CMR

INSTITUTE OF

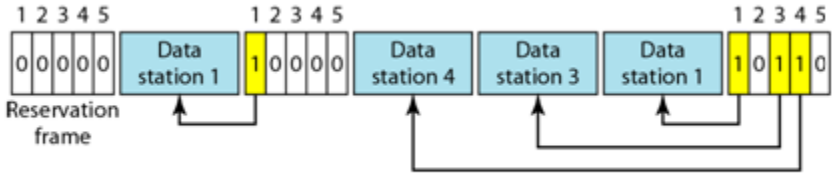
TECHNOLOGY

Scheme and Solution – II April 2019

Sub:	COMPUTER COMMUNICATION NETWORKS							Code:	15EC64
Date:	16/04/2019	Duration:	90 mins	Max Marks:	50	Sem:	VI	Branch:	ECE(A,B,C,D)

Q1(a). Explain Reservation as a controlled access method.

Reservation:



- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals.
- In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are *N* stations in the system, there are exactly *N* reservation minislots in the reservation frame.

Q1(b). Show the behavior of the three persistence methods of CSMA with a neat diagram.

Solution:

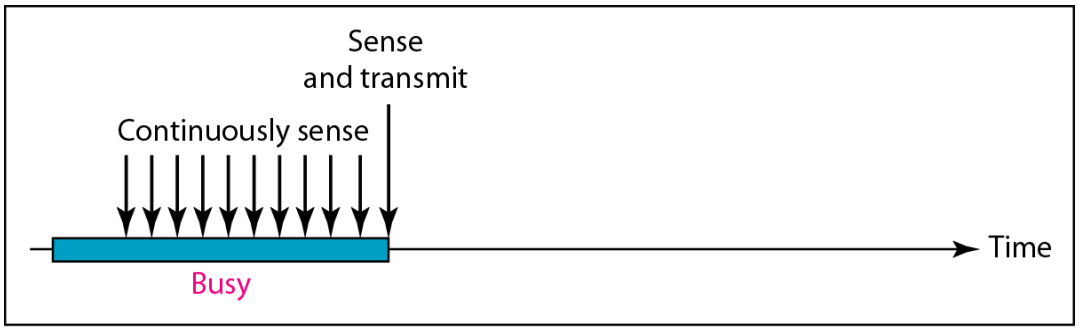
CSMA: Carrier Sense Multiple Access

- Each station "sense before transmit" or "listen before talk.“
- In Carrier sense multiple access the station first senses or listen to the medium before transmitting.

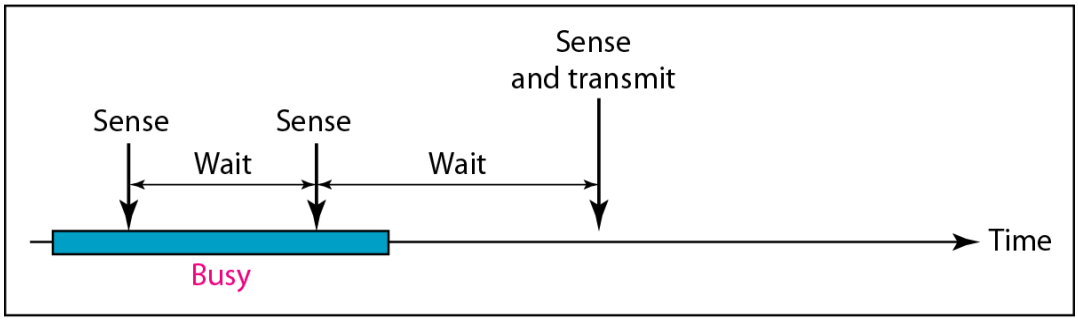
- The chance of collision is reduced by sensing the medium before trying to use it but it cannot eliminate it.
- The possibility of collision still exists because of propagation delay(first bit).
- The frame is composed of the bits and when a frame is transmitted then very first bit of the frame is transmitted first which reaches first at the receiver, but if the intermediate second station can't sense the first bit being transmitted by another station then it assumes that the channel is free and transmits its frame.
- This leads to the collision of two frames.

