Q-1 What is routing ? How routing works in any network.

- Routing is the act of moving information across an inter-network from a source to a destination.
- Routing is usually performed by a dedicated device called a router.
- Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine.
- Each intermediary computer performs routing by passing along the message to the next computer.
- Part of this process involves analyzing a*routing table* to determine the best path.
- routing occurs at Layer 3 (the network layer). The routing is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted.

How it Work.

- Router is the device which is used to transfer data in computer network.
- In routing process router manages router table.
- The routing table is a table of connections between the target machine address and the node according to which the router must deliver the message. In reality it is enough that the message is delivered to the network that contains the machine, it is therefore not necessary to store the complete IP address of the machine: only the network identifier of the IP address
  (i.e. the network ID) needs to be stored.
- The routing table is therefore a table which contains address pairs:

Destination address	Address of the next router directly accessible	Interface

- Using this table, the router knowing the address of the recipient encapsulated in the message, will be able to find out what interface to send the message on (this comes back to knowing which network interface card to use), and to which router, directly accessible on the network to which this card is connected, to send the datagram.
  This mechanism consisting of only knowing the address of the next link leading to the destination is called next-hop routing.
- However, it may be that the recipient belongs to a non referenced network in the routing table. In this case, the router uses a default router (also called thedefault gateway).
- Here, in a simplified way is what a routing table could look like:

Destination address	Address of the next router directly accessible	Interface
194.56.32.124	131.124.51.108	2
110.78.202.15	131.124.51.108	2
53.114.24.239	194.8.212.6	3
187.218.176.54	129.15.64.87	1

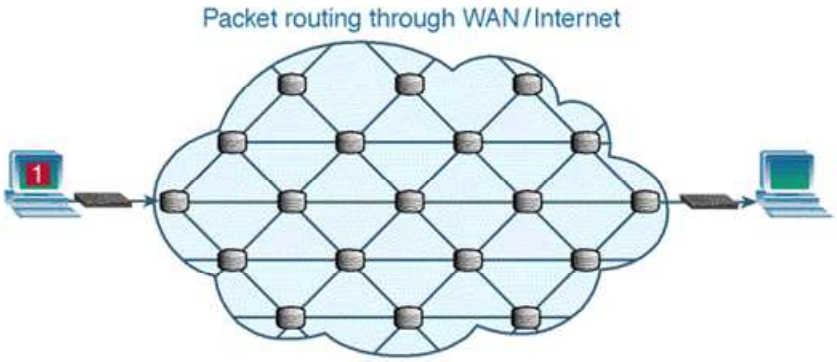
- The message is therefore sent from router to router by successive hops, until the recipient belongs to a network directly connected to a router. This then sends the message directly to the target machine...
- In the case of static routing, it is the administrator who updates the routing table.
  In the case of dynamic routing a protocol called a routing protocol enables the automatic updating of the table so that it contains the optimal route at any time.

Q-2 Difference between circuit switching and packet switching ?

- Packet-switched and circuit-switched networks use two different technologies for sending messages and data from one point to another.
- Each has its advantages and disadvantages depending on what you are trying to do.

Packet Switching

- In packet-based networks, the message gets broken into small data packets.
- These packets are sent out from the computer and they travel around the network seeking out the most efficient route to travel as circuits become available.
- This does not necessarily mean that they seek out the shortest route.
- Each packet may go a different route from the others.
- Each packet is sent with a 'header address' which tells it where its final



