delay product is a measure of the number of bits we can send out of our system while waiting for news from the receiver.

Pipelining:

In networking and in other areas, a task is often begun before the previous task has ended. This is known as pipelining. There is no pipelining in stop and wait ARQ because we need to wait for a frame to reach the destination and be acknowledged before the next frame can be sent. However, pipelining does apply to our next two protocols because several frames can be sent before we receive news about the previous frames. Pipelining improves the efficiency of the transmission if the number of bits in transition is large with respect to the bandwidth delay product.

Go back N Automatic Repeat Request:

To improve the efficiency of transmission multiple frames must be in transition while waiting for acknowledgement. In other words we need to let more than one frame be outstanding to keep the channel busy while the sender is waiting for one frame be outstanding to keep the channel busy while the sender is waiting for acknowledgement. In this section we discuss one protocol that can achieve this goal; in this next section, we discuss one protocol that can achieve this goal; in the next section. We discuss a second.

The first is called go back n automatic repeat request. In this protocol we can send several frames before receiving acknowledgements; we keep a copy of threes frames until the acknowledgements arrive.

Sequence numbers:

Frames from a sending station are numbered sequentially. However, because we need to include the sequence number of each frame in the header, we need to set a limit. If to include the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to 2^m-1. For example if m is 4 the only sequence numbers are o through 15 inclusive. However we can repeat the sequence. So the sequence numbers are 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15, 0,1,2,3,4,5,6,7,8,9,10,11,....

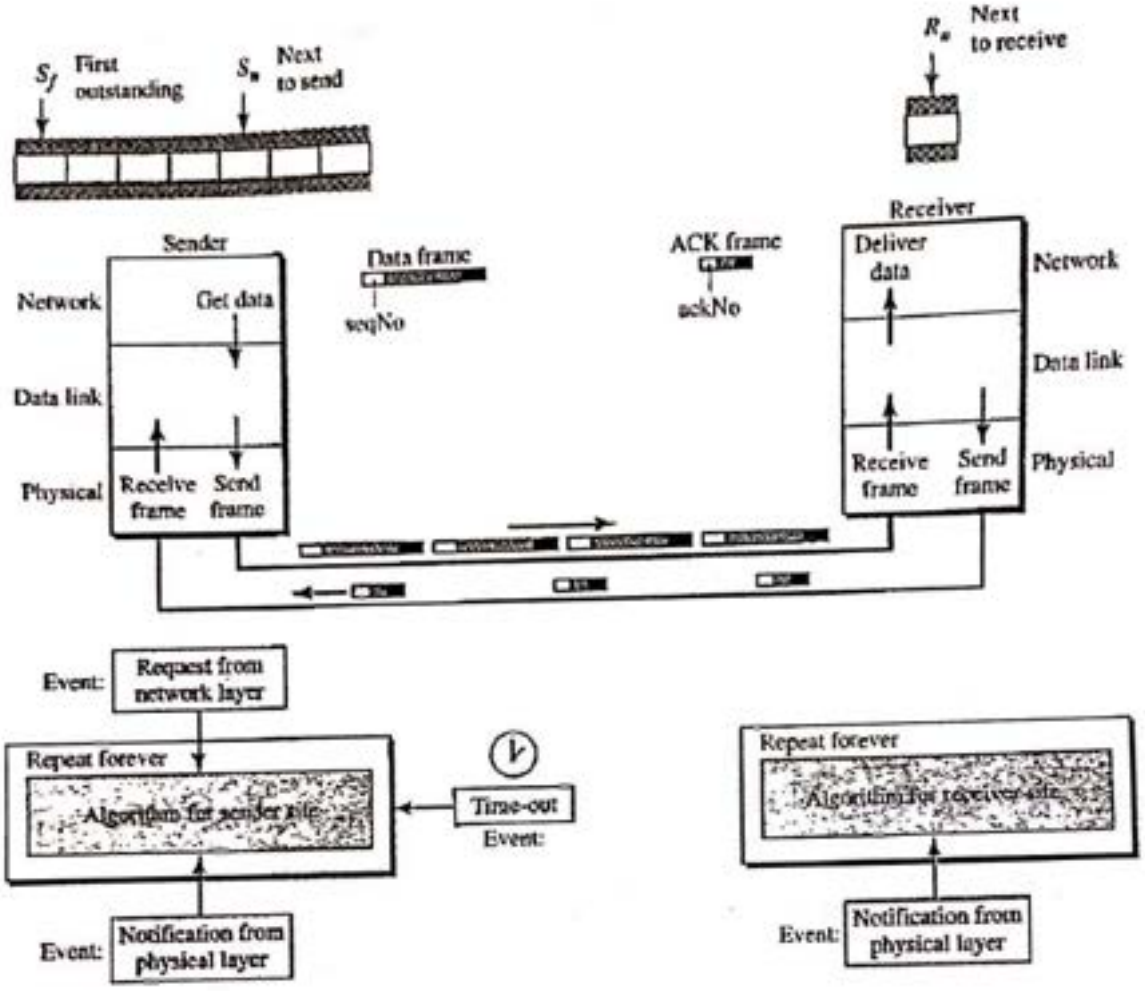
In other words the sequence numbers are modulo 2^m

Slide window:

In this protocol the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words the sender and receiver need to deal with only part of the possible sequence numbers. The range which is the concern of sender is called the send sliding window; the reange that is the concern of the receiver is called the receive sliding window. The maximum window size is 2^m-1.

Timers:

Although there can be a timer for each frame that is sent inour protocol we use only one. The reason is that the timer for the first outstanding frame always expires first; we send all outstanding frames when this timer expires.



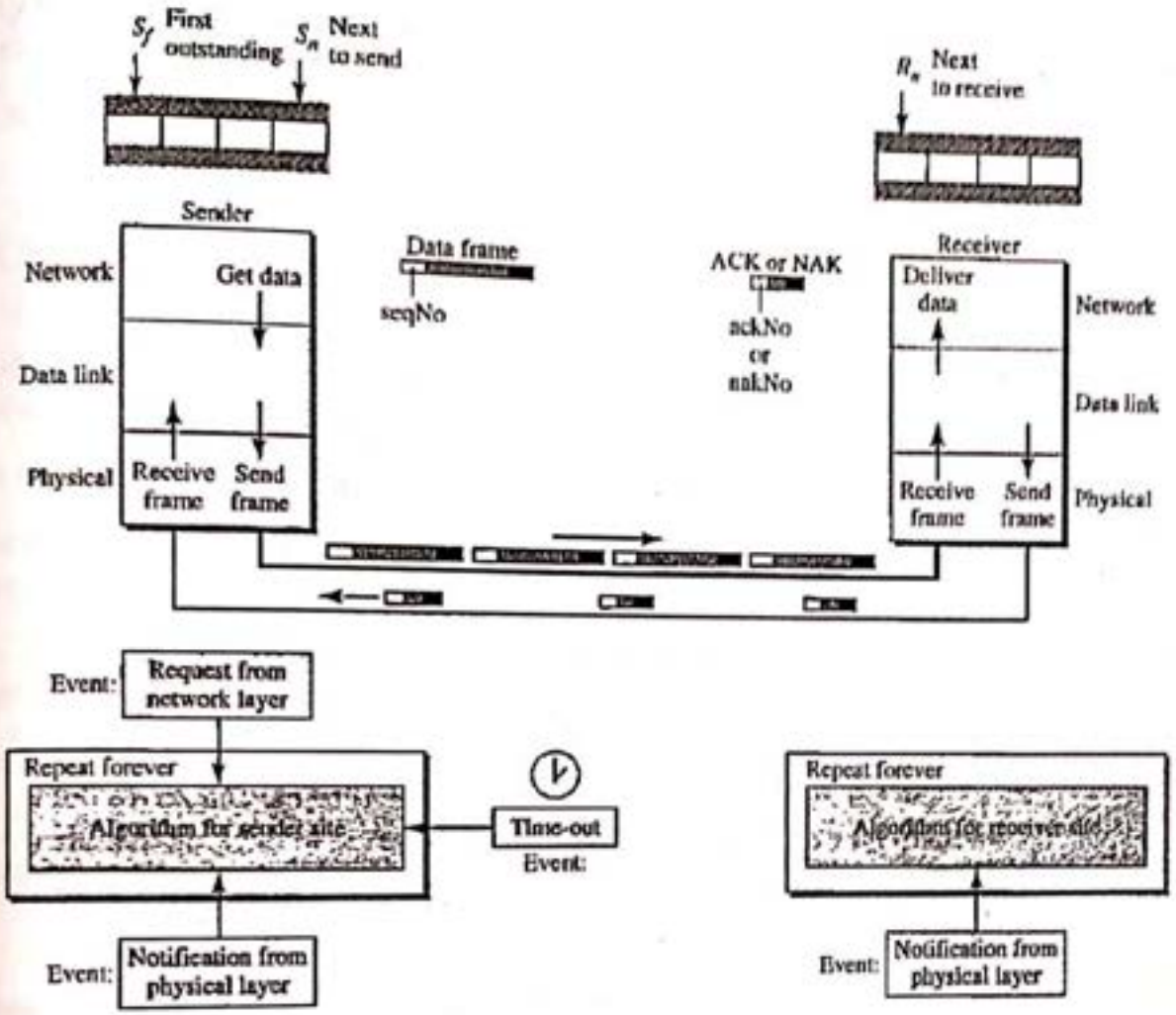
From the above fig as we can see, multiple frames can be in transit in the forward direction, and multiple acknowledgments in the reverse direction. The idea is similar to stop and wait ARQ; the difference is that the send window allows us to have as many frames in transistion as there are slots in the send window.

Selective repeat automatic repeat request

Go back n ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out of order frames; they are simpley discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called **selective repeat ARQ**. It is more efficient for noisy links, but the processing at the receiver is more complex.

Windows:

The selective repeat protocol also uses two windows: a send window and a receive window. However, there are difference between the windows in this protocol and the ones in go back n first, the size of the send window is much smaller ; it is 2 ^m-1 .

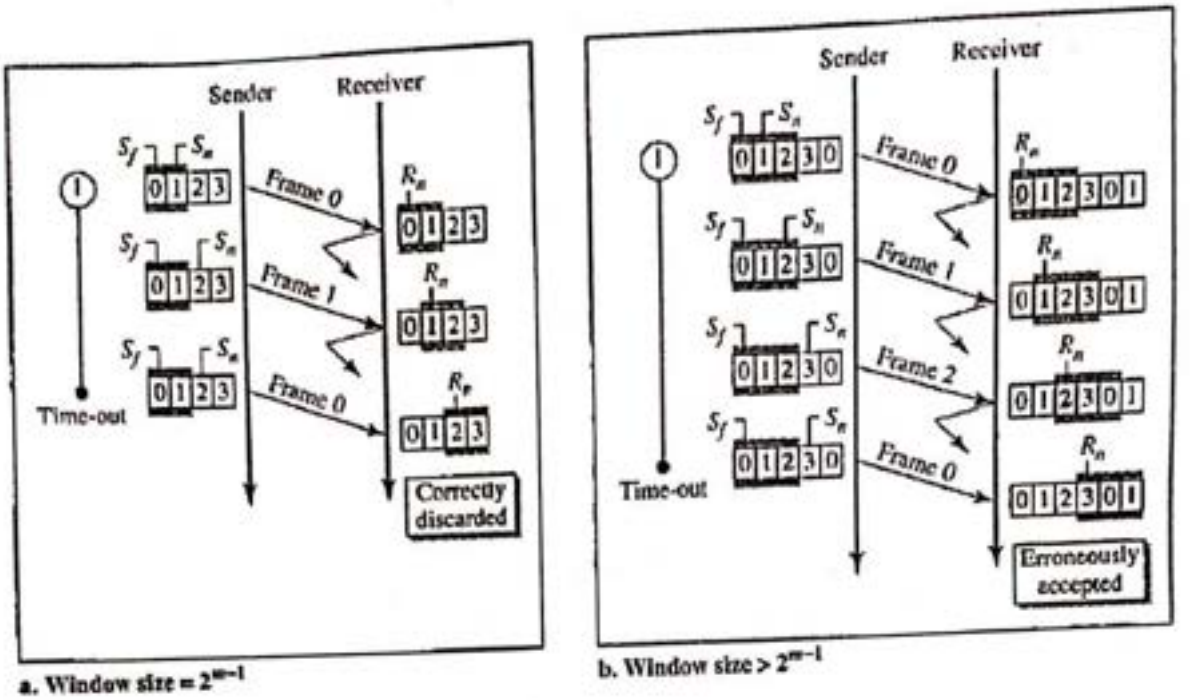


The design in this case is to some extent similar to the one we descrived for the go back n but more complicated as shown in fig

Window size:

Now we can show why the size of the sender and receiver windows must be at most one half of 2 ^m. for an example we choose m=2 which means the size of the window is 2^m/2,or 2. Fig compares a window size of 2 with a window size of 3.

If the size of the window is 2 and all acknowledgments are lost, the timer for frame 0 expires and frame 0 is 2 and all acknowledgments are lost the timer for frame 0 expires and frame 0 is resent. However, the window of the receiver is now expecting frame 2 not frame 0, so this duplicate frame is correctly discarded. When the size of the window is 3 and all acknowledgments are lost the sender sends a duplicate of frame0.



a. Window size = 2^{m-1} b. Window size > 2^{m-1}

However this time this window of the receiver expects to receive frame 0 so it accepts frame0, not as a duplicate but as the first frame in the next cycle. This is clearly an error.

3. Network layer protocols:

There are five network layer protocols:

- ARP
- IP
- ICMP
- IPv6
- ICM

The main protocol in this layer is IP, which is responsible for host-to-host delivery of datagrams from a source to a destination.

1.ARP:

The internet is made of a combination of physical networks connected by devices such as routers. A packet starting from a source host may pass through several different physical networks before finally reaching the destination host.

The host and routers are recognized at the network level by their IP addresses. An IP address is an internetwork address. An IP address is universally unique. Every protocol that deals with interconnecting networks requires IP address.

All the physical network, the hosts and routers are recognized by their MAC addresses. A MAC address is a local address

The MAC address and the IP address are two different identifiers we need both of them because a physical network, such as Ethernet, can have two different protocols at the network layer,

such as IP and IPX. This means that delivery of a packet to a host or a router requires two levels of addressing: IP and MAC. We need to be able to map an IP address to its corresponding MAC address.

Mapping:

we can have two types of address mapping: static and dynamic.

1.Static mapping:

this means creating a table that associates an IP address with a MAC address. This table is stored in each machine on the network. This has some limitations because MAC addresses may change in the following ways.

A machine could change its network card, resulting in a new MAC address.

In some LANs, such as LocalTalk (Apple), the MAC address changes every time the computer is turned on.

A mobile computer can move from one physical network to another, resulting in a change in its MAC address.

2.dynamic mapping:

in dynamic mapping each time a machine knows one of the two addresses, it can use a protocol to find the other one.

Two protocols have been designed to perform dynamic mapping:

Address Resoulution protocol (ARP) and Reverse Address Resolution Protocol(RARP).

ARP associates an IP address with its MAC address. On a typical physical network, such as LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC(Network interface card).

Anytime a host, or a router, needs to find the MAC address of another host or router on its network, it sends an ARP query packet. The packet includes the physical and IP address of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network.

In the below figure ARP request.the system on the left has a packet that needs be dlivered to another system in the right side with IP address 192.168.0.101. system in the left side needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP to send a broadcast request packet to ask for thee physical address of a system ith an IP address of 192.168.0.101

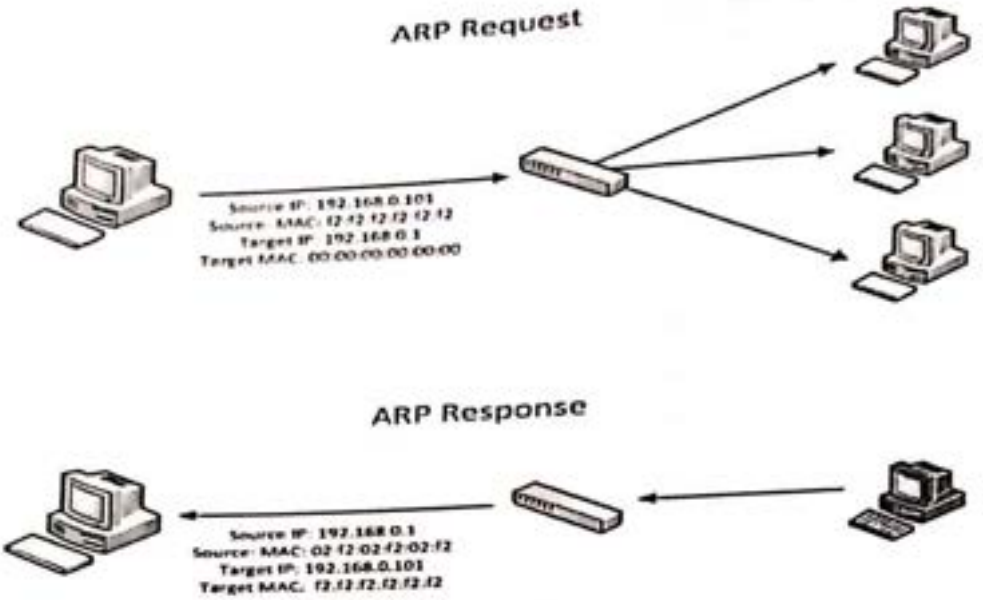


Fig: ARP operation

This packet is received by every system on the physical network, but only the right side system in ARP response will answer it. It sends an ARP reply packet that includes its physical address. Now the left side system can send all the packets it has for this destination, using the physical address it received.

Packet format:

the below fig shows the format of an ARP packet.

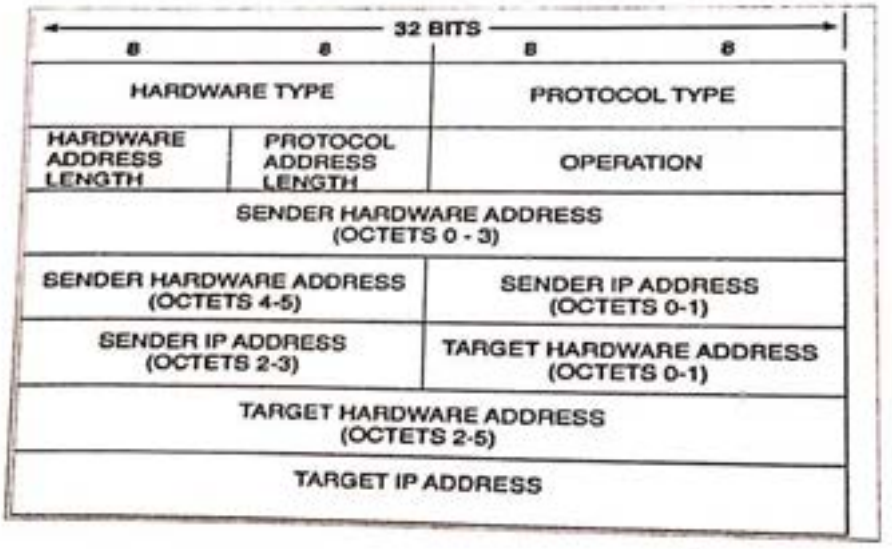


Fig: ARP packet

The fields are as follows:

HTYPE (hardware type). This is a 16-bit field defining the type of betwork on which ARP is running. Each LAN has been assigned an integer based on its type.

PTYPE (protocol type). This is a 16-bit field defining the protocol using ARP.

HLEN (hardware length). This is an 8-bit field defining the length of the physical address in bytes.

PLEN (protocol length). This is an 8-bit field defining the length of the IP address in bytes.

OPER (operation). This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request(1) and ARP reply(2).

SHA (sender protocol address). This is a variable-length field defining the logical address of the sender. For the IP protocol, this field is 4 bytes long.

THA (target hardware address). This is a variable-length field defining the physical address of the target.

TPA (target protocol address). this is a variable-legth field defining the logical address of the target.

Encapsulation:

an ARP packet is encapsulated directly into a data link frame. For example, the below fig shows an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame are an ARP packet.

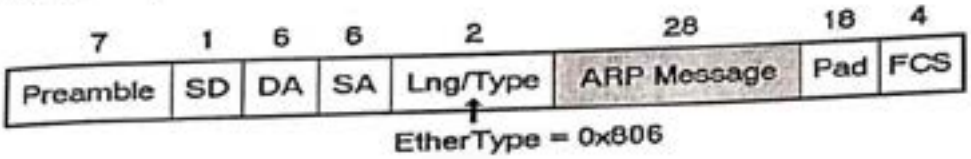


Fig: encapsulation of ARP packet

Operation:

Let us see how ARP functions on the Internet. First we describe the steps involved. Then we discuss the four cases in which a host or router needs to use ARP.

Steps involved:

The sender knows the IP address of the target. We will see the how the sender obtains this shortly.

IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. the target physical address field is filled with 0s.

The message is passed to the data link layer where it is encapsulated in a frame, using the physical address of the sender as the source address and the physical broadcast address as the destination address.

Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP.

The target machine replies with an ARP reply messages that contains its physical address. the message is unicast.

The sender receives the reply messages. It now knows the physical address of the target machine.

The IP diagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

four different cases:

the following are four different cases in which the services of ARP can be used in below fig.

The sender is a host and wants to send a packet to another host on the same network. In this case, the IP address that must be mapped to a physical address is the destination IP address in the datagram header.

The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination.

The sender is a router that has received a datagram destined for a host on another network.

The sender is a router that has received adatagram destined for a host in the same network. The destination IP address of the datagram becomes the IP address that must be mapped to a physical address.

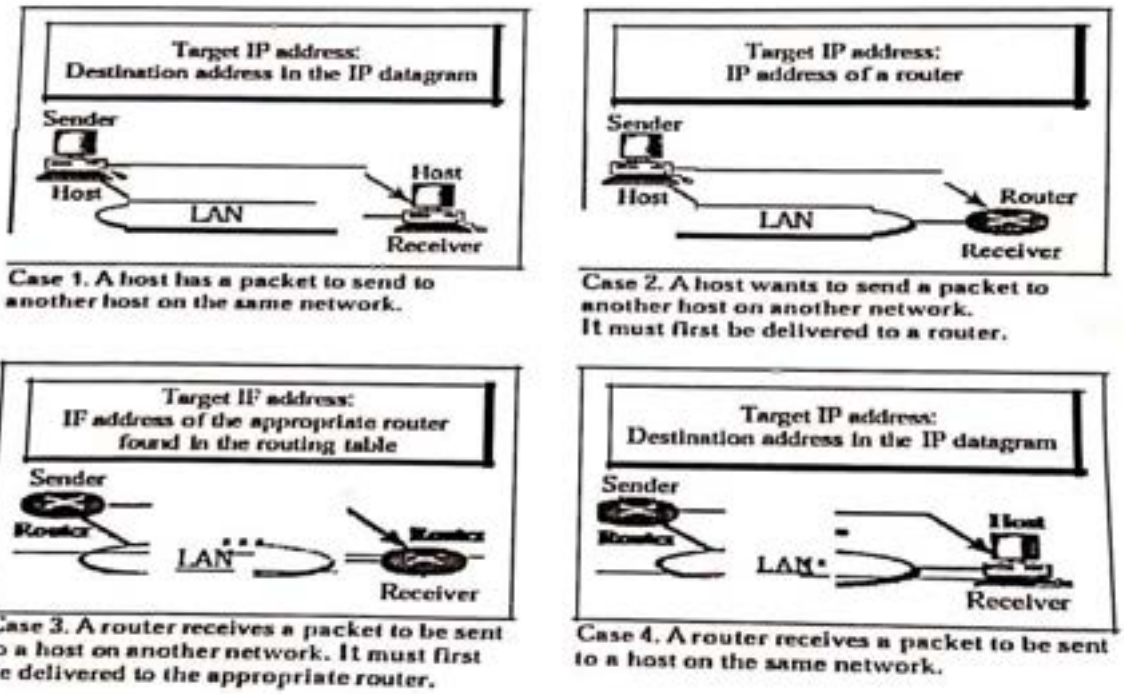


fig: four different cases using ARP

2.IP:

the internet protocol is the host-to-host network layer delivery protocol for the internet. IP is an unreliable and connectionless datagram protocol. IP uses only an error detection mechanism and discards the packet if it is corrupted. IP does its best to deliver a packet to its destination.

IP is also a connectionless protocol for a packet-switching network which uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination.

3.ICMP:

The Internet Control Message Protocol (ICMP) has been designed to compensate for the two deficiencies lack of error control and lack of assistance mechanisms.

ICMP itself is a network layer protocol. The messages are first encapsulated IP datagrams before going to the lower layer.

The value of the protocol field in the IP diagram is 1 to indicate that the IP data are an ICMP message.

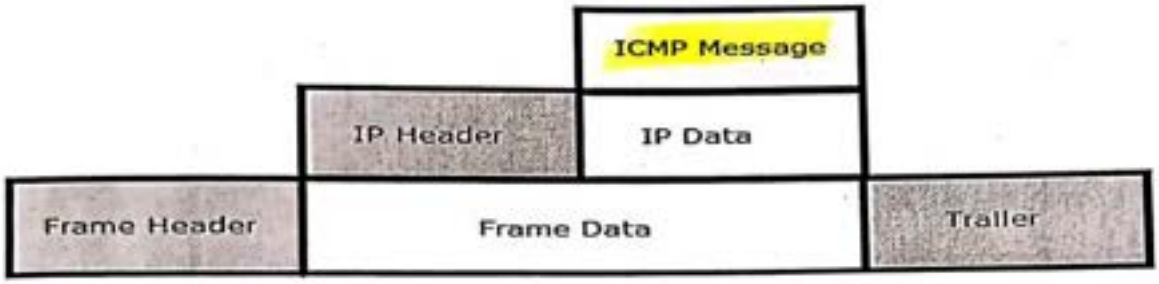


Fig: ICMP encapsulation

Types of messages:

ICMP messages are divided into two broad categories: error-reporting messages and query message.

Error reporting:

One of the main responsibilities of ICMP is to report errors. Error checking and error control are not a concern of IP. ICMP was designed, in part, to compensate for this shortcoming. Error reporting messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses, ICMP uses the source IP address to send the error message to the source of the datagram.

