

Basics of Computer Network

(Code : 214445)

Semester III – Information Technology

(Savitribai Phule Pune University)

Strictly as per the New Choice Based Credit System Syllabus (2019 Course)

Savitribai Phule Pune University w.e.f. academic year 2020-2021

J. S. Katre

M.E. (Electronics and Telecommunication)
Formerly, Assistant Professor
Department of Electronics Engineering
Vishwakarma Institute of Technology (V.I.T.), Pune.
Maharashtra, India

Prof. Nilesh N. Thorat

PhD (Pursuing), M. Tech in CS, B.E. in CE
Assistant Professor in IT Department
JSPM's BSIOTR, Wagholi, Pune
Maharashtra, India.



Basics of Computer Network (Code : 214445)

(Semester III, Information Technology, Savitribai Phule Pune University)

J. S. Katre, Prof. Nilesh N. Thorat

Copyright © by Authors. All rights reserved. No part of this publication may be reproduced, copied, or stored in a retrieval system, distributed or transmitted in any form or by any means, including photocopy, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

This book is sold subject to the condition that it shall not, by the way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior written consent in any form of binding or cover other than which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above.

First Printed in India : July 2001

First Edition : August 2020 (**TechKnowledge Publications**)

This edition is for sale in India, Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Sri Lanka and designated countries in South-East Asia. Sale and purchase of this book outside of these countries is unauthorized by the publisher.

ISBN : 978-93-89889-44-4

Published by :

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner,

Pune - 411 009. Maharashtra State, India

Ph : 91-20-24221234, 91-20-24225678.

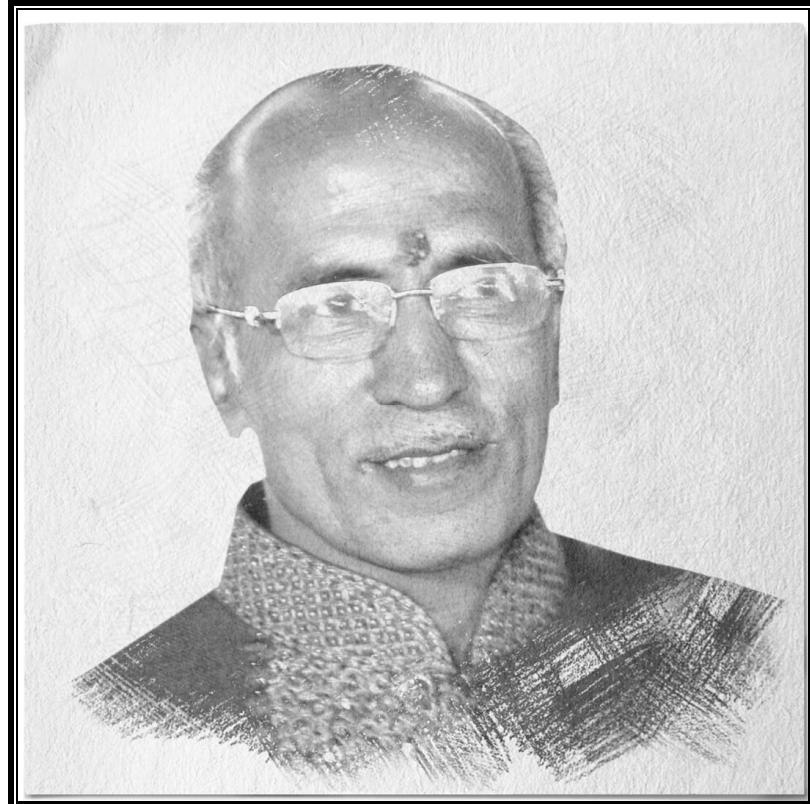
Email : info@techknowledgebooks.com,

Website : www.techknowledgebooks.com

[214445] (FID : PO133) (Book Code : PO133A)

(Book Code : PO133A)

*We dedicate this Publication soulfully and wholeheartedly,
in loving memory of our beloved founder director,
Late Shri. Pradeepji Lalchandji Lunawat,
who will always be an inspiration, a positive force and strong support
behind us.*



“My work is my prayer to God”

- Lt. Shri. Pradeepji L. Lunawat

*Soulful Tribute and Gratitude for all Your
Sacrifices, Hardwork and 40 years of Strong Vision...*

Syllabus...

