Computer Networks

Unit 6

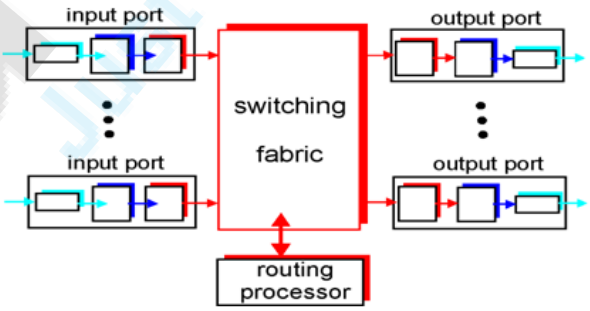
1. What is a router and explain the internal working of router

Router Architecture Overview

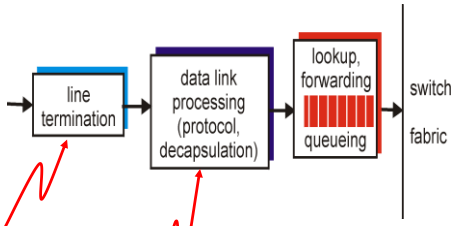
- Routing is the act of moving information across an internetwork from a source to a destination.
- Routing Algorithm is the part of n/w layer and the s/w responsible for deciding on which output line an incoming packet should be transmitted on.

Two key router functions:

- Run routing algorithms/protocol
- Forwarding datagram from incoming to outgoing link



Input Port Functions



Physical layer: bit-level reception

Data link layer: e.g., Ethernet

- It performs the physical layer functionality of terminating an incoming physical link to a router.
- It performs the data link layer functionality by decapsulate the protocols.

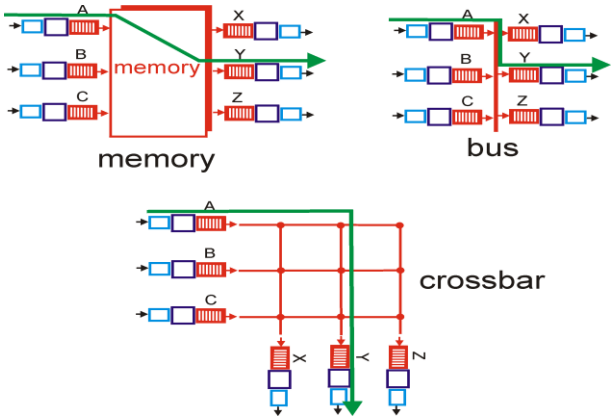
• The lookup/forwarding function contains the routing table , depending on that the routing processor determines the output ports.

•The routing table is locally stored at each input port and updated by the router.

Switching fabrics

- Packets are actually switched from an input port to an output port through switching fabrics
- Three types
  - switching via memory
  - switching via bus
  - switching via interconnection network

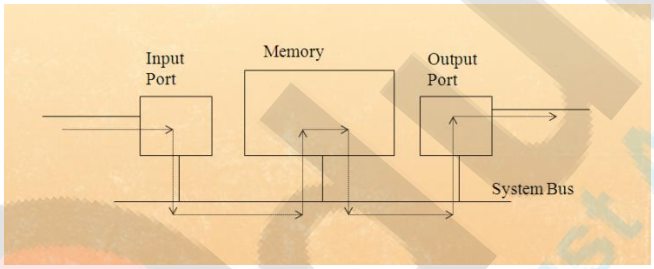
Three types of switching fabrics



Switching Via Memory

First generation routers:

- traditional computers with switching under direct control of CPU
- packet copied to system's memory
- speed limited by memory bandwidth



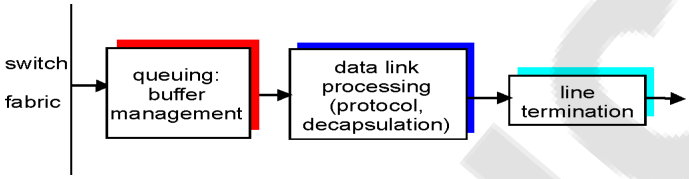
Switching Via a Bus

- datagram from input port memory
- to output port memory via a shared bus
- bus contention: switching speed limited by bus bandwidth
- 1 Gbps bus, Cisco 1900: sufficient speed for access and enterprise routers

Switching Via an Interconnection Network

- overcome bandwidth limitations of a single shared bus
- A cross bar switch is an interconnection network consisting of 2n buses that connects n input ports to n output ports
- A packet arriving at an input port travels along the horizontal bus attached until it intersects with the vertical bus leading to the desired output port
- If the vertical bus is busy, packet is blocked and queued at the input port

Output Ports



- Takes the packets that have been stored in the output ports memory and transmit them over the outgoing link.
- Data link protocol processing and line termination are the send side link and physical layer functionality
- Queuing and buffer management is needed when the switch fabric delivers packets to the output port at the rate that exceeds output link rate

Router Processor

- Router processor executes routing protocols.
- It maintains routing information and forwarding table.

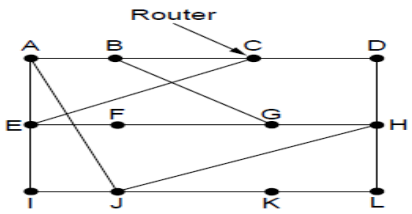
- It manages the network inside the router.

2. Explain Bellman-Ford Algorithm

<u>Distance Vector Routing</u>

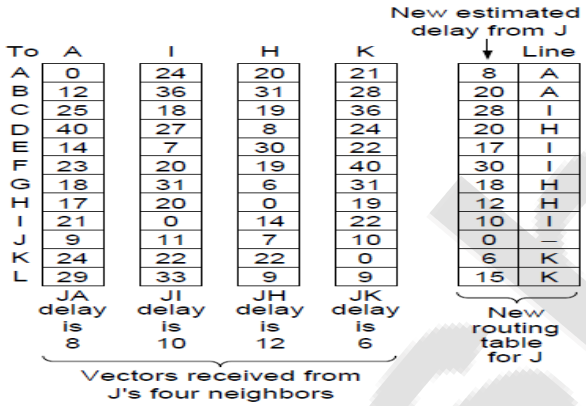
- Developed by Bellman-Ford (1957), Ford-Fulkerson (1962).
- It is also called RIP.
- The Bellman-Ford distance-vector routing algorithm is used by routers on internet.
- It's work to exchange routing information about the current status of the network and how to route packets to their destinations
- Each router keeps routing table (or routing vector) which has one entry for all other routers in the network.
- The entry contains two parts
  - preferred outgoing line
  - Estimate of time or distance to destination
- Routing tables are updated by exchanging routing information with neighbors.
- Each router is assumed to know the distance to its neighbors.
- If the metric is hops , the distance is just one hop
- To know the delay metric, the router sends an ECHO packet to its neighboring router; the neighbor just time stamps the packet and sends it back.
- If the metric used is the number of packets queued along the path then the router examines each queue.