Five types of errors are handled: destination unreachable, source quench, time exceeded, parameter problems and redirection as shown in the below fig

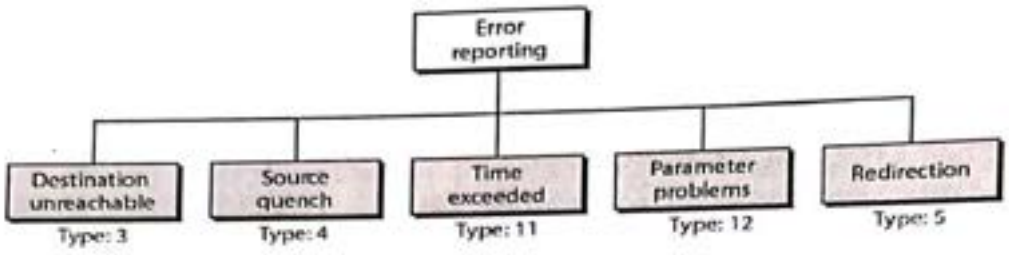


Fig: Error-reporting messages

Destination unreachable when a router cannot route a datagram or a host cannot deliver a datagram is discarded and the router or the host sends a destination unreachable message back to the source host that initiated the datagram.

Source quench: IP is a connectionless protocol. There is no communication between the source host, which produces the datagram; the routers, which forward it; and the destination host, which process it.

The exceeded the time-exceeded message is generated in two cases. First, the router that receives adatagram with a value of 0 in the TTL field discards the datagram.

Parameter problem if a router or the destination host discovers an ambiguous or missing value in any field of the datagram. It discards the datagram and sends a parameter-problem message back to the source.

Redirection when a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router.

Query:

In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages.

Echo request and reply the echo-request and echo-reply messages are designed for diagnostic purpose.

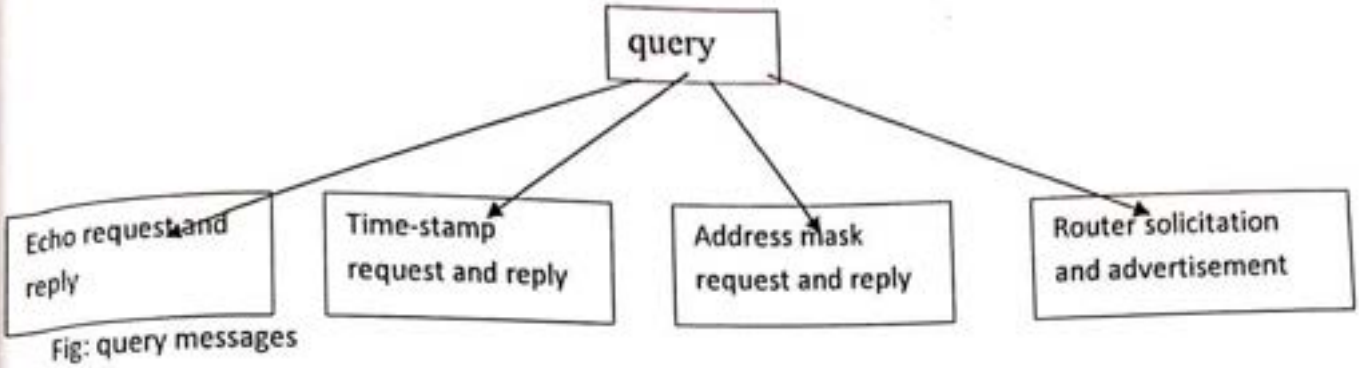


Fig: query messages

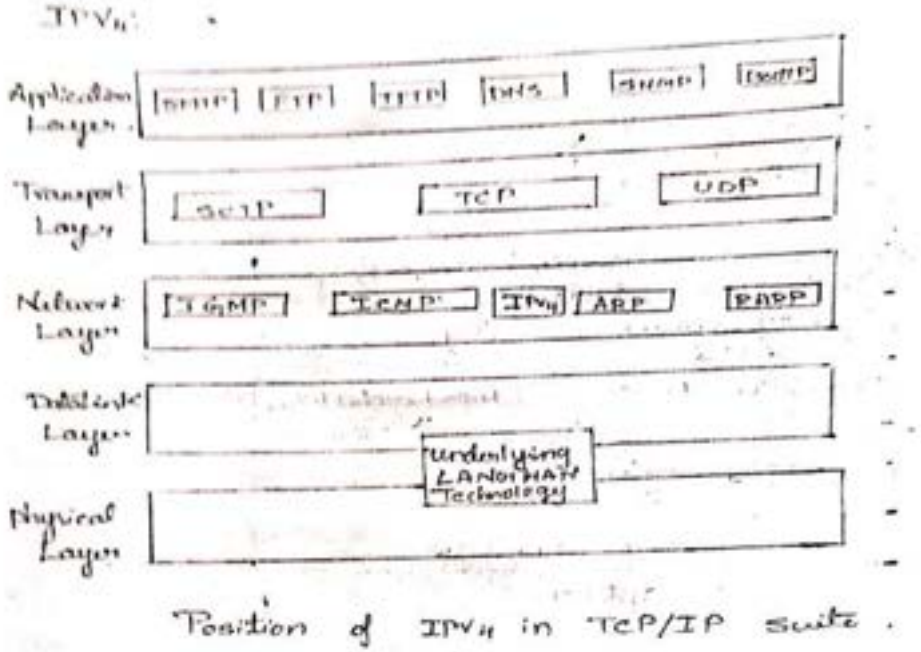
Time-stamp request and reply: two machines can use the time-stamp-request and time-stamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them.

Address mask request and reply: the IP address of a host contains a network address subnet address, and host identifier. A host may know its full IP address, but it may not know which part of the address defines the network and subnetwork address and which part corresponds to the host identifier. In this case, the host can send an address mask reply message.

Router solicitation and advertisement: as we discussed in the redirection-message section, a host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning, the router-solicitation and router-advertisement messages can help in this situation

4.Network layer protocols:

IPv4:



Position of IPv4 in TCP/IP suite.

The internet protocol version four is a delivery mechanism used by the TCP/IP protocol. IPv4 is an un reliable & connectionless datagram protocol and is best effort delivery service. Which means it provides no error control or flow control.

When we anticipate (expecting) reliability from IPv4 it must be paired with a reliable protocol such as TCP.

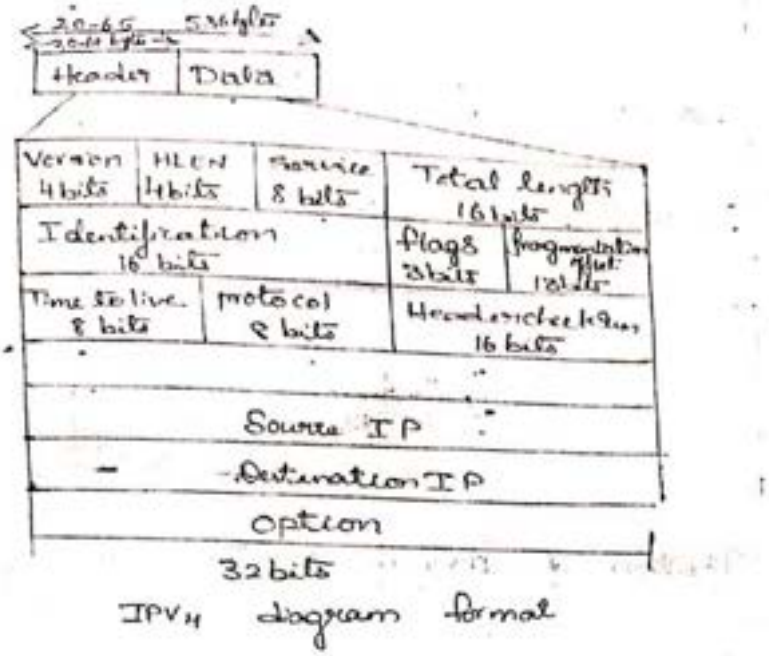
IPv4 acts as connectionless protocol for a packet switching network that uses the datagram approach. In this approach data grams are handling independently and each datagram can flow a different route to the destination. This implies that data grams sent by the same source to the same destination could arrive out of order.

IPv4 relies on a higher level protocol to take care of all their problems.

Datagram:

Packets in the IPv4 are called datagram. A datagram is a variable length consisting of 2 parts,

1.Header
2.Data



IPV4 diagram format

The header is 20-60 bytes in length and contains essential information which helps in routing and delivery systems.

Version of 4 bits:

This 4 bit field defines the version of IPv4 protocol. If the machine is using version6 may replace version4.

Header length:

This 4 bit field defines the total length of the datagram header. This field is needed because the length of the header is variable.

Services:

IETF (Internet Engineering Task Force) has changed the interpretation and name of this 8 bit field. This field previously called "service type" in no differentiated services.

Service type:

In this interpretation the first 3 bit called precedence bits. The next 4 bits called "Type Of Service (TOS)" bits and the last bits are not used.

Precedence:

Precedence is 3 bit service ranging from 0 to 7 (000-111) this precedence defines the priority of the datagram; a datagram which is urgent and import in a network management than another datagram.

TOS bits:

TOS bits is 4 bits sub field with each bit having a special meaning like

0000: normal.

0001: minimize cost.

0010: maximize reliability.

Differentiated services:

When the 3 right most bits are zeros, the 3 left most bits are interpreted the same as the precedence bits if the server type interpretation.

It is compactable with the old interpretation.

Total length:

This is a 16 bit field that defines the total length of the IPv4 datagram in bytes.

Length of data= total length- header length.

Identification:

This field is used in fragmentation. To make IPv4 protocol independent of the physical network. The designers decided to make maximum length of the IPv4 datagram equal to 65535 bytes. This transmission more efficient. We must divide the datagram to make it possible to pass through these networks and is called "Fragmentation".

Flags:

This is a 3 bit field. The first bit is reserved, second bit is called "do not fragment bit". Its value is one; the machine must not fragment the datagram. If the value is zero the datagram is fragmented if necessary.

The third bit is called the more fragment bit its value is one, it means the datagram is not the last fragment.

Fragmentation offset:

This is 13 bit field shows the relation position of this fragment with respect to whole datagram.

Time to live:

A datagram has a limited life time in its travel through a network this field was originally designed to hold a time stamp, the datagram was discarded when the value become zero.

Protocol:

This 8 bit field defines the higher level protocol that uses the service of the IPv4 layer.

Check sum:

The check sum concept is an idea in IPv4 implementation: first the value of the check sum field is set to zero then the entire header is divided into 16 bit section and added to gather. The result is completed and inserted into the check sum field.

Source address:

This 32 bit field defines the IPv4 address of the source. This field must remain unchanged during the time of IPv4 datagram travels from the source to destination.

Destination address:

This 32 bit field defines the IPv4 address of the destination. This field also must remain unchanged during the time of the IPv4 datagram travel to source code to destination code.

IPv6:

The network layer protocol in the TCP IP protocol suit is currently IPv4 provides the host to host communication between systems in the internet

The following of the sum of deficiencies that makes it unsuitable for the fast going of internet.

1. Calculating subnets, classes addressing, NAT address depletion is still a long term problem in the internet.

2. The internet must accommodate real time audio and video transmission this type of transmission requires minimum delays strategies, and reservation of resources which is not provided in IPV4.

3. The internet must accommodate encryption and authentication of data for some applications No encryption or authentication is provided by IPV4

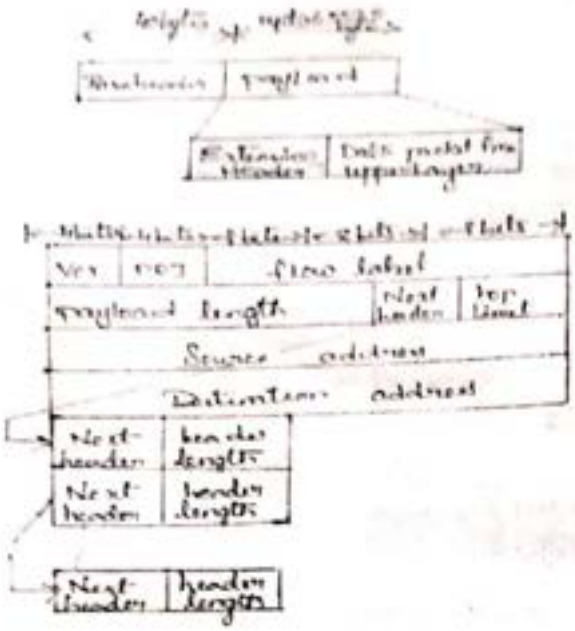
To overcome these efficiencies, IPV6 is also known as IPNG (internet protocol next generation) was proposed.

PACKET FORMAT

The packet of IPv6 consists of two parts.

header

1.Base
2.Payload.



Version:

This 4 bit field defines the version number of IP for IPV6 the values is 6.

Priority:

The 4 bit priority field defines the priority of the packet with respect to traffic conjunction.

Flow Label:

The flow label is 8bytes field that is designed to provide special handling for particular flow of data.

Payload Length

This 2 byte payload length defines the length of IP data gram, excluding the base header.

Next header:

The next header is the 8 bit field defining the header that flows the base header in the data gram: It is an optional extension headers used by IP or it is an encapsulation packet such as UDP (User datagram protocol)or TCP

HOP limit:

A datagram has a limited life time in its travel through a network this field was originally designed to hold a timestamp, the datagram was discarded when the values becomes zero.

Source Address:

The source address field is a 16 bit internet address that defines the original source of the datagram.

Destination Address:

The destination Address field is a 16 bit internet address that usually defines the final destination of the datagram if source routing is used this field contain the address of the next router.

Advantages:

The next generation IP has the following advantages over IPv4

1.Larger address space:

An IPv6 address is 128 bit long: where the IPv4 is 32 bit only, this is a huge that is 2^{96} increasing the address space

2.Better header format :

IPv6 uses a new header format in which options are separated from the base header and inserted, when needed between the base header and upper layer header. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

3.Allowance for extension:

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications

4.Support for resource allocation:

In IPv6 the type of service (TOS) has been removed, mechanism called flow label has been added. To enable to the source to request special handling of the packets.

5.Support for more security:

The encryption and authentication of the IPv6 provide confidentiality and integrity of the packet.

Comparison between IPv4 & IPv6:

The header length field is eliminated in IPv6 because the length of the header is fixed in this version.

The service type field is eliminated in IPv6, the priority and flow label fields to gather take over the function of the service type field.

The total length field is eliminated IPv6 and replace by the payload length.

The time to live field is called HOP limit in IPv6.

The protocol field is replacing by the next header field.

The fragmentation field in the base header section of IPv4 has moved to the fragmentation extension header in IPv6.

The authentication extension header is new in IPv6. The source route option is called the source route extension header in IPv6.

The encrypted security payload extension header is new in IPv6.

5.Explain Uni costing and Multi costing routing protocols?

Routing protocols have been created in response to demand for dynamic routing tables. A routing protocol is a combination of procedures that tell routers in Internet inform one another of changes. There are two types of routing techniques based on how the packet is delivered are:

Uni costing protocols and

Multi costing protocols

Uni costing protocols:-

In this the communication is "One Source to One Destination". The relationship between Source and Destination is One-One. In this both Source and Destination address in IP datagram are uni cost addresses assigned to host.

Optimization:-

This is mainly used that a router receives a packet from a network and usually a router attached to several network. When it takes a packet, to which network should it pass the packet? This decision is based on optimization. Which path is available?

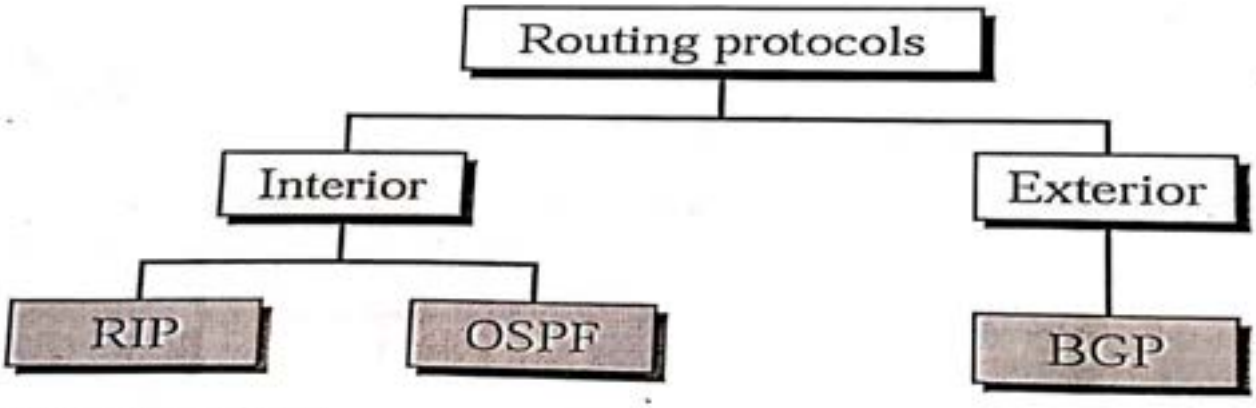
One way to approach is to assign a cost for passing through a network we call this cost a "Metric". Metric is used to assigned each network depends on type of protocol. Some simple protocols which are used by Uni cost routing as: Routing Information Protocol (RIP), Open Shortest Path First(OSPF), Border Gateway Protocol (BGP).

RIP: Treat all network are equals. The cost of passing through a network is same. It is one hop count.

OSPF: It allow administrator to assign a cost afar passing through a network based on type of service required.

BGP: The criterion is policy, which can be set by administrator. The policy defines what paths should be chosen.

Representation of Uni cost popular protocols:-



Intra domain protocols:-

Routing inside an autonomous system is referred as interior/intra domain routing. There are basically two different type of protocol and Link State Protocol.

Distance Vector Protocol:

This is a least-cost routs between two nodes is route with minimum distance. This protocol describes. It routes each router periodically shares its knowledge about entire internet. There are three which is used to understand this protocol as:

a) Sharing Knowledge: tells about entire autonomous system.

b) Sharing Only with Neighbors: Each router sends to its neighbors.

c) Sharing at Regular Intervals: It sends to neighbors at fixed time.

Routing Information Protocol (RIP):-

RIP is an Intra domain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing.

Considerations of RIP:-

1) In an autonomous system, we are dealing with routers and network. The routers have routing tables but network do not.

2) The destination in a routing table is a network, which means the first column defines a new address.

3) RIP uses metric is very simple to each no.of destinations that's why metric is called "hop count".

4) RIP having 15 hops, more than it is treated as infinity.

5) The "next" node column defines address of router to which packet is to be sent to reach its destination.

Initializing Routing Table:-

When a router is added to a network, it initializes a routing table for itself, using its configuration file. The table contains only directly attached networks and hop counts, which are initialized to one.

Link State Vector Routing:-

In this routing, if each node in domains has entire topology of domain, the list of nodes, links. It describes how they are connected including type and condition of links that node is Dijkstra's algorithm to build a routing table. The following diagram shows a simple link state domain with five nodes o routing.

It is clear that form diagram, it follows same topology for each node. i.e., all are dynamic. If any chang in topology must be updated for each node.

Building a Link State Routing:-

It requires four sets of actions to ensure that each node has routing table showing least- c node to every other node.

Creation of links by each node called Link State Packet (LSP).

Dissemination of LSPs to every other router called "flooding" in an efficient and reliable way.

Formation of a shortest path tree for each node.

Calculation of a routing table based on shortest path tree.

Open Shortest Path First (OSPF):-

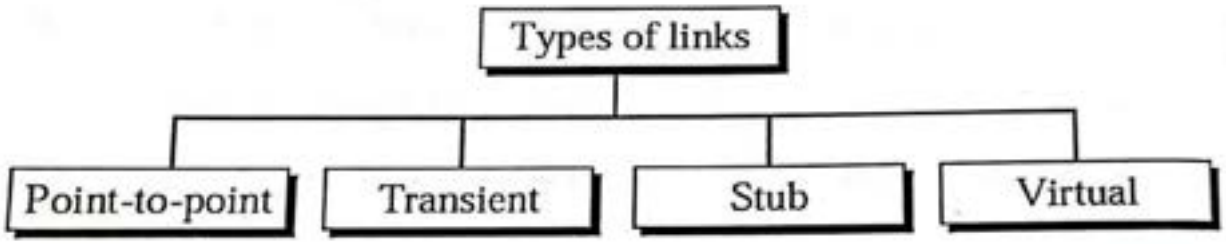
It is an intra domain routing protocol based on link state routing. It is also an autonomous system.

"Areas" to handle routing efficiently and in a timely manner, OSPF divides an autonomous system into areas. Area is an autonomous system. All network inside an area must be connected. At the border of an area, special router called "Area border routers", summarize. The information about area and sent it to other areas. Among areas inside an autonomous system is a special area called "back bone". The router inside back bone are called "back bone routers".

Virtual link between routers must be created by an administrator to allow continuity of the back bone as primary area. "Metric" the OSPF protocol allows the administrator to assign a cost, called metric to each route. The metric can be based on a type of service. A router can have multiple routing tables, each based on a different type of service.

Types of Links:-

In OSPF terminology, a connection is called a link. There are four types of links have bean defined.



Inter domain protocols:- An autonomous system is a group of networks and routers under authority of a single administrator routing between autonomous system is referred as inter domain/exterior domain. In this only exterior routing protocol is usually chosen to handle routing between autonomous systems. This can be supported by border gateway protocol.

Path Vector Routing:-

This routing is different from other network routing. Each in routing table contains destination network next router and path to reach destination, path usually defined list of autonomous system that a packet should travel through to reach destination.

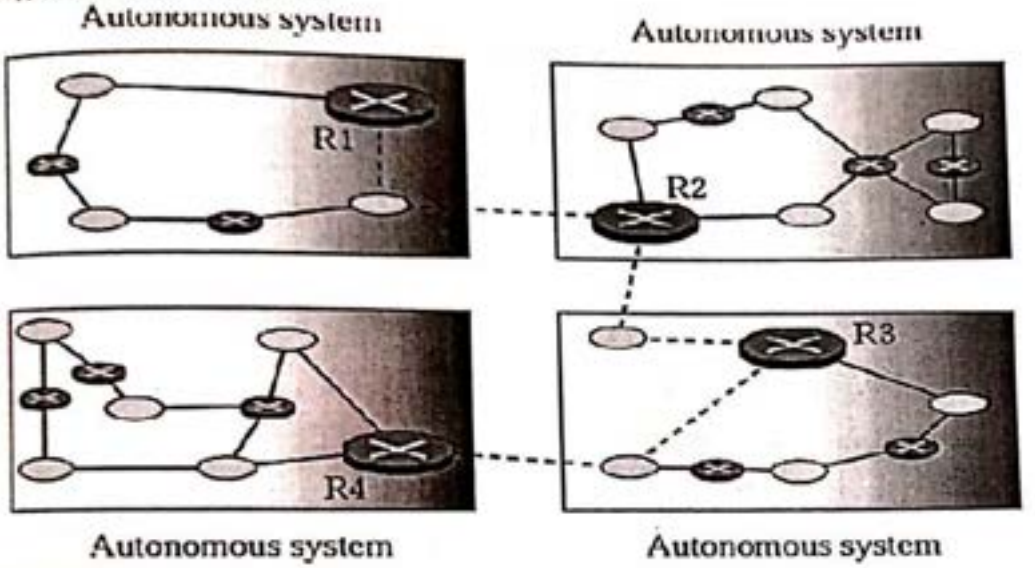
Initialization:-

In path vector routing we assume that there is one node in each autonomous system that acts on behalf of entire autonomous system. This is call as "Speaker node". In this the speaker node can know only reachable of nodes inside its autonomous system. "Shorting" is in path vector routing, a speaker in an autonomous system share its table with immediate neighbors.

"Updating", when a speaker node receives a two column table from a neighbor, it updates its own table by adding nodes that are not in its routing table and adding its own autonomous system and autonomous system that sent table.

BGP (Border Gateway Protocol):-BGP is an inter domain routing protocol using path vector routing. Exchange of routing information between two routers using BGP takes place in a session. A session is a connection that established between two BGP routers only for exchanging routing information.

Typesofautonomoussystem:-



Internet is divided into hierarchical domains called autonomous systems. We can divide autonomous system into three categories namely:

Stub AS: It has only one connection to another AS. The inter domain data traffic in a stub AS can be either created or terminated in AS. Used in small corporations.

Multi homed AS: It has more than one connection to other AS but it is only one source. It is used in multi homed AS.

Transit AS: It is multi homed AS that also allow transient traffic. Used in National and international ISPs.

BGP session:-

The exchange information through routing information between two routers. A session is a connection that is established between two BGP routers only for sake of exchanging routing information. For this BGP divided into two sessions namely:

External BGP and

Internal BGP

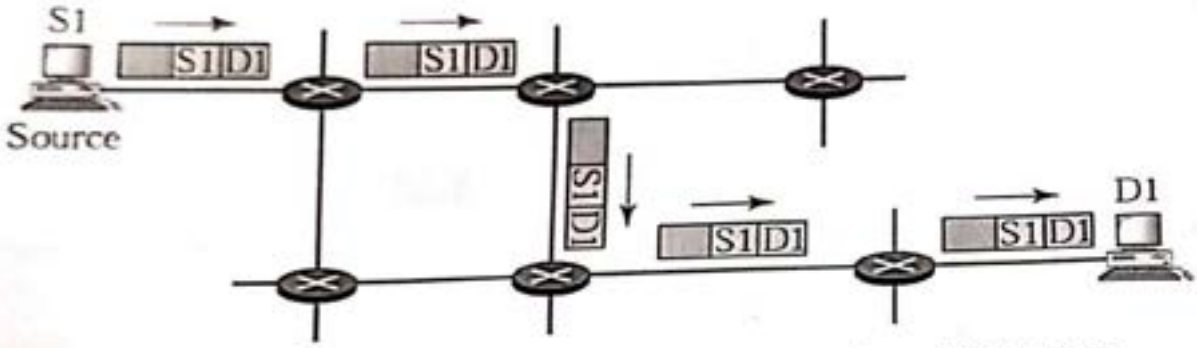
These are representing E-BGP and I-BGP. E-BGP is used to exchange information between two speaker nodes belonging to two different AS. I-BGP is used to exchange routing information between two routers inside an AS.

Multi cost protocols:

A message can be Uni cast, multi cost/broad cost.