Basics of Computer Network : Sem. III, Information Technology (SPPU)

Teaching Scheme : Theory (TH) : 03 Hrs. /Week	Credit Scheme : 03	Examination Scheme : Mid-Semester : 30 Marks End-Semester : 70 Marks
--	-------------------------------------	---

Prerequisite Courses, if any: Basics of communication

Course Objectives :

1. To understand the fundamentals of communication system.
2. To understand the basics of internetworking.
3. To understand services and protocols used at Physical, Data Link, Network, Transport Layer.

Course Outcomes : On completion of the course, students will be able to –

CO1 : Understand and explain the concepts of communication theory and compare functions of OSI and TCP/IP model.

CO2 : Analyze data link layer services, error detection and correction, linear block codes, cyclic Codes, framing and flow control protocols.

CO3 : Compare different access techniques, channelization and IEEE standards.

CO4 : Apply the skills of subnetting, supernetting and routing mechanisms.

CO5 : Differentiate IPv4 and IPv6.

CO6 : Illustrate services and protocols used at transport layer.

Course Contents

Unit I

Data communication and network models :

Introduction to communication Theory - Basics of data communication, Types of Signals, A/D, D/A, A/A, D/D Signal Conversion Methods, Bandwidth Utilization and Data Rate Limits, Multiplexing Techniques, Data rate limits, Topologies, Noise, types of noise, Shannon Hartley Theorem, Channel capacity, Nyquist and Shannon Theorem, Bandwidth S/N trade off. Network Models And addressing - OSI Model TCP/IP Model (Data Format, Addressing Mechanisms, Devices).

Case Study : Study of Physical layer components such as Cable, NIC, hub, etc. available in the computers /laboratories of your department.

(Refer chapters 1 and 2)

Unit II

Error detection, correction and data link control :

Data Link Layer: Data Link Layer Services, Error Detection and Correction: Introduction, Error Detection and Error Correction. Linear Block Codes: hamming code, Hamming Distance, parity check code. Cyclic Codes: CRC (Polynomials), Advantages of Cyclic Codes, Other Cyclic Codes (Examples: CHECKSUM: One's Complement, Internet Checksum). Framing: fixed-size framing, variable size framing. Flow control: flow control protocols. Noiseless channels: simplest protocol, stop-and-wait protocol. Noisy channels: stop-and-wait Automatic Repeat Request (ARQ), go-back-n ARQ, Selective repeat ARQ, piggybacking.

Case Study : Draw PPPoE connection diagram with multiple devices, FFTH connection diagram.

(Refer chapters 3 and 4)

Unit III

Multi-Access mechanism and ethernet standards :

Random Access Techniques: CSMA, CSMA/CD, CSMA/CA, Controlled Access Techniques: Reservation, Polling, Token Passing, Channelization: FDMA, TDMA, CDMA, Ethernet: IEEE Standards- 802.3, 802.4, 802.5, 802.6 Comparison of Ethernet Standards: Standard Ethernet, Fast Ethernet, Gigabit Ethernet with reference to MAC layer and Physical Layer (Wired Network Only).

Case Study : Campus network design case study.

(Refer chapters 5 and 6)

Unit IV

Network Layer : Services and addressing :

Network Layer : Network Layer Services, IPv4 Addresses: Static and Dynamic Configuration Classful and Classless Addressing, Special Addresses, NAT, Subnetting, Supernetting, Delivery and Forwarding of IP Packet, Structure of Router, IPv4: Datagrams, Fragmentation, Options, Checksum, IPv6Addressing: Notations, Address Space, Packet Format, Transition from Ipv4 to IPv6

Case Study : Visit server room of campus and understand how IP addressing is done for your respective Campus → Institute → Department.

(Refer chapter 7)

Unit V

Network Layer : Routing protocols :

Routing: Metric, Static vs Dynamic Routing Tables, Routing Protocol, Unicast Routing Protocols - Optimality Principle, Intra and Inter Domain Routing, Shortest Path Routing, Flooding, Distant Vector Routing, Link State Routing, Path Vector Routing Interior Gateway Routing Protocol- OSPF, EIGRP, RIP, Exterior Gateway Routing Protocol– BGP.

Case Study : Case study on network simulation tools such as Packet tracer.

(Refer chapter 8)

Unit VI

Transport Layer - Services and protocols :

Transport layer : Transport layer services(Duties), TCP: COTS, TCP header, Services, Segments, Connection Establishment, Flow control, Congestion Control, Congestion Control Algorithms, Leaky Bucket, Token Bucket and QoS, Timers, UDP: CLTS, UDP header, Datagram, Services, Applications, Socket: Primitives, TCP & UDP Sockets.

Case Study : Case study on Client server model using simple socket programming, Case Study on Transport Layer Security - Firewall (Stateless Packet Filtering), Stateful, Application.