Distance Vector Routing (Bellman-Ford Algorithm)



Adaptive Algorithm

(a)

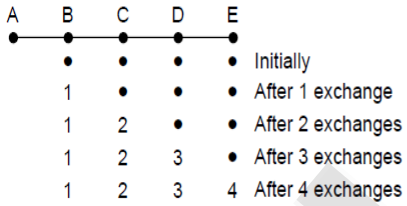


(b)

(a) A network.
(b) Input from A, I, H, K, and the new routing table for J.

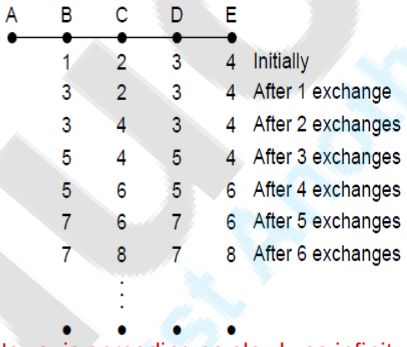
The Count-to-Infinity Problem

Distance vector algorithm works fine in theory but has serious problem in practice as follow:



Good News is spreading at the rate of one hop per exchanges

(a)



Bad News is spreading as slowly as infinity

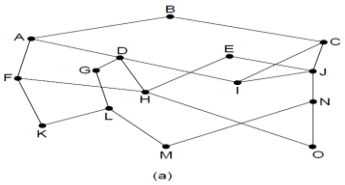
(b)

The count-to-infinity problem

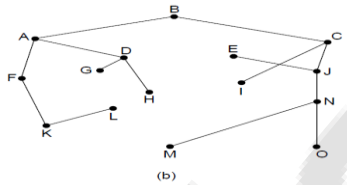
3. What is optimality principle and explain Link State Algorithm

Principle of Optimality:

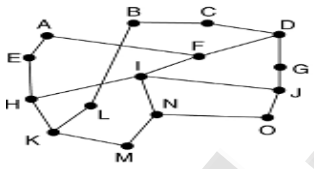
- If router J on optimal path from router I to K then optimal path from J to K also on same route!
- Set of all optimal routes from all sources to a given destination form a tree and such tree is called a sink tree.



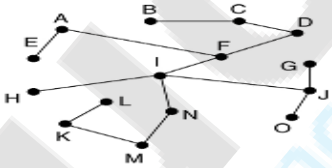
(a) A network



(b) A sink tree for router B.



(a)
Subnet



(b)
Sink tree for router I

- Goal of routing algorithm find sink tree, it does not contain any loops, so each packet will be delivered within a finite and bounded number of hops.

Link State Routing

- Distance vector routing was used in ARPANET until 1979
- In 1979 it was replaced by link state routing
- Problems with distance vector
  - Line bandwidth is not considered

- Converging time is too long

The idea says in five parts as:

- Discover its neighbors and learn their network addresses
- measure the delay or cost to each of its neighbors
- Construct a packet telling all it has just learned
- Send this packet to all other routers.
- Compute the shortest path to every other router.

Finding Neighbors

- When router is booted, its first task is to find who its neighbors are.
- By sending single-hop “hello” packets.
- The router on the other end is expected to send back a reply with its IP address.

Measuring Line Cost:

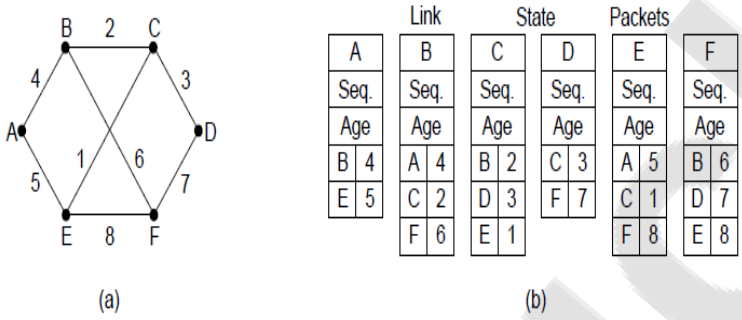
- Each router should have an estimate of delay to each of its neighbors
- Router sends “echo” packet to its neighbors and measure Round Trip Time /2, to calculate line cost.
- For better results, test can be conducted several times and the average is used.

Building Link State Packets

- After collecting information, a packet containing these information's are build by router

- Packet contains following details
  - Sender identity.
  - Sequence number.
  - AGE(when age hit zero , packet is discarded)
  - List of neighbor and delay to that neighbor

Building Link State Packets



(a) A network. (b) The link state packets for this network.

When to build packets?

- periodic updates;
- Whenever some significant event is detected, e.g., link goes down.

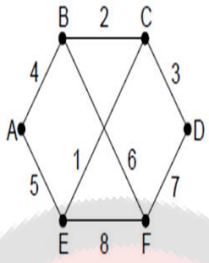
Distributing the packets

- Uses flooding for distribution

- When LSP is received:
  - Check sequence number.
  - If higher than current sequence number, keep it and flood it; otherwise, discard it.
  - Periodically decrement age.
    - When age=0, means LSP discard.
    - Keep age – checking mechanism to avoid duplicates.
    - To protect against errors all LSPs are acknowledged.

Distributing the Link State Packets

The data structure used by router B for the subnet



Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

B's LSP buffer: each row corresponds to a recently LSP that hasn't been processed yet.

Computing Routes

- Routers have global view of network.
  - They receive updates from all other routers with their cost to their neighbors.
  - Build network graph.

- Use Dijkstra's shortest-path algorithm to compute shortest paths to all other nodes.

Link State Routing: Problems

- Scalability: The primary disadvantage of link-state routing is that it requires more storage and more computing to run than distance-vector routing.
  - Storage: kn, where n is number of routers and k is number of neighbors.
  - Computation time.

