R.M.K
GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

R.M.K
GROUP OF
INSTITUTIONS

20CS501
Computer Networks

Department

Computer Science and Engineering
Artificial Intelligence and Data Science

Batch/Year

2020-2024 / III Year

Created by

Ms.S.Srijayanthi (ADS)
Ms.K.Ramya Devi (CSE)
Mr.Kingsley S

Date

30.07.2022

R.M.K GROUP OF INSTITUTIONS

Table of Contents

S NO	CONTENTS
1	Contents
2	Course Objectives
3	Pre Requisites (Course Names with Code)
4	Syllabus (With Subject Code, Name, LTPC details)
5	Course Outcomes
6	CO- PO/PSO Mapping
7	Lecture Plan
8	Activity Based Learning
9	Notes
10	Assignments
11	Part A (Q & A)
12	Part B Qs
13	Supportive Online Certification Courses
14	Real time Applications in day to day life and to Industry
15	Contents Beyond the Syllabus
16	Assessment Schedule
17	Prescribed Text Books & Reference Books

R.M.K GROUP OF INSTITUTIONS

COURSE OBJECTIVES

- To study the fundamental concepts of computer networks and physical layer.
- To gain the knowledge of various protocols and techniques used in the data link layer.
- To learn the services of network layer and network layer protocols.
- To describe different protocols used in the transport layer.
- To understand the application layer protocols.

R.M.K GROUP OF INSTITUTIONS

SYLLABUS

UNIT I **INTRODUCTION AND PHYSICAL LAYER**

Data Communications – Network Types – Protocol Layering – Network Models (OSI, TCP/IP) Networking Devices: Hubs, Bridges, Switches – Performance Metrics – Transmission media - Guided media -Unguided media- Switching-Circuit Switching - Packet Switching.

UNIT II **DATA LINK LAYER**

Introduction – Link-Layer Addressing- Error Detection and Correction - DLC Services – Data Link Layer Protocols – HDLC – PPP - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth

UNIT III **NETWORK LAYER**

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

UNIT IV **TRANSPORT LAYER**

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram Protocol –Transmission Control Protocol – SCTP.

UNIT V **APPLICATION LAYER**

Application layer-WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP

R.M.K GROUP OF INSTITUTIONS

Course Outcomes

CO1: Understand the fundamental concepts of computer networks and physical layer.

CO2: Gain knowledge of various protocols and techniques used in the data link layer.

CO3: Learn the network layer services and network layer protocols.

CO4: Understand the various protocols used in the transport layer.

CO5: Analyze the various application layer protocols.

R.M.K GROUP OF INSTITUTIONS

CO- PO/PSO Mapping

Overall Correlation Matrix of the Course as per Anna University Curriculum

Course Code	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C302	3	1	2									

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes Including Course Enrichment Activities

Course Outcomes (COs)		Programme Outcomes (POs), Programme Specific Outcomes (PSOs)														
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
		K3	K4	K5	K5	K3/K5	A2	A3	A3	A3	A3	A3	A2	K3	K3	K3
C302.1	K2	2	1											2	2	2
C302.2	K4	3	3	2	2									3	3	3
C302.3	K4	3	3	2	2									3	3	3
C302.4	K4	3	2	2	2									3	3	3
C302.5	K3	3	2	1	1									3	3	3
C302.6	K2	2	1											2	2	2
C302.7	A2												3			
C302.8	A2								2	2	2		3			
C302.9	A3						3	3		3	3		3			
C302		3	3	2	2		1	1	1	3	3		3	3	3	3

R.M.K GROUP OF INSTITUTIONS

LECTURE PLAN

UNIT – II							
S No	Topics	No of periods	Proposed date	Actual Lecture Date	pertaining CO	Taxonomy level	Mode of delivery
1	Introduction	1	01.09.2022			K1	Chalk & Talk
2	Link Layer Addressing	1	02.09.2022			K1	ICT Tools
3	Error Detection and Correction	1	03.09.2022			K2	ICT Tools
4	DLC Services	1	05.09.2022			K2	ICT Tools
5	Data Link Layer Protocols	1	06.09.2022			K2	ICT Tools
6	DLL protocol HDLC	1	07.09.2022			K2	ICT Tools
7	Data link Layer Protocol PPP	1	08.09.2022			K2	ICT Tools
8	Wired LANs Ethernet	1	09.09.2022			K2	ICT Tools
9	Wireless LANs Introduction	1	10.09.2022			K2	ICT Tools
10	IEEE802.11	1	14.09.2022			K2	ICT Tools
11	Bluetooth	1	15.09.2022			K2	ICT Tools

R.M.K GROUP OF INSTITUTIONS

ACTIVITY BASED LEARNING
(MODEL BUILDING/PROTOTYPE)

S NO	TOPICS
1	https://drive.google.com/file/d/1tpKCE5A7FkmLWtoMntzcj9Hafxnrue M_/view

INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

UNIT II DATA-LINK LAYER & MEDIA ACCESS

Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP - Media Access Control - Wired LANs: Ethernet - Wireless LANs – Introduction –IEEE 802.11, Bluetooth – Connecting Devices.

2.1 INTRODUCTION

- The Internet is a combination of networks glued together by connecting devices.
- If a packet is to travel from a host to another host, it needs to pass through these networks.
- Communication at the data-link layer is made up of separate logical connections between the data-link layers in the path.
- Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router.

Nodes and Links

- Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point as shown in Figure 2.1.
- These LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as ***nodes*** and the networks in between as ***links***.

Figure 2.1: Nodes and links

- The first node is the source host and the last node is the destination host.
- The other four nodes are four routers.
- The first, the third, and the fifth links represent the three LANs;
- The second and the fourth links represent the two WANs.

Reference video

https://www.youtube.com/watch?v=pi7mMjiixiY&feature=youtu.be

Services

Framing

- The first service provided by the data-link layer is framing.
- The data-link layer at each node needs to encapsulate the datagram in a frame before sending it to the next node.
- The node also needs to decapsulate the datagram from the frame received on the logical channel.

Flow Control

- The sending data-link layer at the end of a link is a producer of frames; the receiving data-link layer at the other end of a link is a consumer.
- If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed.
- We have two choices.
- The first choice is to let the receiving data-link layer drop the frames if its buffer is full.
- The second choice is to let the receiving data-link layer send a feedback to the sending data-link layer to ask it to stop or slow down.

R.M.K GROUP OF INSTITUTIONS

Error Control

At the sending node,

- a frame in a data-link layer needs to be changed to bits
- Transformed to electromagnetic signals and transmitted through the transmission media.

At the receiving node,

- Electromagnetic signals are received
- Transformed to bits and put together to create a frame.
- Since electromagnetic signals are susceptible to error, a frame is susceptible to error.
- The error needs first to be detected.
- After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.
- Since error detection and correction is an issue in every layer.

Two Categories of Links

- In a point-to-point link, the link is dedicated to the two devices;
- In a broadcast link, the link is shared between several pairs of devices.

Two Sublayers

- Data link control (DLC)
- Media access control (MAC).

The data link control sublayer deals with **all issues common to both point-to-point and broadcast links.**

The media access control sublayer deals only with **issues specific to broadcast links.**The sublayers are shown in Figure 2.2.

a. Data-link layer of a broadcast link

b. Data-link layer of a point-to-point link

Figure 2.2: Dividing the data-link layer into two sublayers

R.M.K GROUP OF INSTITUTIONS

2.2 LINK-LAYER ADDRESSING

- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.

- These two addresses are changed every time the frame moves from one link to another.

- We have three links and two routers.

For each host, two addresses,

The IP addresses (N) and the link-layer addresses (L). As shown in Figure 2.3,

- Three frames, one in each link. Each frame carries the same datagram with the same source and destination addresses (N1 and N8),

- But the link-layer addresses of the frame change from link to link.

- In link 1, the link-layer addresses are L1 and L2. In link 2, they are L4 and L5. In link 3, they are L7 and L8.

- For IP addresses, the source address comes before the destination address

- For link layer addresses , the destination address comes before the source.

Figure 2.3:IP addresses and link-layer addresses in a small internet

Three Types of addresses

Some link-layer protocols define three types of addresses: unicast, multicast, and broadcast.

Unicast Address

- Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Multicast Address

- Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication.

Broadcast Address

- Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

Address Resolution Protocol (ARP)

- The ARP protocol is one of the auxiliary protocols defined in the network layer, as shown in Figure 2.4.

Figure 2.4: Position of ARP in TCP/IP protocol suite

- The sender sends the ARP query packet on the network which is broadcasted to all the other host or router present in the network.

- The ARP query packet contains the logical and physical address of the sender and the logical address of the receiver.

- All the host and router receiving the ARP query packet process it but, only the intended receiver identifies its logical address present in the ARP query packet.

- The receiver then sends ARP response packet which contains the logical (IP) address and physical address of the receiver.

- The ARP response packet is unicast directly to the sender whose physical address is present in the ARP query packet. It is shown in Figure 2.5.

b. ARP reply is unicast

Figure 2.5: ARP request and ARP reply

- In Figure, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address N2. System A needs to pass the packet to its data-link layer for the actual delivery, but it does not know the physical address of the recipient.

- It uses the services of ARP by asking the ARP protocol to send abroad cast ARP request packet to ask for the physical address of a system with an IP address of N2.

- This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure.

- System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination using the physical address it received.

Packet Format

Figure 2.6 shows the format of an ARP packet.