Uni costing:-

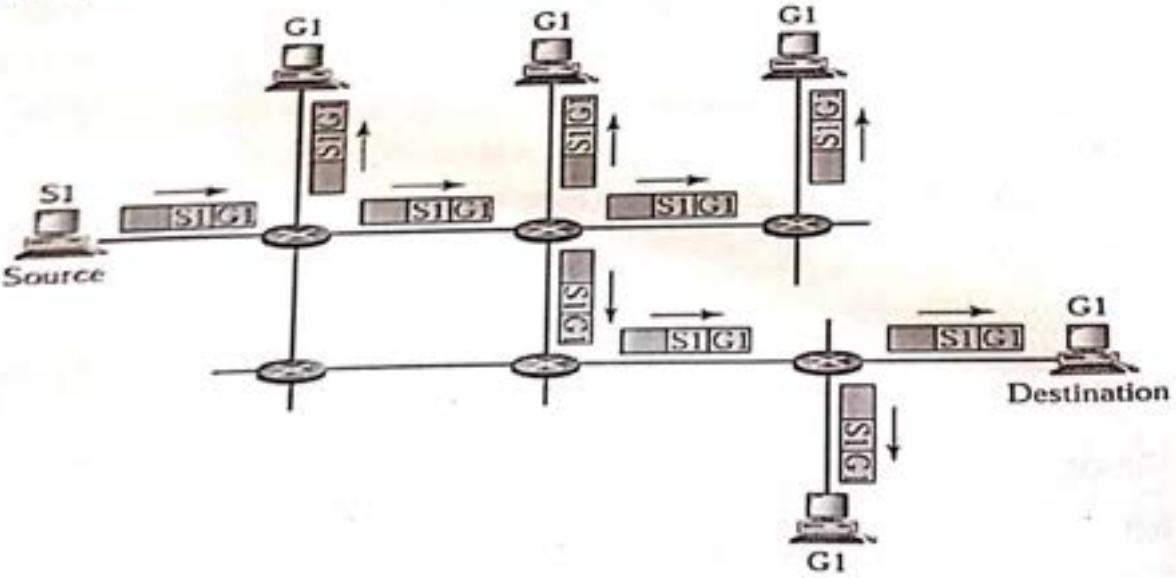
In this communication, there is one source and one destination the relationship between source and destination addresses, in IP data gram, are the uni cast addresses assigned to hosts. The following diagram shows uni costing:



In uni costing, the router forwards the received packet through only one of its interfaces.

Multi costing:-

In this communication, there is one source and group of destinations the relationship is one-to on-many. In this type of communication source address is a uni cost address, but destination address is a group address identifies the members of group. The following diagram shows idea of multi costing.



In multi costing, router may forward received packet through several of its interfaces.

Broad costing:-

In this communication, the relationship between source and destination is one to all. i.e., one source, all destinations. Internet does not explicitly support broad costing because huge amount of traffic.

Applications of Multi costing protocol:-

Multi costing has may applications today such as access to distributed that is information is stored in more than one location, usually time of production. The user needs to access database does not know location of information.

Information Dissemination:-

Business often needs to send information to their customers. If nature of information is same for each customer, it can be multi cost. In this way business can send one message that can reach many customers.

Dissemination of news:-

One single message can be sent to those interested in particular topic.

Teleconferencing:-

It involves multi costing. The individuals attending a teleconferencing all need to receive same information at same time.

Distance Learning:-

One growing area in use of multi costing is distance learning.

6. Explain UDP and TCP of Transport layer

User Datagram Protocol (UDP):

The simple unreliable transport layer protocol in the internet layer is called the user Datagram protocol.

- UDP is a connectionless, unreliable transport protocol that has no flow and error control
- It uses port numbers to multiplex data from the application layer.
- The services of IP except for providing process to process communication. Also, it performs very limited error checking.
- IF UDP is so powerless
- UDP is a very simple control with a minimum of overhead
- Sending a small message using UDP takes much a less interaction between the sender and receiver than using UDP
- UDP is a convenient protocol for multimedia and multicasting applications.

Port Numbers

UDP uses port numbers as the addressing mechanism in the transport layer.

The following table shows the some of the port numbers.

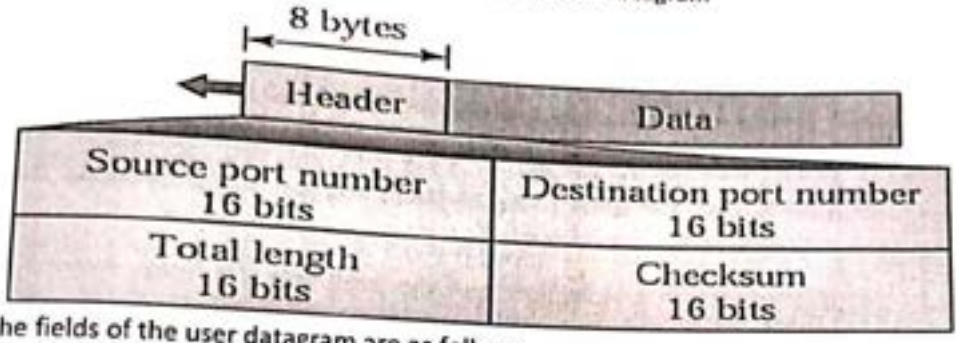
	Protocol	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call

123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

User Datagram

UDP packets, called **User Data grams**, have a fixed size header of 8 bytes

The following diagram shows the format of a user Datagram



The fields of the user datagram are as follows

Source port number:

- The port number used by the process running on the source host.
- It is 16 bits long, which means that the port number can range from zero to 65,535.

Destination port number:

- This is the port number used by the process running on the destination host .
- It is 16 bits long.

Length:

- This defines the total length of the user datagram, header plus data.
- It is 16 bit field .
- This is 16 bit field.
- The 16 bits can define a total length of 0 to 65,535 bytes.

Checksum:

- This is used to detect errors over the entire user datagram.
- The UDP checksum should be based on the UDP header and payload, the designers added a part of the IP header as a part of the checksum calculation
- This ensures that those fields have not been changed from source to the destination.
- The calculation of the checksum and its inclusion in a user datagram are optional.

- If the checksum is not calculated, the field is filled with 0's.

Applications of UDP:

- ❖ UDP is suitable for a process that requires simple request response communication with little concern for flow and error control.
- ❖ It is not usually used for a process that needs to send bulk data, such as FTP.
- ❖ UDP is suitable for a process with internal flow and error control mechanisms.

Eg: *Trivial file Transport Protocol (TFTP)*

- ❖ UDP is suitable transport protocol for multicasting .multicasting capabilities are embedded in the UDP software but not in the TCP software
- ❖ UDP is used for some route updating protocol such as routing information protocol (RIP).
- ❖ UDP is used in conjunction with the Real Time Transport Protocol (RTP) to provide a transport layer mechanism for real time data.

Transmission Control Protocol (TCP)

The reliable, but complex transport layer protocol in the internet is called **Transmission Control Protocol (TCP).**

- TCP is also called a Stream connection oriented and reliable transport protocol.
- It adds connection oriented and reliability features to the services of IP.

Port Numbers:

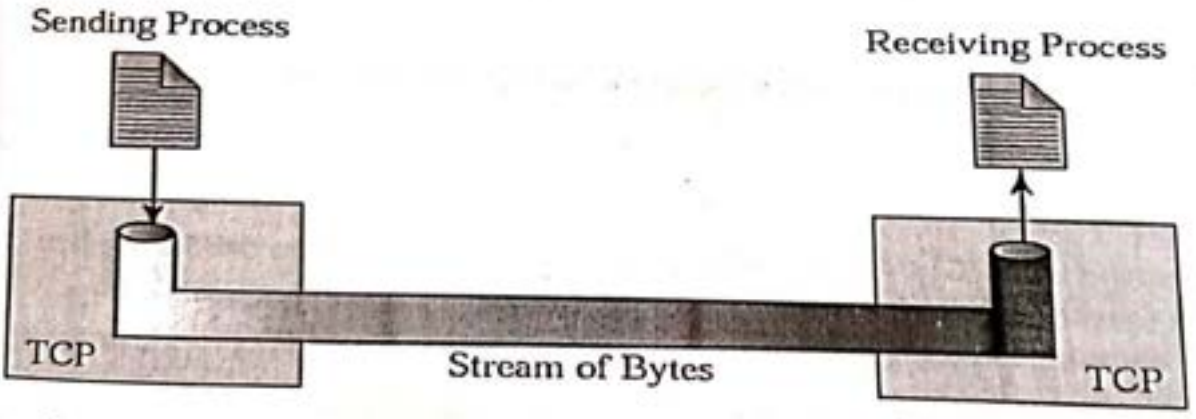
Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)

23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

TCP Services

The following are the TCP services

1. **Stream Delivery Services:**
   A. TCP is Stream oriented protocol.
   B. The TCP allows the process to deliver data as stream of bytes and the receiving process to obtain data as a stream of bytes
   C. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the internet.
   D. The sending process produces the stream of bytes and the receiving process consumes it.



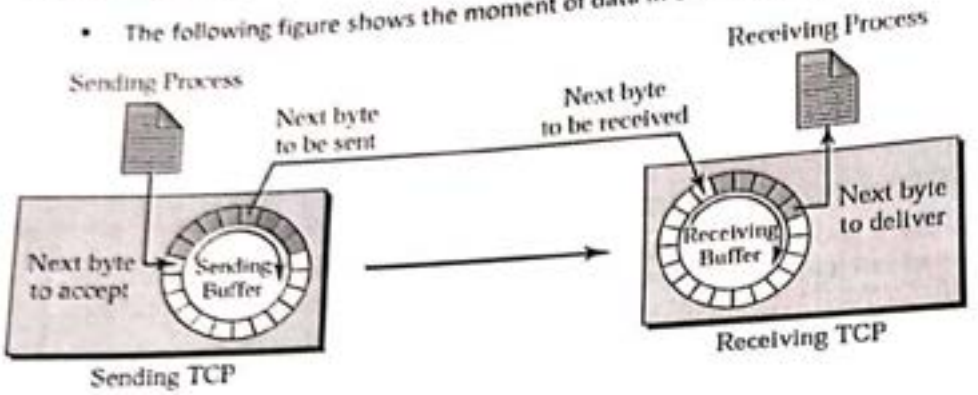
Sending and Receiving buffers

- The sending and receiving processes may not produce and consume data at the same speed

- TCP needs 2 buffers for storage they are

1. Sending buffer
2. Receiving buffer

- The following figure shows the moment of data in one direction

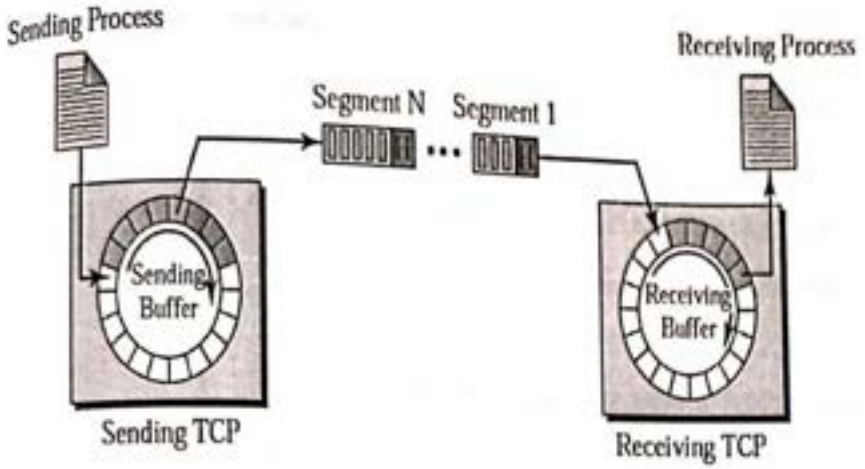


- The sending buffers has three types locations
- The white section contains empty locations that can be filled by the sending process
- The grey area holds bytes that have not been sent not yet acknowledged. TCP keeps bytes in the buffer until receives an acknowledgement.
- The colored areas are bytes are bytes to be sent by the sending TCP
- The operation of the buffer at the receiver site is simpler. the circular buffer is divided into two areas. they are
    a. The white color contains empty locations to be filled by bytes received from the network
    b. The colored sections contain received bytes that can be consumed by the receiving process.

TCP Segment:

At the transport layer, TCP groups a number of bytes together into a packet called a **Segment.** TCP adds a header to each segment and delivers the segment to the IP layer to the transmission. The entire operation is transparent to the receiving process.

The following figure shows how segments are created from the bytes in the buffers.



Full duplex services

TCP offers full duplex service where data can flow in both directions at the same time. Each TCP then has sending and receiving buffers and segments are sending in both directions.

Connection oriented Service:

TCP is a connection oriented protocol. When

Process at site A wants to send and receive data from another process at site B the following occurs

1. A's TCP informs B's TCP and gets approval from B's TCP.
2. A's TCP and B's TCP exchange data in both directions.
3. After both processes have no data left to send and the buffers are empty, the two TCPS destroy their buffers.

Byte Numbers:

TCP receives bytes of data from the process and stores them in the sending buffer, it numbers them.

The numbering doesn't necessarily start from zero. it starts with randomly generated.

Sequence number:

TCP assigns sequence number to each segment that is being sent.

The sequence number for each segment is the number of the first byte carried in that segment.

Eg:

Imagine a TCP connection is transferring a file of 6000 bytes. The first byte is numbered 10010. What are the sequence numbers for each segment if data are sent in five segments with the first four segments carrying 1000 bytes and the last segment carrying 2000 bytes?

The following shows the sequence number for each segment:

Segment 1 ==> sequence number: 10,010 (range: 10,010 to 11,009)

Segment 2 ==> sequence number: 11,010 (range: 11,010 to 12,009)

Segment 3 ==> sequence number: 12,010 (range: 12,010 to 13,009)

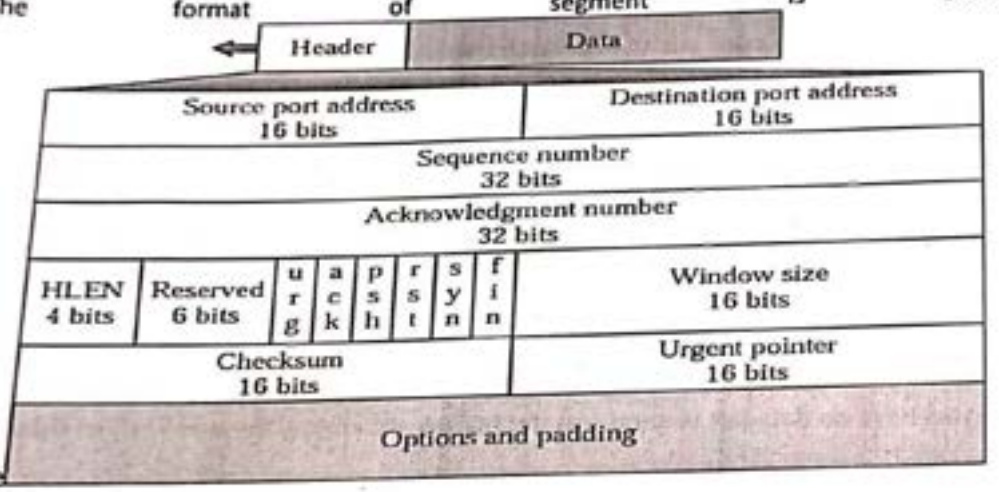
Segment 4 ==> sequence number: 13,010 (range: 13,010 to 14,009)

Segment 5 ==> sequence number: 14,010 (range: 14,010 to 16,009)

Segment:

The unit of data transfer between two devices using TCP is a segment.

The format of segment is shown in figure



Source port Address:

- *It defines the port number of the application program in the host that is sending the segment.*
- *It is 16 bit field*

Destination port Address:

- *It defines the port number of the application program in the host that receiving the segment .*
- *It is 16 bit field.*

Sequence number:

- *It defines the number assigned to the first byte of data contained in the segment.*
- *It is 32 bit field.*

Acknowledgement number:

- It defines the byte number that the sender of the segment is expecting to receive from the other party.
- It is 32 bit field.

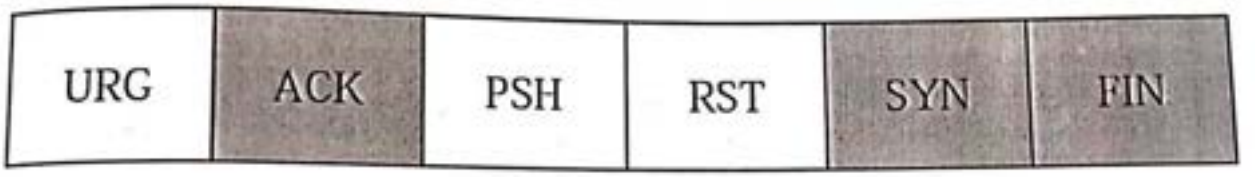
Header Length:

- It indicates the number of 4 byte word in the TCP.
- It is 4 byte field.

Reserved:

- It is 6 bit field reserved for future reference **Control:**
- This fields defines 6 different control bits or flags is as shown bellow

URG: Urgent pointer is valid	RST: Reset the connection
ACK: Acknowledgment is valid	SYN: Synchronize sequence numbers
PSH: Request for push	FIN: Terminate the connection



Connections:

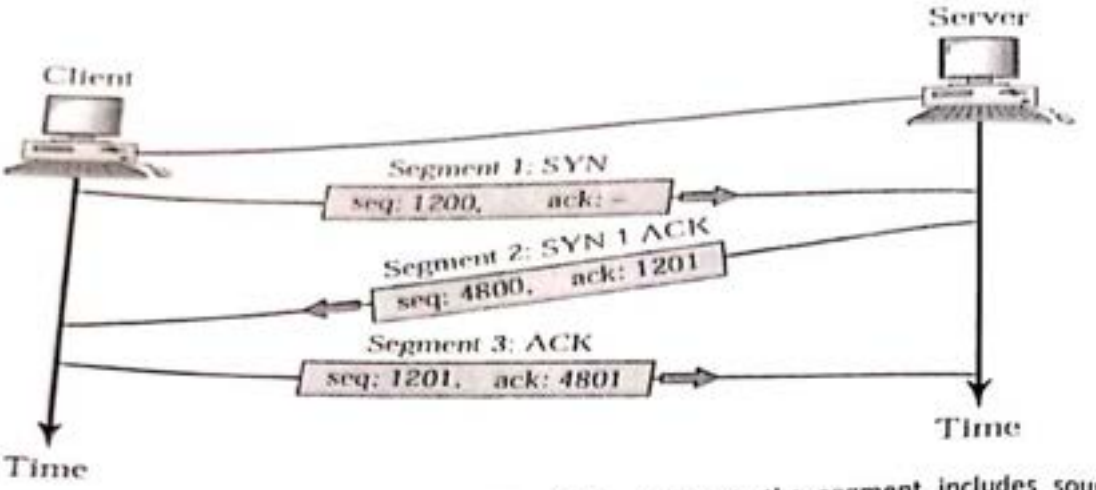
TCP is a connection oriented protocol. it establishes a virtual path between the source and destination.In TCP, connection oriented transmission requires two procedures they are

1.Connection establishment

2.Connection termination

Connection establishment:

When two TCP s in two machines are connected ,they are able to send segments to each other simultaneously .the second and third steps can be combined to create a Three step connection, called **Three Way Handshake** is as shown bellow



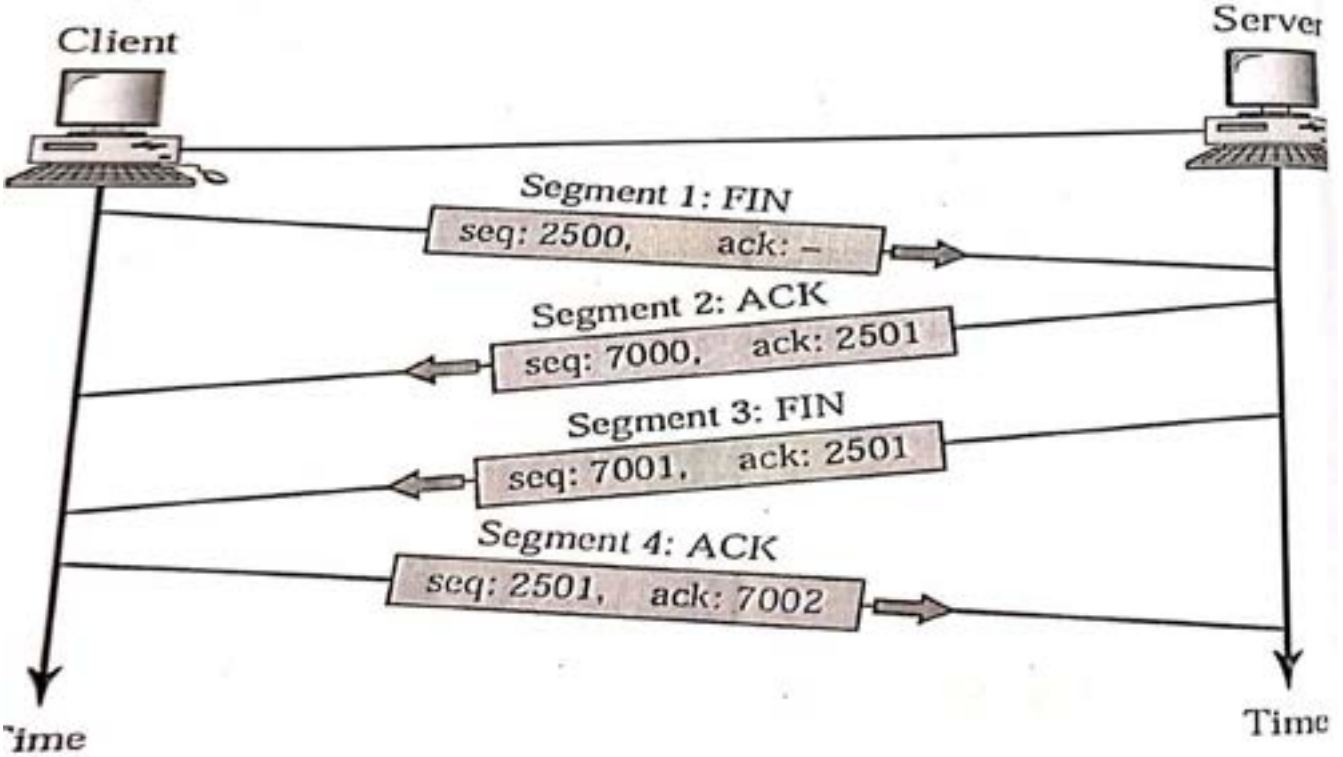
1) The client sends the first Segment, a SYN segment .the segment includes source and destination port numbers

2) The server sends the second segment a SYN and ACK segment .this segment has dual purpose. it contains the initialization sequence numbers used to number the bytes sent from the server to the client.

3) The client sends the third segment, ACK segment .it acknowledge the receipt of the second segment .Data can be sent with the third packet.

Connection termination:

Any of the two parties involved in exchanging data can close the connection .there fore four steps are needed to close the connections in both directions, as shown as follows



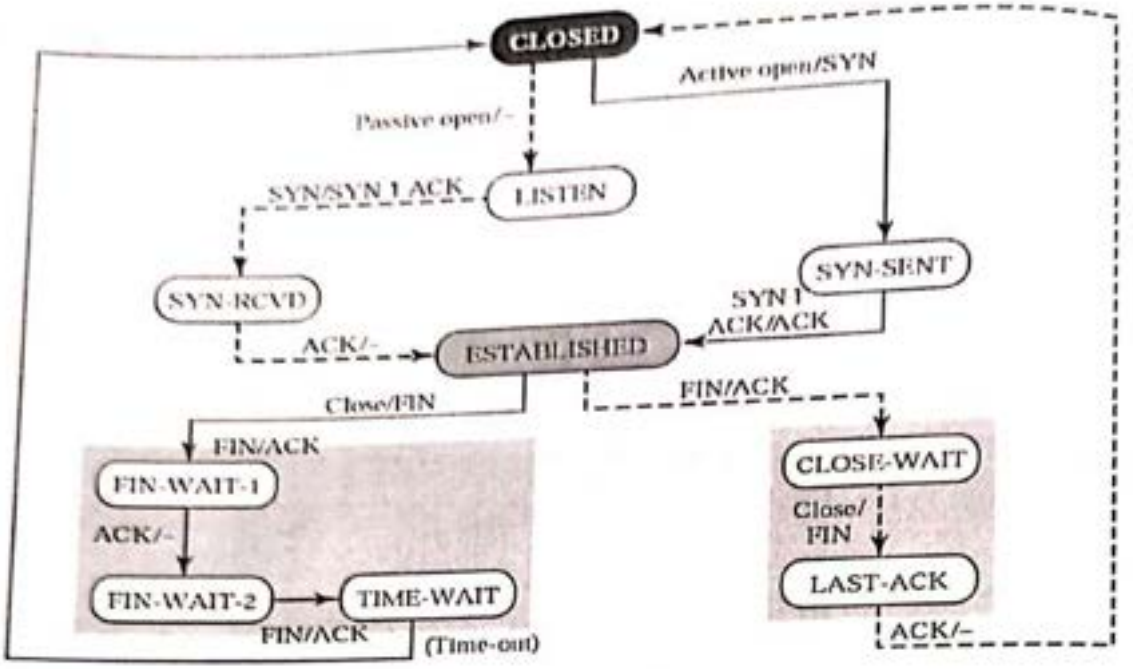
1) The client TCP sends the first segment, a FIN segment.
2) The server TCP sends the second segment, an ACK segment to conform the receipt of the FIN segment from the client.
3) The server TCP can continue sending the data in the server client direction. This segment is a FIN segment
4) The client TCP sends the fourth segment, to conform the receipt of the FIN segment from the TCP server

State Transition Diagram:

The following are the some of the States for TCP

State	Description
CLOSED	There is no connection.
LISTEN	The server is waiting for calls from the client.
SYN-SENT	A connection request is sent; waiting for acknowledgment.
SYN-RCVD	A connection request is received.
ESTABLISHED	Connection is established.
FIN-WAIT-1	The application has requested the closing of the connection.
FIN-WAIT-2	The other side has accepted the closing of the connection.
TIME-WAIT	Waiting for retransmitted segments to die.
CLOSE-WAIT	The server is waiting for the application to close.
LAST-ACK	The server is waiting for the last acknowledgment.

The following diagram shows the state transition diagram for both client and server.



Client Diagram:

The client can having the following states: CLOSED,SYN-SENT,ESTAB-LISHED,FIN WAIT-1,FIN WAIT-2 and TIME WAIT

- The client TCP starts with CLOSED state .The client TCP can receive an active open request from the client application program. and next TCP goes to the SYN_SENT state.
- And next TCP can receive SYN+ACK segment from other TCP and goes to the established state.
- After The client TCP can receive a close request from the client program and after goes to the FIN-WAIT-1 state.
- The client TCP waits to receive an ACK from the server TCP after it goes to the FIN-WAIT-2.
- After the time out the client goes to the closed state, where it begins.