(Refer chapter 9)

**Case Studies may be assigned as self-study to students
and to be excluded from theory examinations**



**Unit I****Chapter 1 : Introduction to Communication Theory****1-1 to 1-54**

Syllabus : Basics of data communication, Types of signals, A/D, D/A, A/A, D/D signal conversion methods, Bandwidth utilization and data rate limits, Multiplexing techniques, Data rate limits, Topologies, Noise, Types of noise, Shannon Hartley theorem, Channel capacity, Nyquist and Shannon theorem, Bandwidth S/N trade off.

1.1	Introduction	1-3
1.2	Basics of Data Communication	1-3
1.2.1	Characteristics of Data Communication System	1-3
1.3	Components of Data Communication System	1-4
1.4	Data Communication System	1-4
1.5	Analog and Digital Signals	1-5
1.5.1	Analog and Digital Data	1-5
1.6	Analog Signals	1-5
1.6.1	Simple Analog Signal	1-6
1.6.2	Composite Analog Signal	1-6
1.7	Digital Signals	1-6
1.7.1	Sources of Digital Signal	1-6
1.7.2	Advantages of Digital Signals	1-6
1.7.3	Bit Interval	1-6
1.7.4	Bit Rate (Data Rate)	1-6
1.7.5	Bauds (or Baud Rate)	1-7
1.7.6	Bit Length	1-8
1.8	Signal Conversion Methods	1-8
1.8.1	Encoding and Modulation	1-8
1.8.2	Signal Conversion Methods	1-8
1.9	A to D Conversion	1-8
1.9.1	Block Diagram	1-9
1.9.2	Graphical Representation of A/D Conversion Process	1-9
1.9.3	Sampling Process	1-10
1.9.4	Quantization Process	1-10
1.9.5	Quantization Error or Quantization Noise ∈	1-11
1.10	Pulse Code Modulation (PCM)	1-11
1.10.1	PCM Transmitter (Encoder)	1-12
1.10.2	PCM Receiver (Decoder)	1-12

1.10.3	Applications of PCM	1-13
1.10.4	Advantages of PCM	1-13
1.10.5	Disadvantages of PCM	1-13
1.11	Delta Modulation (D.M.)	1-13
1.11.1	Delta Modulator Transmitter	1-14
1.11.2	D.M. Receiver	1-15
1.11.3	Applications of D.M.	1-15
1.11.4	Distortions in the DM System	1-15
1.11.5	Advantages of Delta Modulation	1-16
1.11.6	Disadvantages of Delta Modulation	1-16
1.12	D to A Conversion	1-16
1.12.1	Types of Digital CW Modulation	1-17
1.13	Amplitude Shift Keying (ASK)	1-17
1.13.1	ASK Generation (Transmitter)	1-17
1.13.2	Transmission Bandwidth of the ASK Signal	1-18
1.13.3	ASK Receiver	1-18
1.13.4	Constellation Diagram	1-18
1.13.5	Constellation Diagram of ASK	1-19
1.13.6	Application	1-19
1.14	Frequency Shift Keying (FSK)	1-19
1.14.1	FSK Generation	1-20
1.14.2	Bandwidth of FSK Signal	1-20
1.14.3	FSK Receiver	1-20
1.14.4	Application	1-20
1.15	Phase Shift Keying (PSK)	1-21
1.15.1	BPSK Transmitter	1-21
1.15.2	BPSK Receiver	1-21
1.15.3	Bandwidth of BPSK	1-22
1.15.4	Constellation Diagram of BPSK	1-22
1.15.5	Applications	1-22
1.16	A to A Conversion	1-23
1.17	Amplitude Modulation (AM)	1-23
1.17.1	Expression of AM wave	1-24
1.17.2	Modulation Index	1-24
1.17.3	Frequency Spectrum of the AM Wave	1-24
1.17.4	Disadvantages of AM (DSBFC)	1-25
1.17.5	Advantages of AM	1-25
1.17.6	Applications of AM	1-25
1.18	Frequency Modulation (FM)	1-26
1.18.1	Frequency Deviation (δ)	1-27
1.18.2	Mathematical Expression for F.M.	1-27



