USN | | | | | | | | | | |

Internal Assessment Test II – Feb 2024

Sub:	Computer Networks					Sub Code:	21CS52	Branch:	CSE
Date:	6/02/2024	Duration:	90 mins	Max Marks:	50	Sem /Sec:	V / A,B & C Sec		

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1.A	What are the design issues of Data link layer, Briefly explain the different framing methods with examples.	8	CO2	L2
1.B	A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then what will be the input bit-string	2	CO2	L2
2.A	Consider the cyclic redundancy check (CRC) based error detecting scheme having the generator polynomial $x^5 + x^4 + x^2 + 1$. Suppose the message M = 1010001101 is to be transmitted. Check bits are appended at the end of the message by the transmitter using the above CRC scheme. Find bitstring with databits and checkbit sequence that will be transmitted.	7	CO2	L3
2.B	Assume that a 12-bit Hamming code word consisting of 8-bit data and 4 check bits is $d_8d_7d_6d_5c_8d_4d_3d_2c_4d_1c_2c_1$, where the data bits and the check bits are given in the following tables: what should be the values if x and Y Data bits d_8 d_7 d_6 d_5 d_4 d_3 d_2 d_1 1 1 0 x 0 1 0 1 c_8 c_4 c_2 c_1 Y 0 1 0	3	CO2	L3

3.A	In the given procedure for positive acknowledgement with retransmission protocol. Fill in the blank statements to complete the procedure.
	
	void sender (void)
	{
	Seq_nr next_frame_to_send;
	frame s;
	packet buffer;
	event_type event;
	next_frame_to_send = 0;
	from_network_layer(&buffer);
	while (true)
	{
	s.info = ----------;
	s.seq = ----------;
	----------;
	Start-timer(s.seq);
	wait_for_event (&event);
	if (event == frame arrival)
	{
	from physical layer(&s);
	if (s.ack == ----------)
	{
	stop_timer(s.ack);
		5	CO2	L3

	from_network_layer(&buffer);
	----------;
	
	}
	}
	}
	}			

3.B	In SR protocol, suppose frames through 0 to 4 have been transmitted. Now imagine that 0 times out and a new frame 5 is transmitted, frame 1 times out, frame 2 times out and 6 another new frame is transmitted. With a neat diagram show what will be the outstanding packets in the sender window.	5	CO2	L3
4	Explain CSMA and show the behavior of three persistence methods of CSMA.	10	CO2	L2
5	What is hidden terminal problem in wireless networks? Explain in detail. Also give the solution for hidden terminal problem.	10	CO2	L2
6.A	Differentiate between pure Aloha and slotted Aloha with examples	4	CO2	L2
6.B	Explain any three collision free protocols	6	CO2	L2

CCI CI HOD

\

1.a) What are the design issues of Data link layer, Briefly explain the different framing methods with examples.

DATA LINK LAYER DESIGN ISSUES

The following are the data link layer design issues

1. Services Provided to the Network Layer

The network layer wants to be able to send packets to its neighbors without worrying about the details of getting it there in one piece.

2. Framing

Group the physical layer bit stream into units called frames. Frames are nothing more than "packets" or "messages". By convention, we use the term "frames" when discussing DLL.

3. Error Control

Sender checksums the frame and transmits checksum together with data. Receiver re-computes the checksum and compares it with the received value.

4. Flow Control

Prevent a fast sender from overwhelming a slower receiver.

Different framing methods.