Server Diagram:

The Server having the following States: CLOSED, LISTEN, SYN-RCVD, ESTABLISHED, CLOSE-WAIT AND LAST-ACK

Flow Control:

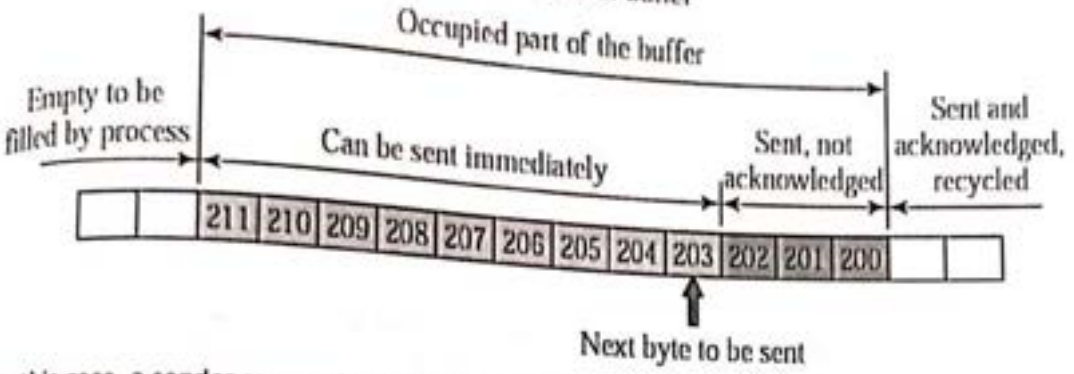
Flow control defines the amount of data a source can send before receiving an acknowledgement from the destination

The TCP has a solution that stands some where between .it defines a window that is imposed on the buffer of data deliver from the application program and is ready to be send. TCP sends as many data as are defined by the sliding window protocol.

Sliding window protocol:

A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become over whelmed with data .TCP's sliding windows are byte oriented.

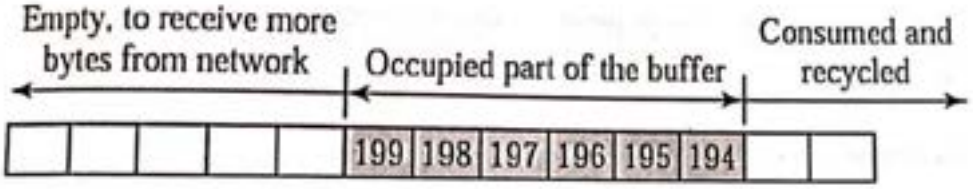
The following figure shows the sender buffer



In this case, a sender can go ahead and send al the bytes in its buffer, without regard to the condition of the receiver, the receiver's buffer, with its limited size could completely fill up because the receiving process is not consuming data fast enough.

Receiver window:

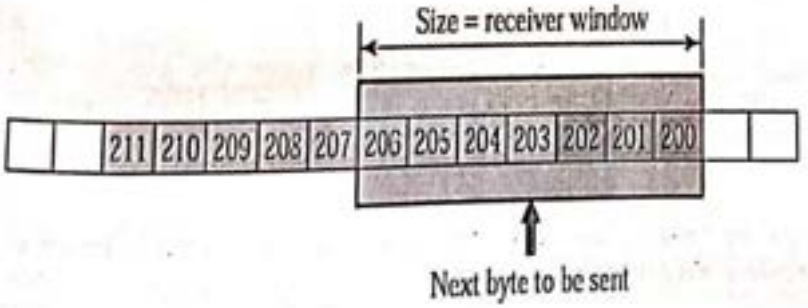
The following figure shows the receiver buffer. The total size of the receiving buffer is N and M locations are already occupied only N-M more bytes can be received .this value is called **Receiver window.**



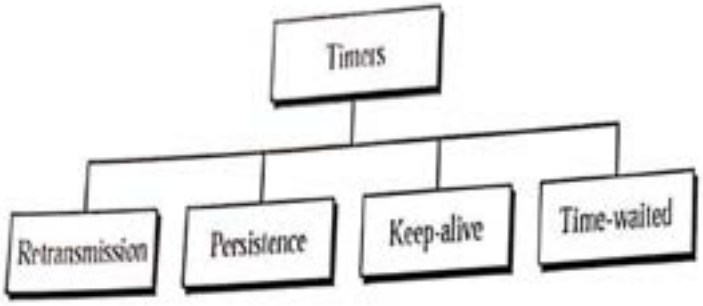
Sender window:

We have flow control if the sender creates a window the sender window with less than are equal to the size of the receiver window

The following figure shows the sender window



TCP Timers:



Retransmission Timer:

TCP employs a Retransmission timer that handles the retransmission time. When TCP sends a segment, it creates a retransmission timer for that particular segment .two situations may occur

1) If an acknowledgement is received for this particular segment before the timer goes off, the timer is destroyed.
2) If the timer goes off, before the acknowledgement arrives, the segment is retransmitted and the time is reset.

Calculation of retransmission time:

Retransmission time can be made dynamic by using it on the round trip time (RTT).Several formulas are used for this purpose .the most common is to set the retransmission time equal to twice the RTT.

Retransmission time=2*RTT

Calculation of RTT:

The value of RTT used in the calculation of the transmission time of the next segment is the updated value of the RTT and the transmission time are

RTT=(previous RTT)+(1-)(current RTT)

Persistence timer:

TCP uses a Persistence Timer for each connection. when the sending TCP receives an acknowledgement with a window size of zero it starts a persistence timer .when a persistence timer goes off the sending TCP sends a special called a **probe.** this segment contains only 1 byte of data.

The value of the persistence timer is set to the value of the transmission time if a response is not received from the receiver another probe segment is sent and the value of the

persistence timer is doubled and reset the sender continuous sending the probe segment doubling and resetting the value of the persistence timer until the values reaches a threshold

Keep Alive Timer:

A keep alive timer is used in some implementations to prevent a long idle connection between two TCP's suppose. Suppose that a client opens a TCP connection to a server, to transfer a data and becomes a silent. Perhaps the client has crashed. In this case the connection remains open forever

Time Waited Timer:

The time waited timer is used during connection termination. When TCP closes connections it does not consider the connection really closed. The connection is held in limbo for a time waited period. This allows duplicate FIN segment s, if any to arrive at the destination to be discarded. The value for this timer is usually 2 times the expected lifetime of a segment.

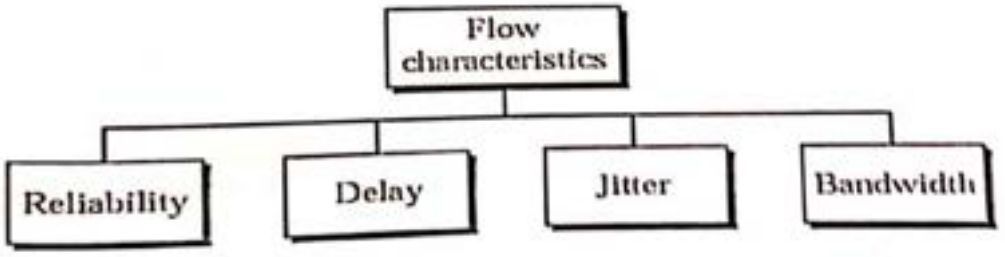
7.QUALITY OF SERVICE

Quality of service (QoS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain.

Flow Characteristics:

Traditionally, four types of characteristics are attributed to a flow:

1. **Reliability**
2. **Delay**
3. **Jitter**
4. **Bandwidth**



1. Reliability:

Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgment, which entails retransmission. However, the sensitivity of

application programs to reliability is not the same. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

2. Delay:

Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

3. Jitter:

Jitter is the variation in delay for packets belonging to the same flow. For example, if four packets depart at times 0, 1, 2, and 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time. On the other hand, if the above four packets arrive at 21, 23, 21, and 28, they will have different delays: 21, 22, 19, and 24.

For applications such as audio and video, the first case is completely acceptable; the second case is not. For these applications, it does not matter if the packets arrive with a short or long delay as long as the delay is the same for all packets. For this application, the second case is not acceptable.

4. Bandwidth:

Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an E-mail may not reach even a million.

Flow classes:

Based on the flow characteristics, we can classify flows into groups, with each group having similar levels of characteristics. This categorization is not formal or universal; some protocols such as ATM have defined classes.

8.THREE WAYS OF HANDSHAKING TECHNIQUES

A sequence of events for connection establishment or termination consisting of the request,then the acknowledgement of the request,and then confirmation of the acknowledgement

The TCP three-way handshake in transmission control protocol (also called the TCP-handshake

three message handshake and/or SYN-SYN- ACK is the method used by TCP set up a TCP/IP connection over an internet protocol based network.

TCP's three way handshaking technique is often referred to as "SYN-SYN-ACK"(or more accurately SYN,SYN-ACK,ACK)because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers.

The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests.

This 3-way handshake process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time.

Being able to negotiate multiple TCP socket connections in both directions at the same time allows a single physical network interface, such as Ethernet, to be multiplexed to transfer multiple streams of TCP data simultaneously.

A simple handshaking protocol might only involve the receiver sending a message meaning "I received your last message and I am ready for you to send me another one."

A more complex handshaking protocol might allow the sender to ask the receiver

If he is ready to receive or for the receiver to reply with a negative acknowledgement meaning "I did not receive your last message correctly, please resend it" (e.g. if the data was corrupted en route).

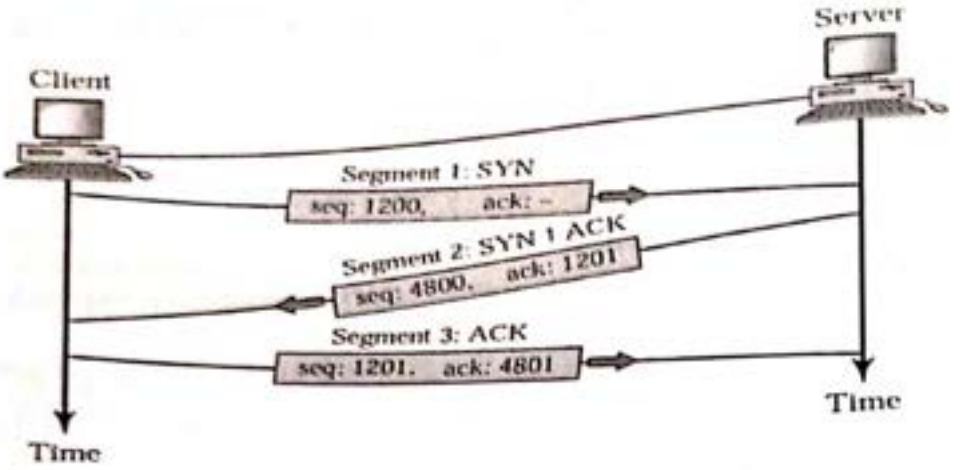
Handshaking makes it possible to connect relatively heterogeneous systems or equipment over a communication channel without the need for human intervention to set parameters.

One classic example of handshaking is that of modems,which typically negotiate communication parameters for a brief period when a connection is first established, and thereafter use those parameters to provide optimal information transfer over the channel as a function of its quality and capacity.

The "squealing" (which is actually a sound that changes in pitch 100 times every second) noises made by some modems with speaker output immediately after a connection is established are in fact the sounds of modems at both ends engaging in a handshaking procedure.

Once the procedure is completed, the speaker might be silenced, depending on the settings of operating system or the application controlling the modem

Three step connection establishment:



To establish a connection, TCP uses a three-way handshake

Before a client attempts to connect with a server, the server must first Bind to and listen at a port to open it up for connections.

Connections: This is called a passive open.

Once the passive open is established, a client may initiate an Active open.

To establish a connection, the three-way (3-way) handshake occurs.

1. SYN:

- The active open is performed by the client sending a SYN to the server.
- The client sets the segment's sequence number to a random value A.

2. SYN-ACK:

In response, the server replies with a SYN-ACK.

The acknowledgment number is set to one more than the received sequence number (A + 1), and the sequence number that the server chooses for the packet is another random number, B.

3. ACK:

Finally, the client sends an ACK back to the server.

The sequence number is set to the received acknowledgement value i.e. A + 1, and the acknowledgement number is set to one more than the received sequence number i.e. B + 1.

At this point, both the client and server have received an acknowledgment of the connection.

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged.

The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

9.HTTP and SMTP:

The Hypertext Transfer Protocol (HTTP) is used mainly used to access data on the World Wide Web. The protocol transfers data in the form of plaintext, hypertext, audio, video, and so on. It is called the Hypertext Transfer Protocol is it is used in an environment where there are rapid jumps from one document to another.

HTTP functions like a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it uses only one TCP connection.

HTTP is like SMTP because the data transferred between the client and the server are similar to SMTP messages. In addition, the format of the messages is controlled by MIME-like headers. However, HTTP differs from SMTP in the way the messages are sent from the client to the server and from the server to the client. Unlike SMTP messages, the HTTP messages are not destined to be read by humans they are read and interpreted by the HTTP server and HTTP client. SMTP messages are stored and forwarded, but HTTP messages are delivered immediately.

DNS:

Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the internet or a private network. It associates various information with domain names assigned to each of the participating entities.

A DNS resolves queries for these names into IP addresses for the purpose of locating computer services and devices World Wide. By providing a World Wide distributed keyword-based redirection service, the DNS is an essential component of the functionality of the internet.

It defines the DNS protocol, a detailed specification of the data structures and exchanges used in DNS, as part of the Internet protocol suite.

DDNS:

DDNS is a method of keeping a domain name linked to a changing IP address as not all computers use static IP addresses. Typically, when a user connects to this internet, the users ISP assigns an unused IP address from a pool of IP addresses and this address is used only for the duration of the specific connection.

A DDNS service provider uses a special program that runs on the users computer, contacting the DNS service each time the IP address provided by the IP changes and subsequently updating the DNS database to reflect the change in IP address in the way even though a domain names

IP address will change often other users do not have to know the changed IP address in order to connect with other computer.

To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

FTTP:

File Transfer protocol is the standard mechanism provided by the Internet for copying a file from one host to another.

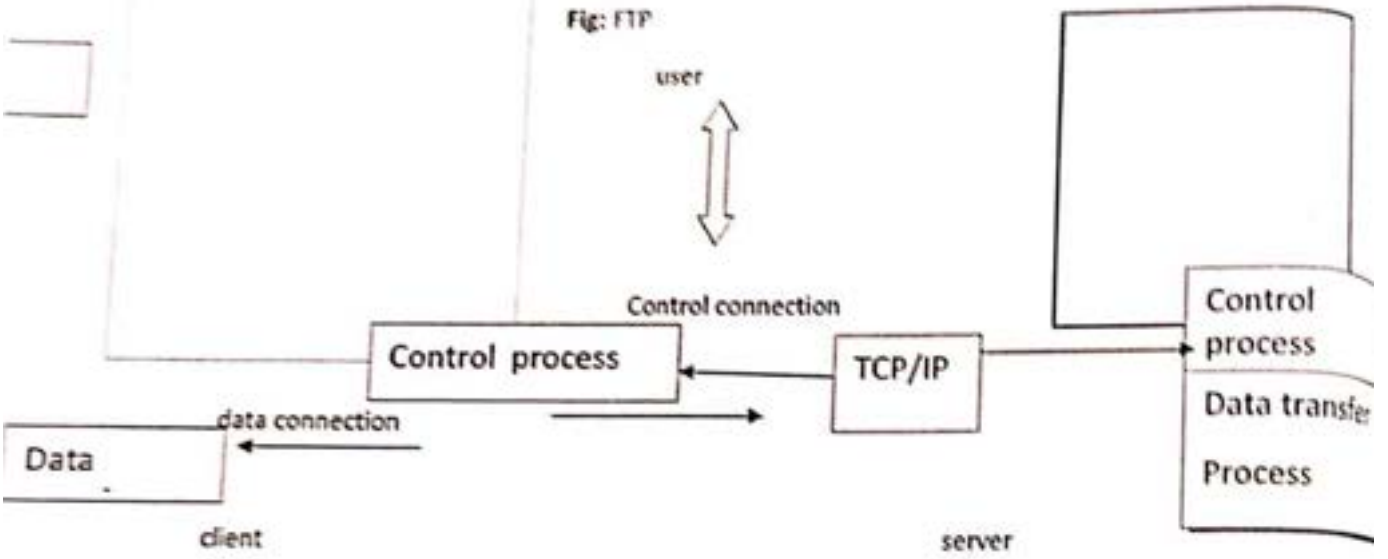


Fig: FTP

Transferring file from one computer to another is one of most common tasks expected from tasks expected from a networking or internetworking environment.

FTP differs from other client-server applications in that it establishes two connections between the client and the server. One connection is used for data transfer, the other for control information. Separation of commands and data transfer makes FTP more efficient.

The above fig shows the basic model of FTP. The client has three components: user interface, client control process, and the client data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes. The control connection is maintained during the entire interactive FTP session. The data connection is opened and then closed for each file transferred.

World Wide Web:

The World Wide Web is a repository of information spread all over the world and linked together. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the internet.

The WWW project was initiated by CERN (European Laboratory for particle physics) to create a system to handle distributed resources necessary for scientific research.

The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called websites

Email:

One of the most popular network services is electronic mail (email). Electronic mail is used for sending a single message that includes text, voice, video, or graphics to one or more recipients. Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the internet.

Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

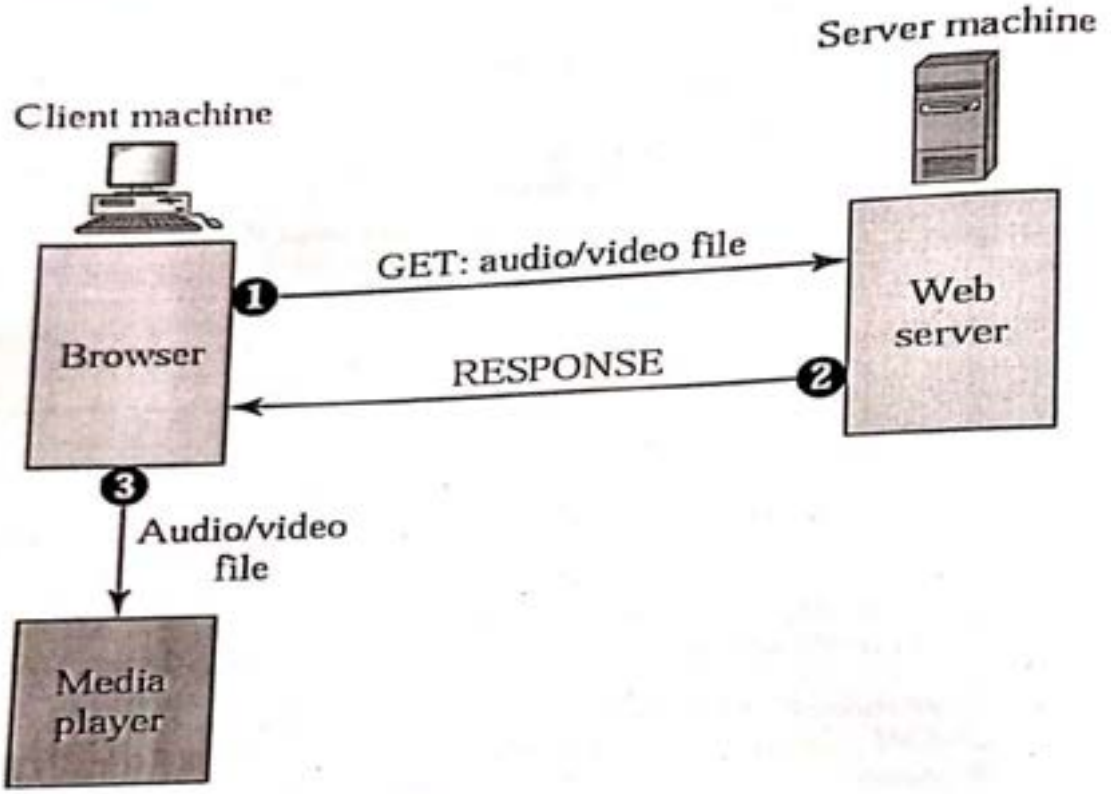
An Internet email message consists of three components, the message envelop, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

10.STREAMING STORED AUDIO/VIDEO

We have discussed digitizing and compressing audio/video, we turn our attention to specific applications. the first is streaming stored audio and video. Downloading these types of files from a web server can different from downloading other types of files. To understand the concept, let us discuss four approaches , each with a different complexity.

FIRST APPROACH: Using a web server

A compressed audio/vodeo file can be downloaded as text file. The client(browser) can use the services of HTTP and send a GET message to downloaded the file. The web server can send the compressed file to the browser. the browser can then use a help application , normally called a media player, to play the file.



This approach is very simple and does not involve streaming . however , it has a drawback. An audio/video file is usually large even after compression . an audio file may contain tens of megabits ,and a video file contain hundreds of megabits.in this approach , the file needs to download completely before it can be played.

SECOND APPROACH:

Using a web server with a metafile.

In another approach , the media player is directly connected to the web server for downloading the audio/video file. The actual audio/video file and a metafile that holds information about the audio/video file.

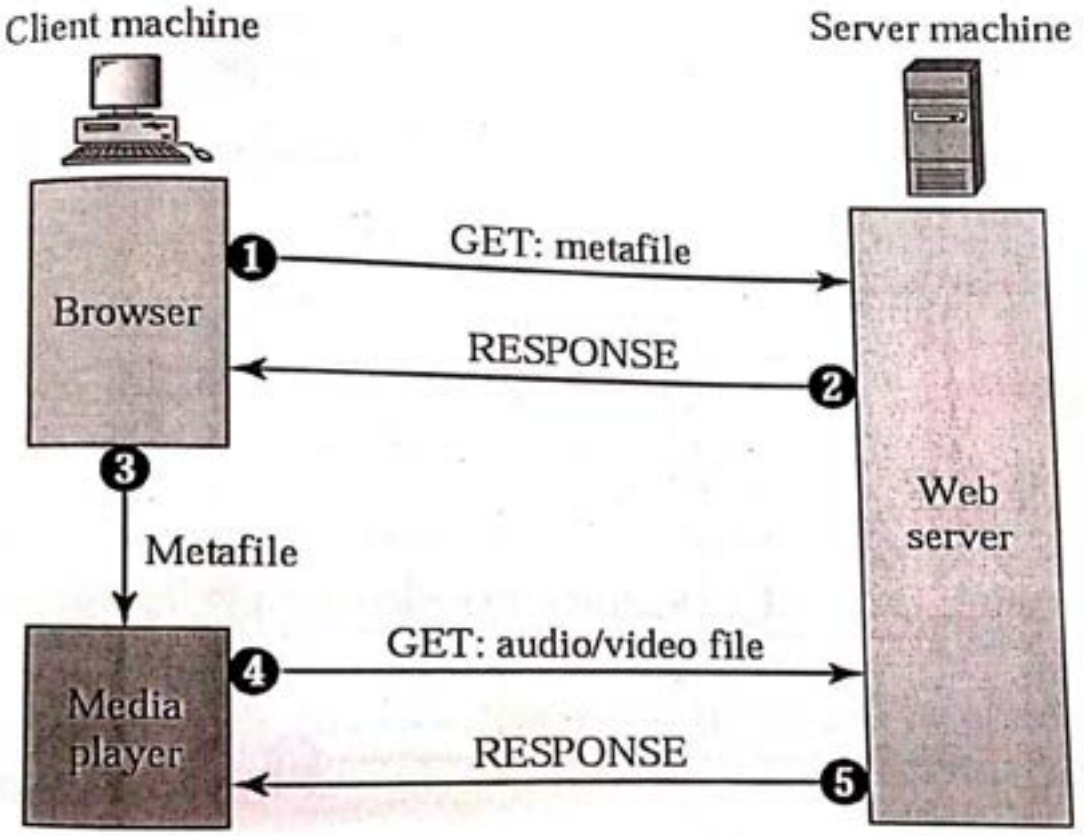
the HTTP client accesses the web server by using the GET message.

the information about the metafile comes in the response.

the metafile is passed to the media player.

the media player uses the metafile to access the audio/video file.

the web server responds.



THIRD APPROACH: Using a media server.

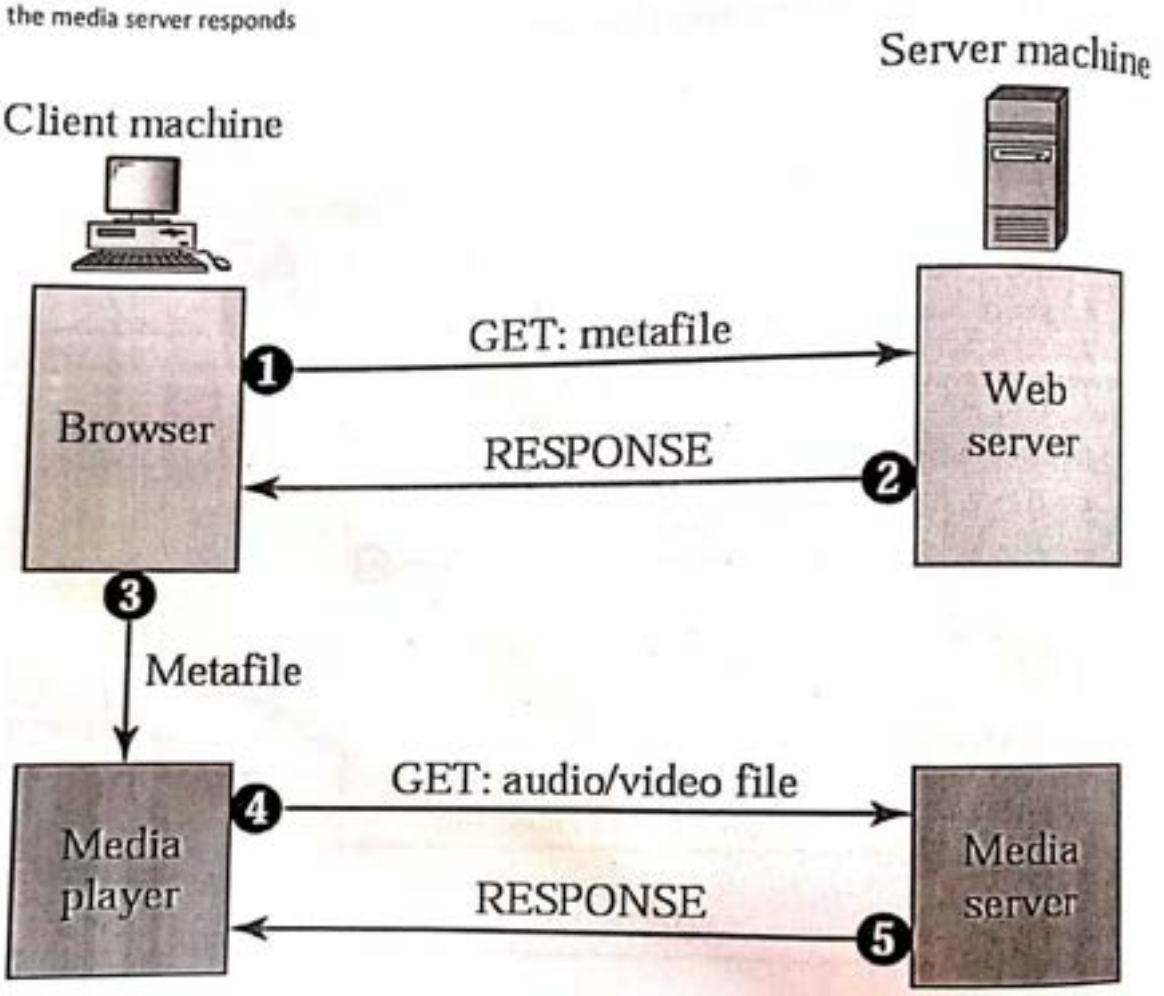
The problem with the second approach is that the browser and the media player both use the services of HTTP.HTTP is designed to run over TCP.this is appropriate for retrieving the metafile, but not for retrieving the video/ audio file. http , which accesses the web server , and the web server itself are designed for TCP; we need another server , a media server.

the HTTP client accesses the web server by using a GET message.

the information about the metafile comes in the response.