Persistence Methods:

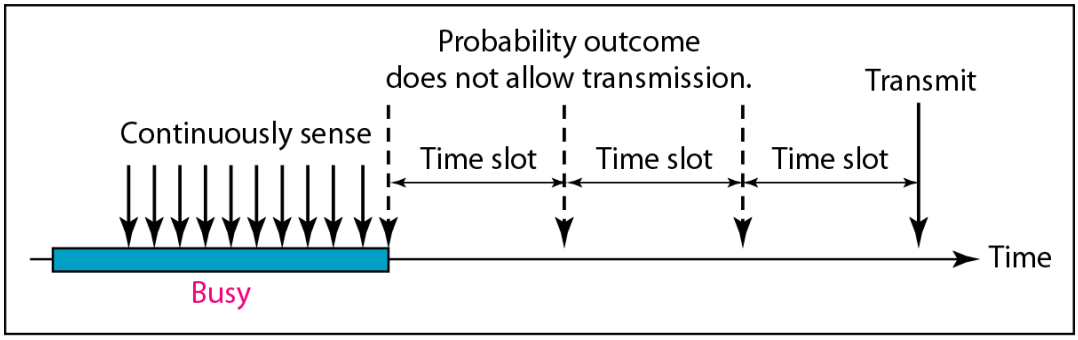
Persistence methods defines what a station should do if it finds the channel to be busy or idle. There are three methods



a. 1-persistent



b. Nonpersistent



c. p-persistent

1-persistent method:

In this method, the station keeps on sensing the channel, if the station finds the line idle, it sends its frame immediately with probability 1.

This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

Non persistent method:

In the non persistent method, a station that has a frame to send senses the line.

- If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
- The non persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-persistent method:

- Combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.
- Channel has time slots equal to propagation time.
- In this method, after the station finds the line idle it follows these steps:

  1. With probability *p, the station sends its frame.*
  2. With probability *q = 1 - p, the station waits for*

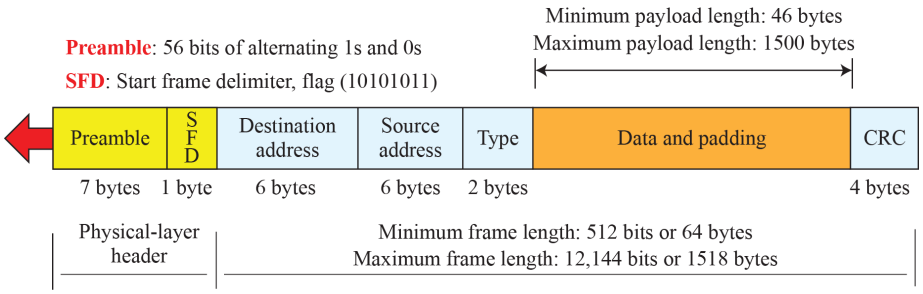
     the beginning of the next time slot and checks

     the line again.

- a. If the line is idle, it goes to step 1.
- b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

Q2.(a)Explain the format of standard Ethernet frame. . What are the minimum and maximum frames lengths?

Ethernet frame



(b)

A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses. The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01010010
First address: 167.199.170.64/27	10100111	11000111	10101010	01000000

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01011111
Last address: 167.199.170.95/27	10100111	11000111	10101010	01011111

3)An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 sub blocks of addresses to use in its three subnets: one sub block of 10 addresses, one sub block of 60 addresses, and one sub block of 120 addresses. Design the sub blocks.