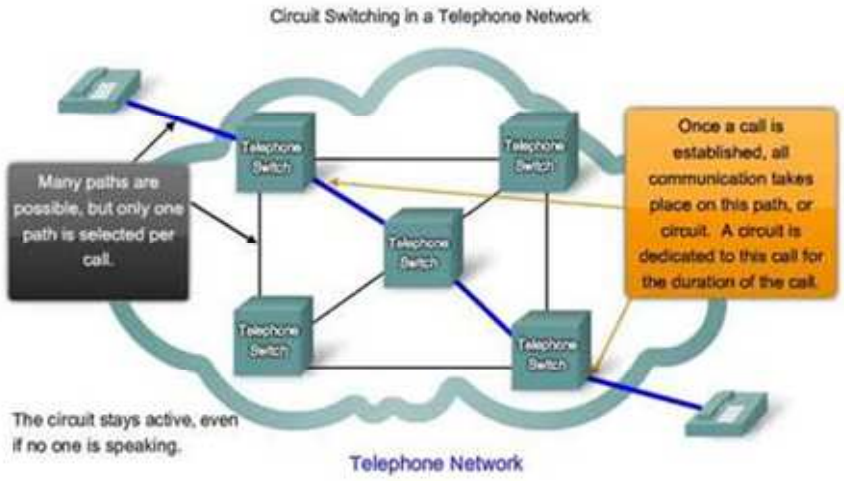
destination is, so it knows where to go.

- The header address also describes the sequence for reassembly at the destination computer so that the packets are put back into the correct order.
- One packet also contains details of how many packets should be arriving so that the recipient computer knows if one packet has failed to turn up.
- If a packet fails to arrive, the recipient computer sends a message back to the computer which originally sent the data, asking for the missing packet to be resent.
  - **Advantages**
    - » Security
    - » Bandwidth used to full potential
    - » Devices of different speeds can communicate
    - » Not affected by line failure (redirects signal)
    - » Availability – no waiting for a direct connection to become available
    - » During a crisis or disaster, when the public telephone network might stop working, e-mails and texts can still be sent via packet switching

- **Disadvantages**
  - » Under heavy use there can be a delay
  - » Data packets can get lost or become corrupted
  - » Protocols are needed for a reliable transfer
  - » Not so good for some types data streams (e.g. real-time video streams can lose frames due to the way packets arrive out of sequence)

Circuit Switching

- Circuit switching was designed in 1878 in order to send telephone calls down a dedicated channel.
- This channel remains open and in use throughout the whole call and cannot be used by any other data or phone calls.



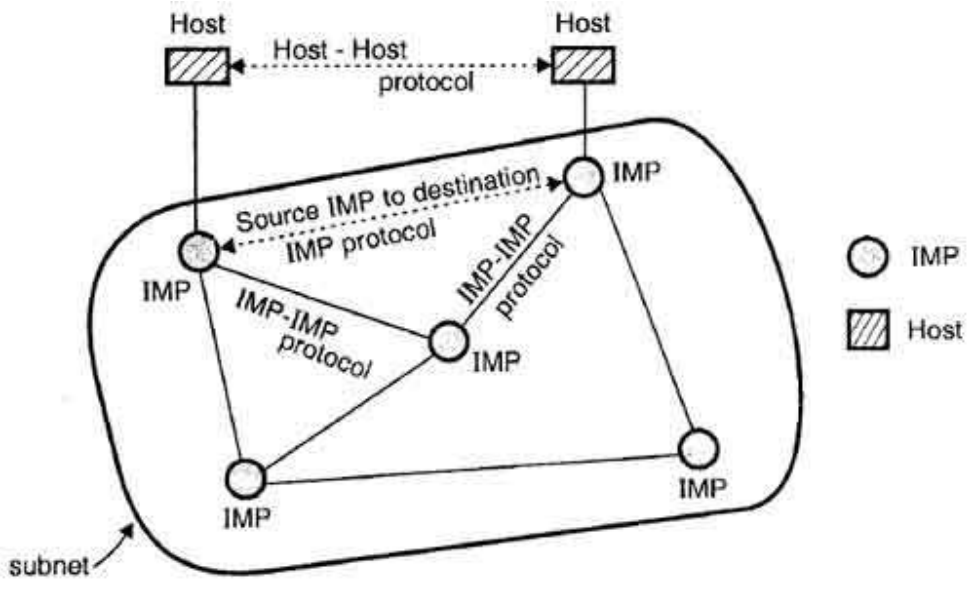
- There are three phases in circuit switching:
  - o Establish
  - o Transfer
  - o Disconnect
- The telephone message is sent all together; it is not broken up.
- The message arrives in the same order that it was originally sent.
- In modern circuit-switched networks, electronic signals pass through several switches before a connection is established.
- During a call no other network traffic can use those switches.
- The resources remain dedicated to the circuit during the entire data transfer and the entire message follows the same path.
- Circuit switching can be analog or digital.
- With the expanded use of the Internet for voice and video, analysts predict a gradual shift away from circuit-switched networks.
- A circuit-switched network is excellent for data that needs a constant link from end-to-end, for example, real-time video.
- **Advantages**
  - o Circuit is dedicated to the call – no interference, no sharing
  - o Guaranteed the full bandwidth for the duration of the call
  - o Guaranteed quality of service