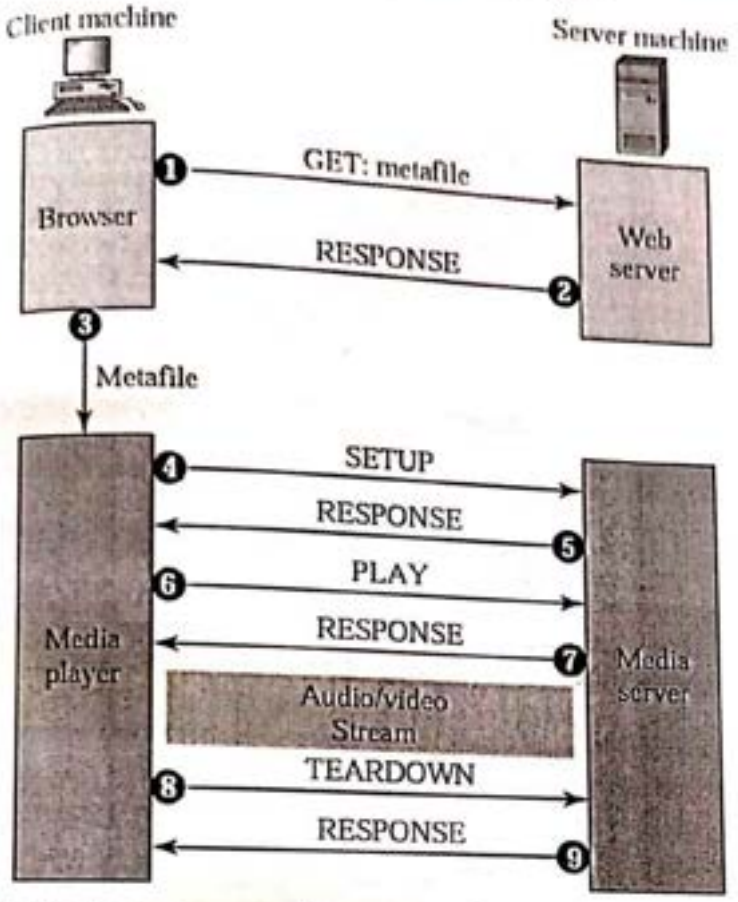
the metafile is passed to the media player.

the media server responds



OURTH APPROACH: Using a media server and RTSP

The real-time streaming protocol (RTSP) is a control protocol designed to tad more functionalities to the streaming process , using RTSP. We can control the playing of audio/video. RTSP is an out-of band control that is similar to the second connection in FTP.



the HTTP Client accesses the web server by using a GET message.

the information about the metafile comes in the response.

the metafile is passed to the media player.

the media player sends a SETUP message to create a connection with the media server.

the media server responds.

the media player sends a PLAY message to start playing(downloading).

the audio/video file is downloaded by using another protocol that runs over UDP.

the connection is broken by using the TERADOWN message.

the media server responds.

11. Voice over IP

Let us concentrate on one real-time interactive audio/video application: **Voice over IP**, or internet telephony. The idea is to use the internet as telephone network with some additional capabilities. Instead of communicating over a circuit-switched network, this Application allows communication between two parties over the packet-Switched internet. Two protocols have been designed to handle this type of communication:

SIP and H.323. We briefly discuss below.

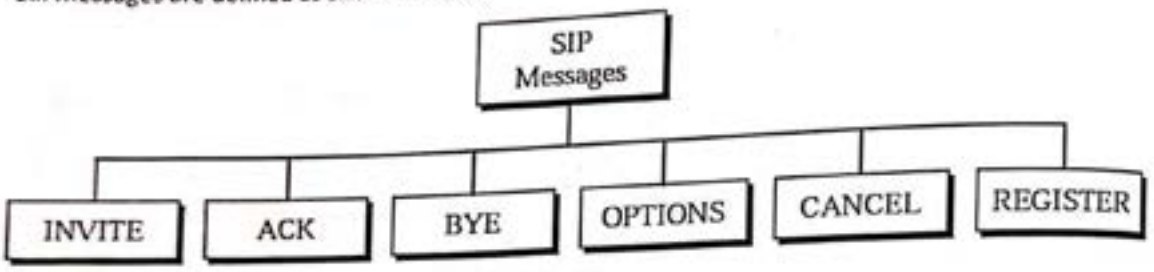
SIP:

The **session initiation protocol (SIP)** was designed by IETF. It is an application layer protocol that establishes, manages, and terminates a multimedia session (call). It can be used to create two- party, multiparty, or multicast sessions. SIP is designed to be independent of the underlying transport layer; it can run on either UDP or TCP.

Messages:

SIP is a text based protocol like HTTP. SIP, like HTTP, uses messages.

Six messages are defined as shown in figure.



- Each message has a header and a body.
- The header consists of several lines that describe the structure of the message, caller's capability, media type, and so on.
- We give a brief description of each message. Then we show their applications in the sample sessions.
- The caller initializes a session with the INVITE message. After the callee answers the call, the caller sends an ACK message for confirmation.
- The BYE message terminates a session.
- The OPTIONS message queries a machine about its capabilities.
- The CANCEL message cancels an already started initialization process.
- The REGISTER message makes a connection when the callee is not available.

Address:

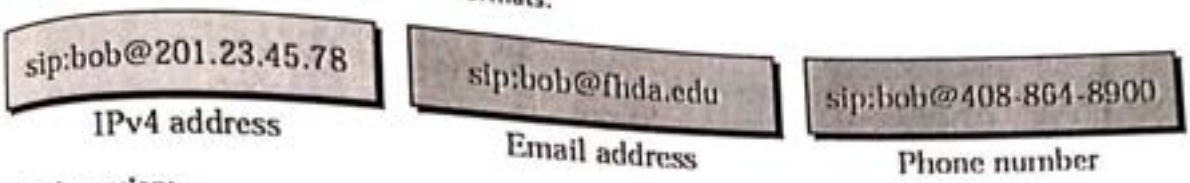
In a regular telephone communication a telephone number identifies the sender, and Another telephone number identifies the receiver.

•SIP is very flexible.

• In SIP, an email address, an IP address, a telephone number, and other types of address can be used to identify the sender and receiver.

However, the address needs to be in SIP format (also called scheme).

The below figure shows some common formats:



Simple session:

A simple session using SIP consists of three modules: Establishing, communicating, and terminating.

Establishing a session:

Establishing a session in SIP requires a three-way handshake. The caller sends an INVITE massage, using UDP or TCP, to begin the Communication. If the callee is willing to start the session, she sends a reply message. To confirm that a reply code has been received, the caller sends an ACK message.

Communicating:

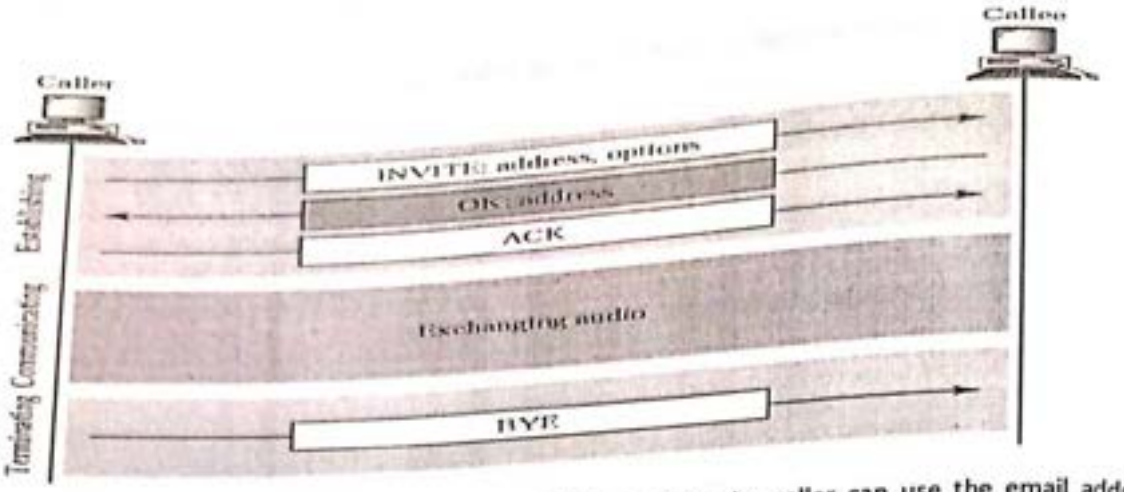
After the session has been established, the caller and the callee can communicate using two temporary ports.

Terminating the session:

The session can be terminated with a BYE message sent by either party.

Tracking a callee:

What happens if the callee is not sitting at her terminal? She may be away from her system or at another terminal. She may not even have a fixed IP address if DHCP is being used. SIP has a mechanism (similar to one in DNS) that finds the IP address of the terminal at which the callee is sitting. To perform this tracking, SIP uses the concept of registration. SIP defines some servers as registrars. At any moment a user is registered with at least one **registrar server**; this server knows the IP address of the callee.

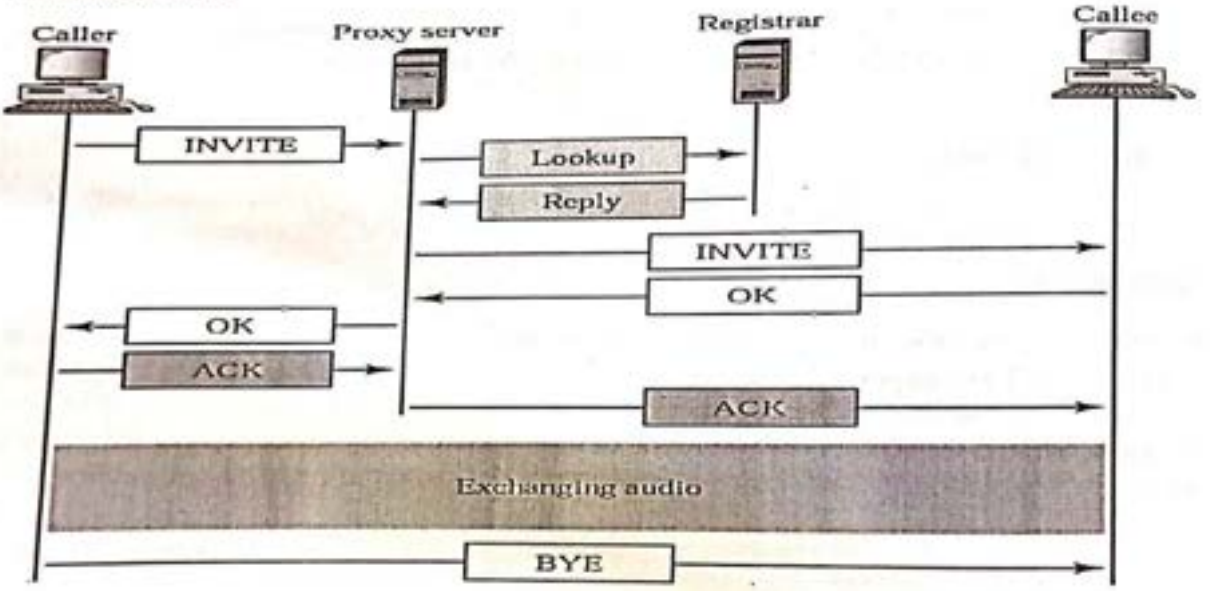


When a caller needs to communicate with the callee, the caller can use the email address instead of the IP address in the INVITE message. The message goes to a proxy server. The proxy server sends a lookup message to some registrar from the registrar server, the proxy server takes the caller's INVITE message and inserts the newly discovered IP address of the callee. This message is then sent to the callee. Figure shows the process.

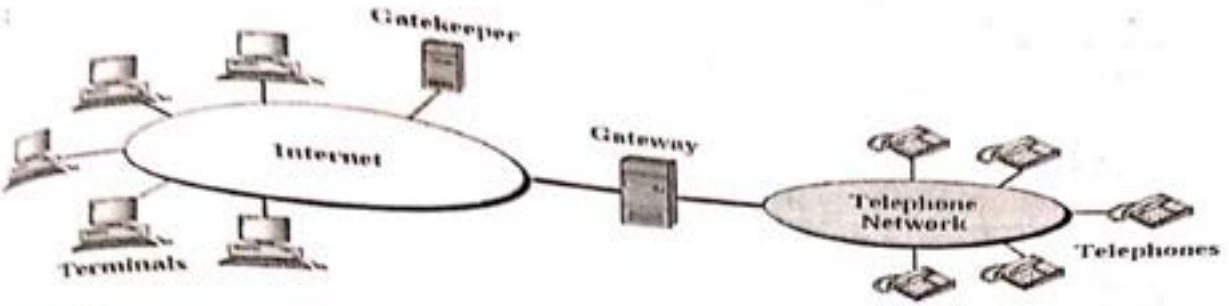
H.323:

H.323 is a standard designed by ITU to allow telephones on the public telephone network to talk to computers connected to the internet. The figure shows the general architecture of H.323.

Tracking the callee

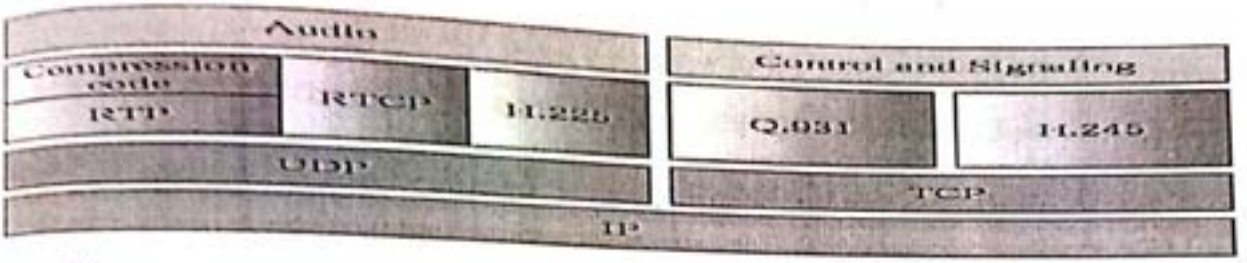


H.323 architecture:



Protocols:

H.323 users a no. of protocols to establish and maintain voice (or video) commutation figure shows this protocol.

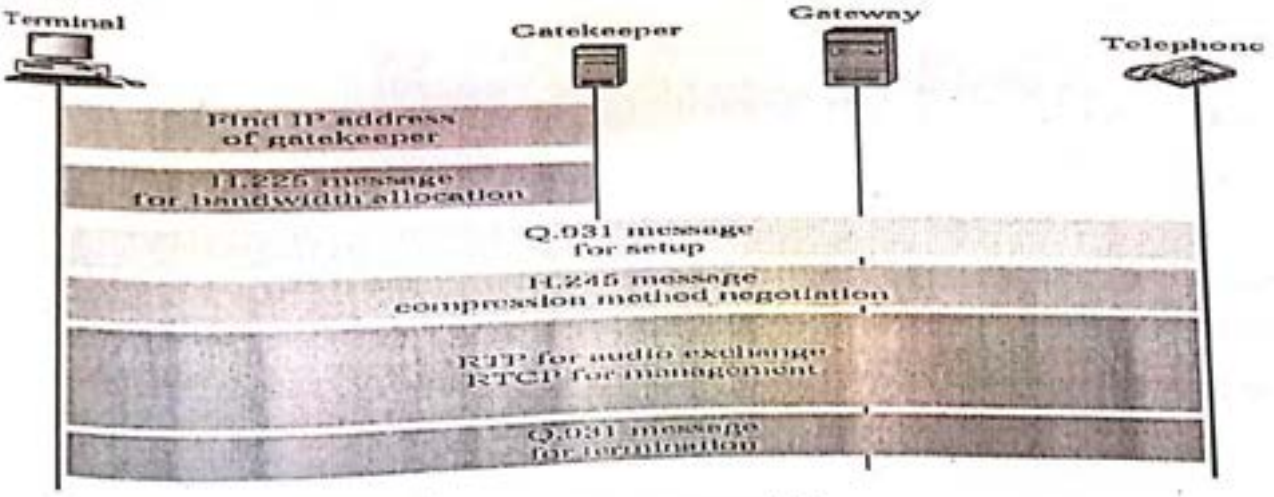


Operation:

The operation of a telephone communication using H.323 with a simple example. The below figure shows the steps used by a terminal to communicate with a telephone.

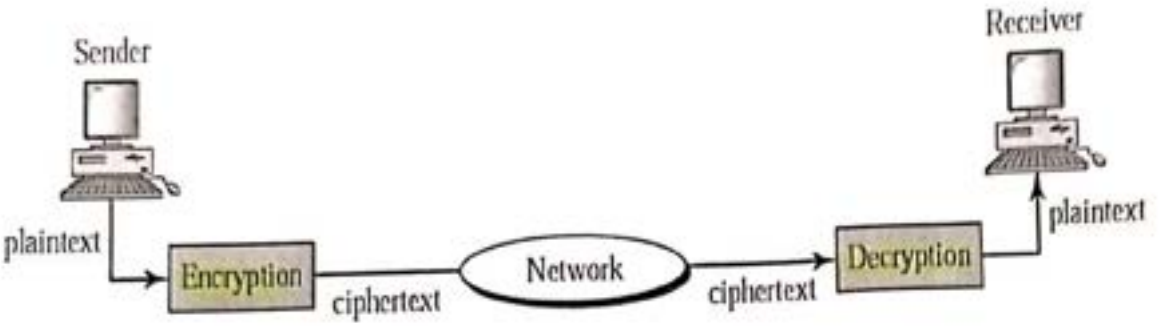
- The terminal sends a broadcast message to the gate keeper. The gate keeper responds with its IP address.
- The terminal and gate keeper communicate, using H.225 to negotiate bandwidth.

H.323 example:



12. Explain Cryptography?

The word cryptography in Greek means 'secret writing." However the term today refers to the science and art of transforming messages to make them secure and immune to attacks. The following fig shows the components involved in cryptography.



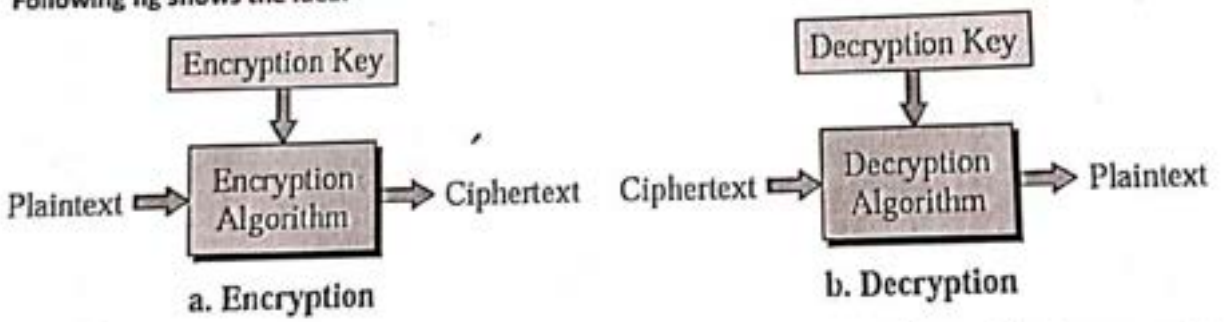
Cryptography components:

The original message, before being transformed is call plaintext. After The message is transformed it is call cipher text. An encryption

n algorithm transforms the plaintext to cipher text a decryption algorithm transforms the cipher text back to plain text . The sender uses an encryption algorithm and the receiver uses a decryption algorithm.

This is not to say that every sender=receiver pair needs its very own unique cipher for a secure communication. Instead, through the use of public ciphers with secret keys, one cipher can serve million of communicating pairs. A key is a number (value) that the cipher, as an algorithm operates on. To encrypt a message, we need an encryption algorithm, an encryption and the plaintext. These create the cipher text . To decrypt reveal the Original plaintext .

Following fig shows the idea.

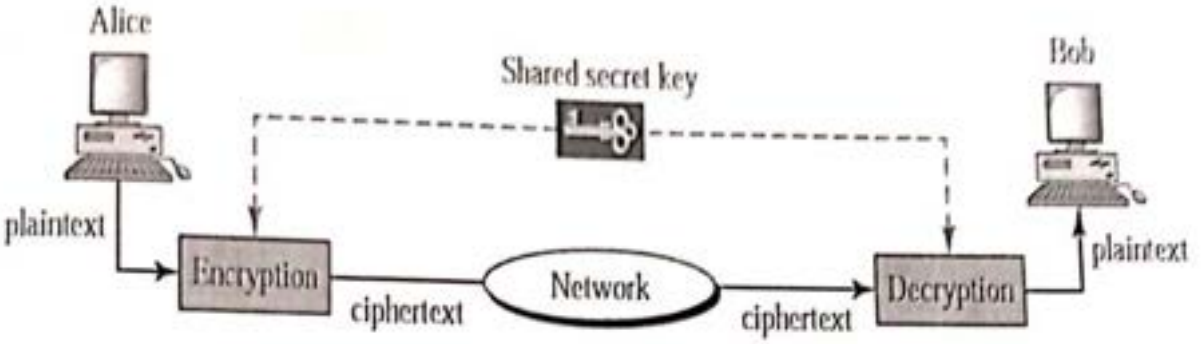


The encryption and decryption algorithms are public anyone can access them . The keys are secret they need to be protected.

"The cryptography, and encryption/decryption algorithms are public; the keys are secret".

Symmetric- key cryptography:

In symmetric-key cryptography the same key is used by both parties. The sender user this key and an encryption algorithm to encrypt data the and the corresponding decryption algorithm to decrypt the data



1. In symmetric-key cryptography the same key is used by the sender and the receive the key is shared.
2. In Symmetric key cryptography , the same key is used in both directions.
3. Symmetric – key cryptography is often used for long messages.

A symmetric –key algorithm has two major disadvantages. Each pair of users muct have a unique symmetric key. This means that if N people in the world want to use this method, there needs to be N(N-1)/2 symmetric keys. For 1 million people to communicate 500 billion symmetric keys are needed. The distribution of the keys between two parties can be difficult.

Traditional Ciphers:

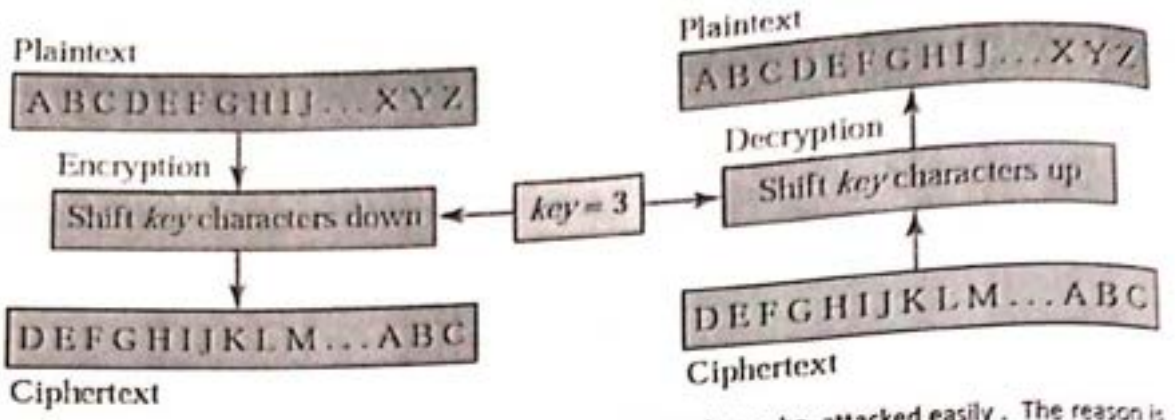
In the earliest and simplest ciphers, character was the unit of data to be encrypted. These traditional ciphers involved either substitution or transposition.

Substitution Cipher:

A Cipher using the substitution method substitutes one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another . For example we can replace character a with D and character T with Z. If the symbols are digits (0 to 9) we can replace 3 with 7 and 2 with 6. We will concentrate on alphabetic characters. Substitution can be categorized as either monoalphabetic or ployaphabetic

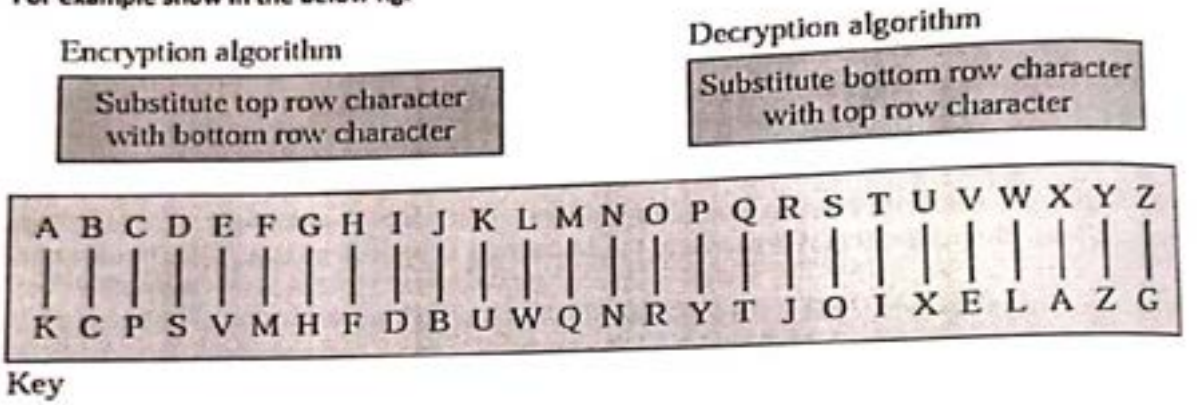
Polyalphabetic:

Monialphabetic substitution in Monialphabetic substitution , a character in the plaintext is always changed to the same character in the cipher text regardless of its position in the text. For example , if the algorithm says that character A in the plain text must be changed to character D , Every character A is changed to character D, regardless of its position in the text.