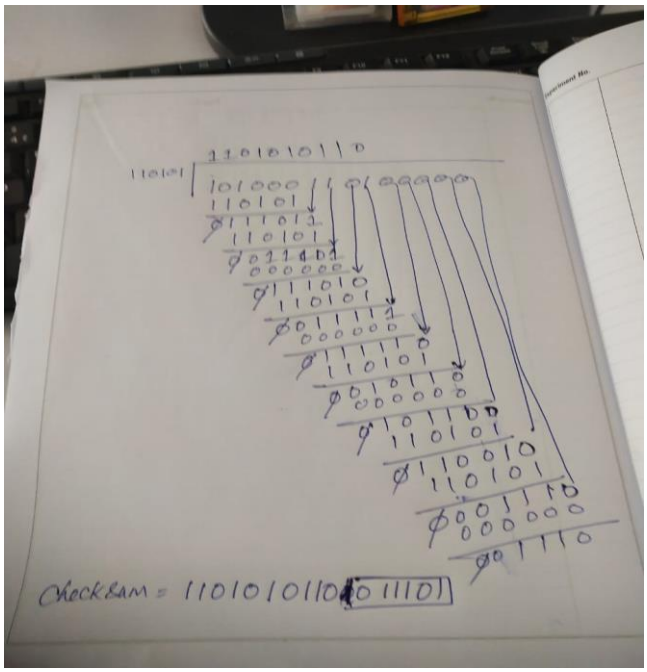
1. **Byte-Oriented Framing**:
   - **Example**: HDLC (High-Level Data Link Control) protocol uses byte-oriented framing. In HDLC, a special flag sequence, such as 01111110, marks the beginning and end of a frame. Additionally, byte stuffing is employed to prevent accidental detection of flags within the data.
2. **Bit-Oriented Framing**:
   - **Example**: Ethernet frames use bit-oriented framing. Ethernet frames are composed of a preamble, start frame delimiter (SFD), destination and source MAC addresses, EtherType field, data payload, and frame check sequence (FCS). The preamble and SFD help in synchronization and framing of the data.
3. **Character-Oriented Framing**:
   - **Example**: PPP (Point-to-Point Protocol) utilizes character-oriented framing. PPP frames begin and end with a flag byte sequence (01111110). The data within the frame can include any character, and character stuffing is employed if the data contains the flag byte sequence.
4. **Start-Stop Framing**:
   - **Example**: Asynchronous serial communication often employs start-stop framing. In this method, each frame begins with a start bit (usually logic low) and ends with one or more stop bits (usually logic high). UART (Universal Asynchronous Receiver-Transmitter) communication commonly uses start-stop framing.
5. **Frame Delimiter Framing**:
   - **Example**: Token Ring networks utilize frame delimiter framing. Frames in Token Ring networks are identified by a special start of frame delimiter (SFD) and end of frame delimiter (EFD) sequences. These delimiters help synchronize the transmission and reception of frames in the network.

These framing methods ensure that data sent over the physical medium is properly delineated into individual frames, allowing for accurate transmission and reception of data between network devices at the data link layer. Each method has its own characteristics and is chosen based on factors such as efficiency, compatibility, and the specific requirements of the communication protocol.

1.b) A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then what will be the input bit-string

Solution: 0111110101

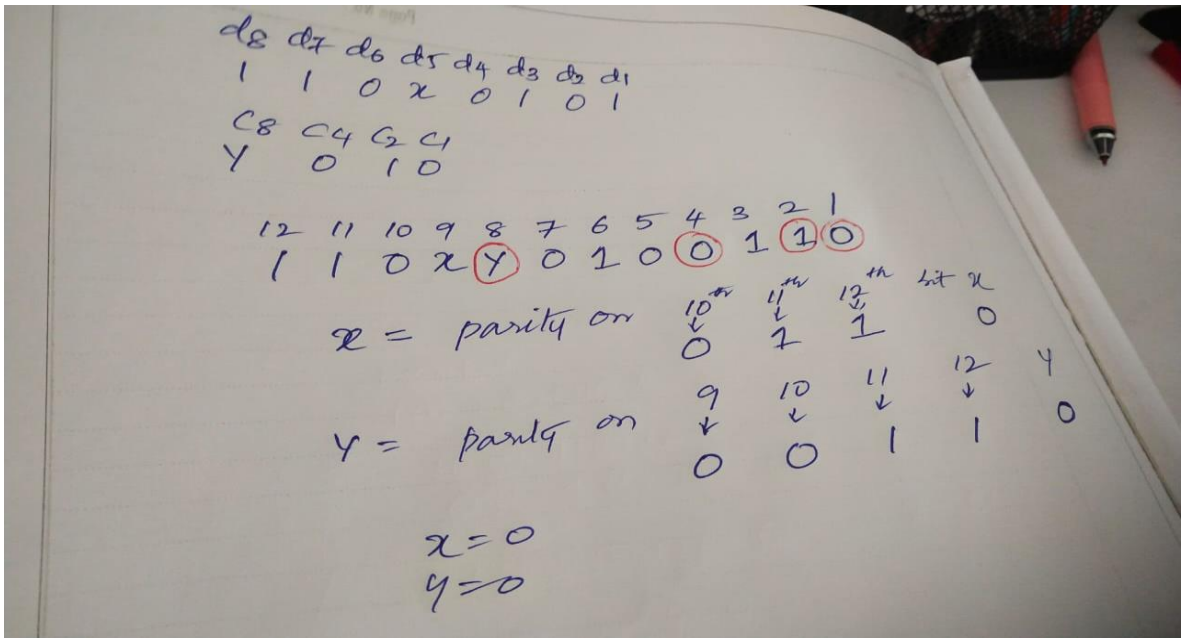
2.a) Consider the cyclic redundancy check (CRC) based error detecting scheme having the generator polynomial $x^5 + x^4 + x^2 + 1$. Suppose the message M = 1010001101 is to be transmitted. Check bits are appended at the end of the message by the transmitter using the above CRC scheme. Find bitstring with databits and checkbit sequence that will be transmitted.