4. Explain NAT in detail

NAT: Network Address Translation

- It enables a user to have a large set of addresses internally and one address or a small set of address externally.
- It provides a solution for shortage of addresses
- NAT connects two networks and translates the private (inside local) addresses into public addresses (inside global) before packets are forwarded to another network.
- In other word Address translation allows to translate internal private addresses to public addresses before these packets leave internal network.

Situation where you should use NAT

- ISP did not provide sufficient public IP address
- To hide internal IP address space from outside
- To assign the same IP address to multiple machines

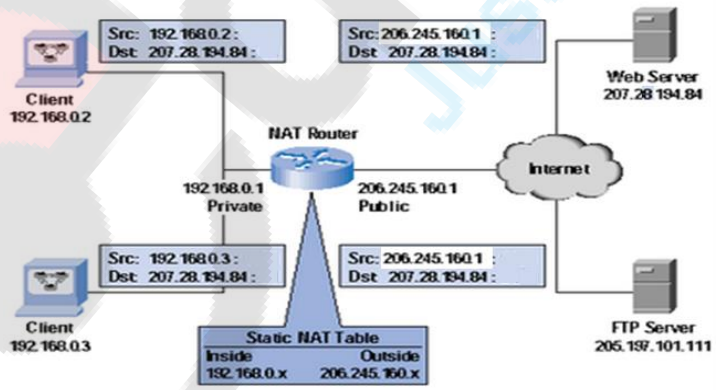
Local network uses just one IP address as far as outside world is concerned:

- no need to be allocated range of addresses from ISP: - just one IP address is used for all devices
- can change addresses of devices in local network without notifying outside world
- The addresses of the devices which are inside local net not explicitly visible to outside world (a security plus).

Types of NAT

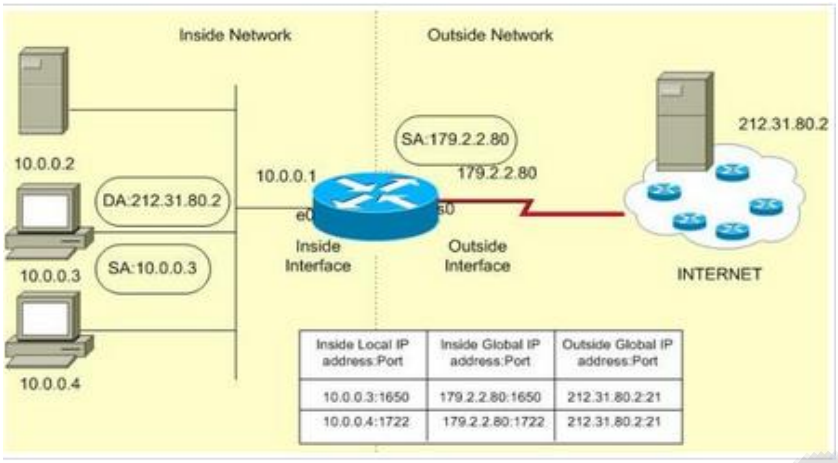
- Static NAT
- Dynamic NAT
- PAT

Static NAT



Static Translation is done for inside resource that outside people want to access.

Dynamic NAT



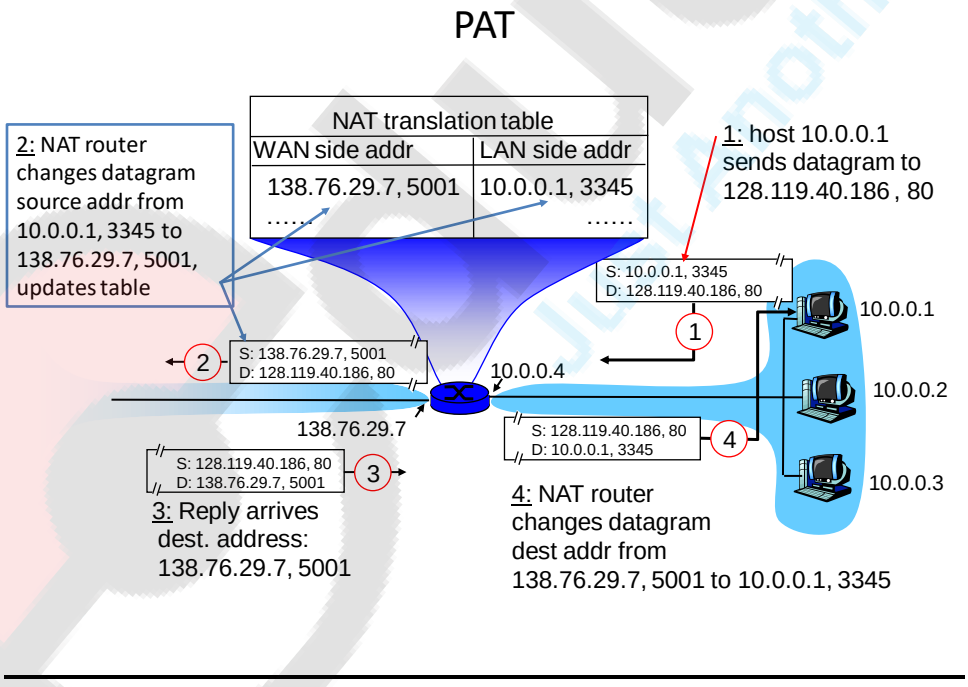
- Dynamic NAT is used when inside users needs to access outside resources.

- When an inside user sends traffic through the router, it examines the source IP address and compares it to the internal local address pool.
- If it finds a match, then it determines which inside global address pool it should use for the translation.
- It then dynamically picks an address in the global address pool that is not currently assigned to an inside device.
- The router adds this entry in its address translation table, the packet is translated, and the packet is then sent to the outside world.
- If no matching entry is found in the local address pool, the address is not translated and is forwarded to the outside world in its original state.

<u>Port Address Translation</u>

Implementation: NAT router must:

- outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #) . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr.
- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
- incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table



5. Numericals on IP addressing

Unit 7

1. Discuss different design issues of data link layer and explain framing technique in data link layer

The main purpose of this layer is to make sure that bits are delivered in exactly the same order in which they are sending. It has to deal with transmission error and regulate flow control also.