Disadvantages

- Inefficient – the equipment may be unused for a lot of the call; if no data is being sent, the dedicated line still remains open.
- It takes a relatively long time to set up the circuit.
- During a crisis or disaster, the network may become unstable or unavailable.
- It was primarily developed for voice traffic rather than data traffic.

Q-3 Write detailed note on Arpanet.

- ARPANET was the network that became the basis for the Internet. Based on a concept first published in 1967
- ARPANET was built to accommodate research equipment on packet switching technology and to allow resource sharing for the Department of Defense's contractors. The network interconnected research centers, some military bases and government locations. It soon became popular with researchers for collaboration through electronic mail and other services.
- It is basically a WAN. It was developed by the ARPA (Advanced Research Project Agency) in 1968 which is the research arm of 000.
- ARPANET was designed to service even a nuclear attack.
- Before ARPANET, the networks were basically the telephone networks which operated on the circuit switching principle.
- But this network was too vulnerable, because the loss of even one line or switch would terminate all the conversations.
- ARPANET used the concept of packet switching network consisting of subnet and host computers.
- The subnet was a datagram subnet and each subnet consists of minicomputers called IMPs (Interface Message Processors).
- Each node of the network used to have an IMP and a host connected by a short wire.
- The host could send messages of upto 8063 bits to its IMP which would break them into packets and forward them independently toward the destination.
- The subnet was the first electronic store-and-forward type packet switched network. So each packet was stored before it was forwarded.