1.18.3 Modulation Index of FM	1-27	1.29 A Network	1-41
1.18.4 Deviation Ratio.....	1-27	1.29.1 Network Topologies.....	1-41
1.18.5 Frequency Spectrum of FM Wave	1-28	1.29.2 Bus Topology	1-42
1.18.6 Ideal Bandwidth of FM	1-28	1.29.3 Ring Topology	1-43
1.18.7 Applications of FM	1-28	1.29.4 Star Topology	1-44
1.19 Phase Modulation (PM)	1-29	1.29.5 Mesh Topology	1-45
1.19.1 Bandwidth of PM	1-29	1.29.6 Tree Topology	1-46
1.19.2 Comparison of AM, FM and PM	1-29	1.29.7 Logical Topology	1-47
1.20 Digital to Digital Conversion	1-30	1.29.8 Hybrid Topology	1-47
1.20.1 Classification of Line Codes	1-30	1.30 Noise	1-47
1.20.2 Properties of Line Codes	1-31	1.30.1 Sources of Noise	1-48
1.20.3 Unipolar RZ Format	1-31	1.30.2 External Noise	1-48
1.20.4 Unipolar NRZ Format	1-31	1.30.3 Fundamental or Internal Noise	1-48
1.20.5 Polar RZ Format	1-31	1.31 Types of Internal Noise	1-49
1.20.6 Polar NRZ Format	1-32	1.31.1 Shot Noise	1-49
1.20.7 Split Phase Manchester Format	1-32	1.31.2 Partition Noise	1-49
1.20.8 Bipolar NRZ Format (AMI)	1-32	1.31.3 Low Frequency or Flicker Noise	1-49
1.21 Bandwidth Utilization	1-33	1.31.4 Thermal Noise or Johnson Noise	1-49
1.21.1 Signal and Channel Bandwidths	1-34	1.31.5 High Frequency or Transit Time Noise	1-50
1.22 Some Important Definitions	1-34	1.32 Theorems in Data Communication	1-50
1.22.1 Channel Capacity	1-34	1.32.1 Channel Capacity	1-50
1.22.2 Error Rate	1-34	1.32.2 Nyquist Theorem	1-50
1.22.3 Signal to Noise Ratio	1-34	1.32.3 Shannon's Theorem	1-50
1.23 Data Rate Limits	1-35	1.32.4 Shannon Hartley Theorem	1-51
1.24 Introduction to Multiplexing	1-35	1.32.5 S/N Bandwidth Trade off	1-51
1.24.1 Types of Multiplexing	1-36	• Review Questions	1-53
1.25 Frequency Division Multiplexing (FDM)	1-36		
1.25.1 Advantages of FDM	1-37		
1.25.2 Disadvantages of FDM	1-37		
1.25.3 Applications of FDM	1-37		
1.26 Synchronous Time Division Multiplexing	1-37		
1.26.1 Advantages of TDM	1-38		
1.26.2 Disadvantages of TDM	1-38		
1.26.3 Applications of TDM	1-38		
1.27 Statistical (Asynchronous) TDM	1-39		
1.27.1 Data Rate of Statistical TDM	1-39		
1.27.2 Slot Size	1-39		
1.27.3 Bandwidth	1-40		
1.27.4 Comparison of FDM, Synchronous TDM and Statistical TDM	1-40		
1.28 Wavelength Division Multiplexing (WDM)	1-40		
1.28.1 Application of WDM	1-41		

Unit I**Chapter 2 : Network Models and Addressing****2-1 to 2-26**

Syllabus : OSI model, TCP/IP model (Data format, Addressing mechanisms, Devices).

Case study : Study of Physical layer components such as Cable, NIC, hub, etc. available in the computers / laboratories of your department.