2.b) Assume that a 12-bit Hamming code word consisting of 8-bit data and 4 check bits is $d_8d_7d_6d_5c_8d_4d_3d_2c_4d_1c_2c_1$, where the data bits and the check bits are given in the following tables: what should be the values if x and Y

Data bits							
d_8	d_7	d_6	d_5	d_4	d_3	d_2	d_1
1	1	0	x	0	1	0	1

c_8	c_4	c_2	c_1
Y	0	1	0



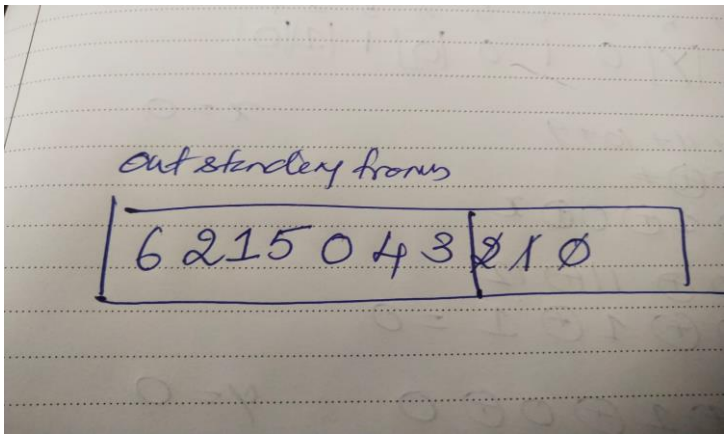
3.a) In the given procedure for positive acknowledgement with retransmission protocol. Fill in the blank statements to complete the procedure.

```
void sender (void)
        {
        Seq_nr  next_frame_to_send;
        frame s;
        packet buffer;
        event_type event;
        next_frame_to_send = 0;
        from_network_layer(&buffer);
        while (true)
             {
               s.info = ----------;
               s.seq =  -----------;
               ----------------------;
               Start-timer(s.seq);
               wait_for_event (&event);
               if (event == frame arrival)
                   {
                     from physical layer(&s);
                     if (s.ack ==  ----------------)
                                 {
                            stop_timer(s.ack);
                            from_network_layer(&buffer);
                              ------------------------------;

                                    }
                         }
                   }
             }
```

SOLUTION:

```
void sender (void)
        {
        Seq_nr  next_frame_to_send;
        frame s;
        packet buffer;
        event_type event;
        next_frame_to_send = 0;
        from_network_layer(&buffer);
        while (true)
             {
               s.info = buffer;
               s.seq =  next frame to send;

               to physical layer(&s);
               Start-timer(s.seq);
               wait_for_event (&event);
               if (event == frame arrival)
                   {
                     from physical layer(&s);
                     if (s.ack ==  next frame to send)
                                 {
                              stop_timer(s.ack);
                              from_network_layer(&buffer);
                               inc(next frame to send);
                                   }
                          }
                     }
               }
```