Data Link Layer Design Issues:

The functions carried out by data link layer are:

1. Service provided to network layer.
2. Determining how the bits of the physical layer are grouped into frames (FRAMING).
3. Dealing with transmission errors (ERROR CONTROL).
4. regulating the flow of frames – slow receivers are not swamped by fast senders (FLOW CONTROL).

1. Service provided to network layer

Principal Service is to transfer data from network layer on the source machine to the network layer on the destination machine. Commonly provided services are

Unacknowledged connectionless service
Acknowledged connectionless service
Acknowledged connection oriented service

Unacknowledged connectionless service

Consist of having the source machine sending independent frames to the destination machine without having destination machine acknowledging them .No logical connection is established. If a frame is lost due to noise, no attempt is made to detect loss or recover it

Acknowledged connectionless service

No logical connection
But each send frame is acknowledged
As a result, sender knows whether frame has arrived correctly or not
If not received has to resend

Acknowledged connection oriented service

First, connection is established by having both sides initialize variables and counters needed to keep track of which frames has been received and which not
Secondly, frames are transmitted
Thirdly, connection is released

2. Framing

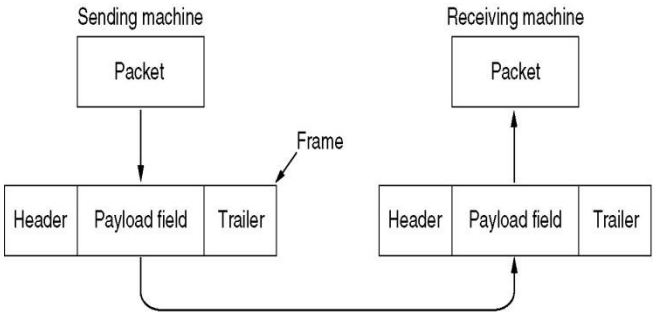
Break bit stream into frames.

Check if frames arrived correctly.

If not:

Discards frame.

In some cases also request retransmission.



Framing Methods:

1. Character count
2. Starting and ending characters, with character stuffing
3. Starting and ending flags, with bit stuffing

Character Counting

- ✓ This method uses a field in the header to specify the number of character in the frame.
- ✓ If the frame slips resynchronization is a problem

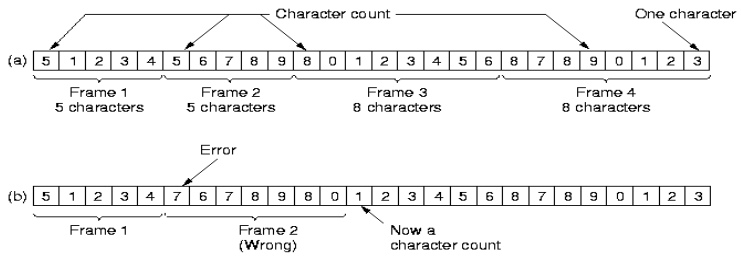


Fig. 3-3. A character stream. (a) Without errors. (b) With one error.

Starting and Ending Character

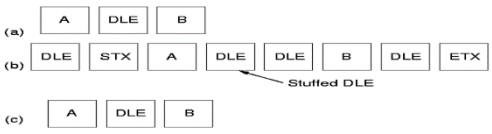


Fig. 3-4. (a) Data sent by the network layer. (b) Data after being character stuffed by the data link layer. (c) Data passed to the network layer on the receiving side.

- **Character stuffing**

  - ✓ Each frame start with character sequence DLE STX and end with DLE ETX
  - ✓ Character stuffing is used when binary data, object program or floating point numbers are being transmitted.
  - ✓ Where DLE : Data Link Escape

    STX: starting text

Starting and Ending flag

Flag pattern: 01111110

ETX: Ending Text

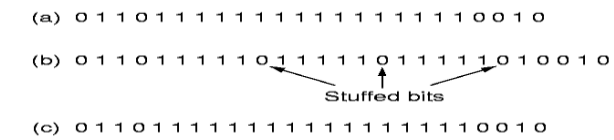


Fig. 3-5. Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

- Each frame begin and end with pattern 01111110
- After 5 consecutive 1 bits, stuff 0 bit in between
- At receiver end destuffs these 0 bit and get original data

3. Error Control

Duties of data link layer: deliver the frames in order without any error; how?

❖ Reliable delivery

-Timers.

-Retransmission.

-Duplicate detection.

❖ Detecting errors.

❖ Detecting & correcting errors.

4. Flow Control

➢ How to cope with fast sender and slow receiver?

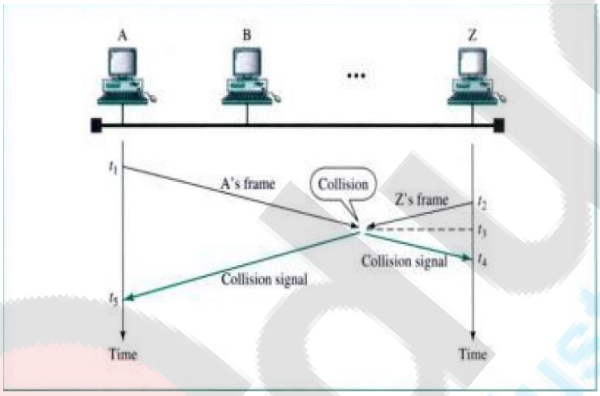
When the connection is established, receiver has to give feedback;

Grant permission to send data as e.g.: Receiver may say send n frames only to the sender.

2. Differentiate between CSMA, CSMA/CD and CSMA/CA

Carrier Sense Multiple Access

- The capacity of ALOHA or slotted ALOHA is limited by the large vulnerable period of a packet.
- CSMA was developed by Kleinrock and Tobagi in 1975.
- It requires station to listen to the medium first and then transmit
- It is based on the principal "sense before transmit"
- Still chances of collision are there
- A station may sense the medium and find it idle, only because the first bit send by the another station has not yet been received.



- Three types of CSMA:

  1-Persistent CSMA

  Non-Persistent CSMA

  P-Persistent CSMA

1-persistent CSMA

- In this when a station has data to send, it first listens to the channel to check whether it is idle or not.
- If the channel is busy, the station waits until it become idle.
- When the station detects an idle channel, it transmits a frame immediately.
- It has the highest chance of collision because two or more stations may find line idle and send their frames immediately
- The protocol is called 1-persistent because the station transmit with the probability of 1 i.e. transmit 100% as channel is free.