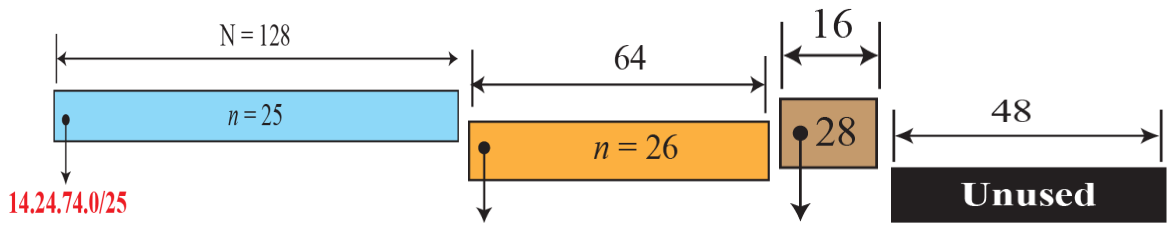
There are $2^{32-24} = 256$ addresses in this block. The first address is 14.24.74.0/24; the last address is 14.24.74.255/24. To satisfy the third requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one.

The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$. The first address in this block is 14.24.74.0/25; the last address is 14.24.74.127/25.

The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$. The first address in this block is 14.24.74.128/26; the last address is 14.24.74.191/26.

The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 16 = 28$. The first address in this block is 14.24.74.192/28; the last address is 14.24.74.207/28.

If we add all addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve. The first address in this range is 14.24.74.208. The last address is 14.24.74.255. Figure shows the configuration of blocks. We have shown the first address in each block



14.24.74.0/25	**14.24.74.128/26;**	**14.24.74.192/28**

4. Explain with a neat diagram VLAN., membership and configuration of VLAN.

We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments.

A LAN can be divided into several logical LANs called VLANs.

Each VLAN is a work group in the organization.

If a person moves from one group to another, there is no need

to change the physical configuration.

The group membership in VLAN is defined by software not hardware

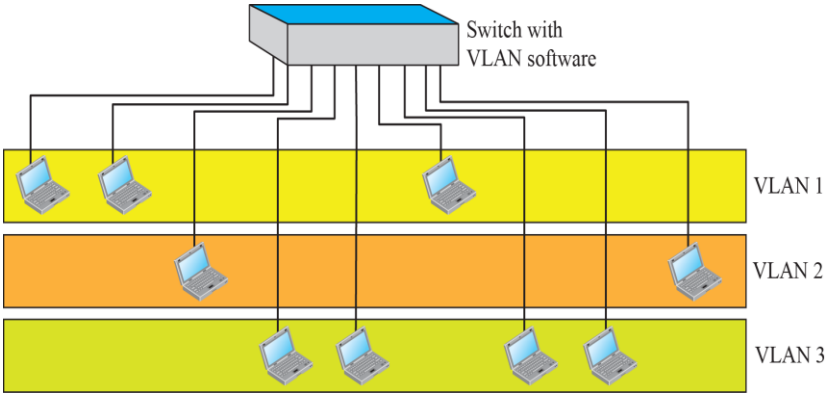
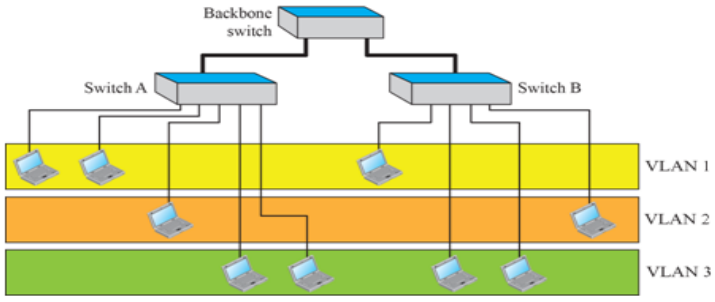


Figure 17.12: Two switches in a backbone using VLAN software



17.62

Characteristic can be used to group stations in a VLAN:-

Vendors use different characteristics such as
interface numbers,
port numbers,
MAC addresses,
IP addresses,
IP multicast addresses,
or a combination of two or more of these.