Monoalphabetic substitution is very simple, but the code can be attacked easily . The reason is that the method cannot hide the natural frequencies of characters in the language being used.

For example show in the below fig.

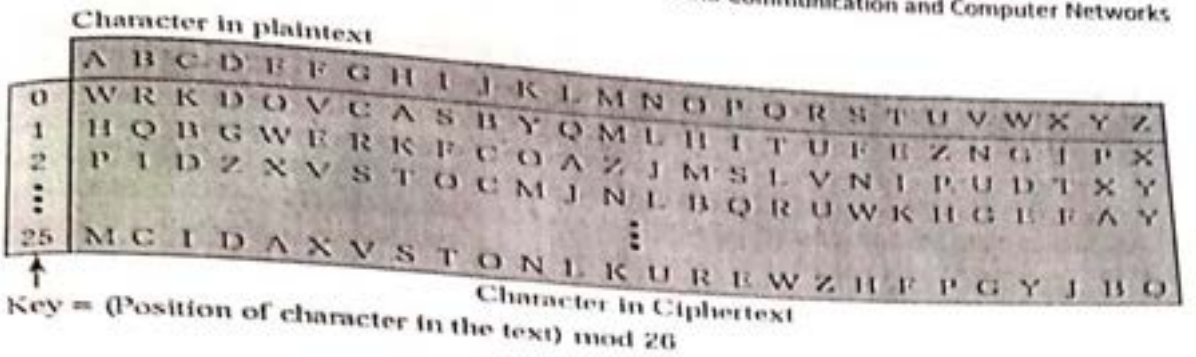


In Monialphabetic substitution , the relationship between a character int eh plaintext to the character in the cipher text is always one-to-one.

Polyalphabetic substitution:

In Polyalphabetic substitution each occurrence of a character can have different substitute. The relationship between a character in the plain text to a character in the cipher text is one-to-many. Character a can be changed to D in the beginning of the text, but it could be changed to N at the middle. There are many interesting Polyalphabetic substitution ciphers. We discuss a very simple one. It is obvious that if the relationship between plain text characters and cipher text characters is one-to-many.

Character in plaintext

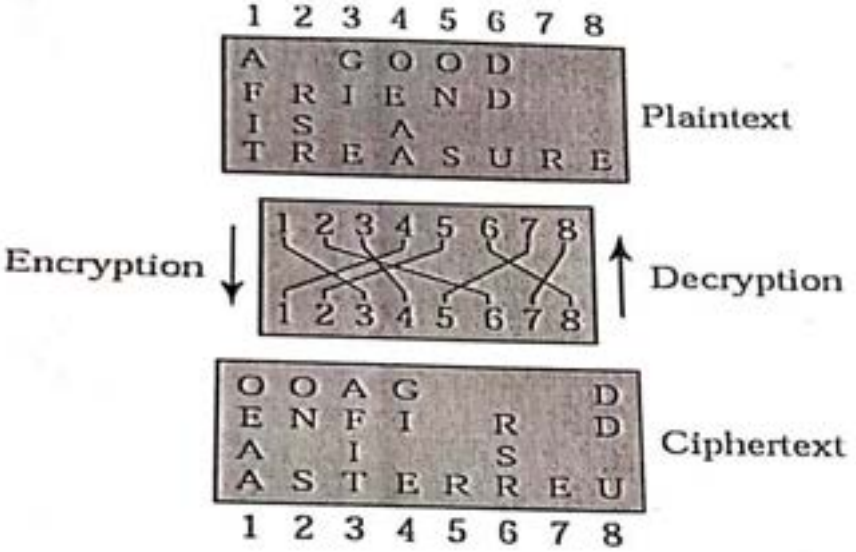


In Polyalphabetic substitution, the relationship between a character in the plaintext and a character in the cipher text is one- to –many.

Transpositional Cipher:

In transpositional cipher the characters retain their plaintext form but change their position to create the cipher text. The text is organized into a two – dimensional table, and the columns are interchanged according to a key.

Transpositonal Cipher

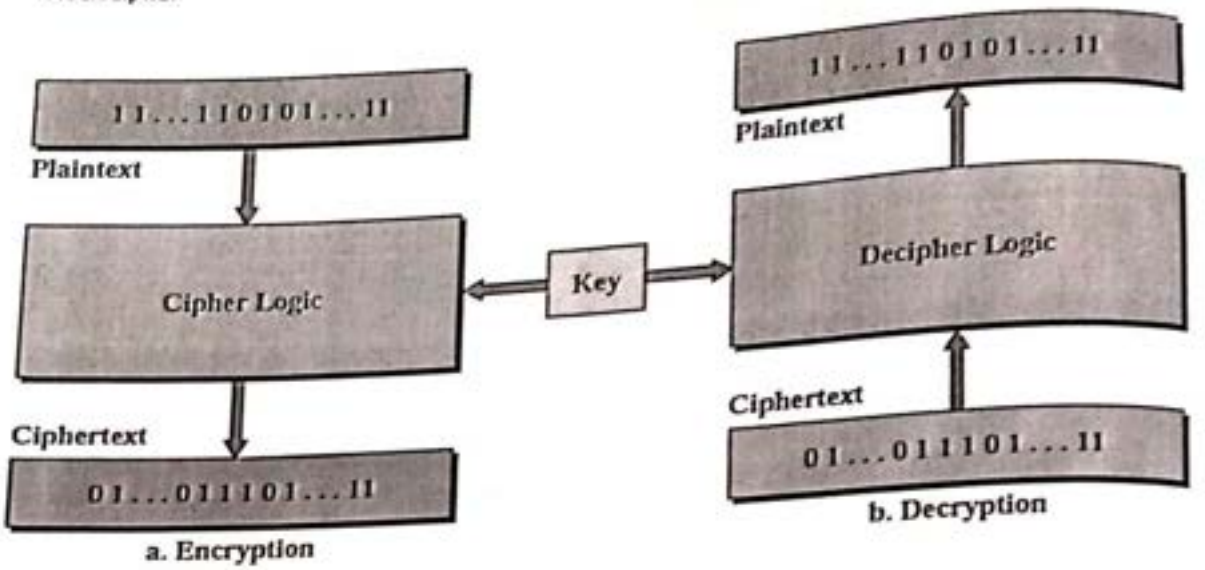


Block Cipher:

Traditional ciphers used a character or symbol as the unit of encryption or decryption . Modern ciphers, on the other hand use a block of bits as the unit of encryption/ decryption.

The fig show the concept of the block cipher the plaintext and cipher text are blocks of bits.

Block cipher



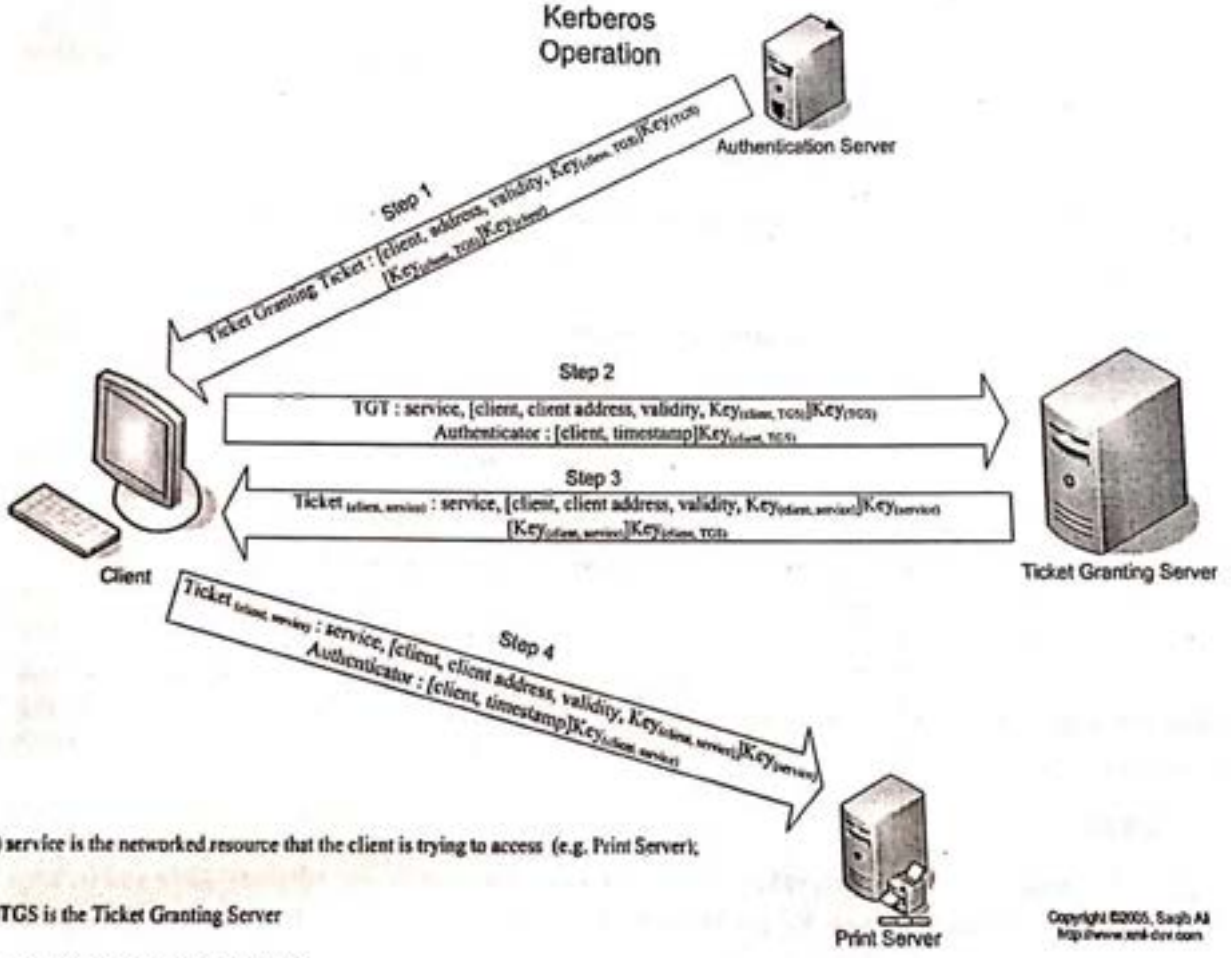
13.EXPLAIN KERBEROS ?

Kerberos is an authentication protocol, and at the same time a KDC that has become very popular . Several systems including windows 2000 use Kerberos. Kerberos is named after the three-headed dog in Greek mythology that guards the gates of Hades. Originally designed at MIT it has gone through several versions. We discuss only version 4, the most popular, and we briefly explain the difference between version 4 and version 5, the latest.

Servers

Three servers are involved in the Kerberos protocol: an authentication server(AS), a ticket-granting server(TGS), and a real(data) server that provides services to others. In our example and figures, Bob is the real server and Alice is the user requesting service.

The following fig shows the relationship between these three servers



1) service is the networked resource that the client is trying to access (e.g. Print Server);

2)TGS is the Ticket Granting Server

Authentication Server(AS)

The KDC in the Kerberos protocol. Each user registers with the AS and is granted a user identity and a password . The As has a database with these identities and the corresponding password . The AS verifies the user, issues a session key to be used between Alice and the TGS, and sends a ticket for the TGS.

Ticket Granting Server(TGS);

The TGS issues a ticket for the real server(BOb) . It also provides the session key(K_{AB}) between Alice and Bob. Kerberos has separated the user verification from ticket issuing. In this way, although Alice verifies her ID just once with AS, she can contact TGS multiple times to obtain tickets for different real servers.

Real Servers:

The real server(Bob) provides services fro the user(Alice). Kerberos is designed for a client-servers program such as FTP, in which a user uses the client process to access the server process. Kerberos is not used for person-to-person authentication.

Operation:

A client process(Alice) can receive a ser vice from a process running on the ral sserver (Bob) in six steps, as shown in fig.

STEP1:

Alice sends her request to AS in plaintext, using her registered identity.

STEP2:

The as sends message encrypted with Alice's symmetric key K_A . The message contains two items a session key K_S that is used by Alice to contact TGS and a ticket for TGS tat is encrypted with the TGS symmetric key K_{TG} Alice does not know K_A .

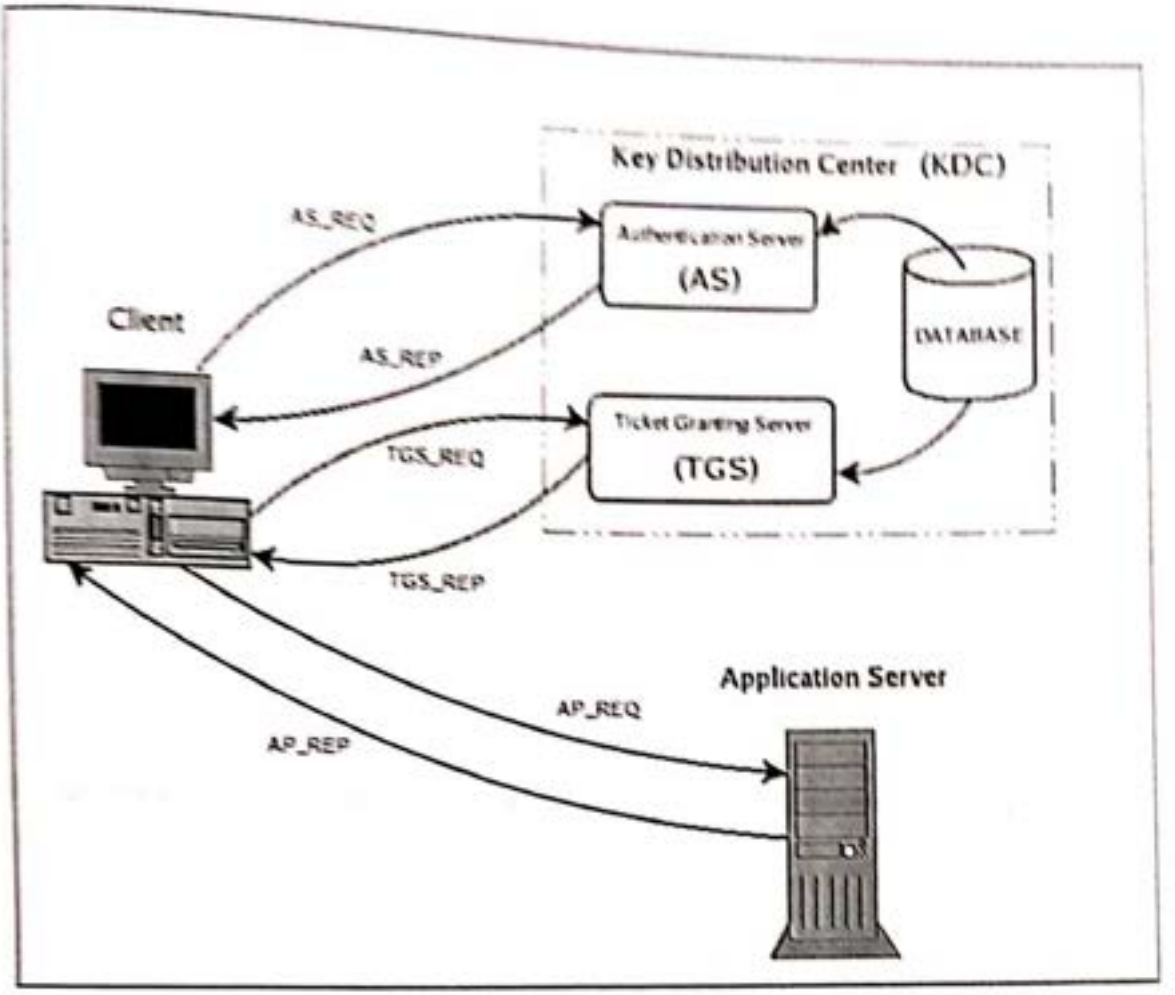
but when the message arrives, she types her password x. The password and the appropriate algorithm together create K_A if the password is correct. The password is then immediately destroyed it is not sent to the network, and it does not stay in the terminal. It is only used for a moment to create K_A . The process now uses K_A to decrypt the message sent K_S and the ticket are extracted.

STEP3:

Alice now sends three items to the TGS. The first is the ticket received from As. The second is the name f the real server (Bob) , and the third is a timestamp which is encrypted by K_S. The timestamp prevents a replay by Eve.

STEP4:

Now, TGS sends two tickets, each containing the session key between Alice and Bob K_{AB} the ticket fro Alice is encrypted with K_S the ticket for Bob is encrypted with Bob's key K_B. she cannot replay step 3 because she cannot replace the time-stamp with anew one . Even if she is very quick and sends she step3 message before the time-stamp has expire, she still receive the same two tickets that she cannot decipher.



STEP 5:

Now each of the previous phases is described in greater detail with reference to Kerberos 5, but pointing out the differences with version 4. Nevertheless, it should be borne in mind that the Kerberos protocol is rather complicated and this document is not intended as a guide for those who wish to know the exact operating details (in any case, these are already written up in RFC1510). The discussion below has been left intentionally abstract, but sufficient for those who examine the KDC logs to understand the various authentication transitions and any problems which occur.

14.Types of Virtual Private Networks(VPN)

Virtual private networks

Virtual private network is a technology that is gaining popularity among large organization that use the global Internet for both intra and interorganization communication but require privacy in their internal communication.

Private networks:

A private networks is designed for use inside an organization. It allows access to shared resources and at the same time, prides privacy. Before discuss some aspect of these networks, let us define two commonly used terms . There are

- Intranet.
- Extranet

Intranet:

An intranet is private network that uses the Internet model. Hower access to the network is limited to the users inside the organization. The network uses application programs defined for the global Internet, such as HTTP , and may have web servers print servers, file servers and so on.

Extranet:

An extranet is the same as an intranet with one major difference some resources may be accessed by specific groups of users outside the organization under the control of the network administrator . For example, and organization may allow authorized customers access to product specifications availability and onlin ordering. A university or a college can allow distance learning students access to the computer lab after passwords have been checked.

Addressing:

A private network that uses the Internet model must use IP addresses. Three choices are available:

- The network cam apply for a set of address from the Internet authorities and use them without being connected to the Internet.
- The network can use any set of addresses without registering with the Internet authorities. Because the network is isolated, the addresses do not have to be unique.
- To overcome the problems associated with the first and second strategies, the Internet authorities have reserved three sets of addressee, below show in table

Prefix	Range	Total
10/8	10.0.0.0 to 10.255.255.255	2^{24}
172.16/12	172.16.0.0 to 172.31.255.255	2^{20}
192.168/16	192.168.0.0 to 192.168.255.255	2^{16}

Address for private network

Any organization can use an address out of this set without permission from the Internet authorities. Everybody knows that these reserved address are for private networks. They are unique inside the organization , but they are not unique globally. No router will forward a packet that has one of these addresses as the destination address.

Achieving Privacy:

To achieve privacy organizations can use ofn of three strategies

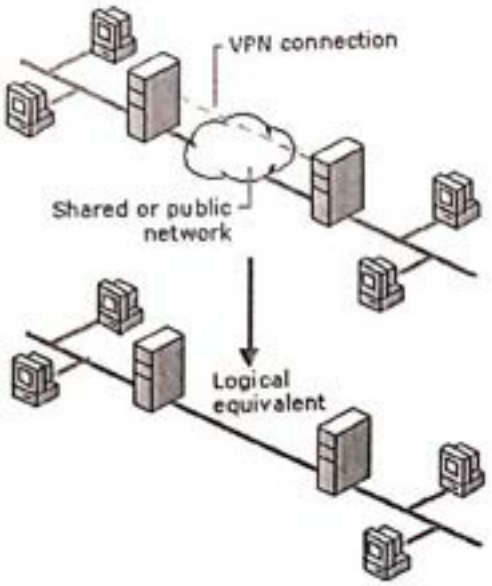
1. Private network.
2. Hybrid networks.
3. Virtual private networks

1.Private networks:

An organization that needs privacy when routing information inside the organization can use a Private network as discussed previously. A small organization with one single site can use an isolated LAN. To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information, which allows the data to traverse the shared or public network to reach its endpoint.

To emulate a private link, the data is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The link in which the private data is encapsulated and encrypted is a virtual private network (VPN) connection.

The following illustration shows the logical equivalent of a VPN connection.



In this situation the organization has created a private internet that is totally isolated from the global Internet. For end to end communcation between stations at different sites, the organization can use the Internet model.

2.Hybrid Networks:

Today most organizations need to have privacy in intraorganization data exchange but, at the same time, they need to be connected to the global Internet for data exchange with other organizations . One solution is the use of a Hybrid network, Hybrid network allows an organization to have its own private internet and at the same time access to the global Internet .

An organization with two sites user routers R1 and R2 to connect the two sites privately through a leased line it uses routers R3 and R4 to connect the two sites to the rest of the world. The organization uses global IP addresses for both types of communication. However packet destined for internal recipients are routed only through routers R1 and R2 . Routers R32 and R4 route the packets destined for outsiders.

3.Virtual private Networks:

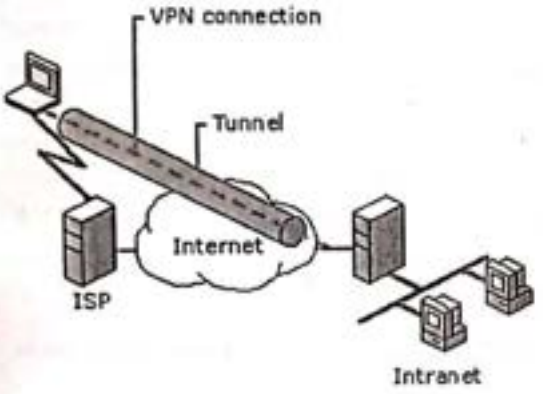
Both private and hybrid networks have a major draw back. Cost Private wide-area networks(WAN's) are expensive. To connect several sits an organization needs several leased lines, which means a high monthly fee. One solution is to use the global Internet for both private and public communications. A technology called virtual private network(VPN) allows organization to use the global Internet for both purposes.

- Remote access VPN connection
- Remote to router VPN connection

Remote access over the Internet

Rather than making a long distance or 01-800 call to a corporate or outsourced network access server (NAS), a remote access client can call a local ISP. By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. Once the VPN connection is created, the remote access client can access the resources of the private intranet.

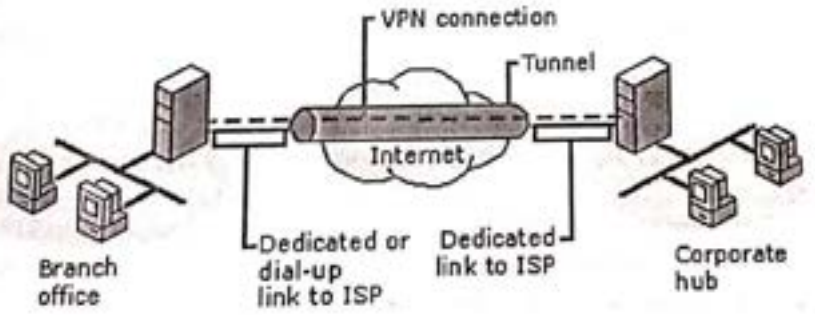
The following illustration shows remote access over the Internet.



Connecting networks over the Internet

When networks are connected over the Internet, a router forwards packets to another router across a VPN connection. This is known as a router-to-router VPN connection. To the routers, the VPN operates as a data-link layer link.

The following illustration shows connecting networks over the Internet.



15.Explain about audio and video compression in multimedia

To send audio or video over the internet compression

Audio compression:

Audio compression can be used for speech or music. For speech we need to compress a 64 kHz devised signals for music we need to compress a 1.411 MHz signal. Two categories of techniques are used for audio compression. They are

1. Predicative encoding

2. Perceptual encoding

1. **Predicative encoding**:

In predicative encoding, the differences between the samples are encoded instead of encoding all the sampled values. This type of compression is normally used for speech. Several standard have been defined such as Gsm (13kbps).G.729(8kbps) and G.723.3

2. **Perceptual encoding**:

The most common compression technique that is used to create cd-quality audio is based on the perceptual encoding. As we mentioned before this type of audio need at least 1.411 mbps, this cannot be sent over the internet without compression.mp3 standard, uses this technique

In frequency masking a loud sound in a frequency range can partially or totally mask a softer sound in another frequency range

In temporarily masking, a loud sound can numb ours ears for a short time ever offer the sound has stopped.

Mp3 uses these two phenomngena, frequency and temporarily masking to compress audio signals' larger numbers of bits are allocated to the frequency ranges that are not masked

Video compression:

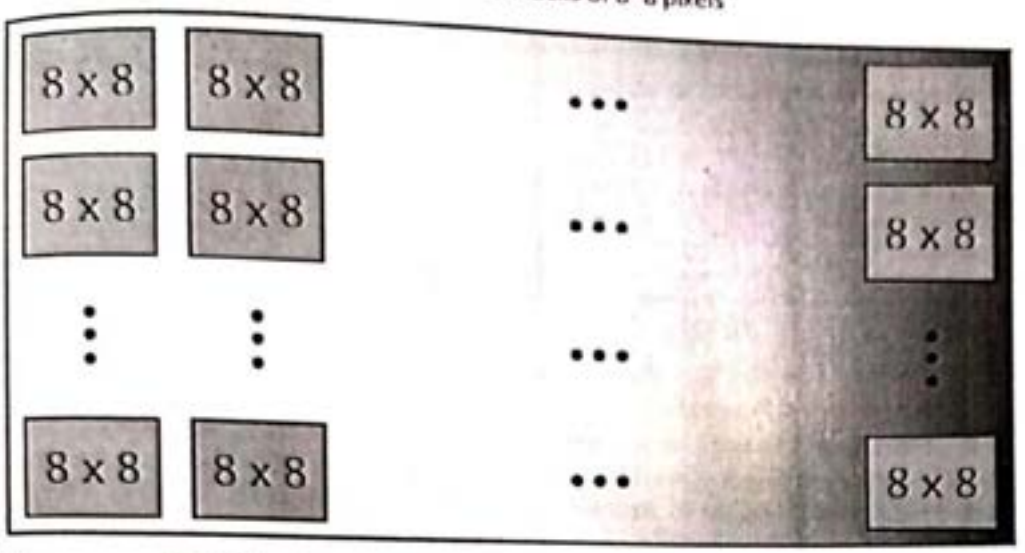
Video is composed of multiple frames. Each frame is one image. We can compress video by first compressing images. Two standards are prevalent in the market.