Hardware: LAN or WAN protocol
Protocol: Network-layer protocol

Figure 2.6: ARP packet format

- The hardware type field defines the type of the link-layer protocol; Ethernet is given the type 1.
- The protocol type field defines the network-layer protocol: IPv4 protocol is (0800)16.
- The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender.
- The destination hardware address and destination protocol address fields define the receiver link-layer and network-layer addresses.
- An ARP packet is encapsulated directly into a data-link frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

ARP Vs RARP

BASIS FOR COMPARISON	ARP	RARP
Full Form	Address Resolution Protocol.	Reverse Address Resolution Protocol.
Basic	Retrieves the physical address of the receiver.	Retrieves the logical address for a computer from the server.
Mapping	ARP maps 32-bit logical (IP) address to 48-bit physical address.	RARP maps 48-bit physical address to 32-bit logical (IP) address.

R.M.K GROUP OF INSTITUTIONS

Reference videos

https://www.youtube.com/watch?v=cn8Zxh9bPio&feature=youtu.be

https://www.youtube.com/watch?v=jQerVWxOGMc&feature=youtu.be

https://www.slideshare.net/secret/3NK3bdmzBjJZy

R.M.K GROUP OF INSTITUTIONS

Error Detection and Correction

Data can be corrupted during transmission. Some applications require that errors be detected and corrected.

Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal.

In a single-bit error, a 0 is changed to a 1 or a 1 to a O.

In a burst error, multiple bits are changed. For example, a 11100 s burst of impulse noise on a transmission with a data rate of 1200 bps might change all or some of the12 bits of information.

Single-Bit Error

The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.

Single-Bit Error The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1

Figure 10.1 shows the effect of a single-bit error on a data unit. To understand the impact of the change, imagine that each group of 8 bits is an ASCII character with a 0 bit added to the left.

In Figure,00000010 (ASCII STX) was sent, meaning start of text, but 00001010 (ASCII LF) was received, meaning line feed.

Single-bit errors are the least likely type of error in serial data transmission.

R.M.K GROUP OF INSTITUTIONS

Burst Error

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Figure shows the effect of a burst error on a data unit. In this case, 0100010001000011 was sent, but 0101110101100011 was received. Note that a burst error does not necessarily mean that the errors occur in consecutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits.

The number of bits affected depends on the data rate and duration of noise.

For example, if we are sending data at I kbps, a noise of 11100 s can affect 10 bits; if we are sending data at I Mbps, the same noise can affect 10,000 bits.

Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection Versus Correction

The correction of errors is more difficult than the detection. A single-bit error is the same as a burst error. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors.

R.M.K GROUP OF INSTITUTIONS

If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities.

Forward Error Correction Versus Retransmission

There are two main methods of error correction.

Forward error correction is the process in which the receiver tries to guess the message by using redundant bits.

Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message.

Resending is repeated until a message arrives that the receiver believes is error-free (usually, not all errors can be detected).

Coding

Redundancy is achieved through various coding schemes.

The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.

The receiver checks the relationships between the two sets of bits to detect or correct the errors. The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme.

Figure shows the general idea of coding. We can divide coding schemes into two broad categories: block coding and convolution coding.

R.M.K GROUP OF INSTITUTIONS

Figure 10.3 *The structure of encoder and decoder*

BLOCK CODING

In block coding, we divide our message into blocks, each of k bits, called datawords.

We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called codewords.

We have a set of datawords, each of size k, and a set of codewords, each of size of n.

With k bits, we can create a combination of 2^k datawords; with n bits, we can create a combination of 2^n codewords. Since n > k, the number of possible codewords is larger than the number of possible datawords.

The block coding process is one-to-one; the same dataword is always encoded as the same codeword. This means that we have 2^n - 2^k codewords that are not used. These codewords are invalid or illegal. Figure shows the situation.

Figure 10.5 *Datawords and codewords in block coding*

Error Detection

If the following two conditions are met, the receiver can detect a change in the original codeword.

1. The receiver has (or can find) a list of valid codewords.
2. The original codeword has changed to an invalid one.

Figure 10.6 shows the role of block coding in error detection.

The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding.

Each codeword sent to the receiver may change during transmission.

If the received codeword is the same as one of the valid codewords, the word is accepted; the corresponding dataword is extracted for use.

If the received codeword is not valid, it is discarded. However, if the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.

This type of coding can detect only single errors. Two or more errors may remain undetected.

Figure 10.6 *Process of error detection in block coding*

Error Correction

Error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received codeword is invalid; in error correction the receiver needs to find (or guess) the original codeword sent.

Figure shows the role of block coding in error correction.

Figure 10.7 *Structure of encoder and decoder in error correction*

2.3 DLC SERVICES

The data link control (DLC) deals with procedures for communication between two adjacent nodes i.e. node-to-node communication and no matter whether the link is dedicated or broadcast.

Data link control functions include 1. Framing 2. Flow Control 3. Error Control.

FRAMING

A frame is a group of bits.

Framing means organizing the bits into a frame that are carried by the physical layer.

The data-link-layer needs to form frames, so that each frame is distinguished from another.

- Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address.
- The destination address defines where the packet is to go.
- The sender address helps the recipient acknowledge the receipt.
-
-
-
-

R.M.K GROUP OF INSTITUTIONS

Why the whole message is not packed in one frame?

- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.

Frame Size Types

1. Fixed Size Framing

In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

2. Variable Size Framing

In variable-size framing, we need a way to define the end of one frame and the beginning of the next.

Two Approaches

1. Character-oriented approach
2. Bit-oriented approach

CHARACTER-ORIENTED APPROACH

- Data to be carried are 8-bit characters from a coding system such as ASCII.
- The header carries the source and destination addresses and other control information.
- The trailer, carries error detection redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit flag is added at the beginning and the end of a frame.

Figure 2.7: Frame format in character-oriented approach

R.M.K GROUP OF INSTITUTIONS

Problem:

- Character-oriented framing was popular when only text was exchanged by the data-link layers.
- The flag could be selected to be any character not used for text communication.
- Now we send other types of information such as graphs, audio, and video.
- Any character used for the flag could also be part of the information.
- If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame.

Solution: A byte-stuffing is used.

Byte stuffing

- A special byte is added to the data-section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte.
- This byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section
- And treats the next character as data, not as a delimiting flag.

Problem:

- What happens if the text contains one or more escape characters followed by a flag?
- The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame.

Solution:

- Escape characters part of the text must also be marked by another escape character. It is shown in Figure 2.8.

R.M.K GROUP OF INSTITUTIONS

Figure 2.8: Byte stuffing and unstuffing

BIT-ORIENTED FRAMING

- In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame, as shown in Figure 2.9.

Figure 2.9: Frame format in bit-oriented approach

- If the flag pattern appears in the data, we need to inform the receiver that this is not the end of the frame.
- We do this by stuffing 1 single bit to prevent the pattern from looking like a flag. The strategy is called bit stuffing.

- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.
- Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. Figure 2.10 shows bit stuffing at the sender and bit removal at th

Figure 2.10: Bit stuffing and unstuffing

- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

FLOW CONTROL AND ERROR CONTROL

- One of the responsibilities of the DLC sublayer is flow and error control at the data-link layer.

FLOW CONTROL

- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.
- If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.
- We need to prevent losing the data items at the consumer site.

Figure 2.11: Flow control at the data-link layer

- At the sending node, as shown in Figure 2.11, the data-link layer tries to push frames toward the data-link layer at the receiving node.
- If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames.
- Here, flow control can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers

- Flow control can be implemented by using buffer.
- A buffer is a set of memory locations that can hold packets at the sender and receiver.
- Normally, two buffers can be used. First buffer at the sender. Second buffer at the receiver.
- The flow control communication can occur by sending signals from the consumer to the producer.
- When the buffer of the receiver is full, it informs the sender to stop pushing frames.

ERROR CONTROL

- Error-control includes both error-detection and error-correction.
- Error-control allows the receiver to inform the sender of any frames lost/damaged in transmission.
- A CRC is added to the frame header by the sender and checked by the receiver.
- At the data-link layer, error control is normally implemented using one of the following two methods.
- First method: If the frame is corrupted, it is discarded; If the frame is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.

- Second method: If the frame is corrupted, it is discarded; If the frame is not corrupted, an acknowledgment is sent to the sender. Acknowledgment is used for the purpose of both flow and error control.

Combination of Flow and Error Control

- Flow and error control can be combined.
- The acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted.
- The lack of acknowledgment means that there is a problem in the sent frame.
- A frame that carries an acknowledgment is normally called an ACK to distinguish it from the data frame.

Connectionless and Connection-Oriented

- A DLC protocol can be either connectionless or connection-oriented.

Connectionless Protocol

- Frames are sent from one node to the next without any relationship between the frames; each frame is independent.
- The term connectionless does not mean that there is no physical connection (transmission medium) between the nodes; it means that there is no connection between frames.
- The frames are not numbered and there is no sense of ordering.
- Most of the data-link protocols for LANs are connectionless protocols.

Connection Oriented Protocol

- A logical connection should first be established between the two nodes (setup phase).
- After all frames that are somehow related to each other are transmitted (transfer phase), the logical connection is terminated (teardown phase).. The frames are numbered and sent in order.
- If the frames are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer.
- Connection oriented protocols are rare in wired LANs, but we can see them in some point-to- point protocols, some wireless LANs, and some WANs.