Non-persistent CSMA

- First it will sense the line
- If the line is idle, it sends immediately
- If line busy, it waits for a random amount of time and then sense again
- It reduce the chance of collision since the waiting time is different for different stations
- Reduces efficiency sine medium remains idle when there may be stations to send frame

P-persistent CSMA

- channel is having time slots it sense the channel and transmit with a slot duration equal or greater than maximum propagation time.

- It sense the channel and if it is free, send data with a probability p
- It defers with a probability q= 1-p
- If that slot is also idle, it either transmits or defer again
- Process is repeated until either frame is transmitted or another station has begun transmitting

<u>COMPARISION OF CSMA'S PROTOCOL</u>

1-persistent CSMA (IEEE 802.3)

- If medium idle, transmit; if medium busy, wait until idle; then transmit with p=1.
- If collision, waits random period and starts again.

Non-persistent CSMA: if medium idle, transmit; otherwise wait a random time before re-trying.

- Thus, station does not continuously sense channel when it is in use.

P-persistent: when channel idle detected, transmits packet in the first slot with *p*.

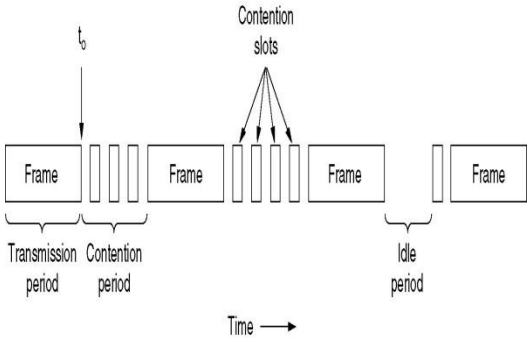
- Slotted channel, i.e., with probability q = p-1, defers to next slot.

<u>CSMA / CD</u> (CSMA WITH COLLISION DETECTION)

- Station that wants to transmit first listens to check if another transmission is in progress.
- The station aborts the transmission as soon as they detect a collision.
- Problem: when frames collide, medium is unusable for duration of both damaged frames.
- This quickly terminating of damage frames saves time and bandwidth and avoids damage to rest of the frames.
- Station after aborting waits a random period of time known as back-off delay and tries the same thing again.
- A jam signal is send due to which all transmitters' stops transmitting by random intervals, reducing the probability of collision after first retry.
- It is widely use in LAN in the MAC sub layer
- The minimum time to detect collision is the time it take signal to propagate from one station to another.
- It can be in three states

  - Transmission
  - Contention
  - Idle

- Contention slot – after detecting collision station stops transmitting, waits random amount of time and again starts transmitting assuming that no other station is transmitting in this time
- This time slot is considered as contention slot
- Idle slot – when no station is transmitting , channel is idle



The following procedure is used to initiate a transmission.

- Is my frame ready for transmission? If yes, it goes on to the next point.
- Is medium idle? If not, wait until it becomes ready
- Start transmitting and monitor for collision during transmission
- Did a collision occur? If so, go to collision detected procedure.
- Reset retransmission counters and end frame transmission.
- The procedure is complete when the frame is transmitted successfully or a collision is detected during transmission

Collision detected procedure

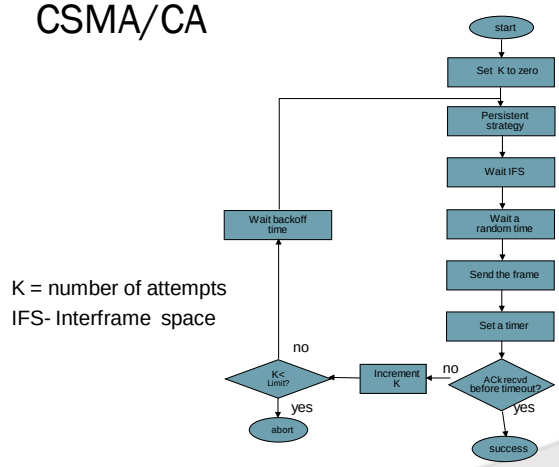
- The following procedure is used to resolve a detected collision.
- Continue transmission (with a jam signal instead of frame header/data/CRC) until minimum packet time is reached to ensure that all receivers detect the collision
- Increment retransmission counter

- Was the maximum number of transmission attempts reached? If so, abort transmission.
- Calculate and wait random back off period based on number of collisions.
- Re-enter main procedure at stage 1.
- The procedure is complete when retransmission is initiated or the retransmission is aborted due to numerous collisions.

CSMA/CA(COLLISON AVOIDANCE)

- *CSMA/CA (Carrier Sense Multiple Access and Collision Avoidance*) is a variation of CSMA/CD used in wireless LANs because it is difficult to detect collisions in such networks.
- When CSMA/CA is used, each node must wait a random time interval after detecting a clear medium before transmitting.

CSMA/CA



3. Explain PPP in detail

- Point to Point Protocol establishes a connection of the PC to ISP (Internet Service Provider) via a modem.
- PPP is a Data Link layer protocol that supports the Internet Protocol over point to point connections for delivering the packets.
- PPP provide connection authentication, transmission, encryption and compression to negotiate the two devices when establishing a link.

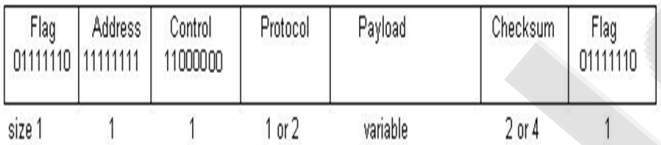
PPP provides several services:

- It defines the format of the frame to be exchanged between devices.
- Error detection
- Ability to bring lines up and down.
- Defines how n/w layer data encapsulated in the data link frame.

- It defines how two devices can authenticate each other.
- It defines how two devices can negotiate the establishment of the link and the exchange of data.