3. b) In SR protocol, suppose frames through 0 to 4 have been transmitted. Now imagine that 0 times out and a new frame 5 is transmitted, frame 1 times out, frame 2 times out and 6 another new frame is transmitted. With a neat diagram show what will be the outstanding packets in the sender window



4.) Explain CSMA and show the behavior of three persistence methods of CSMA.

CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense

The medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it

waits till the channel becomes idle.

However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data.

However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent :** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent :** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent :** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(b) CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

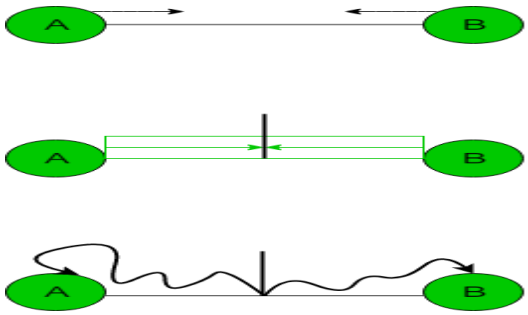
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Back-off Algorithm for CSMA/CD

Back-off algorithm is a **collision resolution** mechanism which is used in random access MAC protocols (CSMA/CD). This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.

If a collision takes place between 2 stations, they may restart transmission as soon as they can after the collision. This will always lead to another collision and form an infinite loop of collisions leading to a deadlock. To prevent such scenario back-off algorithm is used.

Let us consider an scenario of 2 stations A and B transmitting some data:



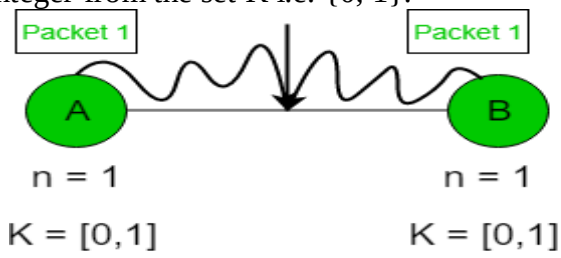
After a collision, time is divided into discrete slots ($\mathbf{T_{slot}}$) whose length is equal to 2t, where t is the maximum propagation delay in the network.
The stations involved in the collision randomly pick an integer from the set K i.e {0, 1}. This set is called the contention window. If the sources collide again because they picked the same integer, the contention window size is doubled and it becomes {0, 1, 2, 3}.

Now the sources involved in the second collision randomly pick an integer from the set {0, 1, 2, 3} and wait that number of time slots before trying again. Before they try to transmit, they listen to the channel and transmit only if the channel is idle. This causes the source which picked the smallest integer in the contention window to succeed in transmitting its frame.

So, Back-off algorithm defines a *waiting time for the stations involved in collision*, i.e. for how much time the station should wait to re-transmit.

Example
–Case-1

Suppose 2 stations A and B start transmitting data (Packet 1) at the same time then, collision occurs. So, the collision number n for both their data (Packet 1) = 1. Now, both the station randomly pick an integer from the set K i.e. {0, 1}.



Value of K

A	B
0	0
0	1
1	0
1	1

- **When both A and B choose K = 0**
  –> Waiting time for A = 0 * T_{slot} = 0
  Waiting time for B = 0 * T_{slot} = 0

- Therefore, both stations will transmit at the same time and hence collision occurs.

Probability that A wins = 5/8

Probability that B wins = 1/8

Probability of collision = 2/8

So, probability of collision decreases as compared to Case 1.

Advantage –

- Collision probability decreases exponentially.

Disadvantages –

- **Capture effect:** Station who wins ones keeps on winning.
- Works only for 2 stations or hosts.

(d) CSMA/CA –

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred.

To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

1. **Inter frame space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called 'Inter frame space' or 'IFS'. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations.

