Scheme of Evaluation Internal Assessment Test 3 –AUG 2022

Sub:	Data Communication							**Code:**	18CS46
Date:	4/8/2022	Duration:	90mins	Max Marks:	50	**Sem:**	IV	**Branch:**	ISE

Note: **Answer Any five full questions.**

Question #		**Description**	**Marks Distribution**		**Max Marks**
1	a)	Explain the concept of checksum algorithm. Illustrate the algorithm for given data 24, 11, 12, 7, 13, 4 for corrupted and uncorrupted data **Explanation+ Solving problem**	5M	5M	10M
2	a)	What is the Taxonomy of MAC Protocol? Discuss in brief CSMA/CA. **Taxonomy+ Explanation**	2M+4M	6M	6M
2	b)	Explain about i)Simplest Protocol and ii)Stop and Wait Protocol i)Simplest Protocol **Explanation**	2M+2M	4M	4M
3		List out protocols in Random Access protocol taxonomy and explain Pure ALOHA and Slotted ALOHA. **List+Figure + Explanation**	2M+3M+5M	10M	10M

4		What is class full addressing scheme of IPv4? Explain each class in detail. **Definition** **Explanation**	2M+8M	10 M	10M
5		Explain the architecture of IEEE 802.11 standards. **Explanation+objective+Architecture**	5M+2M+3M	10 M	10M
6	a)	Explain different persistence methods involved in CSMA. **Types+ Explanation**	3M+3M	6M	6M
	b)	A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free? **Solving Problem**	4M	4M	4M

Scheme Of Evaluation Internal Assessment Test 3– AUG 2022

Sub:	Data Communication							**Code:**	18CS46
Date**:**	4/8/2022	Duration:	90mins	Max Marks:	50	**Sem:**	IV	**Branch:**	ISE

Note: **Answer Any full five questions**

Q1)Explain the concept of checksum algorithm. Illustrate the algorithm for given data 24, 11, 12, 7, 13, 4 for corrupted and uncorrupted data.

A checksum is a technique used to determine the authenticity of received data, i.e., to detect whether there was an error in transmission. Along with the data that needs to be sent, the sender uses an algorithm to calculate the checksum of the data and sends it along.

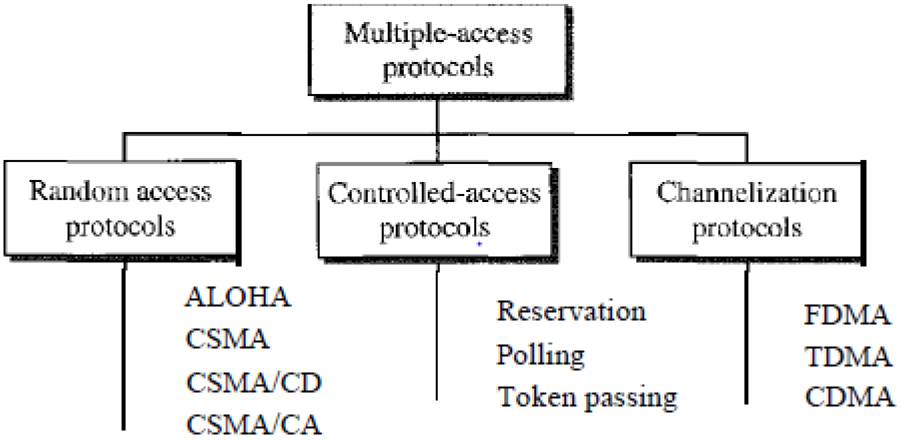
The Checksum is an error detecting method that is applied to the higher layer protocols. In this technique, the generator subdivides the data unit into equal segments of n bits. These segments are added using 1's complement method in a way such that the result is also n-bit long. The sum is then 1's complemented and appended to the data unit as redundant bits that are called the Checksum field**.**

The receiver subdivides the data unit into segments of n bits. The segments are then added using 1's complement method such that the result is n bit long. The result is then 1's complemented. If it is zero then the data unit is correct, otherwise, there must be some error within it.

Q 2a)What is the Taxonomy of MAC Protocol? Discuss in brief CSMA/CA.

1. RANDOM ACCESS:

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.