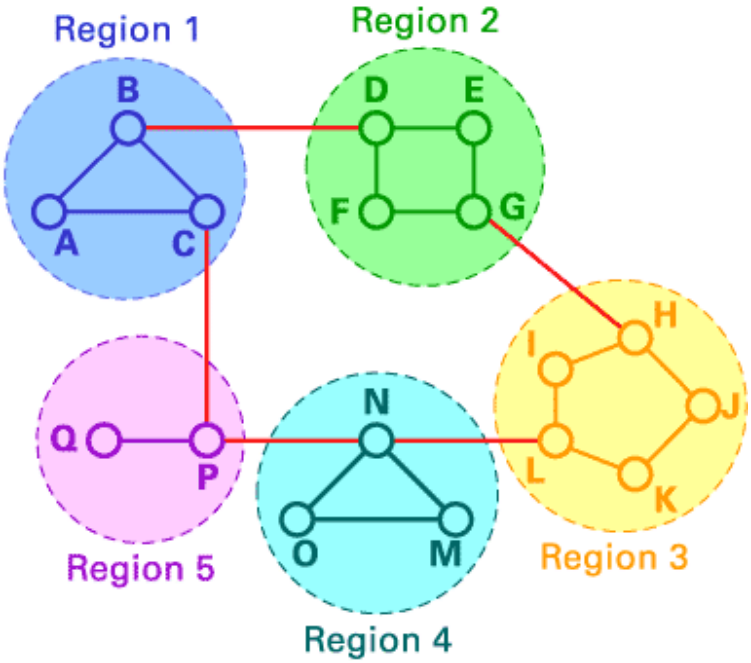


ARPANET

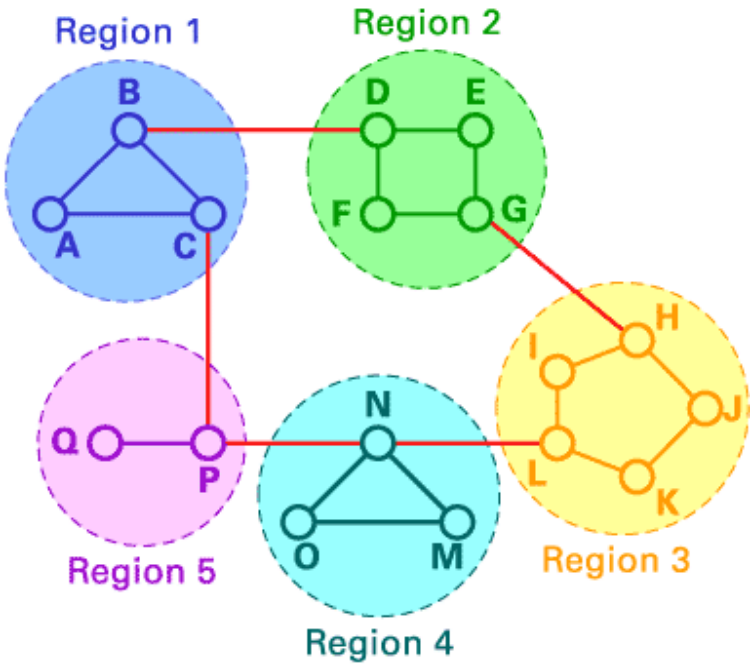
- The software for ARPANET was split into two parts namely subnet and host.
- In 1974 the TCP/IP model and protocol were invented specifically to handle communication over internetwork because more and more networks were getting connected to ARPANET.
- The TCP/IP made the connection of LANs to ARPANET easy.
- During 1980s so many LANs were connected to ARPANET that finding hosts became increasingly difficult and expensive.
- So DNS (Domain Naming System) was created for organizing machines into domains and map host names onto IP address.
- In 1983 the management of ARPANET was handed over to the Defense Communications Agency (DCA) which separated the military portion into a separate MILNET.
- By 1990 the ARPANET was shut down and dismantled, however MILNET continues to operate.

Q-4 Explain Hierarchical routing.

- In hierarchical routing, routers are classified in groups known as**regions**. 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 (see below).



- 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 can be summarized, so network efficiency improves. The above example shows two-level hierarchical routing. We can also use three- or four-level hierarchical routing.



- 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 or routers. Hierarchical routing is widely used in Internet routing and makes use of several routing protocols.

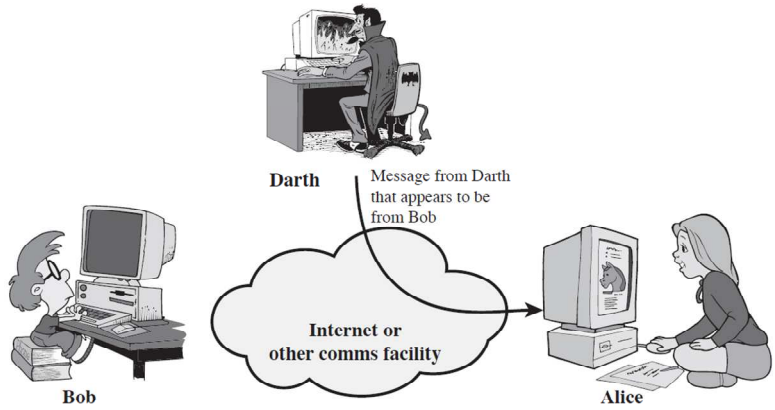
Q- 5 What is active and passive attack?