2.1 Introduction	2-2
2.1.1 Layered Tasks	2-2
2.1.2 Protocol	2-2
2.1.3 Network Architecture	2-3
2.2 Network Software	2-3



2.2.1	Protocol Hierarchies (Layered Architecture)	2-3	2.7	Encapsulation and Decapsulation	2-21
2.2.2	Reasons for having Layered Protocols and its Benefits	2-3	2.7.1	Encapsulation at the Source Host	2-21
2.2.3	How does Data Transfer Take Place ?	2-4	2.7.2	Decapsulation and Encapsulation at the Router	2-21
2.3	Reference Models	2-4	2.7.3	Decapsulation at the Destination Host	2-22
2.4	OSI Model	2-4	2.8	Addressing in TCP/IP	2-22
2.4.1	Layered Architecture	2-4	2.8.1	MAC Address (Physical Address)	2-23
2.4.2	A More Detailed OSI Model	2-5	2.8.2	Logical Addresses (IP Addresses)	2-23
2.4.3	Peer to Peer Processes	2-6	2.8.3	Port Address	2-24
2.4.4	Organization of the Layers	2-6	2.8.4	Specific Addresses	2-24
2.4.5	Functions of Different Layers	2-7	2.9	Multiplexing and Demultiplexing in TCP / IP	2-24
2.4.6	Exchange of Information using the OSI Model	2-8	2.10	Comparison of OSI and TCP/IP	2-25
2.4.7	Physical Layer	2-9	2.10.1	Similarities between OSI and TCP/IP Models	2-25
2.4.8	Data Link Layer	2-9	2.10.2	Difference between OSI & TCP/IP	2-25
2.4.9	Network Layer	2-10	2.10.3	Demerits of TCP/IP Model	2-25
2.4.10	Transport Layer	2-11	2.10.4	Hybrid (Internet) Reference Model	2-25
2.4.11	The Session Layer	2-12	•	Review Questions	2-26
2.4.12	Presentation Layer	2-12			
2.4.13	Application Layer	2-13			
2.4.14	Merits of OSI Reference Model	2-14			
2.4.15	Demerits of OSI Model	2-14			
2.5	TCP/IP Model	2-14			
2.5.1	Introduction to TCP/IP	2-14			
2.5.2	Overview of TCP/IP Architecture	2-15			
2.5.3	Description of TCP/IP Model	2-15			
2.5.4	Communication through Internet	2-16			
2.5.5	Logical Connections	2-17			
2.6	Detailed Description of Each Layer in TCP/IP	2-18			
2.6.1	Physical Layer	2-18	3.1	Introduction	3-2
2.6.2	Data Link Layer	2-19	3.1.1	Position of Data Link Layer	3-2
2.6.3	Network Layer	2-19	3.1.2	Functions of Data Link Layer	3-2
2.6.4	Transport Layer	2-20	3.1.3	Introduction to Error Control	3-3
2.6.5	Application Layer	2-20	3.1.4	Need of Error Control Coding	3-3
2.6.6	TCP/IP Model with Protocol	2-21	3.1.5	Types of Errors	3-3
			3.1.6	Disadvantages of Coding	3-4
			3.1.7	Redundancy	3-4

Unit II**Chapter 3 : Error Control Coding**

3-1 to 3-32

Syllabus : Data link layer : Data link layer services, Error detection and correction : Introduction, Error detection, Error correction, Linear block codes : Hamming code, Hamming distance, Parity check code, Cyclic codes : CRC (Polynomials), Advantages of cyclic codes, Other cyclic codes (Examples : Checksum : Ones complement, Internet checksum).

3.1	Introduction	3-2
3.1.1	Position of Data Link Layer	3-2
3.1.2	Functions of Data Link Layer	3-2
3.1.3	Introduction to Error Control	3-3
3.1.4	Need of Error Control Coding	3-3
3.1.5	Types of Errors	3-3
3.1.6	Disadvantages of Coding	3-4
3.1.7	Redundancy	3-4



3.2	Error Detection and Correction	3-5
3.3	Forward Error Correction Versus Retransmission	3-5
3.3.1	The ARQ Technique	3-5
3.3.2	FEC	3-5
3.3.3	Error Correction Technique	3-5
3.3.4	FEC (Forward Error Correction)	3-5
3.4	Error Correction	3-6
3.4.1	ARQ Technique (Retransmission)	3-6
3.4.2	Types of ARQ System	3-7
3.5	Coding	3-7
3.5.1	Modular Arithmetic	3-7
3.5.2	Modulo – 2 Arithmetic	3-7
3.6	Linear Block Codes	3-7
3.6.1	Code Word Structure	3-8
3.7	Error Detection in Block Coding	3-8
3.8	Error Correction using Block Codes	3-9
3.8.1	Hamming Weight of a Code Word	3-9
3.8.2	Hamming Distance	3-9
3.8.3	Minimum Hamming Distance d_{min}	3-9
3.9	Linear Block Codes	3-10
3.9.1	Some Linear Block Codes	3-10
3.9.2	Error Detection	3-11
3.9.3	Parity Checking	3-11
3.9.4	Use of Parity Bit to Decide Parity	3-11
3.9.5	Simple Parity Check Block Code	3-12
3.9.6	Two Dimensional Parity Check (Block Parity)	3-13
3.10	Hamming Codes	3-14
3.10.1	Generation of Hamming Code	3-15
3.10.2	Selection of Parity Bits	3-16
3.10.3	Detection and Correction of Errors	3-17
3.10.4	Solved Examples	3-17
3.11	Cyclic Codes	3-22
3.12	Cyclic Redundancy Check (CRC)	3-22
3.12.1	CRC Encoder and Decoder	3-23
3.12.2	Procedure to obtain CRC	3-24
3.12.3	Requirements of CRC	3-24
3.12.4	CRC Generator	3-24
3.12.5	CRC Checker	3-25
3.12.6	Advantages of Cyclic Codes	3-28
3.12.7	Disadvantage of Cyclic Codes	3-29
3.13	Other Cyclic Codes	3-29