- Joint Photographic Experts Group (JPEG)
- Moving Picture Experts Group (MPEG)

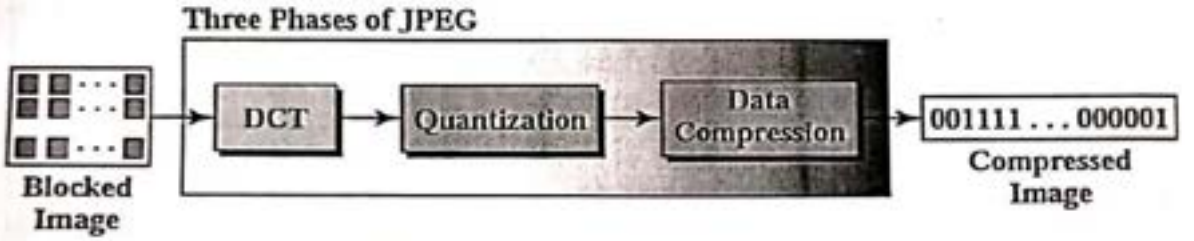
Image compression:JPEG

If the picture is not in color(gray scalar),each pixel can be represented by an 8 bit integer(256levels).if the picture is in color, each pixel can be represented by 24bits(3*8 bits),with each 8 bits representing red,blue,or green(RBG).to simplify the discussion, we concentrate on a gray scale picture

In JPEG, agray scale picture is divided in two blocks of 8*8 pixels



The purpose of dividing the picture into blocks is to decrease the number of calculations because; the number of mathematical operations for each picture is the square of the number of units. The whole idea of JPEG is to change picture into a linear set of numbers reveals the redundancies can then be removed by using one of the text compression methods .A simplified scheme of the process is shown in fig

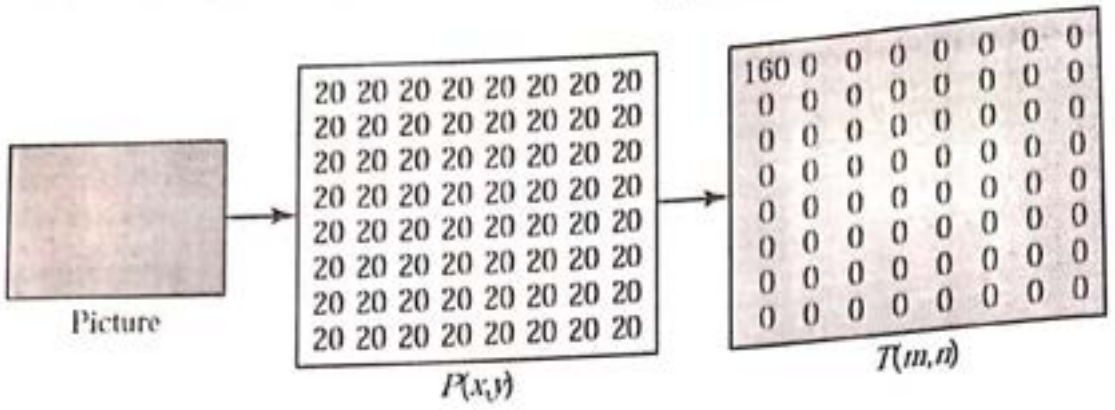


Discrete Cosine Transform (DCT):

Each block of 64pixels goes through a transformation called the "Discrete Cosine transform". The transformation changes the 64 values so that the relative relationships between pixels are kept but the redundancies are revealed. The results of the information for three cases:

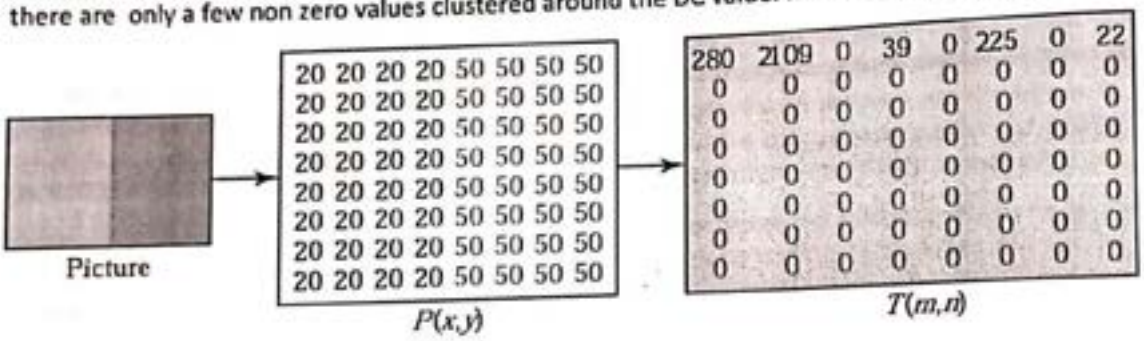
Case 1:

The value of pixel is 20 the information we get non zero value for the first element, the rest of the pixels a value of 0.the value of T (0, 0) is the average values and is called DC value (direct current borrowed from electricity engineering).the rest of the values called AC values in T (m, n) represents changes in the pixel values. But because there are no changes, the rest of the values are 0s



Case 2:

In the second case a block with two uniform sections. There is a sharp change in the values of the pixels(from 20 to 50).when we do the transformations, we get a DC value as well as nonzero AC values, there are only a few non zero values clustered around the DC value. Most of the values are 0



Case 3:

In the third case a block that changes gradually. That is, there is no sharp change between the values of neighboring pixels. When we do the in formations, we get a DC values with many nonzero AC values

Compression:

Compression basically employs redundancy in the data:

- Temporal -- in 1D data, 1D signals, Audio etc.
- Spatial -- correlation between neighboring pixels or data items
- Spectral -- correlation between color or luminescence components. This uses the frequency domain to exploit relationship between frequencies of change in data.
- Psycho-visual -- exploit perceptual properties of the human visual system.

Compression can be categorized in two broad ways:

Lossless Compression

-- Where data is compressed and can be reconstituted (uncompressed) without loss of detail or information. These are referred to as bit-preserving or reversible compression systems also.

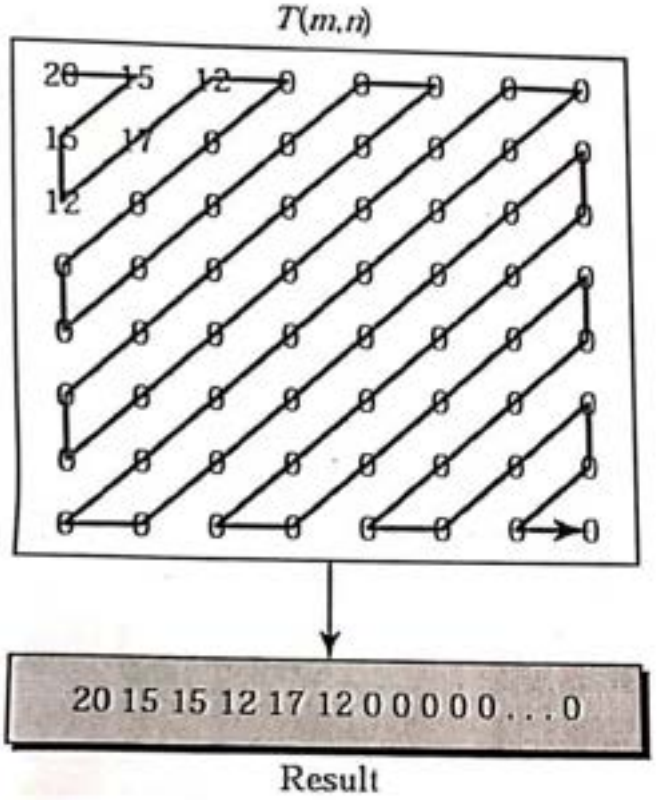
Lossy Compression

-- Where the aim is to obtain the best possible *fidelity* for a given bit-rate or minimizing the bit-rate to achieve a given fidelity measure. Video and audio compression techniques are most suited to this form of compression.

If an image is compressed it clearly needs to uncompressed (decoded) before it can viewed/listened to. Some processing of data may be possible in encoded form however.

Lossless compression frequently involves some form of *entropy encoding* and are based in information theoretic techniques

Lossy compression use source encoding techniques that may involve transform encoding, differential encoding or vector quantization



Video compression MPEG:

The moving picture experts group is used to compress video. In principle a notion picture is a rapid flow a set of frames where each frame is an image. In other words a frame is a spatial combination of frames that are sent one after another.

Spatial compression:

The spatial compression of each frame is done with JPEG each frame is picture that can be independently compressed

Temporal compression:

In temporal compression of each frame is redundant frames are removed. When we receive 50 frames per seconded temporally compress data, the MPEG method first divides frames into three categories I-frames-frames and B-frames

I-frames:

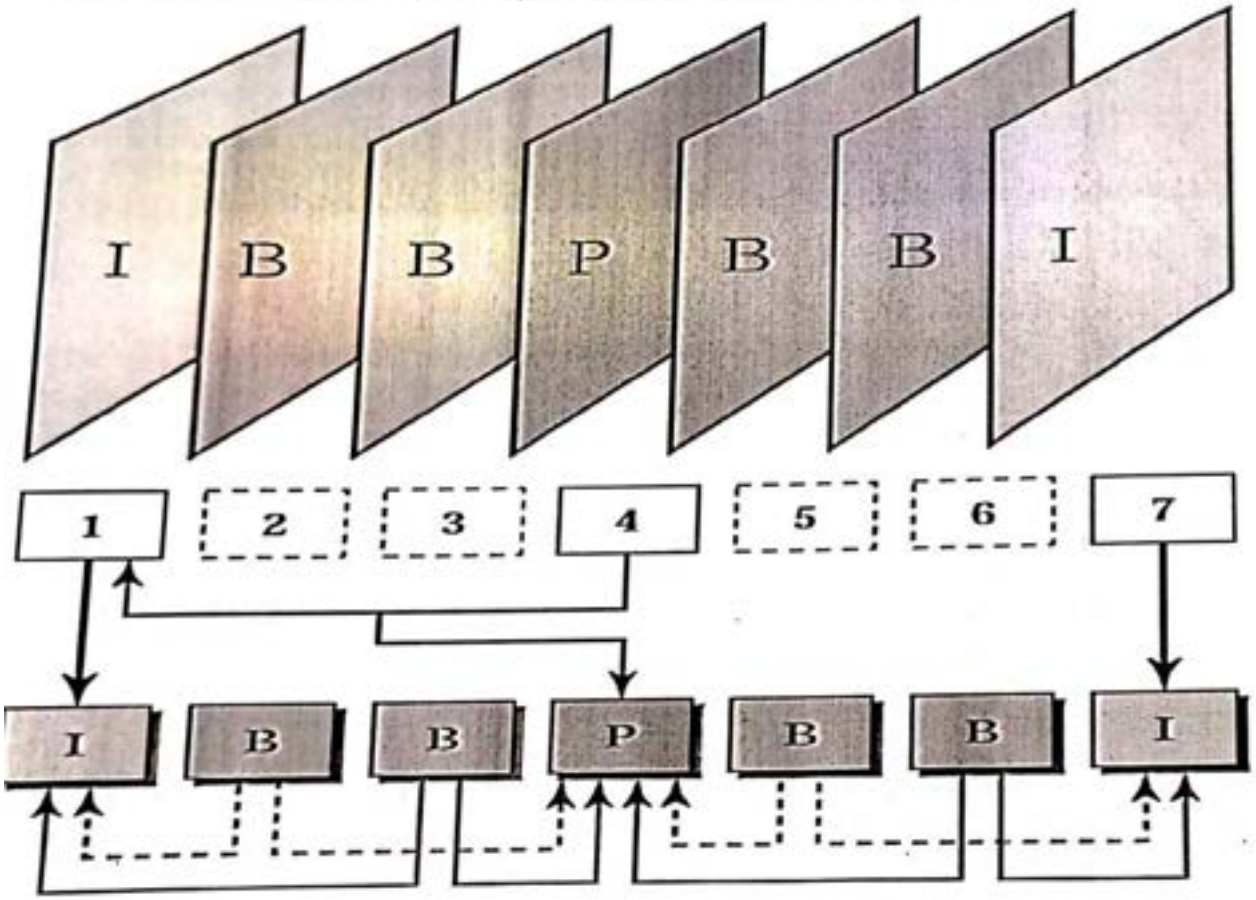
An interceded frame (I-frame)is an independent frame that is not related to any other frame. They are present at regular intervals

P-frames:

A predict frames (p-frame) is related to the preceding I-frame or p-frame. In other words each p-frame contains only the from preceding frame

B-frames:

A bidirectional frame (B-fame) is related to the preceding and following I-frame or p-frame. In the other words each B-frame is relative to the past and the future B-frame is never related to another B-frame



16.LOCAL AREA NETWORKS

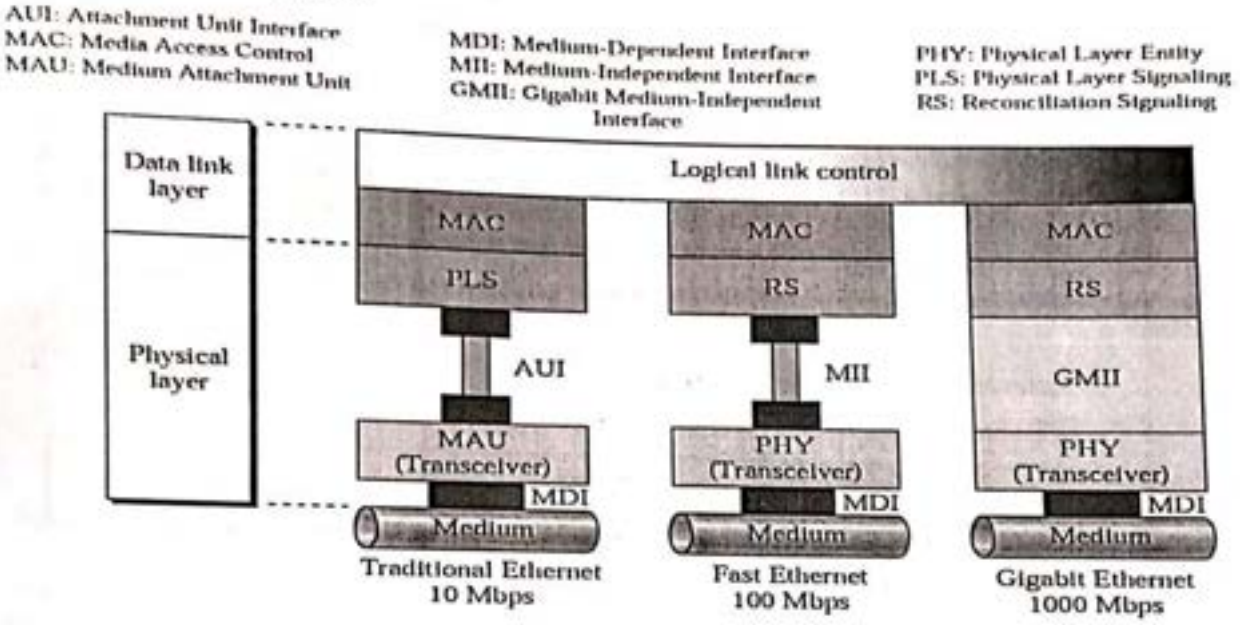
Local-area network (LAN)

Local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network

(WAN) or the Internet.

The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology.

Three generations of Ethernet



Media Access Control (MAC)

In Chapter 12, we discussed multiple access methods including random access, controlled access, and channelization. IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the tokenpassing method for Token Ring and Token Bus LANs. As we discussed in the previous section, part of the framing function is also handled by the MAC layer.

In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

Physical Layer

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Traditional Ethernet, there is a different physical layer specifications for each Ethernet implementations as we will see later.

TRADATIONAL ETHERNET

Tradational Ethernet designed to operate at 10mbps.Acess to the network by a device is through a connection method(CSMA/CD).The media are shared between all station.

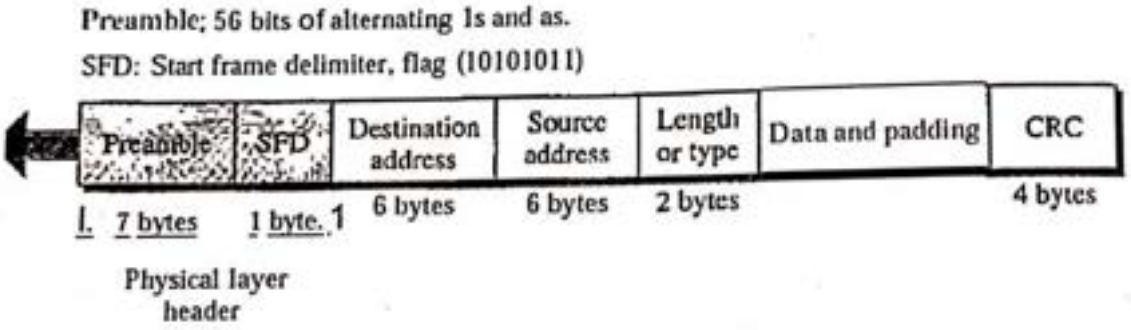
MAC Sublayer

In Traditional Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format ofthe MAC frame is shown in Figure

MACframe



Preamble: The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.

Start frame delimiter (SFD): The second field (I byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

Destination address (DA): The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet. We will discuss addressing shortly.

Source address (SA): The SA field is also 6 bytes and contains the physical address of the sender of the packet. We will discuss addressing shortly.

Length or type: This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE Traditional used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data: This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes, as we will see later.

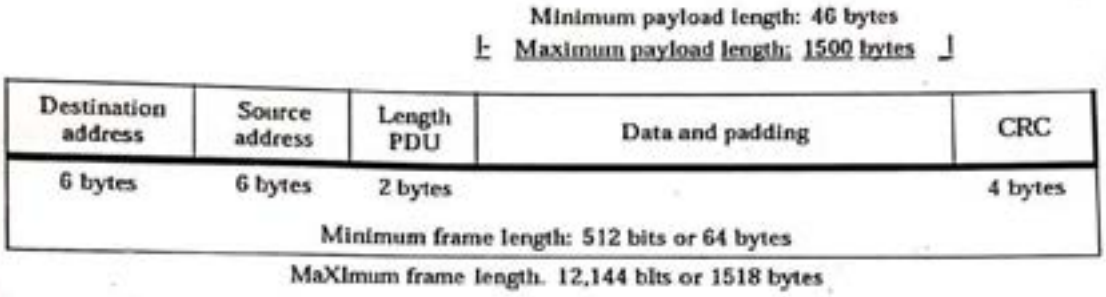
CRC: The last field contains error detection information.

Frame Length:

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame,

as shown in Figure

Minimum and maximum lengths:



The minimum length restriction is required for the correct operation of CSMAICD as we will see shortly. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The Traditional defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons

Addressing:

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in Figure 13.6, the Ethernet address is 6 bytes (48 bits), nonnally written in hexadecimal notation, with a colon between the bytes.

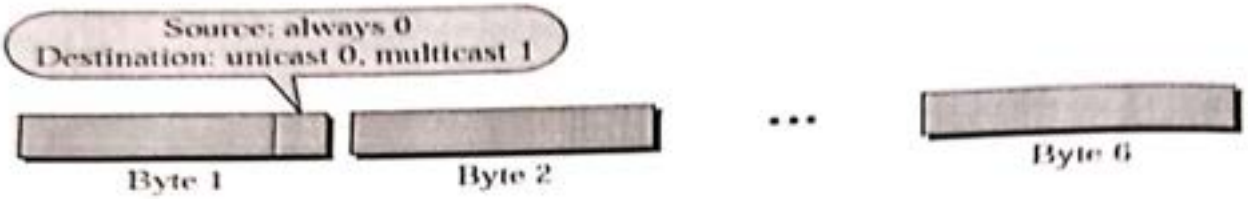
Example of an Ethernet address in hexadecimal notation

06:01 :02:01:2C:4B

6 bytes = 12 hex digits = 48 bits

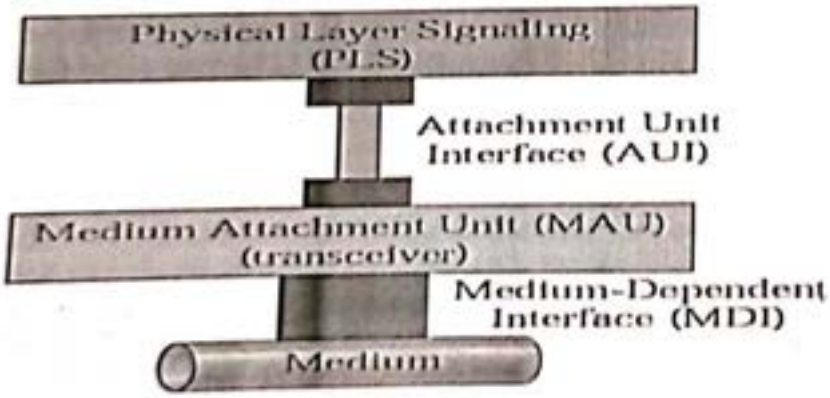
Unicast, Multicast, and Broadcast Addresses A source address is always a unicast address the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. Figure 13.7 shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

Unicast and multicast addresses:



The least significant bit of the first byte defines the type of address. If the bit is 0, the address is unicast; otherwise, it is multicast. A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight Is. The broadcast destination address is a special case of the multicast address in which all bits are Is.

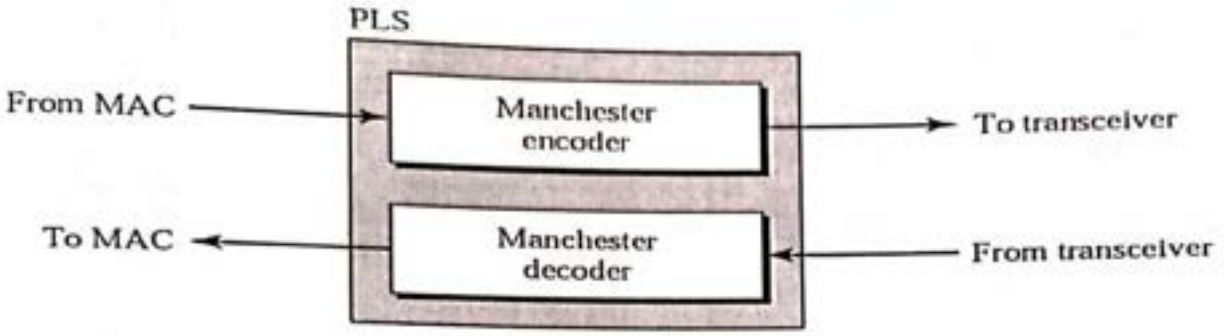
Physical Layer



The Traditional Ethernet defines several physical layer implementations; four of the most common, are shown in Figure

Encoding and Decoding

All Traditional implementations use digital signaling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data. Manchester encoding is self-synchronous, providing a transition at each bit interval. Figure shows the encoding scheme for Traditional Ethernet.



CHANGES IN THE TRADITIONAL:

The 10-Mbps Traditional Ethernet has gone through several changes before moving to the higher data rates. These changes actually opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs. We discuss some of these changes in this section.

Bridged Ethernet

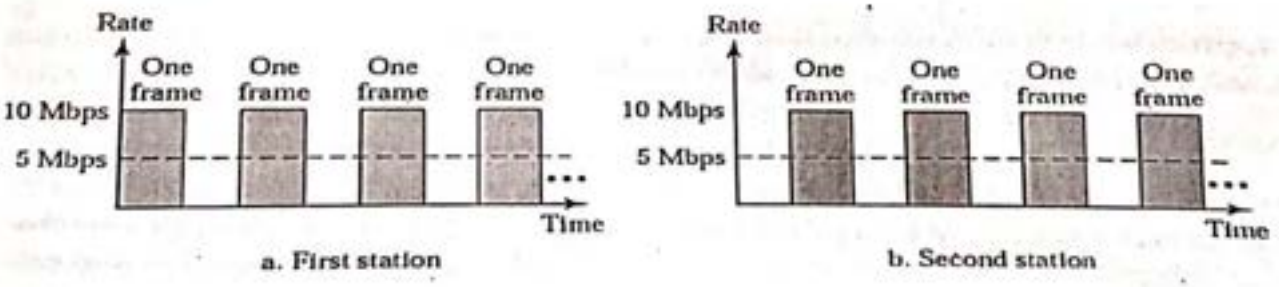
The first step in the Ethernet evolution was the division of a LAN by bridges. Bridges have two effects on an Ethernet LAN: They raise the bandwidth and they separate collision domains.

Raising the Bandwidth:

In an unbridged Ethernet network, the total capacity (10 Mbps) is shared among all stations

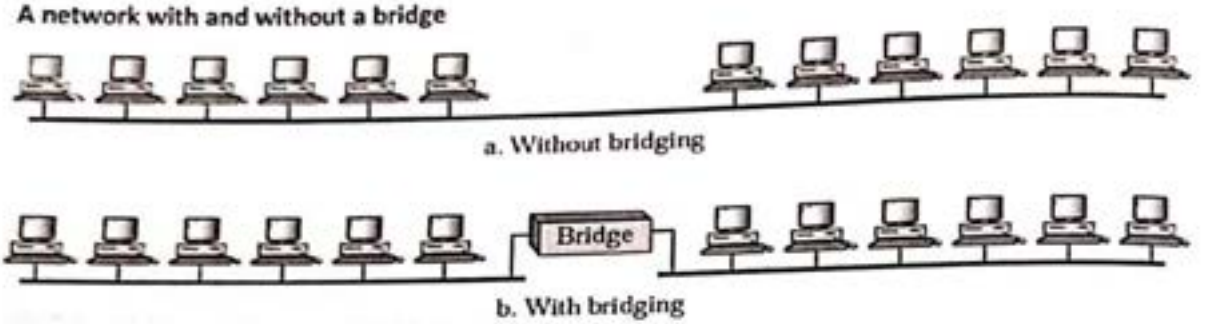
with a frame to send; the stations share the bandwidth of the network. If only one station has frames to send, it benefits from the total capacity (10 Mbps). But if more than one station needs to use the network, the capacity is shared. For example, if two stations have a lot of frames to send, they probably alternate in usage. When one station is sending, the other one refrains from sending. We can say that, in this case, each station on average, sends at a rate of 5 Mbps. Figure shows the situation.

Sharing bandwidth



The bridge, as we will learn in Chapter 15, can help here. A bridge divides the network into two or more networks. Bandwidth-wise, each network is independent. For example, in Figure 13.15, a network with 12 stations is divided into two networks, each with 6 stations. Now each network has a capacity of 10 Mbps. The IO-Mbps capacity in each segment is now shared between 6 stations (actually 7 because the bridge acts as a station in each segment), not 12 stations. In a network with a heavy load, each station theoretically is offered 10/6 Mbps instead of 10/12 Mbps, assuming that the traffic is not going through the bridge. It is obvious that if we further divide the network, we can gain more bandwidth for each segment. For example, if we use a four-port bridge, each station is now offered 10/3 Mbps, which is 4 times more than an unbridged network.