Active attacks

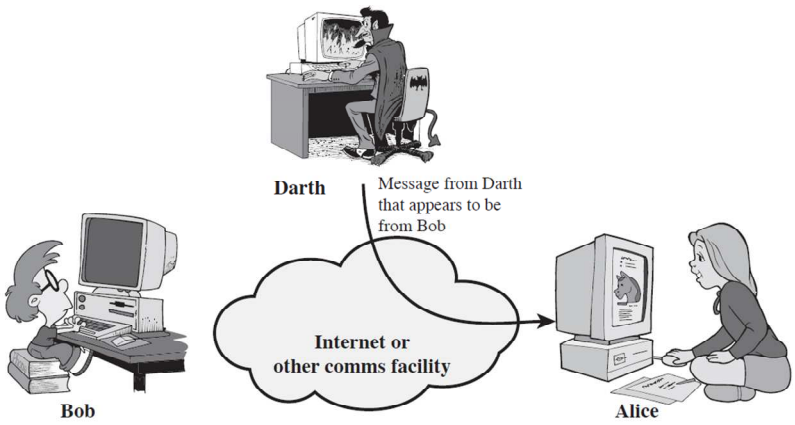
- An active attack is one in which an unauthorised change of the system is attempted. This could include, for example, the modification of transmitted or stored data, or the creation of new data streams. Figure 2(see Section 3.2) shows four sub-categories here: masquerade or fabrication, message replay, message modification and denial of service or interruption of availability.

Masquerade attacks.

- as the name suggests, relate to an entity (usually a computer or a person) taking on a false identity in order to acquire or modify information, and in effect achieve an unwarranted privilege status. Masquerade attacks can also incorporate other categories.

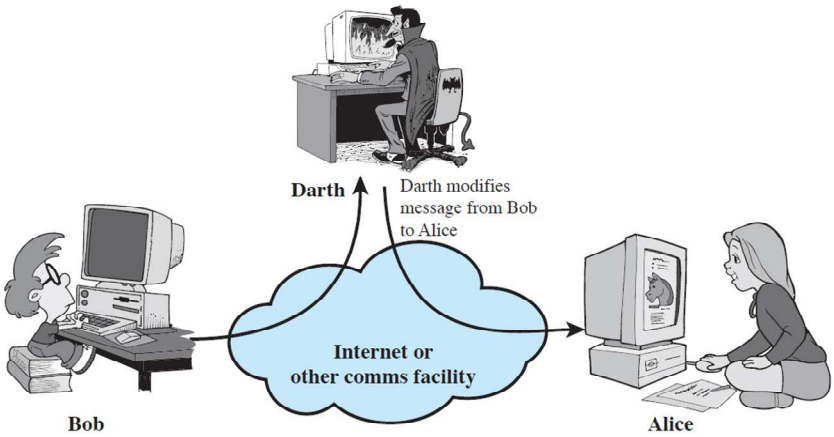


Message replay



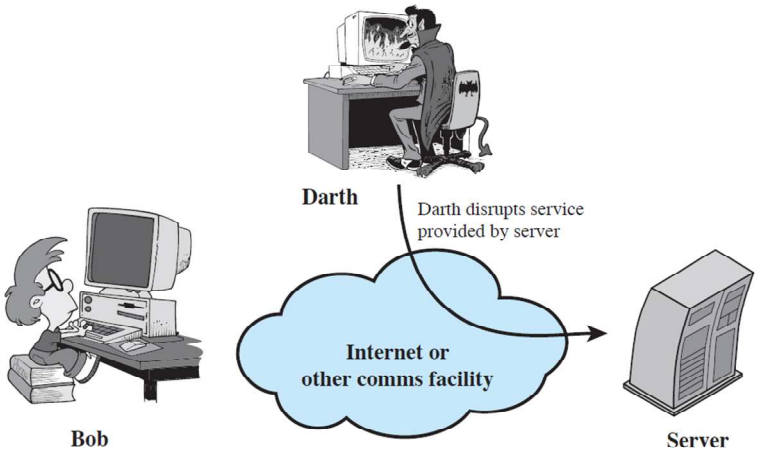
- It involves the re-use of captured data at a later time than originally intended in order to repeat some action of benefit to the attacker: for example, the capture and replay of an instruction to transfer funds from a bank account into one under the control of an attacker. This could be foiled by confirmation of the freshness of a message.