3.13.1	Checksum	3-29
3.13.2	One's Complement Checksum	3-30
3.13.3	Internet Checksum	3-31
3.13.4	Performance	3-32
•	Review Questions	3-32

Unit II**Chapter 4 : Data Link Control****4-1 to 4-24**

Syllabus : Data link layer services, Framing : Fixed-size framing, Variable size framing, Flow control : Flow control protocols, Noiseless channels : Simplest protocol, Stop-and-wait protocol, Noisy channels : Stop-and-wait automatic repeat request (ARQ), Go-back-n ARQ, Selective repeat ARQ, Piggybacking.

Case study : Draw PPPoE connection diagram with multiple devices, FFTH connection diagram.

4.1	Introduction	4-2
4.1.1	Position of Data Link Layer	4-2
4.2	Services Provided to Network Layer	4-2
4.2.1	Types of Services Provided	4-2
4.2.2	Unacknowledged Connectionless Service	4-2
4.2.3	Acknowledged Connectionless Service	4-3
4.2.4	Acknowledged Connection Oriented Service	4-3
4.3	Framing	4-3
4.3.1	Fixed Size Framing	4-3
4.3.2	Variable Size Framing	4-3
4.3.3	Character Count	4-4
4.3.4	Starting and Ending Character with Character Stuffing	4-4
4.3.5	Starting and Ending Flags, with Bit Stuffing	4-5
4.3.6	Physical Layer Coding Violations	4-6
4.3.7	Frame Synchronization	4-6
4.4	Error Control	4-7
4.4.1	Function of a Timer	4-7
4.5	Flow Control	4-7
4.6	Elementary Data Link Protocols	4-8
4.6.1	An Unrestricted Simplex Protocol	4-8
4.6.2	A Simplex Stop and Wait Protocol	4-8
4.6.3	A Simplex Protocol for Noisy Channel ...	4-9



4.6.4	Piggybacking	4-10
4.7	Sliding Window Protocols	4-10
4.7.1	Sender and Receiver Sliding Windows	4-11
4.7.2	Movement of Sender's Window	4-12
4.7.3	Movement of Receiver's Windows	4-12
4.8	A One Bit Sliding Window Protocol (Stop and Wait ARQ)	4-14
4.9	A Protocol using GO Back n	4-16
4.9.1	Pipelining	4-18
4.10	Selective Repeat ARQ	4-18
4.11	Protocol Performance	4-19
4.11.1	How to Improve the Throughput Efficiency ?	4-21
4.12	Solved Examples	4-21
•	Review Questions	4-23

Unit III**Chapter 5 : Random Access Techniques 5-1 to 5-22**

Syllabus : Random access techniques : CSMA, CSMA / CD and CSMA / CA, Controlled access techniques : Reservation, Polling, Token passing, Channelization : FDMA, TDMA, CDMA.

5.1	Introduction	5-2
5.1.1	MAC and LLC Sublayers	5-2
5.2	The Channel Allocation Problem	5-2
5.2.1	Static Channel Allocation in LANs and MANs	5-2
5.2.2	Dynamic Channel Allocation	5-3
5.3	Multiple Access	5-3
5.3.1	Random Access	5-3
5.3.2	Evolution of Random Access Methods	5-4
5.4	Multiple Access (ALOHA System)	5-4
5.4.1	Pure ALOHA	5-4
5.4.2	Protocol Flow Chart for ALOHA	5-5
5.4.3	Efficiency of an ALOHA Channel	5-5
5.4.4	Slotted ALOHA	5-6
5.4.5	Comparison of Pure and Slotted ALOHA	5-7
5.5	Carrier Sense Multiple Access (CSMA)	5-8
5.5.1	Carrier Sense Multiple Access/Collision Detection (CSMA/CD)	5-8
5.5.2	CSMA/CD Procedure	5-9