The stations grouped into different VLANs:-

Stations are configured in one of three ways:
manually- the network administrator uses the VLAN software to manually assign the stations
semi-automatically- Initializing is done manually with migrations done automatically

automatically.- stations are automatically connected or disconnected from a VLAN using the criteria defined by the administrator

5)With a neat diagram explain how can a NAT help in address translation using one IP Address?

Many are not happy with one address; many have created small networks with Several hosts and need an IP address for each host. With the shortage of addresses, this is a serious problem. A quick solution to this problem is called network address Translation (NAT). NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

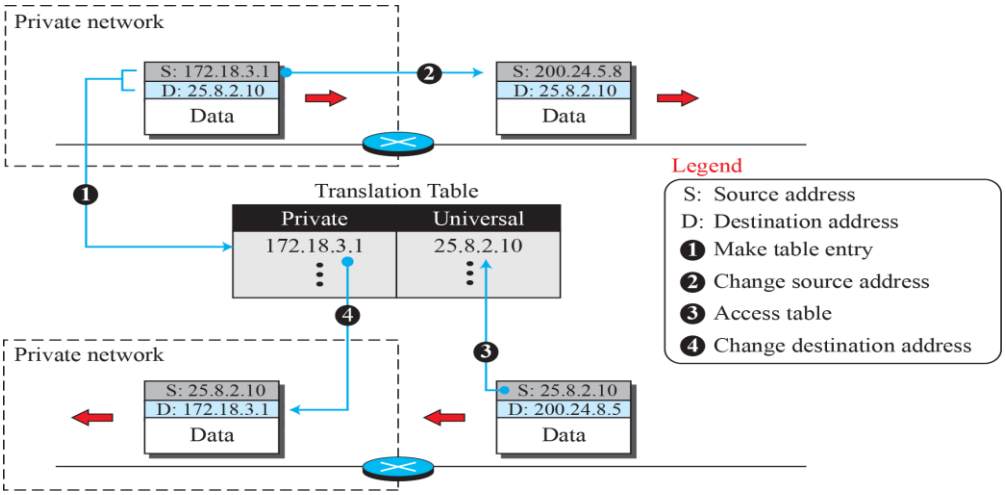
The traffic inside can use the large set; the traffic outside, the small set. In most situations, only a portion of computers in a small network need access to the Internet simultaneously.

A technology that can provide the mapping between the private and universal addresses is Network Address Translation (NAT).

The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.

All the outgoing packets go through the NAT router, which replaces the *source address* in the packet with the global NAT address.

All incoming packets also pass through the NAT router, which replaces the *destination address in the packet (the NAT router global* address) with the appropriate private address.



6)With relevant diagrams describe Distance Vector Routing(DVR). What is two node instability in DVR.

The **distance-vector (DV) routing** uses the goal we discussed in the introduction, to find the best route. In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors.

The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet. We can say that in distance-vector routing, a router continuously tells all of its neighbors what it knows about the whole internet (although the knowledge can be incomplete).

The concept of a **distance vector** is the rationale for the name *distance-vector routing*.

A least-cost tree is a combination of least-cost paths from the root of the tree to all destinations.

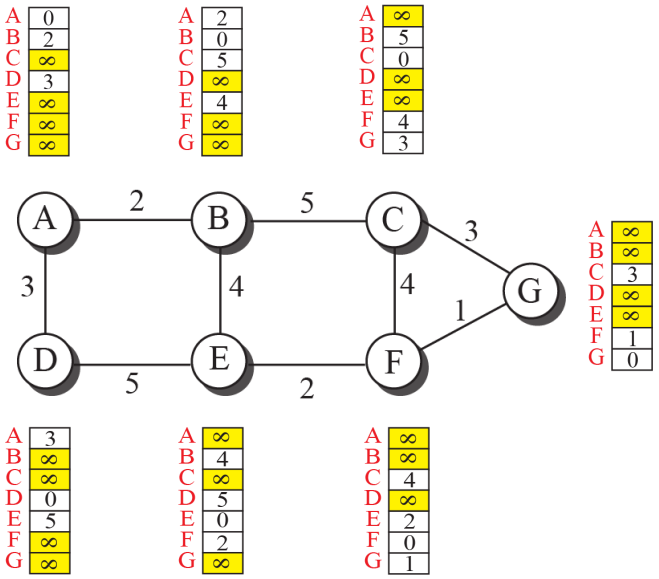
These paths are graphically glued together to form the tree. Distance-vector routing unglues these paths and creates a *distance vector*, a one-dimensional array to represent the tree. Figure 20.4 shows the tree for node A in the internet in below Figure and the corresponding distance vector.Note that the *name* of the distance vector defines the root, the *indexes* define the destinations, and the *value* of each cell defines the least cost from the root to the destination.