Controlled Access Protocols

In controlled access, the stations seek information from one another to find which station

has the right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium.

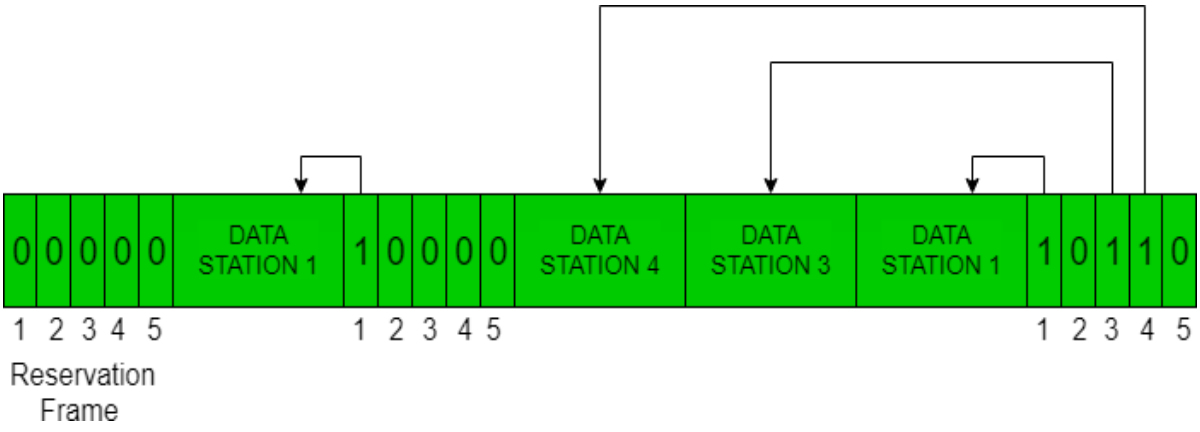
The three controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  1. Reservation interval of fixed time length
  2. Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station hasone slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other stationis allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit intoi th slot. After all N slots have been checked, each station knows which stations wishtotransmit.

The following figure shows a situation with five stations and a five slot reservation frame. In the firstinterval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

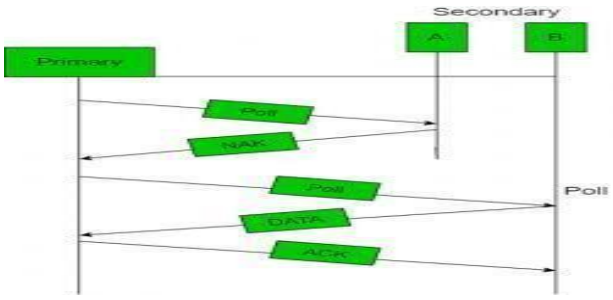


Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a

controllersends a message to each node in turn.

- In this, one acts as a primary station(controller) and the others are secondary stations. Alldata exchanges must be made through the controller.
- Although all nodes receive the message but the addressed one responds to it and sends data,
  if any. If there is no data, usually a "poll reject"(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence onthereliability of the controller.

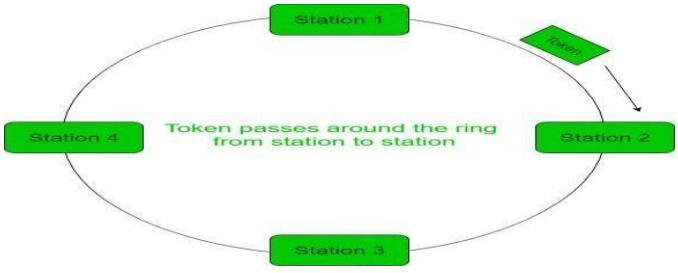


Efficiency

Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

Token Passing

- In token passing scheme, the stations are connected logically to each other in form ofringand access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to thenext in the some predefined order.
- After sending a frame, each station must wait for all N stations (including itself) to send thetoken to their neighbors and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable



operation of this scheme.

Performance

Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, which is a measure of time between when a packet is ready and when it is

delivered. So, the average time (delay) required to send a token to the next station = a/N.