R.M.K GROUP OF INSTITUTIONS

2.4 DATA-LINK LAYER PROTOCOLS

- Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:

- Simple
- Stop-and-Wait
- Go-Back-N
- Selective-Repeat

- The first two protocols are common at the data-link layer, the last two are no longer used.
- The behavior of a data-link-layer protocol can be better shown as a finite state machine (FSM). An FSM is thought of as a machine with a finite number of states. It is shown in Figure 2.12.
- The machine is always in one of the states until an event occurs.
- Each event is associated with two reactions: defining the list of actions to be performed and determining the next state.

Figure 2.12: Connectionless and connection-oriented service represented as FSMs

- One of the states must be defined as the initial state, the state in which the machine starts when it turns on.
- In Figure 2.12, we show an example of a machine using FSM.

- The figure shows a machine with three states. There are only three possible events and three possible actions.
- The machine starts in state I. If event 1 occurs, the machine performs actions 1 and 2 and moves to state II.
- When the machine is in state II, two events may occur. If event 1 occurs, the machine performs action 3 and remains in the same state, state II.
- If event 3 occurs, the machine performs no action, but move to state I.

Simple Protocol

- Our first protocol is a simple protocol with neither flow nor error control.
- Assume that the receiver can immediately handle any frame it receives.
- Figure 2.13 shows the layout for this protocol.

Figure 2.13: Simple protocol

- The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.
- The data-link layers of the sender and receiver provide transmission services for their network layers.
- The sender site should not send a frame until its network layer has a message to send.
- The receiver site cannot deliver a message to its network layer until a frame arrives.

R.M.K GROUP OF INSTITUTIONS

FSMs

- We can show these requirements using two FSMs.
- Each FSM has only one state, the ready state.
- The sending machine remains in the ready state until a request comes from the process in the network layer.
- When this event occurs, the sending machine encapsulates the message in a frame and sends it to the receiving machine.
- The receiving machine remains in the ready state until a frame arrives from the sending machine.
- When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.
- Figure 2.14 shows the FSMs for the simple protocol.

Figure 2.14: FSMs for the simple protocol

FLOW DIAGRAM

Figure 2.15: Flow diagram for the simple protocol

R.M.K GROUP OF INSTITUTIONS

Stop-and-Wait Protocol

- The Stop-and-Wait protocol uses both flow and error control.
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- Corrupted frames are detected with a CRC to each data frame.
- Figure shows the outline for the Stop-and-Wait protocol. Note that only one frame and one acknowledgment can be in the channels at any time.

Figure 2.16: Stop and Wait protocol

FSM

Figure 2.17: FSM for the Stop and Wait protocol

Sender States

- The sender is initially in the ready state, but it can move between the ready and blocking state.

Ready State

- When the sender is in this state, it is only waiting for a packet from the network layer.
- If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame.
- The sender then moves to the blocking state.

Blocking State

- When the sender is in this state, three events can occur:
- If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.
- If a corrupted ACK arrives, it is discarded.
- If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

Receiver States

- The receiver is always in the ready state. Two events may occur:
- If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.
- If a corrupted frame arrives, the frame is discarded.

Example

Figure 11.12 shows an example. The first frame is sent and acknowledged. The second frame is sent, but lost. After time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgment is lost. The frame is resent. However, there is a problem with this scheme. The network layer at the receiver site receives two copies of the third packet, which is not right. In the next section, we will see how we can correct this problem using sequence numbers and acknowledgment numbers.

Figure 2.18: Example for Stop and Wait protocol

- The first frame is sent and acknowledged.
- The second frame is sent, but lost.
- After time-out, it is resent.
- The third frame is sent and acknowledged, but the acknowledgment is lost.
- The frame is resent.

Sequence and Acknowledgment Numbers

- Duplicate packets, as much as corrupted packets, need to be avoided. We need to add sequence numbers to the data frames and acknowledgment numbers to the ACK frames.
- Sequence numbers are 0, 1, 0, 1, 0, 1, . . . ; the acknowledgment numbers can also be 1, 0, 1, 0, 1, 0, …
- In other words, the sequence numbers start with 0, the acknowledgment numbers start with 1. An acknowledgment number always defines the sequence number of the next frame to receive.

Piggybacking

- The two protocols are designed for unidirectional communication in which data is flowing only in one direction although the acknowledgment may travel in the other direction.
- It is used to improve the efficiency of the bidirectional protocols.
- Protocols have been designed in the past to allow data to flow in both directions.
- However, to make the communication more efficient, the data in one direction is piggybacked with the acknowledgment in the other direction.

Reference Video : https://www.youtube.com/watch?v=kSgtZnffCog

2.5 HDLC

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- It implements the Stop-and-Wait protocol.
- HDLC provides 2 common transfer modes that can be used in different configurations:

1. Normal response mode (NRM) 2. Asynchronous balanced mode (ABM).

- The station configuration is unbalanced.
- We have one primary station and multiple secondary stations.
- A primary station can send commands, a secondary station can only respond.
- The NRM is used for both point-to-point and multiple-point links.

Figure 2.19: Normal response mode

ABM

- The configuration is balanced.
- Link is point-to-point, and each station can function as a primary and a secondary (acting as peers).
- This is the common mode today.

Figure 2.20: Asynchronous response mode

Framing

- To provide the flexibility necessary to support all the options possible in the modes and configurations, HDLC defines three types of frames:

i.Information frames (I-frames): are used to transport user data and control information relating to user data (piggybacking).

ii.Supervisory frames (S-frames): are used only to transport control information.

iii.Unnumbered frames (U-frames): are reserved for system management. Information carried by U-frames is intended for managing the link itself.

- Each type of frame serves as an envelope for the transmission of a different type of message.

Frame Format

Figure 2.21: HDLC frames

Various fields of HDLC frame are:

Flag Field

- This field has a synchronization pattern 01111110.
- This field identifies both the beginning and the end of a frame.

Address Field

- This field contains the address of the secondary station.
- If a primary station created the frame, it contains a to-address.
- If a secondary creates the frame, it contains a from-address.
- This field can be 1 byte or several bytes long, depending on the needs of the network.

Control Field

- This field is one or two bytes used for flow and error control.

Information Field

- This field contains the user's data from the network-layer or management information.
- Its length can vary from one network to another.

FCS Field

- This field is the error-detection field. (FCS . Frame Check Sequence)
- This field can contain either a 2- or 4-byte standard CRC.

R.M.K GROUP OF INSTITUTIONS

Control Fields of HDLC Frames

- The control field determines the type of frame and defines its functionality.

Figure 2.22: Control field format for the different frame types

1. Control Field for I-Frames

- I. frames are designed to carry user data from the network-layer.
- In addition, they can include flow and error-control information (piggybacking).
- The subfields in the control field are:
  1) The first bit defines the type.
- If the first bit of the control field is 0, this means the frame is an I-frame.
  1) The next 3 bits N(S) define the sequence-number of the frame. With 3 bits, we can define a sequence-number between 0 and7.
  2) The last 3 bits N(R) correspond to the acknowledgment-number when piggybacking is used.
  3) The single bit between N(S) and N(R) is called the P/F bit.
- The P/F field is a single bit with a dual purpose. It can mean poll or final.
  1) It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver).
  2) It means final when the frame is sent by a secondary to a primary(when the address field contains the address of the sender).

2. Control Field for S-Frames

- Supervisory frames are used for flow and error-control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment).
- S-frames do not have information fields.

R.M.K GROUP OF INSTITUTIONS

- The subfields in the control field are:

1. If the first 2 bits of the control field is 10, this means the frame is an S-frame.
2. The last 3 bits N(R) corresponds to the acknowledgment-number (ACK) or negative acknowledgment-number (NAK).
3. The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames:

1.)Receive Ready (RR) = 00

- This acknowledges the receipt of frame or group of frames.
- The value of N(R) is the acknowledgment-number.

2.)Receive Not Ready (RNR) = 10

- This is an RR frame with 1 additional function:
- It announces that the receiver is busy and cannot receive more frames.
- It acts as congestion control mechanism by asking the sender to slow down.
- The value of N(R) is the acknowledgment-number.

3.)ReJect (REJ) = 01

- It is a NAK frame used in Go-Back-N ARQ to improve the efficiency of the process.
- It informs the sender, before the sender time expires, that the last frame is lost or
- damaged.
- The value of N(R) is the negative acknowledgment-number.

4.)Selective REJect (SREJ) = 11

- This is a NAK frame used in Selective Repeat ARQ.
- The value of N(R) is the negative acknowledgment-number.

3. Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.

R.M.K GROUP OF INSTITUTIONS

- U-frames contain an information field used for system management information, but not user data.
- Much of the information carried by U-frames is contained in codes included in the control field.
- U-frame codes are divided into 2 sections:
  I. A 2-bit prefix before the P/F bit
  II. A 3-bit suffix after the P/F bit.
- Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

2.6 POINT-TO-POINT PROTOCOL (PPP)

- One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP).
- Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP.
- They are connected to the Internet through a telephone line, which provides the services of the physical layer.
- But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data-link layer.PPP is by far the most common.

Services

1. Services Not Provided by PPP

- PPP does not provide flow control. A sender can send several frames one after another with no concern about the receiver.
- PPP has a very simple mechanism for error control. A CRC field is used to detect errors.
- If the frame is corrupted, it is discarded; Lack of error control and sequence numbering may cause a packet to be received out of order.
- PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

R.M.K GROUP OF INSTITUTIONS

2. Services Provided by PPP

- Format of the frame to be exchanged between devices.
- Establishment of the link and the exchange of data.
- PPP is designed to accept payloads from several network layers.
- Authentication is also provided in the protocol.
- It provides network address configuration.
- It is useful when a home user needs a temporary network address to connect to the Internet. The new version of PPP, called Multilink PPP.