5.5.3	CSMA/CA	5-10
5.6	Collision Free Protocols	5-10
5.6.1	Bit-map Protocol	5-10
5.6.2	Binary Countdown	5-11
5.6.3	Limited Contention Protocols	5-11
5.6.4	The Adaptive Tree Walk Protocol	5-12
5.7	Controlled Access	5-12
5.7.1	Reservation Systems	5-13
5.7.2	Polling	5-14
5.7.3	Token Passing	5-15
5.8	Channelization / Multiple Access Techniques	5-15
5.8.1	FDMA	5-16
5.8.2	TDMA	5-17
5.8.3	Code Division Multiple Access (CDMA)	5-18
5.8.4	Comparison of FDMA, TDMA and CDMA	5-19
•	Review Questions	5-22

Unit III**Chapter 6 : Ethernet 6-1 to 6-22**

Syllabus : IEEE standards - 802.3, 802.4, 802.5, 802.6, Comparison of Ethernet standards : Standard Ethernet, Fast Ethernet, Gigabit Ethernet with reference to MAC layer and physical layer (Wired Network Only).

Case study : Campus network design case study.

6.1	Ethernet	6-2
6.1.1	Traditional Ethernet	6-2
6.1.2	Bridged Ethernet	6-3
6.1.3	Switched Ethernet	6-3
6.1.4	Full Duplex Ethernet	6-3
6.1.5	Fast Ethernet	6-3
6.1.6	Gigabit Ethernet	6-3
6.2	IEEE Standards	6-3
6.3	Traditional Ethernet (IEEE 802.3)	6-4
6.3.1	Traditional Ethernet Frame	6-4
6.3.2	Frame Length	6-5
6.3.3	Addressing	6-5
6.3.4	Types of Addresses	6-5
6.3.5	Physical Properties of Ethernet	6-5
6.3.6	Physical Layer Implementation of Standard Ethernet	6-6
6.4	Changes in the Standards	6-7



6.5	Bridged Ethernet	6-7
6.6	Switched and Full Duplex Ethernet	6-8
6.6.1	Switched Ethernet	6-8
6.6.2	Full Duplex Ethernet	6-8
6.7	Fast Ethernet	6-9
6.7.1	Autonegotiation	6-9
6.7.2	Physical Layer Implementation	6-9
6.8	Gigabit Ethernet	6-10
6.8.1	MAC Sublayer	6-11
6.8.2	Physical Layer	6-12
6.8.3	Physical Layer Implementation	6-12
6.8.4	Ten Gigabit Ethernet	6-13
6.8.5	Comparison of Standard and Gigabit Ethernet	6-13
6.9	Token Bus IEEE 802.4	6-13
6.10	Token Ring System [IEEE 802.5]	6-15
6.10.1	Comparison of Access Control Methods	6-17
6.11	High Level Data Link Control (HDLC) Protocol	6-17
6.11.1	Frame Structure in HDLC	6-18
6.11.2	Frame Types in HDLC	6-19
6.11.3	Transparency in HDLC	6-20
6.11.4	Bit Stuffing	6-21
6.11.5	Why is CRC in Data Link Protocols in Trailer and not in Header ?	6-21
6.12	IEEE 802.6 Standard	6-21
•	Review Questions	6-22

Unit IV**Chapter 7 IP Addressing** **7-1 to 7-62**

Syllabus : Network layer services, IPv4 addresses : Static and dynamic configuration, Classful and classless addressing, Special addresses, NAT, Subnetting, Supernetting, Delivery and forwarding of IP packets, Structure of router, IPv4 : Datagrams, Fragmentation, Options, Checksum, IPv6 Addressing : Notations, Address space, Packet format, Transition from IPv4 to IPv6.

Case study : Visit server room of campus and understand how IP addressing is done for your respective campus → Institute → Department.

7.1	Network Layer	7-2
7.2	Network Layer Services	7-2

7.2.1	Logical Addressing	7-2
7.2.2	Services Provided at the Source Computer	7-2
7.2.3	Services Provided at Each Router	7-4
7.2.4	Services Provided at the Destination Computer	7-4
7.3	Routing and Forwarding	7-4
7.3.1	Routing	7-4
7.3.2	Forwarding	7-5
7.4	Other Services	7-5
7.4.1	Error Control	7-5
7.4.2	Flow Control	7-5
7.4.3	Congestion Control	7-5
7.4.4	Quality of Service (QoS)	7-6
7.4.5	Security	7-6
7.5	IPv4 Addresses	7-6
7.5.1	Uniqueness of IP Addresses	7-6
7.5.2	Address Space	7-6
7.5.3	Notation	7-6
7.5.4	IPv4 Address Format	7-7
7.6	Classful Addressing	7-7
7.6.1	IPv4 Address Classes	7-7
7.6.2	Formats of Various Classes	7-8
7.6.3	How to Recognize Classes ?	7-8
7.6.4	Two Level Addressing	7-9
7.6.5	Extracting Information in a Block	7-9
7.6.6	Network Address	7-10
7.6.7	Network Mask or Default Mask	7-11
7.6.8	Default Masks for Different Classes	7-11
7.6.9	Finding Network Address using Default Mask	7-12
7.6.10	Three Level Addressing Subnetting	7-12
7.6.11	Special IP Addresses	7-13
7.6.12	Limitations of IPv4	7-13
7.6.13	Classless Addressing	7-14
7.6.14	Supernetting	7-14
7.6.15	Who Decides the IP Addresses ?	7-14
7.6.16	Registered and Unregistered Addresses	7-15
7.6.17	Solved Examples	7-15
7.7	Classless Addressing in IPv4	7-21
7.7.1	Variable Length Blocks	7-21