A network with and without a bridge



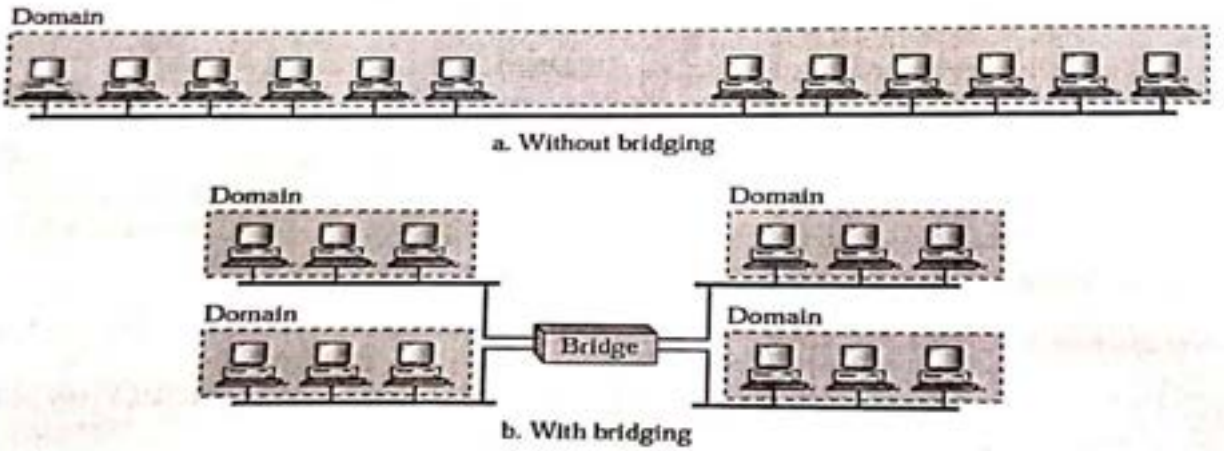
a. Without bridging

b. With bridging

Separating Collision Domains

Another advantage of a bridge is the separation of the collision domain. Figure shows the collision domains for an unbridged and a bridged network. You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously. Without bridging, 12 stations contend for access to the medium; with bridging only 3 stations contend for access to the medium.

Collision domains in an unbridged network and a bridged network



a. Without bridging

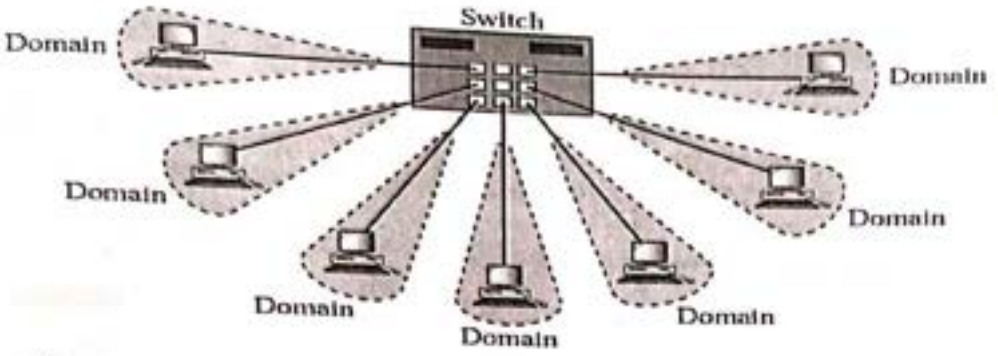
b. With bridging

Switched Ethernet

The idea of a bridged LAN can be extended to a switched LAN. Instead of having two to four networks, why not have N networks, where N is the number of stations on the LAN? In other words, if we can have a multiple-port bridge, why not have an N-port switch? In this way, the bandwidth is shared only between the station and the switch (5 Mbps each). In addition, the collision domain is divided into N

domains. A layer 2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets. Evolution from a bridged Ethernet to a switched Ethernet was a big step that opened the way to an even faster Ethernet, as we will see. Figure shows a switched LAN.

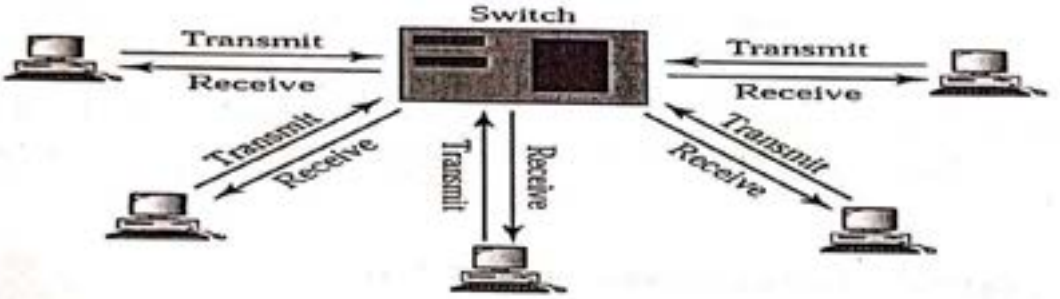
Switched Ethernet



Full-Duplex Ethernet:

One of the limitations of 10Base5 and IOBase2 is that communication is half-duplex (IOBase-T is always full-duplex); a station can either send or receive, but may not do both at the same time. The next step in the evolution was to move from switched Ethernet to full-duplex switched Ethernet. The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps. Figure 13.18 shows a switched Ethernet in full-duplex mode. Note that instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.

Full-duplex switched Ethernet



No Needfor CSMAICD:

In full-duplex switched Ethernet, there is no need for the CSMAICD method. In a fullduplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision. Each link is a point-to-point dedicated path between the station and the switch. There is no longer a need for carrier sensing; there is no longer a need for collision detection. The job of the MAC layer becomes much easier. The carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

MAC Control Layer

Traditional Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control or error control to inform the sender that the frame has arrived at the destination without error. When the receiver receives the frame, it does not send any positive or negative acknowledgment. To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MACsublayer.

FAST ETHERNET:

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Traditional Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Traditional Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sublayer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices, as we saw before: half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full-duplex approach, the connection is made via a switch with buffers at each port. The access method is the same (CSMAICD) for the half-duplex approach; for fullduplex Fast Ethernet, there is no need for CSMAICD. However, the implementations keep CSMA/CD for backward compatibility with Traditional Ethernet.

Autonegotiatioll

A new feature added to Fast Ethernet is called autonegotiation. It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:

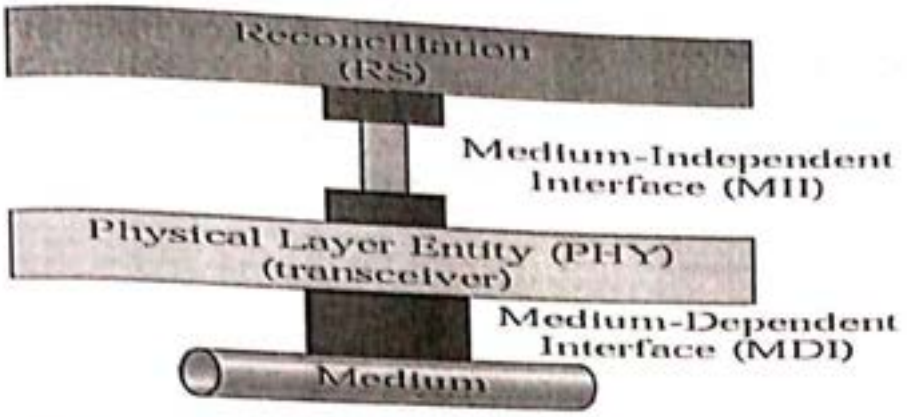
- To allow incompatible devices to connect to one another. For example, a device with

a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).

- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

Physical Layer:

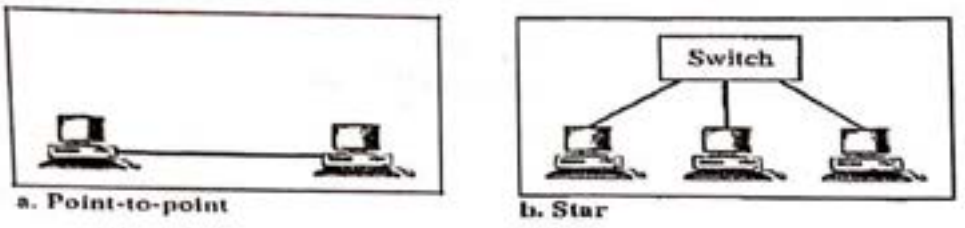
The physical layer in Fast Ethernet is more complicated than the one in Traditional Ethernet. We briefly discuss some features of this layer.



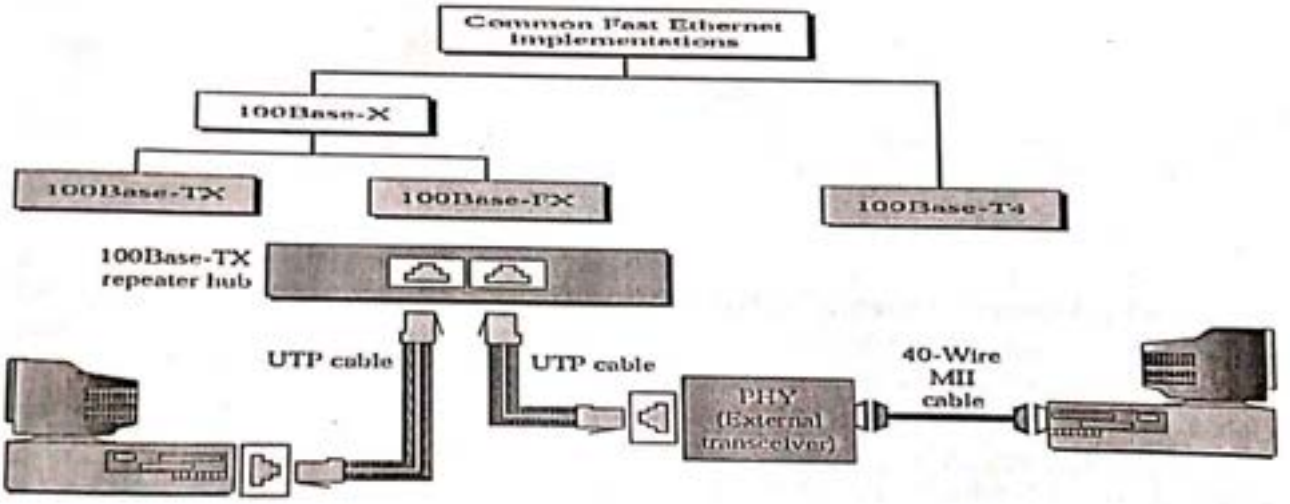
Topology

Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center, as shown in Figure

Fast Ethernet topology



Encoding



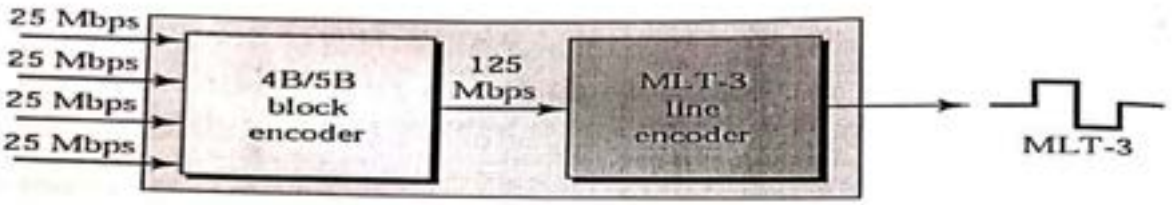
Manchester encoding needs a 200-Mbaud bandwidth for a data rate of 100 Mbps, which makes it unsuitable for a medium such as twisted-pair cable. For this reason, the Fast Ethernet designers sought some alternative encoding/decoding scheme. However, it was found that one scheme would not

perform equally well for all three implementations. Therefore, three different encoding schemes were chosen

Encoding for Fast Ethernet implementation

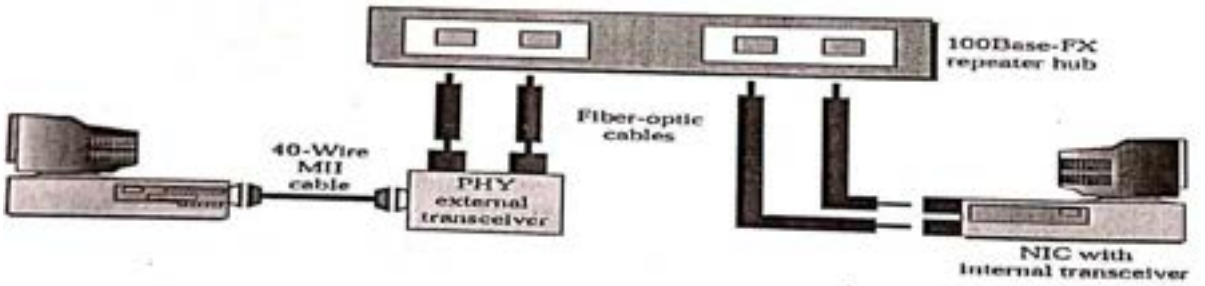
IOOBase-TX uses two pairs oftwisted-pair cable (either category 5 UTP or STP). For this implementation, the MLT-3 scheme was selected since it has good bandwidth performance (see Chapter 4). However, since MLT-3 is not a self-synchronous line coding scheme, 4B/5B block coding is used to provide bit synchronization by preventing the occurrence of a long sequence of Os and Is . This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.

Encoding and decoding in 100Base-TX



IOOBase-FX uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes. The designers of 100Base-FX

100Base-FX implementation



elected the NRZ-I encoding scheme (see Chapter 4) for this implementation. However, NRZ-I has a bit ynchronization problem for long sequences of Os (or Is, based on the encoding), as we saw in Chapter . To overcome this problem, the designers used 4B/5B block encoding as we described for IOOBase-TX. he block encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber- ptic cable.A 1OOBase-TX network can provide a data rate of 100 Mbps, but it requires the use of ategory 5 UTP or STP cable. This is not cost-efficient for buildings that have already been wired for oice-grade twisted-pair (category 3). A new Traditional, called **IOOBase-T4,** was designed to use ategory 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps. coding/decoding in 100Base-T4 is more complicated. As this

implementation uses category 3 UTP, each twisted-pair cannot easily handle more than 25 Mbaud. In this design, one pair switches between sending and receiving. Three pairs of UTP category 3, however, can handle only 75 Mbaud (25 Mbaud) each. We need to use an encoding scheme that converts 100 Mbps to a 75 Mbaud signal.8B/6T satisfies this requirement. In 8B/6T, eight data elements are encoded as six signal elements. This means that 100 Mbps uses only (6/8) x 100 Mbps, or 75 Mbaud.

Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100m	100m	100m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Traditional 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

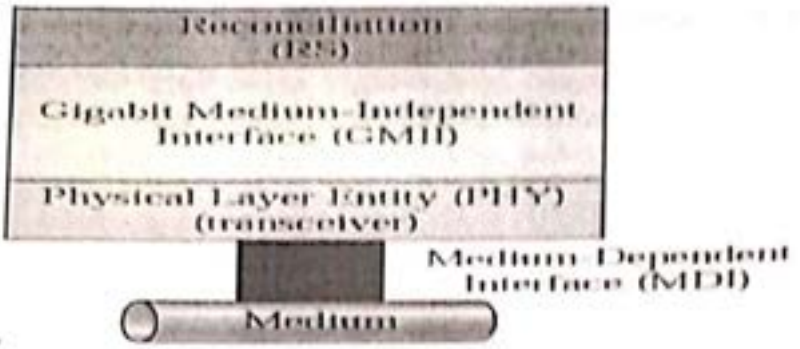
1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Traditional or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

MAC Sublayer

A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate 1 Gbps, this was no longer possible. Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex. Almost all implementations of Gigabit Ethernet follow the full-duplex approach. However, we briefly discuss the half-duplex approach to show that Gigabit Ethernet can be compatible with the previous generations.

Physical Layer

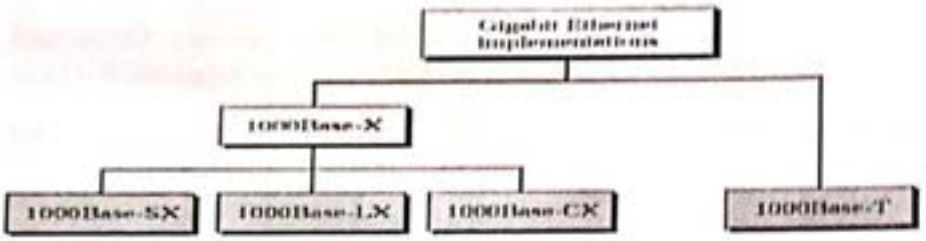
The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: lOGBase-S, lOGBase-L, and lOGBase-E.



Implementation

Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T). In other words, we have four implementations, as shown in Figure 13.23. 1000Base-T was designed in response to those users who

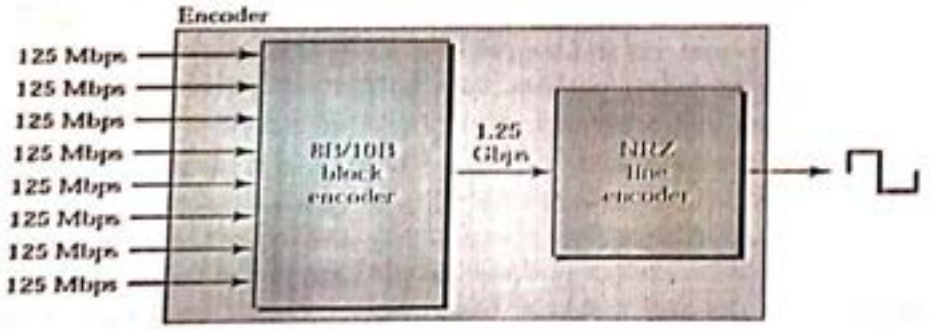
Gigabit Ethernet implementations.



had already installed this wiring for other purposes such as Fast Ethernet or telephone services.

Encoding

Encoding in Gigabit Ethernet Implementations



Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GBaud). The two-wire implementations use an NRZ scheme, but NRZ does not self-synchronize properly. To synchronize bits, particularly at this high data rate, 8B/10B block encoding, discussed in Chapter 4, is used. This block encoding prevents long sequences of 0s or 1s in the stream, but the

resulting stream is 1.25 Gbps. Note that in this implementation, one wire (fiber or STP) is used for sending and one for receiving. In the four-wire implementation it is not possible to have 2 wires for input and 2 for output, because each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP. As a solution, 4D-PAM5 encoding, as discussed in Chapter 4, is used to reduce the bandwidth. Thus, all four wires are involved in both input and output; each

wire carries 250 Mbps, which is in the range for category 5 UTP cable

Ten-Gigabit Ethernet

The IEEE committee created Ten-Gigabit Ethernet and called it Traditional 802.3ae. The

goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Traditional, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN)

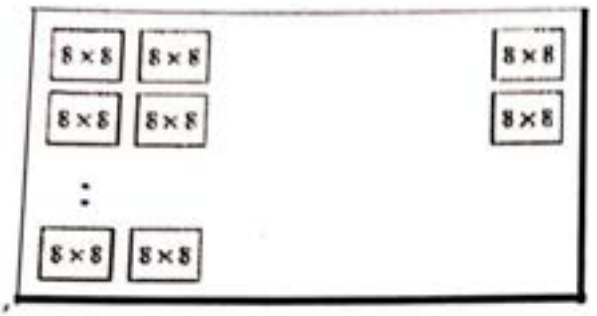
or a wide area network (WAN).

7. Make Ethernet compatible with technologies such as Frame Relay and ATM

17.Image Compression: IPEG

As we discussed previously, if the picture is not in color (gray scale), each pixel can be represented by an 8-bit integer (256 levels). If the picture is in color, each pixel can be represented by 24 bits (3 x 8 bits), with each 8 bits representing red, blue, or green (RBG). To simplify the discussion, we concentrate on a gray scale picture. In JPEG, a gray scale picture is divided into blocks of 8 x 8 pixels

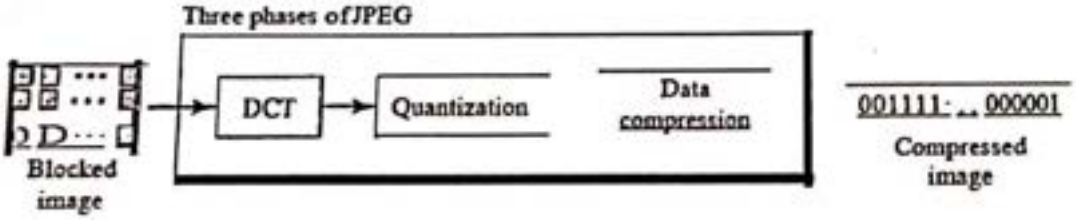
IPEG gray scale



The purpose of dividing the picture into blocks is to decrease the number of calculations because, as you will see shortly, the number of mathematical operations for each picture is the square of the number of units. The whole idea of JPEG is to change the picture into a linear (vector) set of numbers that reveals the redundancies. The redundancies (lack of changes) can then be removed

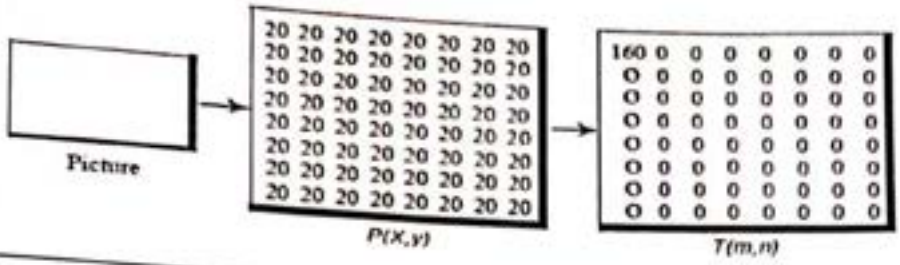
by using one of the text compression methods. A simplified scheme of the process is shown in Figure.

IPEG process



Discrete Cosine Transform (DCT) In this step, each block of 64 pixels goes through a transformation called the discrete cosine transform (DCT). The transformationchanges the 64 values so that the relative relationships between pixels are kept but the redundancies are revealed. We do not give the formula here, but we do show the results of the transformation for three cases.

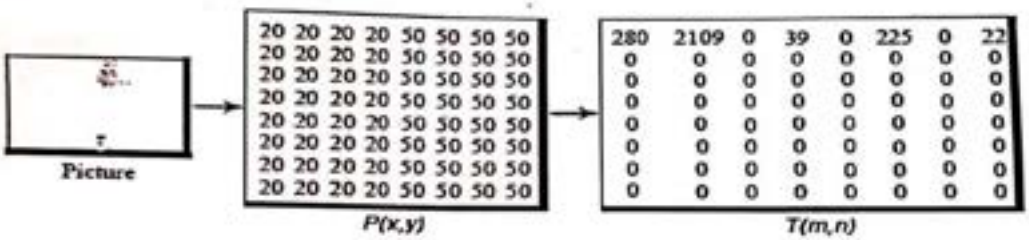
Case 1: In this case, we have a block of uniform gray, and the value of each pixel is 20. When we do the transformations, we get a nonzero value for the first element (upper left comer); the rest of the pixels have a value of O. The value of T(O,O) is the average (multiplied by a constant) of the P(x,y) values and is called the de value (direct current, borrowed from electrical engineering). The rest of the values, called ae values, in T(m,n) represent changes in the pixel values. But because there are no changes, the rest of the values are Os



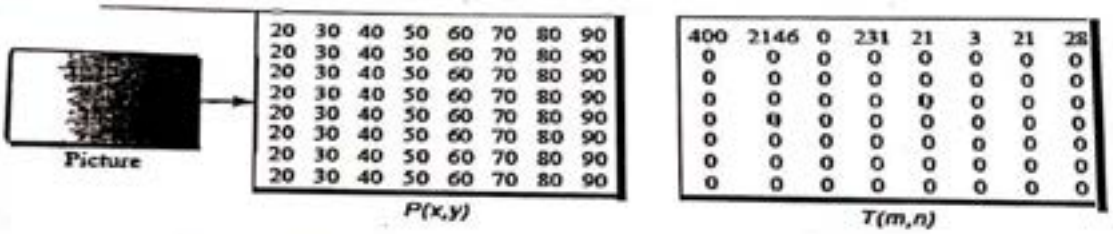
Case 2 In the second case, we have a block with two different uniform gray scale sections. There is a sharp change in the values of the pixels (from 20 to 50). When we do the transformations, we get a dc value as well as nonzero ac values. However, there are only a few nonzero values clustered around the dc value. Most of the values are 0.

Case 3 In the third case, we have a block that changes gradually. That is, there is no sharp change between the values of neighboring pixels. When we do the transformations, we get a de value, with many nonzero ac values also

Case 2: two sections



Case3:Gradientgrayscale

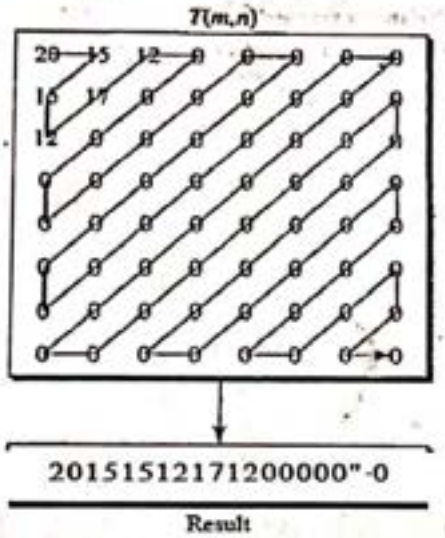


- The transformation creates table T from table P.
- The dc value is the average value (multiplied by a constant) of the pixels.
- The ac values are the changes.
- Lack of changes in neighboring pixels creates Os.

Quantization Mter the Ttable is created, the values are quantized to reduce the number of bits needed for encoding. Previously in quantization, we dropped the fraction from each value and kept the integer part. Here, we divide the number by a constant and then drop the fraction.

This reduces the required number of bits even more. In most implementations, a quantizing table (8 x 8) defines how to quantize each value. The divisor depends on the position of the value in the T table. This is done to optimize the number of bits and the number of Os for each particular application.

Note that the only phase in the process that is not reversible is the quantizing phase. We lose some information here that is not recoverable. As a matter of fact, the only reason that IPEG is called lossy compression is because of this quantization phase.Compression After quantization, the values are read from the table, and redundant are removed. However, to cluster the Os together, the table is read diagonally in a zigzag fashion rather than row by row or column by column. The reason is that if the picture changes smoothly, the bottom right corner of the T table is all Os.



Reading the table