Framing

PPP uses a character-oriented (or byte-oriented) frame. Figure 2.23 shows the format of a PPP frame. The description of each field follows:

Figure 2.23: PPP frame format

❑ Flag.

A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

❑ Address.

The address field in this protocol is a constant value and set to 11111111 (broadcast address).

❑ Control.

- This field is set to the constant value 00000011.
- PPP does not provide any flow control. Error control is also limited to error detection.

❑ Protocol.

The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

R.M.K GROUP OF INSTITUTIONS

❑ Payload field.

- This field carries either the user data or other information.
- The data field is a sequence of bytes - maximum of 1500 bytes.
- The data field is byte-stuffed if the flag byte pattern appears.
- Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value.

❑ FCS - The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Transition Phases

A PPP connection goes through phases shown in a transition phase diagram in Figure 2.24.

Figure 2.24: Transition diagram of a PPP connection

- The transition diagram starts with the dead state.
- There is no active carrier.
- When one of the two nodes starts the communication, the connection goes into the establish state.

I. Options are negotiated between the two parties.
II. If the two parties agree that they need authentication, then the system needs to do authentication; otherwise, the parties can simply start communication.
III. Data transfer takes place in the open state.
IV. When a connection reaches this state, the exchange of data packets can be started.

R.M.K GROUP OF INSTITUTIONS

- The connection remains in this state until one of the endpoints wants to terminate the connection.
- In this case, the system goes to the terminate state.
- The system remains in this state until the carrier is dropped, which moves the system to the dead state again.

Multiplexing

Although PPP is a link-layer protocol, it uses another set of protocols

i. to establish the link,
ii. authenticate the parties involved,
iii. and carry the network-layer data.

Three sets of protocols are defined to make PPP powerful:

- The Link Control Protocol (LCP),
- Two Authentication Protocols (APs),
- Several Network Control Protocols (NCPs).

Link Control Protocol

- The Link Control Protocol (LCP) is responsible for establishing, maintaining, configuring, and terminating links.
- It also provides negotiation mechanisms to set options between the two end points.

Figure 2.25: LCP packet encapsulated in a frame

- Both end points of the link must reach an agreement about the options before the link can be established.
- All LCP packets are carried in the payload field of the PPP frame with the protocol field set to C021 in hexadecimal.

Code	Packet Type	Description
0x01	Configure-request	Contains the list of proposed options and their values
0x02	Configure-ack	Accepts all options proposed
0x03	Configure-nak	Announces that some options are not acceptable
0x04	Configure-reject	Announces that some options are not recognized
0x05	Terminate-request	Request to shut down the line
0x06	Terminate-ack	Accept the shutdown request
0x07	Code-reject	Announces an unknown code
0x08	Protocol-reject	Announces an unknown protocol
0x09	Echo-request	A type of hello message to check if the other end is alive
0x0A	Echo-reply	The response to the echo-request message
0x0B	Discard-request	A request to discard the packet

Table 2.1 LCP packets

Code

- The code field defines the type of LCP packet. There are 11 types of packets. There are three categories of packets.
- The first category - Comprising the first four packet types, is used for link configuration during the establish phase.
- The second category - comprising packet types 5 and 6, is used for link termination during the termination phase.
- The Third category -The last five packets are used for link monitoring and debugging.

ID field

The ID field holds a value that matches a request with a reply.

Length

The length field defines the length of the entire LCP packet.

Information

- The information field contains information, such as options, needed for some LCP packets.
- Options are inserted in the information field of the configuration packets. Information field is divided into three fields: option type, option length, and option data.

Authentication Protocols

- PPP is designed for use over dial-up links where verification of user identity is necessary.

R.M.K GROUP OF INSTITUTIONS

- Authentication means validating the identity of a user who needs to access a set of resources.

- PPP has created two protocols for authentication:
  - ❖ Password Authentication Protocol and
  - ❖ Challenge Handshake Authentication Protocol.

- Note that these protocols are used during the authentication phase.

PAP - Password Authentication Protocol

- It is a simple authentication procedure with a two-step process:
  a. The user who wants to access a system sends authentication identification (usually the user name) and a password.
  b. The system checks the validity of the identification and password and either accepts or denies connection.

- When a PPP frame is carrying any PAP packets, the value of the protocol field is 0xC023.

Figure 2.26: PAP packets encapsulated in a PPP frame

The three PAP packets are authenticate-request, authenticate-ack, and authenticate-nak.

1. The first packet is used by the user to send the user name and password.
2. The second is used by the system to allow access.
3. The third is used by the system to deny access.

CHAP - Challenge Handshake Authentication Protocol

It is a three-way handshaking authentication protocol that provides greater security than PAP.

In this method, the password is kept secret; it is never sent online.

i.The system sends the user a challenge packet containing a challenge value, usually a few bytes.

ii.The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

iii.The system does the same. It applies the same function to the password of the user and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

Figure 2.27: CHAP packets encapsulated in a PPP frame

CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.

CHAP packets are encapsulated in the PPP frame with the protocol value C223 in hexadecimal.

R.M.K GROUP OF INSTITUTIONS

There are four CHAP packets:

Challenge, Response, Success, Failure.

1.The first packet is used by the system to send the challenge value.

2.The second is used by the user to return the result of the calculation.

3.The third is used by the system to allow access to the system.

4.The fourth is used by the system to deny access to the system.

Network Control Protocols

- PPP is a multiple-network-layer protocol.
- It can carry a network-layer data packet from protocols defined by the Internet, OSI, Xerox, DECnet, AppleTalk, Novel, and so on.
- PPP has defined a specific Network Control Protocol for each network protocol.

IPCP

- One NCP protocol is the Internet Protocol Control Protocol (IPCP).
- This protocol configures the link used to carry IP packets in the Internet.
- The value of the protocol field in hexadecimal is 8021.
- IPCP defines seven packets, distinguished by their code values.

Figure 2.28: IPCP packet encapsulated in PPP frame

Code	*IPCP Packet*
0x01	Configure-request
0x02	Configure-ack
0x03	Configure-nak
0x04	Configure-reject
0x05	Terminate-request
0x06	Terminate-ack
0x07	Code-reject

Table 2.2: Code Values for IPCP Packets

7. MEDIA ACCESS CONTROL

- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.

- Many protocols have been devised to handle access to a shared link.

- All of these protocols belong to a sub-layer in the data-link layer called media access control (MAC).

- There are three categories of media access control. They are:

- Random-access protocols -These protocols are mostly used in LANs and WANs
  - ALOHA,
  - CSMA
  - CSMA/CD
  - CSMA/CA

- Controlled-access protocols. – Some of these protocols are used in LANs
  - Reservation
  - Polling
  - Token-passing

- Channelization protocols - These protocols are used in cellular telephony
  - FDMA
  - TDMA
  - CDMA

Figure 2.29: Classification Of Multiple Access Protocols

RANDOM ACCESS PROTOCOLS

- In random-access or contention methods, no station is superior to another station and none is assigned control over another.
- There is no scheduled time for a station to transmit.
- Transmission is random among the stations.
- Stations compete with one another to access the medium. That is why these methods are also called contention methods.
- If more than one station tries to send, there is an access conflict—collision—and the frames will be either destroyed or modified.

ALOHA

- ALOHA, the earliest random access method was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

a)Pure ALOHA

- The original ALOHA protocol is called pure ALOHA.
- Each station sends a frame whenever it has a frame to send (multiple access).
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

Figure 2.30: Frame collisions in pure ALOHA

- As seen in figure 2.30, each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. The diagram shows that only two frames survive: one frame from station 1 and one frame from station 3.

- The pure ALOHA protocol relies on acknowledgments from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back off time TB.
- The vulnerable time during which a collision may occur in pure ALOHA is 2 times the frame transmission time (Tfr).

Pure ALOHA vulnerable time = 2xTfr

Figure 2.31 shows the procedure for pure ALOHA based on the above strategy.

Figure 2.31: Procedure for pure ALOHA

R.M.K GROUP OF INSTITUTIONS

b)Slotted ALOHA

- Pure ALOHA has a vulnerable time of 2 × Tfr.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA we divide the time into slots of Tfr seconds and force the station to send only at the beginning of the time slot.

Figure 2.32: Frame collisions in slotted ALOHA

- A station is allowed to send only at the beginning of the synchronized timeslot, if a station misses this moment, it must wait until the beginning of the next timeslot.
- This means that the station which started at the beginning of this slot has already finished sending its frame.
- There is still the possibility of collision if two stations try to send at the beginning of the same time slot.
- Vulnerable time is now reduced to one-half, equal to Tfr.

CSMA

- Carrier sense multiple access (CSMA) requires that each station first listen to the medium before sending.
- CSMA is based on the principle —sense before transmit|| or —listen before talk.||
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

R.M.K GROUP OF INSTITUTIONS

Figure 2.33: Collision

- In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.
- At time t2 (t2 > t1), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame.
- The two signals collide and both frames are destroyed.

Persistence Methods

Three methods have been devised to answer these questions:

- The 1-persistent method,
- The non-persistent method,
- The p-persistent method.

Figure 2.34 shows the behavior of three persistence methods when a station finds a channel busy.

Figure 2.34: Persistence methods

c. *p*-persistent

Figure 2.34: Persistence methods

1-Persistent

The 1-persistent method is simple and straightforward.

- In this method, after the station finds the line idle, it sends its frame.
- 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

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

The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time.

- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.

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 back-off procedure

CSMA/CD

Carrier senses multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

- a station monitors the medium after it sends a frame to see if the transmission was successful.

- If so, the station is finished. If, however, there is a collision, the frame is sent again.

In Figure 2.35 stations A and C are involved in the collision.

Figure 2.35: Collision

- At time t1, station A has executed its persistence procedure and starts sending the bits of its frame.

- At time t2, station C has not yet sensed the first bit sent by A.

- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.

- The collision occurs sometime after time t2. Station C detects a collision at time t3 when it receives the first bit of A's frame.

- Station C immediately (or after a short time, but we assume immediately) aborts transmission.

- Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.

- A transmits for the duration t4 – t1; C transmits for the duration t3 – t2.

Figure 2.36: Collision in data frames

Procedure

The flow diagram for CSMA/CD is in Figure 2.37.

Figure 2.37: Flow diagram for CSMA/CD

It is similar to the one for the ALOHA protocol, but there are differences.

- The first difference is the addition of the persistence process.
- The second difference is the frame transmission.
- The third difference is the sending of a short jamming signal to make sure that all other stations become aware of the collision.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.

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

1. The interframe space
2. The contention window
3. Acknowledgments.

Figure 2.38: CSMA/CA

Interframe Space (IFS):

When an idle channel is found, the station does not send immediately. It waits for a period of time called the inter frame space or IFS. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.

Contention Window:

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential backoff strategy.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

Acknowledgment:

The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

1.Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with backoff until the channel is idle.

b.After the station is found to be idle, the station waits for a period of time called the DCF interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4.The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

Reference video: https://www.youtube.com/watch?v=iKn0GzF5-IU

CONTROLLED ACCESS PROTOCOLS

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.

1.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 mini slots in the reservation frame.

- Each mini slot belongs to a station.

Figure 2.39: Reservation

- When a station needs to send a data frame, it makes a reservation in its own mini slot.

- The stations that have made reservation scan send their data frames after the reservation frame.

2.Polling

- One device is designated as a primary station and the other devices are secondary stations.

- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

- It is up to the primary device to determine which device is allowed to use the channel at a given time.

- The primary device, therefore, is always the initiator of a session.

- This method uses poll and select functions to prevent collisions.

- The select function is used whenever the primary device has something to send.

Figure 2.40: Polling

- The poll function is used by the primary device to solicit transmissions from the secondary devices.
- However, the drawback is if the primary station fails, the system goes down.

Token Passing

- In the token-passing method, the stations in a network are organized in a logical ring.
- For each station, there is a predecessor and a successor.
- The predecessor is the station which is logically before the station in the ring.
- The successor is the station which is after the station in the ring.
- The current station is the one that is accessing the channel now.
- A special packet called a token circulates through the ring.
- The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor.
- It then holds the token and sends its data.
- When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.
- The station cannot send data until it receives the token again in the next round.

CHANNELIZATION PROTOCOLS

- **Channelization** is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.
- There are 3channelizationprotocols: FDMA, TDMA, and CDMA.

R.M.K GROUP OF INSTITUTIONS

FDMA

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data.
- Each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a band pass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

TDMA

- TDMA, is a physical layer technique that combines the data from slower channels and transmits them by using a faster channel.
- The process uses a physical multiplexer that interleaves data units from each channel.
- TDMA is an access method in the data-link layer. The data-link layer in each station tells its physical layer to use the allocated time slot. There is no physical multiplexer at the physical layer.
- Each station is allocated a time slot during which it can send data.
- Each station transmits its data in its assigned time slot.
- The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot.

CDMA

- CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link.
- It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.

2.8 WIRED LANS: ETHERNET

Ethernet Evolution

- The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.

R.M.K GROUP OF INSTITUTIONS

2.41 Ethernet Evolution

STANDARD ETHERNET

- The original Ethernet technology with the data rate of 10 Mbps is the Standard Ethernet.

Characteristics of the Standard Ethernet:

- Connectionless and Unreliable Service
- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phases.
- The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
- The sender may overwhelm the receiver with frames, which may result in dropping frames.
- If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either.
- Ethernet is also unreliable like IP and UDP.
- If a frame is corrupted during transmission and the receiver finds out about the corruption.
- It is the duty of high-level protocols to find out about it.

Frame Format

- Preamble. This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.

Figure 2.42: Ethernet frame format

- Start frame delimiter (SFD). This field (1 byte: 10101011) signals the beginning of the frame.
- Destination address (DA). This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.
- Source address (SA). This field is also six bytes and contains the link-layer address of the sender of the packet.
- Type. This field defines the upper-layer protocol whose packet is encapsulated in the frame. It is used for multiplexing and demultiplexing.
- Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- CRC. The last field contains error detection information, in this case a CRC-32.

Frame Length

- Minimum frame length: 64 bytes
- Maximum frame length: 1518 bytes
- Minimum data length: 46 bytes
- Maximum data length: 1500 bytes

Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own Network interface card (NIC).
- The NIC fits inside the station and provides the station with a link-layer address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.
- For example, 4A:30:10:21:10:1A

R.M.K GROUP OF INSTITUTIONS

Difference between Unicast, Multicast, and Broadcast Transmission

- In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.

- In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.

- In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

Access

Figure 2.43: Access method in Ethernet

- The standard Ethernet use CSMA/CD. Assume station A has a frame to send to station D.

- Station A first checks whether any other station is sending (carrier sense).If there is no signal energy on the medium, it means that no station is sending (or the signal has not reached station A).

- Station A interprets this situation as idle medium. It starts sending its frame.On the other hand, if the signal energy level is not zero, it means that the medium is being used by another station.

- Station A continuously monitors the medium until it becomes idle for 100 μs. It then starts sending the frame.

- However, station A needs to keep a copy of the frame in its buffer until it is sure that there is no collision. The medium sensing does not stop after station A has started sending the frame.

- Station A needs to send and receive continuously.

Efficiency of Standard Ethernet

- The efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

- Efficiency of standard Ethernet has been measured to be Efficiency = 1 / (1 + 6.4 X a)in which –a‖ is the number of frames that can fit on the medium.

  a = (propagation delay)/(transmission delay)

- Transmission delay is the time it takes a frame of average size to be sent out.

- Propagation delay is the time it takes to reach the end of the because the medium.

Standard Ethernet Implementation

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

Figure 2.44: Ethernet implementation

10BaseX, the number defines the data rate (10 Mbps),

- Term Base means baseband (digital) signal, and

- X approximately defines either the maximum size of the cable in 100 meters or the type of cable,

- T for unshielded twisted pair cable (UTP) and

- F for fiber-optic.

10Base5: Thick Ethernet

- The first implementation is called 10Base5, thick Ethernet, or Thicknet.

- 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver connected via a tap to a thick coaxial cable.

- The transceiver is responsible for transmitting, receiving, and detecting collisions.

- The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving.

- This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed 500 m.

- If a length of more than 500 m is needed, up to five segments, each a maximum of 500 meters, can be connected using repeaters.

Figure 2.45: 10Base5 Ethernet

10Base2: Thin Ethernet

- The second implementation is called 10Base2, thin Ethernet, or Cheaper net.
- 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations.
- In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

Figure 2.46: 10Base2 Ethernet

- The collision here occurs in the thin coaxial cable.
- This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps.
- Installation is simpler because the thin coaxial cable is very flexible.

10Base-T: Twisted-Pair Ethernet

- The third implementation is called 10Base-T or twisted-pair Ethernet.
- 10Base-T uses a physical star topology.
- The stations are connected to a hub via two pairs of twisted cable

Figure 2.47: 10BaseT Ethernet

- Two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub.
- Any collision here happens in the hub.
- Compared to 10Base5 or 10Base2, the hub actually replaces the coaxial cable as far as a collision is concerned.
- The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

10Base-F: Fiber Ethernet

Figure 2.48: 10BaseF Ethernet

R.M.K GROUP OF INSTITUTIONS

- Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F.
- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables

Fast Ethernet

- The goals of Fast Ethernet are:
  1. Upgrade the data rate to 100 Mbps.
  2. Make it compatible with Standard Ethernet.
  3. Keep the same 48-bit address.
  4. Keep the same frame format.
- **Topology :** Star
- **Encoding :**Manchester encoding
- New feature of Fast Ethernet is called **Auto negotiation**.
  - It allows a station or a hub a range of capabilities.
  - Auto negotiation allows two devices to negotiate the mode or data rate of operation.

Gigabit Ethernet

- The goals of Gigabit Ethernet are:
  1. Upgrade the data rate to 1 Gbps.
  2. Make it compatible with Standard or Fast Ethernet.
  3. Use the same 48-bit address.
  4. Use the same frame format.

R.M.K GROUP OF INSTITUTIONS

5. Keep the same minimum and maximum frame lengths.

6. Support auto negotiation as defined in Fast Ethernet.

- **Topology :** Star
- **Encoding :**Manchester encoding
- Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full duplex.
- To improve efficiency, **frame bursting** is used.
  - Instead of adding an extension to each frame, multiple frames are sent. However, to make these multiple frames look like one frame, padding is added between the frames (the same as that used for the carrier extension method) so that the channel is not idle.

10 Gigabit Ethernet

- The goals of the10 Gigabit Ethernet are:
- Upgrading the data rate to 10 Gbps,
- Keeping the same frame size and format
- Allowing the interconnection of LANs, MANs, and WAN possible.
- This data rate is possible only with fiber-optic technology at this time.