Message modification



- It involve modifying a packet header address for the purpose of directing it to an unintended destination or modifying the user data.

Denial-of-service attacks

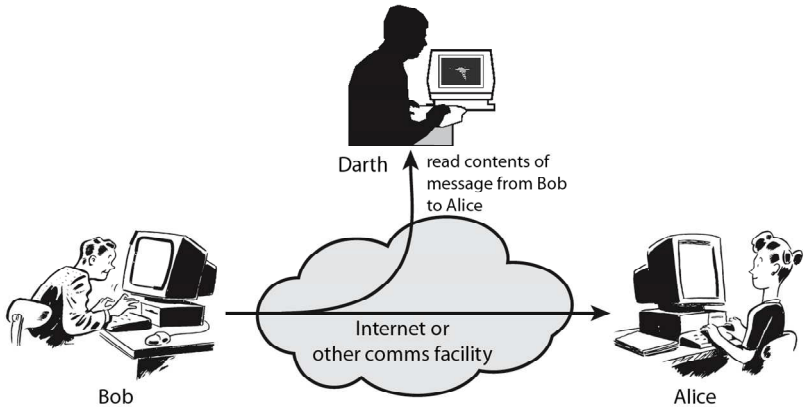


- It prevent the normal use or management of communication services, and may take the form of either a targeted attack on a particular service or a broad, incapacitating attack. For example, a network may be flooded with messages that cause a degradation of service or possibly a complete collapse if a server shuts down under abnormal loading. Another example is rapid and repeated requests to a web server, which bar legitimate access to others. Denial-of-service attacks are frequently reported for internet-connected services.

Passive Attack

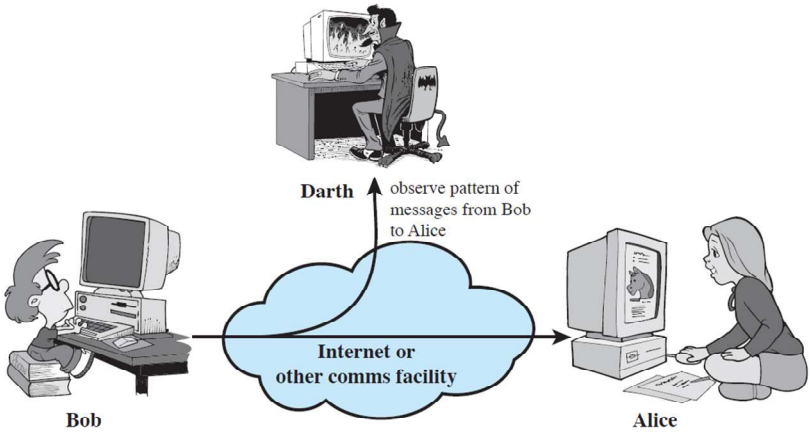
- Passive attacks do not affect system resources. In this type of attack intruder's aim is to Eavesdropping, and monitoring the messages which transfer from source to destination.
- There are two type of passive attacks.
  - **Release of message contents**
  - **Traffic analysis**

Release of message content.



- Form the above figure we can see that Darth read the content of the message which are transfer from Bob to Alice.

Traffic Analysis



- From the figure we can see that Darth analysis the traffic between Bob to Alice. And from that he observe the pattern of the messages.