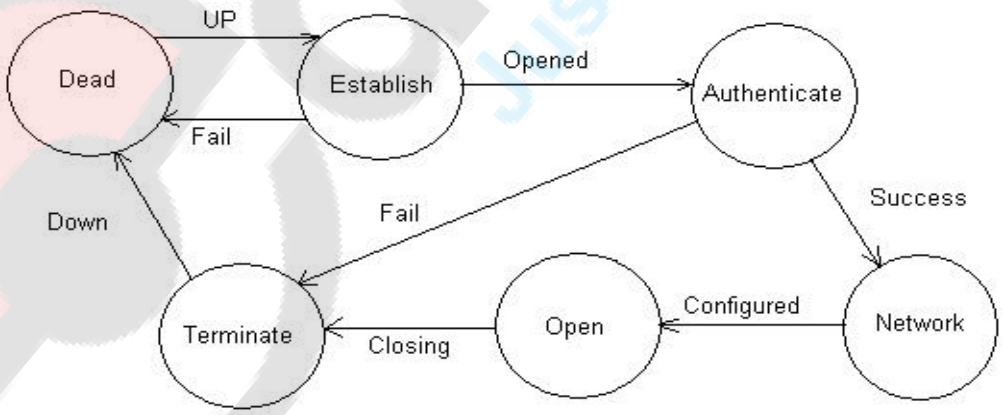
Frame Format

- The frame format for PPP adds a short header and a trailer to the IP packet.



Transition States of PPP

An overview of the PPP operation can be described as a Finite State Diagram.



Dead :

- Dead means that the link is not being used. There is no active carrier, and line is quiet.

  Link Establishment Phase:

- Any end point can start the communication, the connection goes into the establish state.
- In this state, options are negotiated between the two parties; if it is successful then system goes to the authentication state.
- The Link Control Protocol (LCP) is used to establish the connection through an exchange of Configure packets.

  Authentication Phase

  - The two devices send several authentication packets, if result is successful; the connection goes to the networking state otherwise goes to the termination state.

- **Networking state**

  - The exchanges of user control and data packets can be started.

  - The connection remains in the same state until any end point wants to terminate the connection

- **Open State**

  – PPP carries the network-layer protocol packets in this state.

- **Termination Phase**

  - When the link is closing, PPP informs the network-layer protocols so that they may take appropriate action

- LCP is used to close the link through an exchange of Terminate packets.

- After the exchange of Terminate packets, the implementation should signal the physical-layer to disconnect in order to enforce the termination of the link.

Multiplexing

- PPP uses a set of protocols to establish the link, authenticate the parties involved and to carry the network layer data
- They are
    1. LCP
    2. AP
    3. NCP

Link Control Protocol (LCP)

LCP is part of PPP used to control the link.

- is responsible for establishing, maintaining, configuring and terminating links.

-provides negotiation mechanism to set options between the two end points

- All LCP packets are carried in the payload field of the PPP frame

Authentication Protocol (AP)

- It is used during the authentication state.
- It works over the dial-up links where verification of user identity is necessary.
- PPP created two protocols for authentication

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Password Authentication Protocol (PAP)

- Simple authentication procedure
- Two steps

  1. User sends authentication identification and password
  2. System checks the validity and either accepts or deny

- three types of packets are used
  1. Authenticate request
  2. authenticate-ack
  3. authenticate-nak

Challenge Handshake Authentication Protocol (CHAP)

- Provides greater security than PAP
- Password is kept secret, never send online

Steps

1. System sends a challenge packet which contains a challenge value
2. User applies a predefined function that takes challenge value and password and creates a result
3. This result is send as response to the system

4. System does the same process with user's password. If the result matches access is granted otherwise denied.

- Four CHAP packets

- Challenge

- Response

- Success

- Failure

Network Control Protocol (NCP)

- Is used after establishing and authentication of the connection.
  - ❑ One of the functions of NCP is to dynamically assign an IP address to the host that is connecting.
  - ❑ NCP is a set of control protocols to allow the encapsulation of data coming from n/w layer protocols into the PPP frame.

4. Explain IEEE 802.5

<u>IEEE Standard 802.5 :Token Ring</u>

- ❑ Number of stations connected by transmission links in a ring topology.
- ❑ Information flows in one direction along the ring from source to destination and back to source

- ❑ Token circulates around the ring when all stations are idle.
- ❑ Only the station possessing the token is allowed to transmit at any given time.

Token Ring Operation

- When a station wishes to transmit, it must wait for token to pass by and *seize the token.*
  - One approach: change one bit in token which transforms it into a *"start-of-frame sequence"* and appends frame for transmission.
  - Second approach: station claims token by removing it from the ring.
  - Frame circles the ring and is removed by the transmitting station.
- Each station interrogates passing frame, if destined for station, it copies the frame into local buffer. *{Normally, there is a one bit delay as the frame passes through a station.}*
- A ring consists of a collection of ring interface connected by point-to-point lines.
- Ring interface have two operating modes:

  Listen mode

  Transmit mode

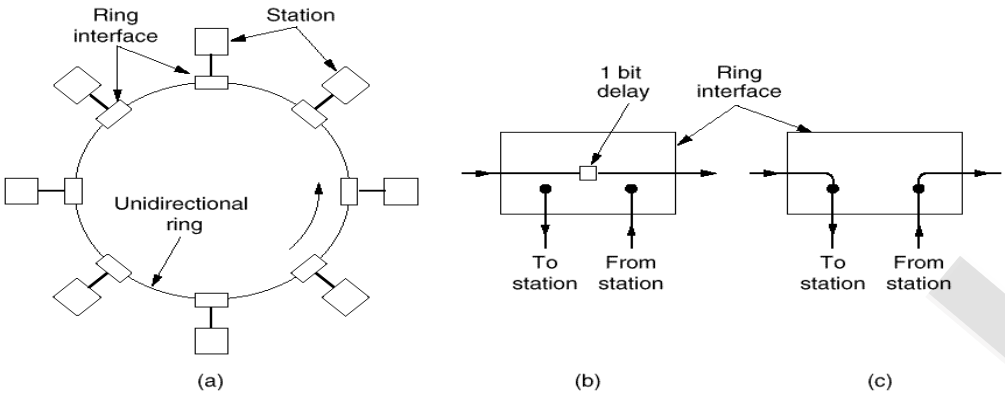
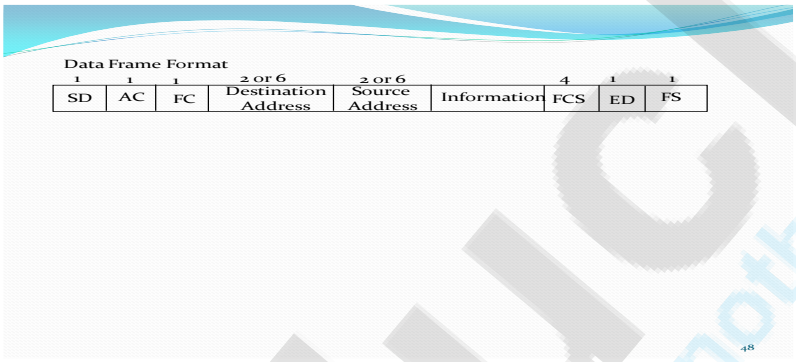


Fig. 4-28. (a) A ring network. (b) Listen mode. (c) Transmit mode.