Reference video:

https://www.youtube.com/watch?v=5u52wbqBgEY

https://www.slideshare.net/secret/hIW9wqV74QDXGJ

R.M.K GROUP OF INSTITUTIONS

2.9 WIRELESS LANS

INTRODUCTION

Difference between wired and wireless LAN

❁Medium

The first difference we can see between a wired and a wireless LAN is the medium. In a wired LAN, we use wires to connect hosts. In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).

❁Hosts

In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its network interface card (NIC). In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network.

❁Isolated LANs

A wired isolated LAN is a set of hosts connected via a link-layer switch. A wireless isolated LA, called an ad hoc network is a set of hosts that communicate freely with each other.

Figure 2.49: Isolated LANs

4.Connection to Other Networks

A wired LAN can be connected to another network or an internetwork such as the Internet using a router. A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN.

Figure 2.50: Connection to other networks

Characteristics of Wireless LANs

❁Attenuation

The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.

❁Interference

Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

❁Multipath Propagation

A receiver may receive more than one signal from the same sender because electromagnetic

waves can be reflected back from obstacles such as walls, the ground, or objects.

❁Error

With the above characteristics of a wireless network, we can expect that errors and error detection are more serious issues in a wireless network than in a wired network.

Access Control

The CSMA/CD algorithm does not work in wireless LANs for three reasons:

1.To detect a collision, a host needs to send and receive at the same time (sending the frame and receiving the collision signal), which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries). They can only send or receive at one time.

2.Because of the hidden station problem, in which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.

3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

To overcome the above three problems, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used.

Hidden Station Problem

- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C.
- Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C.
- However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, w

Figure 2.51: Hidden station problem

Exposed Station Problem

- In this problem a station refrains from using a channel when it is, in fact, available.
- Station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending.
- Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.

Figure 2.52: Exposed station problem

Figure 2.53: Exposed station problem

R.M.K GROUP OF INSTITUTIONS

2.10 IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which is sometimes called wireless Ethernet.

Architecture

The standard defines two kinds of services: the **basic service set (BSS)** and the **extended service set (ESS).**

Basic Service Set (BSS)

BSS is the building blocks of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

Extended Service Set(ESS)

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network. The distribution system connects the APs in the BSSs. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.

Figure 2.54 : Services of IEEE 802.11

Figure 2.55: BSS connected to Server/Gateway

IEEE 802.11 defines two MAC sublayers: the **distributed coordination function(DCF)** and **point coordination function (PCF).**

Frame Format

Figure 2.56: Frame format of IEEE 802.11

The MAC layer frame consists of nine fields

- **Frame control (FC):** The FC field is 2 bytes long and defines the type of frame and some control information.

- **D:** This field defines the duration of the transmission that is used to set the value of NAV(Network Allocation Vector)

- **Addresses:** There are four address fields, each 6 bytes long.

- **Sequence control:** This field, often called the SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

R.M.K GROUP OF INSTITUTIONS

- **Frame body:** This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.
- **FCS:** The FCS field is 4 bytes long and contains a CRC-32 error-detection sequence.

Frame Types

- **Management Frames**

Management frames are used for the initial communication between stations and access points.

- **Control Frames**

Control frames are used for accessing the channel and acknowledging frames.

- **Data Frames**

Data frames are used for carrying data and control information.

Addressing Mechanism

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Figure 2.57: Addressing in IEEE 802.11

Case 1: 00 In this case, To DS = 0 and From DS = 0. This means that the frame is not going to a distribution system (To DS = 0) and is not coming from a distribution system (From DS = 0). The frame is going from one station in a BSS to another without passing through the distribution system.

Case 2: 01 In this case, To DS = 0 and From DS = 1. This means that the frame is coming from a distribution system (From DS = 1). The frame is coming from an AP and going to a station.

Case 3: 10 In this case, To DS = 1 and From DS = 0. This means that the frame is going to a distribution system (To DS = 1). The frame is going from a station to an AP. The ACK is sent to the original station.

R.M.K GROUP OF INSTITUTIONS

Case 4: 11 In this case, To DS = 1 and From DS = 1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another A Pin a wireless distribution system. Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

Figure 2.58 : Addressing in IEEE 802.11

Reference video:

https://www.youtube.com/watch?v=inciMfOnGdk

https://www.slideshare.net/secret/odJHu7IPjHFkTM

R.M.K GROUP OF INSTITUTIONS

2.11 BLUETOOTH (IEEE 802.15)

- Bluetooth is a wireless-LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network. This means the network is formed spontaneously.
- The devices find each other and make a network called a piconet (Usually, devices are called gadgets)
- A Bluetooth LAN can even be connected to the Internet if one of the devices has this capability.
- By nature, a Bluetooth LAN cannot be large.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless PAN operable in an area the size of a room or a hall. (PAN - personal-area network)

Applications

- Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- Monitoring devices can communicate with sensor devices in a small health care centre.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Conference attendees can synchronize their laptop computers at a conference.

2.11 BLUETOOTH (IEEE 802.15)

- Bluetooth is a wireless-LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network. This means the network is formed spontaneously.
- The devices

→ find each other and

→ make a network called a piconet (Usually, devices are called gadgets)

- A Bluetooth LAN can even be connected to the Internet if one of the devices has this capability.
- By nature, a Bluetooth LAN cannot be large.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless PAN operable in an area the size of a room or a hall. (PAN - personal-area network)

Applications

- Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- Monitoring devices can communicate with sensor devices in a small health care centre.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Conference attendees can synchronize their laptop computers at a conference.

R.M.K GROUP OF INSTITUTIONS

Architecture

- Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet.

Piconets

- A Bluetooth network is called a piconet, or a small net.
- A piconet can have up to 8 stations. Out of which
- One of station is called the primary.
- The remaining stations are called secondaries.
- All the secondary-stations synchronize their clocks and hopping sequence with the primary station.
- A piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

Figure 2.59: Piconet

- Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.
- Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

R.M.K GROUP OF INSTITUTIONS

Scatternet

- Piconets can be combined to form a scatternet.
- A station can be a member of 2piconets.
- A secondary station in one piconet can be the primary in another piconet. This is called mediator station.
- Acting as a secondary, mediator station can receive messages from the primary in the first piconet.
- Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

Figure 2.60 :Scatternet

Bluetooth Devices

- A Bluetooth device has a built-in short-range radio transmitter.
- The current data-rate is 1 Mbps with a 2.4-GHzbandwidth.
- This means that there is a possibility of interference between the IEEE 802.11b wireless-LANs and Bluetooth LANs.

Bluetooth Layers

- Bluetooth uses several layers that do not exactly match those of the Internet model

Figure 2.61: Bluetooth layers

Radio Layer

- The radio layer is equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

- Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

- Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.

Modulation

- To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering.

Baseband Layer

- The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- The access method is TDMA.
- The primary and secondary communicate with each other using timeslots.
- The length of a time slot is exactly the same as the dwell time, 625μs.
- This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary.
- The communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

R.M.K GROUP OF INSTITUTIONS

TDMA

- Bluetooth uses a form of TDMA that is called ***TDD-TDMA*** (***time-division duplexTDMA)*.** TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex); however, the communication for each direction uses different hops. This is similar to walkie-talkies using different carrier frequencies.

Links

- Two types of links can be created between a primary and a secondary: SCO(synchronous connection-oriented) links and ACL(asynchronous connectionless link) links.
- **SCO**: A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).SCO is used for real-time audio where avoiding delay is all-important.
- **ACL**: An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency.

Logical Link Control and Adaptation Protocol (L2CAP Layer)

- The **Logical Link Control and Adaptation Protocol,** or **L2CAP is** equivalent to the LLC sublayer in LANs and is used for data exchange on an ACL link.
- **Functions of L2CAP:** multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Multiplexing

- At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

R.M.K GROUP OF INSTITUTIONS

Segmentation and Reassembly

The L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. TheL2CAP segments the packets at the source and reassembles them at the destination.

QoS

Bluetooth allows the stations to define a quality-of-service level. Bluetooth offers best-effort service.

Group Management

L2CAP allows multicasting. For example, two or three secondary devices can be part of a multicast group to receive data from the primary.

Reference video

:https://www.youtube.com/watch?v=jzxZUJmOu3o&feature=youtu.be

https://www.slideshare.net/secret/gbdjfuyYi0CqFf

2.12 CONNECTING DEVICES

- Hosts and networks do not normally operate in isolation.
- Connecting devices are used to connect hosts together to make a network or to connect networks together to make an internet.
- Connecting devices can operate in different layers of the Internet model.
- There are three kinds of connecting devices:
    i. Hubs
    ii. Link-layer switches
    iii. Routers

Figure 2.62 :Three categories of connecting devices

Hubs

- A hub is a device that operates only in the physical layer.
- In Ethernet LANs that used bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable.
- Ethernet LANs of today star topology.
- In a star topology, a repeater is a multiport device, often called a hub that can be used to serve as the connecting point and at the same time function as a repeater.

Figure 2.63: Hub

- When a packet from station A to station B arrives at the hub, the hub broadcasts the frame.
- All stations in the LAN receive the frame, but only station B keeps it. The rest of the stations discard it.
- A hub does not have a filtering capability; it does not have the intelligence to find from which port the frame should be sent out.
- A hub or a repeater is a physical-layer device.
- They do not have a link-layer address and they do not check the link-layer address of the received frame.
- They just regenerate the corrupted bits and send them out from every port.