This decision depends on the state of the medium (idle or busy).Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access. Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10% additional energy. This is not useful for effective collision detection. We need to avoid collisions on wireless networks because they cannot be detected.

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network. Collisions are avoided through the use of CSMAICA's three strategies: the interframespace, the contention window, and acknowledgments

Q2b) Explain about i)Simplest Protocol and ii)Stop and Wait Protocol

i)Simplest Protocol

The simplest protocol is a unidirectional protocol in which the data frames are traveling in only one direction from the sender to the receiver. Since the simplest protocol is unidirectional, there is no acknowledgment (ACK). Also, as there is no data loss in the transmission, there is no need for data re-transmission

ii)Stop and Wait Protocol

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Q3)List out protocols in Random Access protocol taxonomy and explain Pure ALOHA and Slotted ALOHA.

Random Access Protocols

- ALOHA.
- Carrier sense multiple access (CMSA)
- Carrier sense multiple access with collision detection (CMSA/CD)
- Carrier sense multiple access with collision avoidance (CMSA/CA)

Pure aloha is used when data is available for sending over a channel at stations. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.

Pure ALOHA

The mode of random access in which users can transmit at any time is called pure Aloha. This technique is explained below in a stepwise manner.

Step 1 − In pure ALOHA, the nodes transmit frames whenever there is data to send.

Step 2 − When two or more nodes transmit data simultaneously, then there is a chance of collision and the frames are destroyed.

Step 3 − In pure ALOHA, the sender will expect acknowledgement from the receiver.

Step 4 − If acknowledgement is not received within specified time, the sender node assumes that the frame has been destroyed.

Step 5 − If the frame is destroyed by collision the node waits for a random amount of time and sends it again. This waiting time may be random otherwise the same frames will collide multiple times.

Step 6 − Therefore, pure ALOHA says that when the time-out period passes, each station must wait for a random amount of time before re-sending its frame. This randomness will help avoid more collisions

Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot

Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

In this method it was proposed that the time be divided up into discrete intervals (T) and each interval correspond to one frame .i.e the user should agree on the slot boundaries and require each station to begin each transmission at the beginning of a slot.

Q4) What is class full addressing scheme of IPv4? Explain each class in detail

An IPv4 address class is a categorical division of internet protocol addresses in IPv4-based routing.

Separate IP classes are used for different types of networks. Some are used for public internet-accessible IPs and subnets, that is, those networks behind a router (as in classes A, B and C). As well, some classes are reserved by the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA) for specific purposes. These special ranges are used for multicasting of identical data to all computers on a network or subnet or for research (as in classes D, E).

Within this notation, classes are mainly differentiated by the number of bits they have for the network and the number of bits used for hosts. IP addresses are notated in four groups of three-digit representations of 8 bits of binary in base 10-formatted notation for a total of 32 bits. The groups are separated by periods starting from zero (which in binary would be 00000000); the highest number in a grouping is 255 (or 11111111).
IPv4 address classes:
Class A IP addresses, where the 1st bit is 0, encompass the range of 0.0.0.0 to 127.255.255.255. This class is for large networks and has 8 bits for network and 24 bits for hosts.
Class B IP addresses, where the 1st two bits are 10, are in the range of 128.0.0.0 to 191.255.255.255. This class is for medium networks and has 16 bits for network and 16 bits for hosts.
Class C IP addresses, where the 1st three bits are 110, are in the range of 192.0.0.0 to 223.255.255.255. This class is for smaller networks and has 24 bits for network and 8 bits for hosts.

Class D or multicast IP addresses, where the 1st four bits are 1110 are in the range of 224.0.0.0 to 239.255.255.255

Class E or experimental IP addresses, where the 1st four bits are 11110, are in the range of 240.0.0.0 to 255.255.255.255.

Prior to the introduction of IPv6 as a solution to the internet's running out of addresses, the idea of opening the class E addresses was hotly debated. While forming the basis for IP address assignment, the system of IP address classes described here is generally bypassed today by use of Classless Inter-Domain Routing (CIDR) addressing.

Q5)Explain the architecture of IEEE 802.11 standards.

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network(WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands

The IEEE developed an international standard for WLANs. The 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer (PHY) and data link layer (DLL).