- When the station has finished transmitting the last bit of its frame, it must regenerate the token and then interface must switch back into listen mode immediately.



Releasing the tokens after transmission

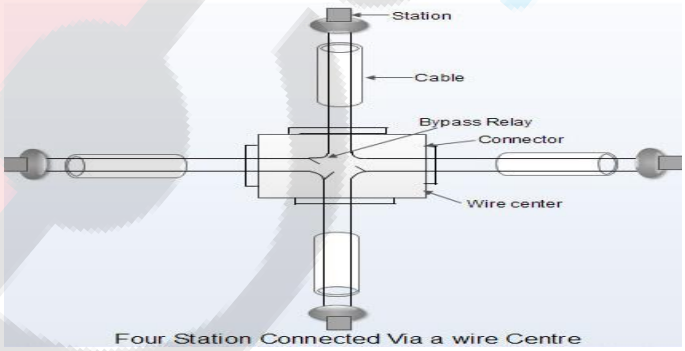
Characteristics:

- Guaranteed access, no collisions
- Good utilization of the network capacity, high efficiency

- Fair, guaranteed response times
- Medium: twisted pair, coaxial cable or optical fiber
- Capacity of 16 Mbps (100Mb/s with optical fiber)
- Differential Manchester Code on layer 1

Disadvantage of ring shaped

- If the cable breaks somewhere the ring dies.
- For this , wire center are used
- Logically this is a ring, but physically each station is connected to the wire center by a cable containing two twisted pair.
- One pair is used for data to the station
- And another is used for data from the station.
- This wire center help in bypassing the stations in case when one station goes down
- This type of ring is known as star shaped ring.



Four Station Connected Via a wire Centre

5. Differentiate between Go back N ARQ and Selective Repeat ARQ

Sliding Window: Basics

- Allows multiple frames to be in transit at the same time before needing an ACK.
- Receiver allocates buffer space for ***n*** frames.
- The sliding window is an imaginary box at both the sender and receiver end.
- Transmitter is allowed to send ***n*** (window size) frames without receiving ACK.

Sequence Numbers

- Frames from a sender are numbered sequentially.
- Setting of a limit is needed to include the sequence number of each frame in the header.
- If the header of the frame allows m bits for sequence number, the sequence numbers range from 0 to $2^m - 1$. for m = 3, sequence numbers are: 0,1, 2, 3, 4, 5, 6, 7.
- The window size will be $2^m - 1$
- We can repeat the sequence number.
- 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1...

Sliding Window: Receiver

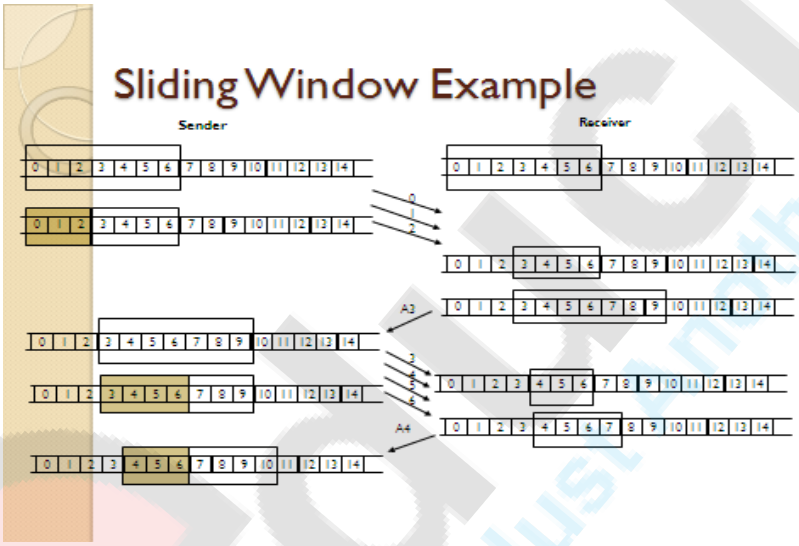
- Receiver ack's frame by including sequence number of next expected frame.
    - Cumulative ACK: ack's multiple frames.

- Example: if receiver receives frames 2,3, and 4, it sends an ACK with sequence number 5, which ack's receipt of 2, 3, and 4.
- Transmission window shrinks each time as frame is sent, and grows each time an ACK is received.
- The receiver window shrinks when data are received and expands when ACK are sent.

  Example-1:If the sequence of transmission for 7 bit frame is as follow : window size 7

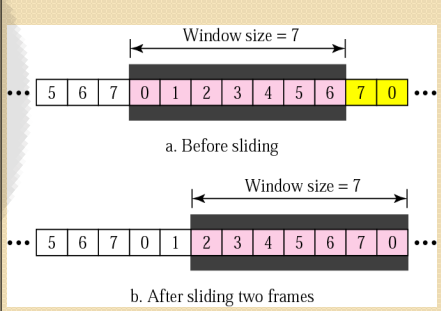
  ->data0 ->data1 <-ack2 ->data2 <-ack3

  ->data3 ->data4 ->data5 <-ack6



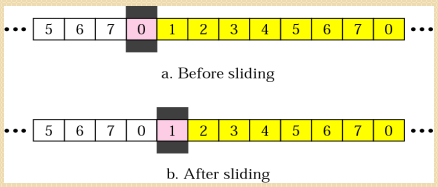
SENDER SLIDING WINDOW

- At the sending site, to hold the outstanding frames until they are acknowledged, we use the concept of a window.
- The size of the window is at most 2^m -1 where m is the number of bits for the sequence number.
- Size of the window can be variable, e.g. TCP.
- The window slides to include new unsent frames when the correct ACKs are received



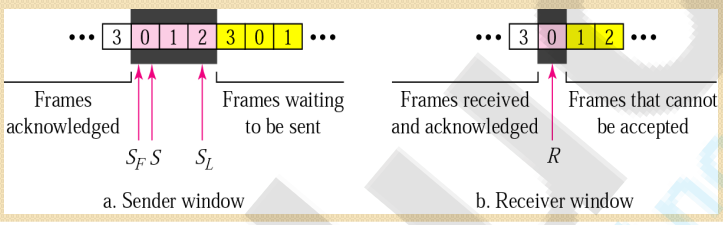
RECEIVER SLIDING WINDOW

- Size of the window at the receiving site is always 1 in this protocol.
- Receiver is always looking for a specific frame to arrive in a specific order.
- Any frame arriving out of order is discarded and needs to be resent.
- Receiver window slides as shown in fig. Receiver is waiting for frame 0 in part a.