R.M.K GROUP OF INSTITUTIONS

Link-Layer Switches

- A link-layer switch (or switch) operates in both the physical and the data-link layers.
- As a physical-layer device, it regenerates the signal it receives.
- As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.
- A link-layer switch has filtering capability. It can check the destination address of a frame and can decide from which outgoing port the frame should be sent.

Example:

Consider a LAN with four stations that are connected to a link-layer switch. If a frame destined for station 71:2B:13:45:61:42arrives at port 1, the link-layer switch consults its table to find the departing port. According to its table, frames for 71:2B:13:45:61:42 should be sent out only through port 2; therefore, there is no need for forwarding the frame through other ports.

Figure 2.64: Link layer switches

Transparent Switches

- A transparent switch is a switch in which the stations are completely unaware of the switch's existence.
- If a switch is added or deleted from the system, reconfiguration of the stations is unnecessary.
- A system equipped with transparent switches must meet three criteria:
- Frames must be forwarded from one station to another.
- The forwarding table is automatically made by learning frame movements in the network.
- Loops in the system must be prevented.

R.M.K GROUP OF INSTITUTIONS

Loop Problem

Loops can be created only when two or more broadcasting LANs are connected by more than one switch.

Figure 2.65: Loop problem in a learning switch

- Station A sends a frame to station D. The tables of both switches are empty. Both forward the frame and update their tables based on the source address A.
- Now there are two copies of the frame on LAN 2. The copy sent out by the left switch is received by the right switch, which does not have any information about the destination address D; it forwards the frame. The copy sent out by the right switch is received by the left switch and is sent out for lack of information about D.T he tables of both switches are updated, but still there is no information for destination D.
- Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies are sent to LAN2.
- The process continues on and on.

R.M.K GROUP OF INSTITUTIONS

Spanning Tree Algorithm

- To solve the looping problem, a spanning tree is used.
- The process for finding the spanning tree involves the following steps:

i. Every switch has a built-in ID (normally the serial number, which is unique). Each switch broadcasts this ID so that all switches know which one has the smallest ID.

ii. The switch with the smallest ID is selected as the root switch (root of the tree). We assume that switch S1 has the smallest ID. It is, therefore, selected as the root switch.

iii. The algorithm tries to find the shortest path (a path with the shortest cost) from the root switch to every other switch or LAN. The shortest path can be found by examining the total cost from the root switch to the destination. The combination of the shortest paths creates the shortest tree.

iv. Based on the spanning tree, we mark the ports that are part of it, the **forwarding ports (solid lines),** which forward a frame that the switch receives. We also mark those ports that are not part of the spanning tree, the **blocking ports (broken lines),** which block the frames received by the switch system.

Figure 2.66: Spanning tree algorithm

- This means there is only one path from one LAN to any other LAN. No loops are created

Figure 2.67:Finding the shortest path

Figure 2.68: Forwarding and blocking ports

Advantages of Switches

Collision Elimination

A link-layer switch eliminates the collision, thus increasing the average bandwidth available to a host in the network.

Connecting Heterogeneous Devices

A link-layer switch can connect devices that use different protocols at the physical layer (data rates) and different transmission media.

R.M.K GROUP OF INSTITUTIONS

Routers

- A router is a three-layer device; it operates in the physical, data-link, and network layers.
- As a physical-layer device, it regenerates the signal it receives.
- As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet.
- As a network-layer device, a router checks the network-layer addresses.
- A router is an internetworking device; it connects independent networks to form an internetwork.
- There are three major differences between a router and a repeater or a switch.

1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.
3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.

Figure 2.69: Connecting devices

Reference Video :

https://www.youtube.com/watch?v=eMamgWllRFY

https://www.slideshare.net/secret/NUVxW8dgbW5Gw1

QUIZ TIME

https://quizizz.com/join/quiz/5f1c0eda5b9019001ba722ab/start?from=soloLinkShare&referrer=5f1c0e90d2ce03001b845401

R.M.K GROUP OF INSTITUTIONS

ASSIGNMENT – II

1. Imagine the length of an Ethernet cable is 2500 meters. If the speed of propagation in the cable is 200,000,000 meters / second, how long does it take for a bit to travel from the beginning to the end of the network? Ignore any propagation delay. b.
2. Using the data from part a, find the maximum time it takes to sense a collision. Recall that the worst case occurs when data are sent from one end of the cable and the collision happens at the other end. c.
3. Assume that the data rate is 10 Mbps. How long does it take to generate one bit?
4. Using data from parts b and c, find the minimum size of an Ethernet frame for collision detection to work properly.

R.M.K GROUP OF INSTITUTIONS

UNIT II QUESTION BANK

PART –A

1. List the advantages of a centralized scheme. (K3,CO3)

It may afford greater control over access for priorities, overrides, and guaranteed capacity.

It enables the use of relatively simple access logic at each station.

It avoids problems of distributed coordination among peer entities.

2. What are the responsibilities of data link layer (issues)? (K1,CO3)

Specific responsibilities of data link layer include the following.

a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

3. What are the ways to address the framing problem? (K1,CO3)

Byte-Oriented Protocols(PPP)

Bit-Oriented Protocols(HDLC)

Clock-Based Framing(SONET)

4.What do you mean by framing? (May/June 2015, Nov/ Dec 2014, Nov/Dec 2013) (K2,CO3)

The datalink layer divides the stream of bits received from network layer into manageable data units called frames. This process is called framing.

5.What will be the maximum number of frames sent but unacknowledged for a sliding window of size n-1 (n is the sequence number)? (May/June 2014) (K3,CO3)

Sender maintains a window of size W_s frames. After frame 0 is sent, transmitter sends W_s -1 frames. This is the maximum number of frames that can be outstanding (i.e., unacknowledged).

6. Write short notes on CRC. (K1,CO3)

The third and most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC) CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

R.M.K GROUP OF INSTITUTIONS

7. Mention the advantage and disadvantage of error detection by receiver as compared to error detection. (May/June 2013)(K4,CO3)

Advantages:

- One is to notify the sender that the message was corrupted so that the sender can retransmit a copy of the message.
- If bit errors are rare, then in all probability the retransmitted copy will be error-free.

Disadvantages:

- Sends n-redundant bits for n-bit message.
- Many errors are undetected if both the copies are corrupted.
- Instead of adding entire data, some bits are appended to each unit.
  This is called redundant bit because the bits added will not give any new information. These bits are called error detecting codes

8. What are the two different types of errors occurred during data transmission? (May/June 2012)(K1,CO3)

Single-bit error

The term Single-bit error means that only one bit of a given data (such as byte, character, data unit or packet) is changed from 1 to 0 or from 0to 1.

Burst Error

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

9. Define checksum. (K1,CO3)

The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy.

10. Define Error Detection and Error correction. (Nov/Dec 2011)(K1,CO3)

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. They can be handled in two ways

1.When an error is discovered, the receiver can have the sender to retransmit the entire data unit.

2. A receiver can use an error correcting code, which automatically corrects

R.M.K GROUP OF INSTITUTIONS

11. What do you mean by error control? (Nov/Dec 2010)(K1,CO3)

Error control- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

12. What is flow control? (Nov/Dec 2011)(K1,CO3)

If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the Data link layer imposes a flow ctrl mechanism.

13. Mention the categories of flow control?(K2,CO3)

There are 2 methods have been developed to control flow of data across communication links. a) Stop and wait- send one from at a time. b) Sliding window- send several frames at a time.

14.Why sliding window flow control is considered to be more efficient than stop and wait flow control?(K4,CO3)

In sliding window flow control, the transmission link is treated as a pipeline that may be filled with frames in transit. But with stop-and-wait flow control only one frame may be in the pipe at a time.

15. Define bit stuffing. (May 2017, May/June 2011) (K1,CO3)

HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110. To guarantee that a special sequence does not appear in advertently anywhere else in the frame, HDLC uses a process called bit stuffing.

16. Define Piggybacking? (K1,CO3)

The technique of temporarily delaying outgoing acknowledgment so that they can be hooked onto the next outgoing data frame is widely known as piggybacking.

R.M.K GROUP OF INSTITUTIONS

17. What do you understand by CSMA protocol? (May/June 2015)(K1,CO3)

Carrier sense multiple access

- As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.
- CSMA is usually implemented in conjunction with a method for resolving the media contention.
- The two commonly used methods are:

CSMA/Collision Detection CSMA/Collision Avoidance

18.Define persistent and non-persistent CSMA. (Nov/Dec 2014)(K1,CO3)

- In1-persistenprotocolan adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.
- In general, a p-persistent algorithm transmits with probability $0 \leq p \leq 1$after a line becomes idle, and defers with probability $q = 1 - p$.

19. List the rules for CSMA/CD. (K2,CO3)

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, and then transmit immediately.
3. If a collision detected during transmission, transmit a brief jamming signal to all station to indicate collision has occurred and then cease transmission.

20. What is CSMA/CD? (Nov 11)(K1,CO3)

Carrier Sense Multiple Access with Collision Detection is one of the methods of medium access. It is used to sense whether a medium is busy before transmission. If the medium is busy, it refrains from transmitting the data or else proceeds with the transmission. Also has the ability to check whether a transmission has collided with another.

21. Mention some of the physical properties of Ethernet. (May 11) (K2,CO3)

The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link. An Ethernet is like a bus that has multiple stations plugged into it.

R.M.K GROUP OF INSTITUTIONS

22)What is the average size of an Ethernet frame? (May/June 2014)(K1,CO3)

The original Ethernet IEEE 802.3 standard defined the minimum Ethernet frame size as 64 bytes and the maximum as 1518 bytes. The maximum was later increased to 1522 bytes to allow for VLAN tagging. The minimum size of an Ethernet frame that carries an ICMP packet is 74 bytes.