A distance vector does not give the path to the destinations as the least-cost tree does; it gives only the least costs to the destinations. Later we show how we can change a distance vector to a forwarding table, but we first need to find all distance vectors for an internet.

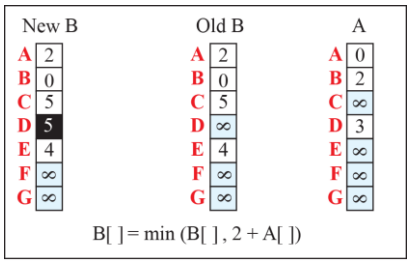
We know that a distance vector can represent least-cost paths in a least-cost tree, but the question is how each node in an internet originally creates the corresponding vector. Each node in an internet, when it is booted, creates a very rudimentary distance vector with the minimum information the node can obtain from its neighborhood. The

node sends some greeting messages out of its interfaces and discovers the identity of the immediate neighbors and the distance between itself and each neighbour

The first distance vector for an internet

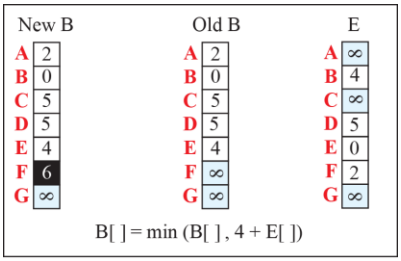


Updating distance vectors



a. First event: B receives a copy of A's vector.

Note:
X[ ]: the whole vector



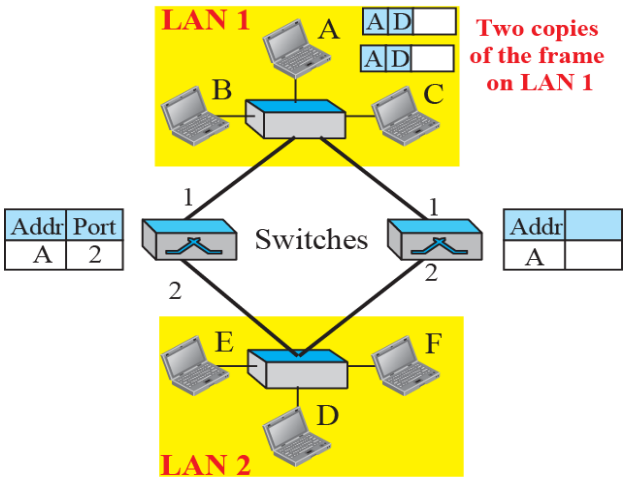
b. Second event: B receives a copy of E's vector.

---

7)Explain the loop problem in learning switch and discuss the solution for the same.

System administrator likes to have redundant switches to make the system more reliable. Such redundancy can create loops in the system which is very undesirable. Both

switches forward the frame and update their tables. so there are two copies of the frame on LAN 2. It is repeated and both the copies are sent to LAN1. The process continues on and on.