- Passive attacks are very difficult to detect
  - **Message transmission apparently normal**
    - **No alteration of the data**
  - **Emphasis on prevention rather than detection**
    - **By means of encryption**

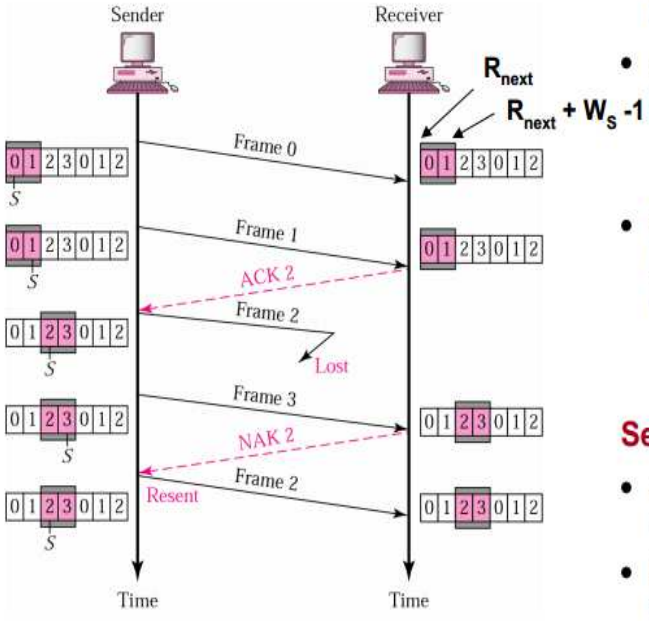
Q-6 Explain selective repeat AQR.

- While transferring the data in a channel there are high error rates. AQR protocol is used to overcome this problem.
- There are some limitation of Go-Back-N protocol. Is is not suitable protocol while the channel has a lot's of traffic to pass.
- To overcome this problem selective repeat AQR is Introduced with two extra features.
- Selective Repeat ARQ overcomes the limitations of Go-Back-N by adding 2 new features

(1) receiver window > 1 frame , so that out-of-order but error-free frames can be accepted

(2) retransmission mechanism is modified –only individual frames are retransmitted.

Selective Repeat AQR Operation.



Receiver:

- **window advances whenever next in-order frame arrives**
- **out-of-order frames are accepted only if their sequence numbers satisfy**

$$R_{next} < R_{frame} < R_{next} + W_s$$

- **a negative ACK (NAK) with sequence number R_{next} is sent whenever an out-of-sequence frame is observed**

Sender:

- **window advances whenever an ACK arrives**
- **if a timer expires, the corresponding frame is resent, and the timer is reset**
- **whenever a NAK arrives, R_{next} frame is resent**

Q-7 Explain internet bird's eye view

- A bird's-eye view is an elevated view of an object from above, with a perspective as though the observer were a bird, often used in the making of blueprints, floor plans and maps.
- It can be an aerial photograph, but also a drawing. Before manned flight was common, the term "bird's eye" was used to distinguish views drawn from direct observation at high locations (for example a mountain or tower), from those constructed from an imagined (bird's) perspectives. Bird's eye views as a genre have existed since classical times. The last great flourishing of them was in the mid-to-late 19th century, when bird's eye view prints were popular in the United States and Europe.
- The terms aerial view and aerial viewpoint are also sometimes used synonymous with bird's-eye view. The term *aerial view* can refer to any view from a great height, even at a wide angle, as for example when looking sideways from an airplane window or from a mountain top. Overhead view is fairly synonymous with*bird's-eye view* but tends to imply a less lofty vantage point than the latter term. For example, in computer and video games, an "overhead view" of a character or situation often places the vantage point only a few feet (a meter or two) above human height. See top-down perspective.
- Recent technological and networking developments have made satellite images more accessible. Microsoft Bing Maps offers direct overhead satellite photos of the entire planet but also offers a feature named Bird's eye view in some locations. The *Bird's Eye* photos are angled at 40 degrees rather than being straight down. Satellite imaging programs and photos have been described as offering a viewer the opportunity to "fly over" and observe the world from this specific angle.