23)How is the minimum size of Ethernet frame determined? (May/June 2013)(K1,CO3)

An Ethernet frame can vary between a minimum of 72 bytes and a maximum of 1526bytes. Thus, the frame rate on an Ethernet will vary with the frame size.

24) What are the advantages of Ethernet?(K2,CO3)

An Ethernet is extremely easy to administer and maintain. Second, it is inexpensive

25) What is the exponential back off? (K1,CO3)

The strategy of doubling the delay interval between each retransmission attempt is a general technique known as exponential back off.

26)What is meant by the contention period of Ethernet? How many lines are required to connect n systems in Direct Mesh topology?(K1,CO3)

When several stations on an Ethernet have data to send, there are contention periods during which collisions happen and no data is successfully transmitted. n (n-1)/2 lines are required.

27) What is the need for fragmentation? (May 2019) (K2,CO3)

Breaking the packets into smaller pieces are known as fragmentation that includes header on each packet. Whenever packets enter into a different network with some size then the router needs fragments into a smaller size that fit into new MTU.

28) Draw the frame format of Ethernet. (May 2019) (K1,CO3)

R.M.K GROUP OF INSTITUTIONS

29) Define IEEE 802.11. (May 2018) (K1,CO3)

IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4, 5, and 60 GHz frequency bands.

30) List out any four IEEE 802 standard with its name. (May 12) (K2,CO3)

- The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC).
- The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

31)What is the access method used by wireless LAN? (May 14) (K1,CO3)

The access method used by wireless LAN is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

32) Define hidden node problem. (May 16) (K1,CO3)

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in media access control sub layer.

33)What is the access method used by wireless LAN? (May/June 2014) (K1,CO3)

The Request To Send/Clear To Send (RTS/CTS) mechanism.

34)List the functions of bridge. (May 2017, Nov 2010, May/June 2015) (K2,CO3)

- A bridge is connected between two LANs with port.
- By using the port number the LANs are addressed.

Connected LANs are known as extended LAN.

35) List the two main limitations of Bridges. (Nov/Dec 2013) (K2,CO3)

- Scaling
- Heterogeneity

R.M.K GROUP OF INSTITUTIONS

36)What is the difference between bridge and a switch? (May/June 2012, Nov/Dec 2012)(K3,CO3)

Switch	Bridge
1.Switch that is used to forward packets between shared-media LANs such as Ethernets. 2. It is also called as LAN switches.	1.A node between the two Ethernets and have the node forward frames from one Ethernet to the other, this node is called bridge. 2.And a collection of LANs connected by one or more bridges is usually said to form an extended LAN.

37)List out any four IEEE 802 standards with its name. (May/June 2012)(K2,CO3)

- 802.3 – Ethernet
- 802.6 – Metropolitan Area Network (MAN)
- 802.11- Wireless LAN/Wi-Fi
- 802.15.1 – Bluetooth

38)What does IEEE 10 Base 5 standard signify?(K1,CO3)

10 represents data rate 10 Mbps , 5 refers to segment length 5* 100 m that can run without repeaters. Base represents Base band communication.

39) Define Repeater and Hub. (K1,CO3)

Repeaters and hubs are interconnecting devices.

Repeater: Repeaters extends the Ethernet segment and it repeats the signal. It does not amplify the signal.

Hub: A Hub has several point to point segments coming out. It is a multi way repeater. It broadcasts any signal through all outgoing lines.

40)Mention the different types of bridge. What are the limitations of bridges?(K2,CO3) (Nov 13)

- Simple Bridge connects two LAN
- Multi port Bridge connect more than 2 LANs
- Transparent Bridge it learns on its own about connected LANs.

The limitations of bridges: Scalability and Heterogeneity

R.M.K GROUP OF INSTITUTIONS

41) What is Bluetooth?(K1,CO3)

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices. Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs).

42) What is the need for ARP? (Nov/Dec 2013)(K2,CO3)

The goal of ARP is to enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.

43) Define RARP.(K1,CO3)

RARP allows a host to discover its IP address when it knows only its physical address.

44)Differentiate fast Ethernet and gigabit Ethernet. (Nov/Dec 2012) (K3,CO3)

Fast Ethernet

1. A 100-Mbps version called Fast Ethernet.
2. 100-Mbps Ethernets are designed to be used in full-duplex, Point-to-point configurations, which means that they are typically used in switched networks.

Gigabit Ethernet

1. A 1000-Mbps version called Gigabit Ethernet.
2. 1000-Mbps Ethernets are designed to be used in full-duplex, point-to-point configurations, which means that they are typically used in switched networks.

R.M.K GROUP OF INSTITUTIONS

UNIT – II

PART-B & PART – C

1. Discuss in detail about the Byte- oriented Protocols (PPP), Bit-oriented Protocols (HDLC) (May 16) (K2,CO3)
2. Discuss different ways to address framing problem. (May 2019, May 2018, May/June 2016, May June 2011) (K2,CO3)
3. How frame order and flow control is achieved using the data link layer? (May 14) (K2,CO3)
4. Explain various flow control mechanisms. i)Stop Wait protocol ii)Sliding window protocol (Nov 15) (K2,CO3)
5. Explain selective repeat ARQ flow control method. (8) (Nov/Dec 2016) (K2,CO3)
6. Explain in detail about the access method and frame format used in Ethernet. (May 2018, Nov 2016, May/June 2015, Nov 2014, May/June 2012) (K2,CO3)
7. Explain CSMA in detail. Describe the CSMA/CD protocol and comment on its performance for medium access. (May 11,14,17) (K2,CO3)
8. Explain the functioning of wireless LAN in detail. (Nov 10,12,15)(May 15) (K2,CO3)
9. Explain how hidden node and exposed node problem is solved in IEEE 802.11 (Nov 13) (K2,CO3)
10. Give the comparison between various wireless technologies. Enumerate 802.11 protocol stack in detail. Or Explain the architecture of IEEE 802.11 Wireless LAN. (May 2019, May/June 2016)
11. Explain the functions of MAC layer present in IEEE 802.11 with necessary diagrams. (May 17)
12. Explain the functions of ARP with frame formats. (May 2019, May 2018, Nov 2015)

(i) Discuss the MAC layer functions of IEEE802.11. (8) (May 2017)

(ii) Briefly define key requirements of Wireless LAN. (8) (May/June 2015)

(iii)Explain the various connecting devices in detail

(iv)Define Bluetooth and explain its architecture in detail. (May 2019)

R.M.K GROUP OF INSTITUTIONS

SUPPORTIVE ONLINE COURSES

S No	Course provider	Course title	Link
1	Coursera	The Bits and Bytes of Computer Networking	https://www.coursera.org/learn/computer-networking?action=enroll
2	Coursera	Computer Communications specialization	https://www.coursera.org/specializations/computer-communications
3	Udemy	Computer networks for beginners	https://www.udemy.com/course/computer-networks-for-beginners-it-networking-fundamentals/
4	Udemy	Computer Network Cabling: Ethernet Wiring Infrastructure	https://www.udemy.com/course/network-cabling/
5	Udemy	Tech Basics: Cables & Connectors	https://www.udemy.com/course/tech101-cables-and-connectors/

MINI PROJECT

Through the Internet, use socket programs to setup a simple link layer protocol between your computer and a server to fulfills the following tasks:

1) Read the small jpeg file umdlogo.jpeg or other files in a binary format using the transmitter computer or phone.
2) Pack the bit stream of the file into many I-frames with sizes of 1024bit (or others) payload.
3) Each frame contains a header of 01111110.
4) Each frame has a frame counter (1Byte). 5) Each frame attach with a CRC check by using a divisor x4 + x3 + x2 + 1 (11101) or standard CRC16.
6) The server will bounce back the packets at a packet error rate of 20% randomlly. When receiving the packet, perform CRC check.
7) Use stop and wait automatic repeat request (ARQ) for error control by resenting incorrect packet until it is correctly received.
8) Write the receiver bit stream to a file in binary format and play/show it.

R.M.K GROUP OF INSTITUTIONS

REAL TIME APPLICATIONS IN DAY TO DAY LIFE AND TO INDUSTRY

1. Communication protocols for Vehicular Ad hoc NET works

   https://www.youtube.com/watch?v=14fOqMBn9aw

1. 5G and the Future of Connected Cars

   https://www.youtube.com/watch?v=x6DfzkeQpQ0

R.M.K GROUP OF INSTITUTIONS

CONTENT BEYOND THE SYLLABUS

Introduction to network security

https://www.youtube.com/watch?v=6Jubl1UnJTE

R.M.K GROUP OF INSTITUTIONS

Assessment Schedule

- **Tentative schedule for the Assessment During 2022-2023 odd semester**

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	IAT 1	16.09.2022	22.09.2022	UNIT 1 & 2
2	IAT 2	02.11.2022	08.11.2022	UNIT 3 & 4
3	REVISION	26.11.2022	29.11.2022	UNIT 5 , 1 & 2
4	MODEL	01.12.2022	10.12.2022	ALL 5 UNITS

R.M.K GROUP OF INSTITUTIONS

Prescribed Text Books & Reference Books

TEXT BOOK

Behrouz A. Forouzan, Data Communications and Networking, Fifth Edition TMH, 2013.

REFERENCES

R.M.K GROUP OF INSTITUTIONS

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

R.M.K GROUP OF INSTITUTIONS