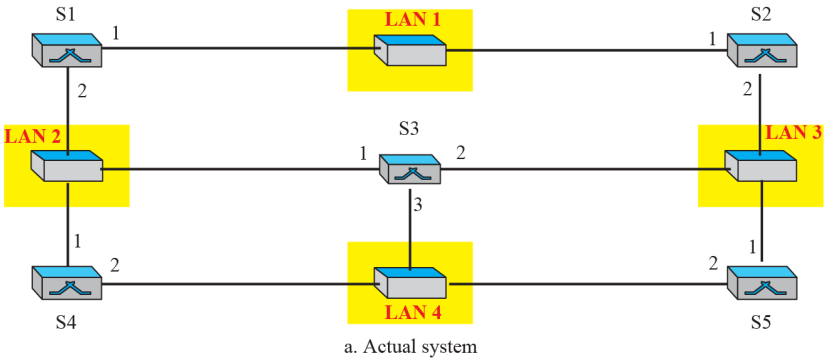


Implement spanning-tree-algorithm for the whole LAN network is the solution for this.

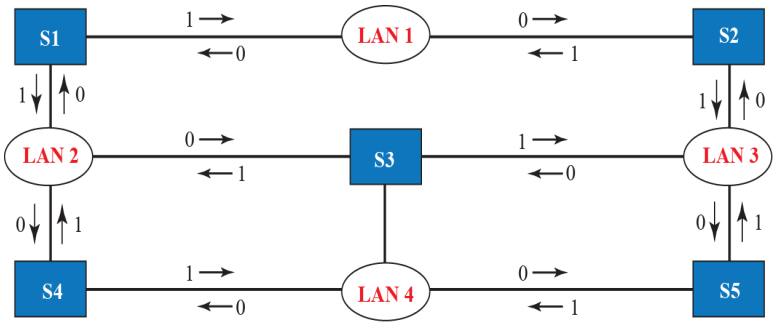
- To find the spanning tree we need to assign a cost to each arc. We have chosen the minimum hops. 1 from a switch to LAN and 0 in the reverse direction.
- The process for finding the spanning tree involves

1. Every switch has a built in ID and it broadcasts this ID so that all switches know which one has the smallest ID. The switch with smallest ID is selected as the root switch.
2. The algorithm tries to find the shortest path from the root to every other switch or LAN. Here Dijkstra algorithm is used
3. Creates the shortest tree

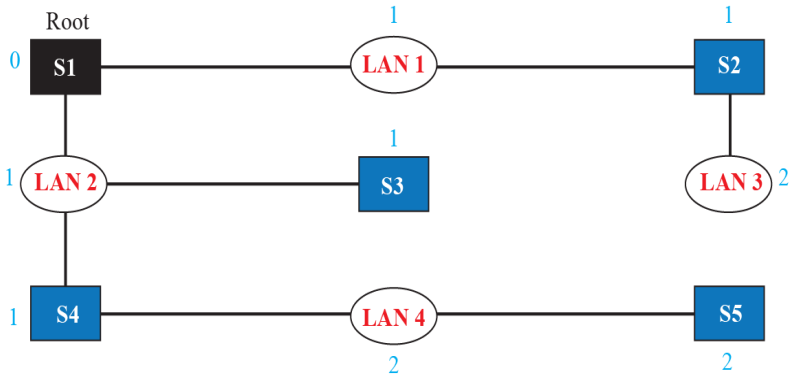
7. Mark the ports that are part of it as forwarding ports and others are blocking ports,which block the frames received by the switch.

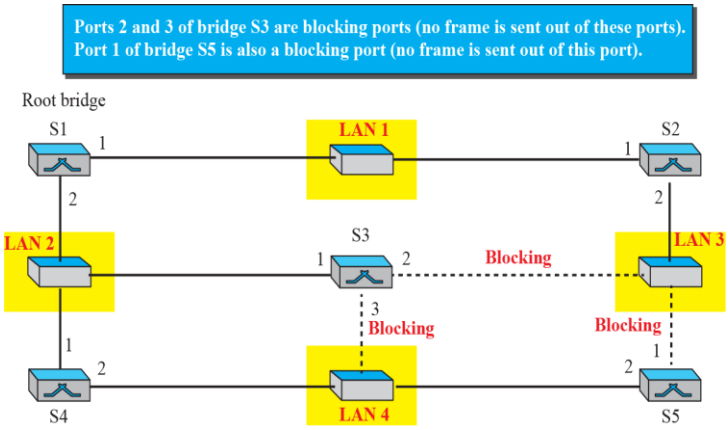


a. Actual system



b. Graph representation with cost assigned to each arc





Q8a) Explain CSMA/CA and frame exchange time line diagram with proper figures.