The objective of the IEEE 802.11 standard was to define a medium access control (MAC) sublayer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.

The three physical layers are an IR base band PHY, an FHSS radio in the 2.4 GHz band, and a DSSS radio in the 2.4 GHz.

IEEE 802.11 Architecture:

The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations. This type of architecture has several advantages. It is tolerant of faults in all of the WLAN equipment and eliminates possible bottlenecks a centralized architecture would introduce. The architecture is flexible and can easily support both small, transient networks and large, semi permanent or permanent networks. In addition, the architecture and protocols offer significant power saving and prolong the battery life of mobile equipment without losing network connectivity

Two network architectures are defined in the IEEE 802.11 standard:

Infrastructure network: An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources. The transition of data from the wireless to wired medium occurs via an AP. An AP and its associated wireless clients define the coverage area. Together all the devices form a basic service set (refer figure 1).

Point-to-point (ad-hoc) network: An ad-hoc network is the architecture that is used to support mutual communication between wireless clients. Typically, an ad-hoc network is created spontaneously and does not support access to wired networks. An ad-hoc network does not require an AP.

Q6 a)Explain different persistence methods involved in CSMA.

The three types of Carrier Sense Multiple Access (CSMA) Protocols are as follows −

- 1-persistent CSMA
- Non- Persistent CSMA
- p-persistent CSMA

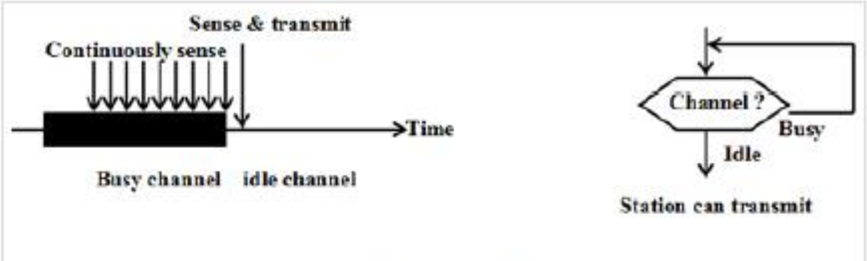
1-persistent CSMA

In this method, to transmit data the station wants to continuously sense the channel to check whether the channel is busy or idle.

Suppose, if the channel is busy, then the station will wait until it becomes idle. Whenever the station detects an idle-channel, then it transmits the frame with probability. Therefore this persistence is called 1-persistent CSMA.

The 1-persistent CSMA has the highest chance of collision because two or more stations identify a channel to be idle at the same time and transmit their frames.

Whenever the collision occurs, the stations will wait a random amount of time and start again. The structure of 1-persistent CSMA is as follows −



1-persistent CSMA

Drawback of 1-persistent

In this 1-persistence the propagation delay time is more.

For example − If station 1 begins its transmission, at the same time station 2 is also ready to send its data and senses the channel. If the station 1 signal has not still reached station 2, station 2 thought that the channel is idle and will begin its transmission. This will result in a collision.

Even though the propagation delay time is zero, the collision will occur. If two stations are ready in the middle of the third station's transmission, then both stations have to wait till the transmission of the first station ends and then both will begin their transmission exactly at the same time. This will also result in collision.

p-persistent CSMA

The p-persistent CSMA is used whenever the channel has time slots so that the time slot duration is equal to or greater than the maximum propagation delay time. The p-persistence senses the channel whenever a station becomes ready to send.

Suppose if the channel is busy, then the station has to wait till the next slot is available.

The p-persistence transmits with a probability p when the channel is idle. With a probability q=1-p, the station has to wait for the beginning of the next time slot. If the next slot is idle, it either transmits or waits again with probabilities p and q.

This process will continue until the frame has been transmitted or another station has begun transmitting. If another station is transmitting, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

Advantages

The advantages of p-persistent CSMA are as follows −

- The p-persistence reduces the chance of collision.
- Improves the efficiency of the network.

Q 6b) A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

- Average frame transmission time
  Tfr = 200 bits/200 kbps or 1 ms

  Vulnerable time = 2x Tfr = 2 × 1 ms = 2 ms.

****