2. **Throughput**, which is a measure of the successful traffic.

5) What is hidden terminal problem in wireless networks? Explain in detail. Also give the solution for hidden terminal problem.

The hidden terminal problem is a challenge encountered in wireless networks, particularly in scenarios where multiple devices communicate with a single access point (AP) or within a shared wireless medium. In such environments, certain terminals may be hidden from each other due to obstacles or physical distance, even though they are within range of the AP. This can lead to interference and collisions during data transmission, ultimately degrading network performance.

To understand the hidden terminal problem, let's consider a simple scenario involving three wireless devices: A, B, and C, all within the range of an access point (AP). A and B can communicate directly with the AP, as can B and C. However, A and C are not within direct communication range of each other, leading to the hidden terminal problem.

Here's a step-by-step breakdown of how the hidden terminal problem occurs:

1. Device A wants to transmit data to the AP.
2. Device B is within range of both A and the AP.
3. Device C, however, is hidden from A's perspective.
4. Device C, unaware of A's transmission, decides to transmit data to the AP simultaneously.
5. The AP receives conflicting signals from both A and C, leading to a collision.
6. As a result, the data transmitted by both A and C may be corrupted or lost, requiring retransmission and reducing overall network efficiency.

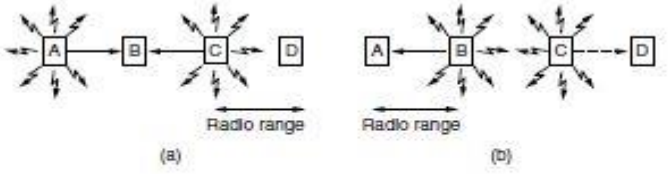


Figure 4-11. A wireless LAN. (a) *A* and *C* are hidden terminals when transmitting to *B*. (b) *B* and *C* are exposed terminals when transmitting to *A* and *D*.

This scenario illustrates the hidden terminal problem, where devices are unable to detect each other's presence due to physical obstacles or distance, leading to collisions and degraded network performance.

To mitigate the hidden terminal problem, several solutions have been proposed and implemented in wireless networking protocols:

1. **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**: This protocol, commonly used in Wi-Fi networks, incorporates a mechanism where devices listen to the wireless medium before transmitting data. If the medium is busy (indicating ongoing transmissions), devices wait for a random backoff period before attempting to transmit. While CSMA/CA can help reduce collisions, it doesn't completely solve the hidden terminal problem.
2. **Request to Send/Clear to Send (RTS/CTS)**: In this scheme, before transmitting data, a device sends a Request to Send (RTS) frame to the AP. If the AP receives the RTS frame without any interference, it replies with a Clear to Send (CTS) frame. This exchange reserves the channel for the duration of the transmission, reducing the likelihood of collisions caused by hidden terminals.

By implementing these techniques and protocols, network administrators can effectively mitigate the hidden terminal problem and improve the overall performance and reliability of wireless networks. However, it's essential to consider the specific characteristics and requirements of the network environment when selecting and deploying these solutions.

6. a) Differentiate between pure Aloha and slotted Aloha with examples

Pure ALOHA and Slotted ALOHA are both random access protocols used in packet-switched networks, particularly in the context of early Ethernet and satellite communication systems. They share similarities but also have key differences in terms of how they handle the transmission of data packets. Here's a comparison between the two:

1. **Timing Mechanism**:
   - **Pure ALOHA**: In Pure ALOHA, there is no strict timing mechanism. Devices attempt to transmit data whenever they have packets ready, leading to a completely random access approach. Collisions are resolved after they occur.
   - **Slotted ALOHA**: Slotted ALOHA introduces a timing mechanism by dividing time into fixed-size slots. Devices are only allowed to transmit at the beginning of each time slot. This synchronization reduces the chances of collisions and simplifies collision resolution.
2. **Transmission Time**:
   - **Pure ALOHA**: Devices can attempt to transmit data at any time, leading to the possibility of collisions occurring at any moment. As a result, the efficiency of Pure ALOHA is lower compared to Slotted ALOHA.
   - **Slotted ALOHA**: With the introduction of time slots, devices are restricted to transmitting only at the beginning of each slot. This reduces the probability of collisions and improves overall network efficiency compared to Pure ALOHA.
3. **Collision Handling**:
   - **Pure ALOHA**: Collisions are detected after the entire packet has been transmitted. If a collision is detected, devices wait for a random backoff period before attempting to retransmit the packet.
   - **Slotted ALOHA**: Collisions are more predictable in Slotted ALOHA since transmissions occur at the beginning of each time slot. If a collision occurs, devices wait for the next time slot to retransmit the packet, reducing the likelihood of further collisions.
4. **Efficiency**:
   - **Pure ALOHA**: Pure ALOHA has lower efficiency compared to Slotted ALOHA due to the higher probability of collisions and the need for random backoff periods.
   - **Slotted ALOHA**: Slotted ALOHA offers higher efficiency compared to Pure ALOHA because of the synchronization provided by time slots, which reduces the probability of collisions and simplifies collision resolution.
5. **Implementation Complexity**:
   - **Pure ALOHA**: Pure ALOHA is simpler to implement since it does not require synchronization or time slot management.
   - **Slotted ALOHA**: Slotted ALOHA introduces additional complexity due to the need for time slot synchronization and management.

In summary, while both Pure ALOHA and Slotted ALOHA are random access protocols used in packet-switched networks, Slotted ALOHA introduces a timing mechanism with fixed-size time slots, leading to higher efficiency and simpler collision resolution compared to Pure ALOHA. However, this comes at the cost of increased implementation complexity.

---

6 .b) Explain any three collision free protocols

1. **Bit map protocol**
2. **Token Passing**
3. **Binary Countdown**

Bit map Protocol

In bit-map method, each contention period consists of exactly *N* slots. If station 0 has a frame to send, it transmits a 1 bit during the slot 0. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 bit during slot 1, but only if it has a frame queued. In general, station *j* may announce that it has a frame to send by inserting a 1 bit into slot *j*. After all *N* slots have passed by, each station has complete knowledge of which stations wish to transmit. At that point, they begin transmitting frames in numerical order.

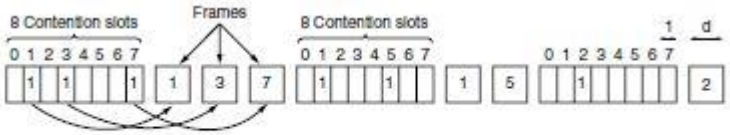


Figure 4-6. The basic bit-map protocol.

Token Passing

The essence of the bit-map protocol is that it lets every station transmit aframe in turn in a predefined order. Another way to accomplish the same thing is to pass a small message called a **token** from one station to the next in the same predefined order. The token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it simply passes the token

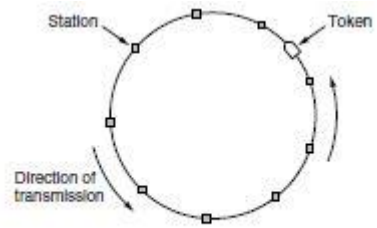


Figure 4-7. Token ring.

Binary Count down

A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high order bit. All addresses are assumed to be the same length. The bits in each address position from different stations are BOOLEAN OR ed together by the channel when they are sent at the same time. We will call this protocol **binary countdown**. To avoid conflicts, an arbitration rule must be applied: as soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up. For example, if stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0, 0, 1, and 1, respectively. These are OR ed together to form a 1. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue. The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up. The winner is station 1010 because it has the highest address. After winning the bidding, it may now transmit a frame, after which another bidding cycle starts

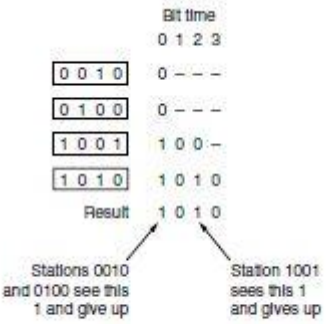


Figure 4-8. The binary countdown protocol. A dash indicates silence.