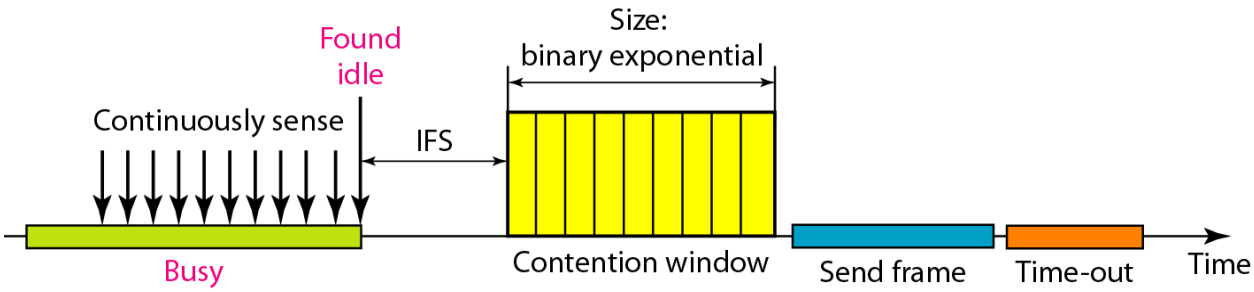
Solution:

- In a wired network, the received signal has almost the same energy as the sent signal but during collision the detected energy almost doubles.

- But in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy and moreover a collision may add only 5 to 10 percent. Hence
- Hence Carrier sense multiple access with collision avoidance was invented to avoid collisions in wireless network as they cannot be detected.

Collisions are avoided through the use of CSMA/CA's three strategies:

The interframe space, the contention window, and acknowledgments,



Continuously sense:

- First the channel keeps on sensing the medium to be free.
- If the channel is busy the station will backoff
- If the channel is free (i.e. idle) then the station will not immediately transmit the frame but will wait for a period called interframe space

Interframe space (IFS):

- IFS time period is required as if some other distinct stations are already transmitting then let them finish the transmission first.
- After the IFS period if the station founds the channel to be free then it again waits for time period equal to contention window.
- IFS also assigns the priorities to the stations and frame, for example the station that has the short IFS is assigned highest priority.

Contention window:

- The complete period of the window is divided into time slots.
- The station which is ready to transmit chooses the random number of time slots as its waiting time period.
- At the beginning of each time slot the station senses the channel to be free.
- If the channel is free then it start the timer and immediately transmits the frame.
- But if the channel is not free then this waiting time period doubles each time according to binary exponential backoff strategy.
- The timers helps to find the stations with the longest time waiting period. (This gives priority to the station with the longest time period.

Acknowledgement:

- After all the precautions if the data is corrupted then the positive acknowledgements and timers guarantees that the frame has been received.

Q8 b). In slotted ALOHA network transmits 200 bit frames on a shared channel of 200 Kbps. What is the throughput if the system produces:

a) 1000 frames/sec b) 500 frames/sec c) 250 frames/sec.

Solution:

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is *200/200* kbps or 1 ms.

a. G=1. So S =G x e^{-G} or $S = 0.368$ (36.8 percent).

   Throughput= 1000 x 0.0368 =368 frames. Hence only 368 out of 1000 frames will probably survive.

b. Here G = ½, S =G x e^{-G} or S =0.303 (30.3 percent).

   Throughput= 500 x 0.0303 =151. Hence only 151 frames out of 500 will probably survive.

c. Now G=1/4, S =G x e^{-G} or S =0.195 (19.5 percent).
   Throughput= 250 x 0.195 = 49.
   Only 49 frames out of 250 will probably survive.

.