CONTROL VARIABLES

- Sender has 3 variables: S, S_F, and S_L
- S holds the sequence number of recently sent frame
- S_F holds the sequence number of the first frame
- S_L holds the sequence number of the last frame
- Receiver only has the one variable, R, that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of R, the frame is accepted, otherwise rejected.

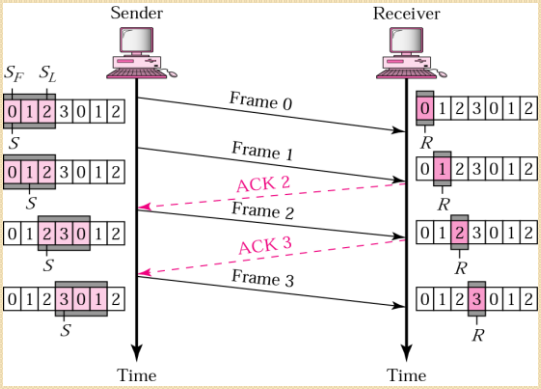


Go Back N- ARQ

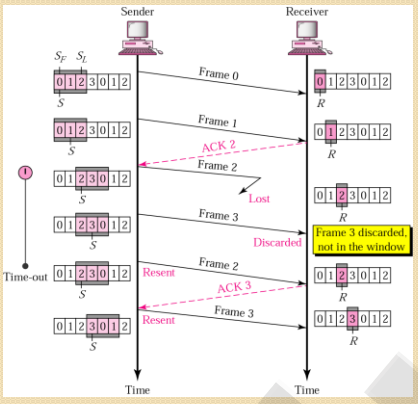
- Receiver sends positive ACK if a frame arrived safe and in order.
- If the frames are damaged/out of order, receiver is silent and discard all subsequent frames until it receives the one it is expecting.
- The silence of the receiver causes the timer of the unacknowledged frame to expire.
- Then the sender resends all frames, beginning with the one with the expired timer.
- For example , suppose the sender has sent frame 6, but the timer for frame 3 expires (i.e. frame 3 has not been acknowledged), then the sender goes back and sends frames 3, 4, 5, 6 again. Thus it is called Go-Back-N-ARQ
- The receiver does not have to acknowledge each frame received, it can send one cumulative ACK for several frames.
- Sender can send up to W frames before worrying about ACKs.

GO-BACK-N ARQ, NORMAL OPERATION

- The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



GO-BACK-N ARQ, LOST FRAME



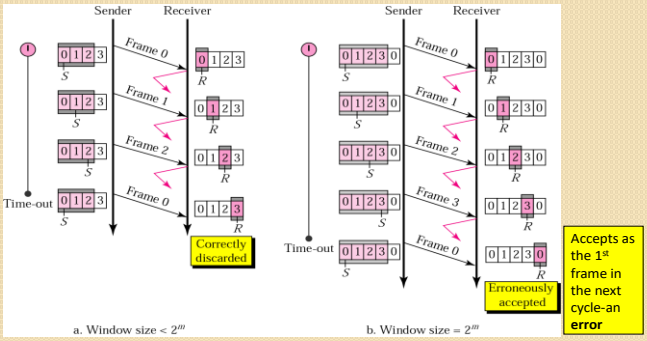
- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window).
- After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)

GO-BACK-N ARQ, DAMAGED/LOST/DELAYED ACK

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
  - Example ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- A delayed ACK also triggers the resending of frames

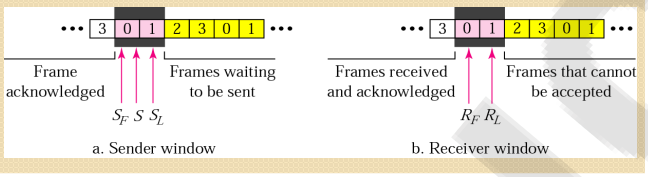
GO-BACK-N ARQ, SENDER WINDOW SIZE

- Size of the sender window must be less than 2^m. Size of the receiver is always 1. If m = 2, window size = $2^m - 1 = 3$.
- Fig compares a window size of 3 and 4.



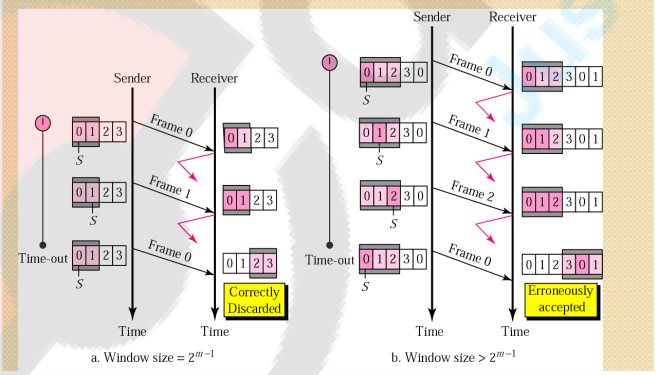
SELECTIVE REPEAT ARQ, SENDER AND RECEIVER WINDOWS

- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It's bandwidth is inefficient and slows down the transmission.
- In Selective Repeat ARQ, the size of window of sender and receiver is almost same.
- only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



SELECTIVE REPEAT ARQ, SENDER WINDOW SIZE

- Size of the sender and receiver windows must be at most one-half of 2^m. If m = 2, window size should be $2^m/2 = 2^{m-1} = 2$. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an **error**.



6. Numericals on

- **CRC**

- **Checksum**
- **Hamming Code**
- **VRC,LRC**