7.7.2	The Slash Notation (CIDR Notation)	7-22	7.14	Options	7-39
7.7.3	Network Mask	7-22	7.14.1	Format	7-39
7.7.4	Extracting the Block Information	7-23	7.15	Option Types	7-40
7.7.5	Block Allocation	7-24	7.15.1	No Operation Option	7-41
7.7.6	Relation to Classful Addressing	7-25	7.15.2	End of Option Option	7-41
7.7.7	Subnetting	7-25	7.15.3	Record-Route Option	7-41
7.7.8	Designing Subnets	7-25	7.15.4	Strict-Source-Route Option	7-41
7.7.9	Finding Information about Each Network	7-25	7.15.5	Loose-Source-Root Option	7-42
7.7.10	Address Aggregation	7-26	7.15.6	Time Stamp Option	7-42
7.8	Special Addresses	7-27	7.16	Checksum	7-42
7.8.1	Special Blocks	7-27	7.16.1	Checksum Calculation at the Sender	7-42
7.8.2	All Zeros Address	7-27	7.16.2	Checksum Calculation at the Receiver	7-43
7.8.3	All one Address-Limited Broadcast Address	7-28	7.17	Network Layer Security	7-43
7.8.4	Loopback Address	7-28	7.17.1	IPsec (IP security)	7-43
7.8.5	Private Addresses	7-28	7.17.2	Modes of Operation of IPsec	7-44
7.8.6	Multicast Addresses	7-28	7.17.3	Comparison between Transport and Tunnel Mode	7-45
7.8.7	Special Addresses in Each Block	7-28	7.17.4	Security Protocols of IPsec	7-45
7.8.8	Network Address	7-28	7.17.4.1	Authentication Header (AH)	7-45
7.8.9	Direct Broadcast Address	7-28	7.17.4.2	Encapsulating Security Payload (ESP)	7-46
7.9	NAT – Network Address Translation	7-28	7.17.5	Services Provided by IPsec	7-47
7.10	Delivery and Forwarding of IP Packets	7-29	7.17.6	Security Association	7-47
7.10.1	Delivery	7-29	7.17.7	Internet Key Exchange (IKE)	7-47
7.10.2	Forwarding	7-30	7.17.8	Virtual Private Networking (VPN)	7-48
7.11	Structure of a Router	7-32	7.18	IPv6 (Next Generation IP)	7-48
7.11.1	Components of a Router	7-32	7.18.1	Advantages of IPv6	7-48
7.11.2	Input Ports	7-32	7.19	IPv6 Addressing	7-49
7.11.3	Output Ports	7-32	7.19.1	IPv6 Address	7-49
7.11.4	Routing Processor	7-32	7.19.2	Notations	7-49
7.11.5	Switching Fabric	7-33	7.19.3	Abbreviation	7-49
7.11.6	Types of Switching Fabrics	7-33	7.20	IPv6 Packet Format	7-50
7.11.7	Crossbar Switch	7-33	7.20.1	Payload	7-51
7.11.8	Banyan Switch	7-33	7.20.2	Extension Headers	7-52
7.11.9	Batcher Banyan Switch	7-33	7.21	Address Space	7-53
7.12	Internet Protocol Version 4 (IPv4)	7-34	7.21.1	Address Types	7-53
7.12.1	Position of IP	7-34	7.21.2	Broadcasting and Multicasting	7-53
7.12.2	Internet Protocol (IP)	7-34	7.22	Address Space Allocation	7-53
7.12.3	Datagrams	7-34	7.22.1	The First Section	7-54
7.12.4	IPv4 Header Format	7-35	7.22.2	Second Section	7-54
7.13	Fragmentation	7-38	7.22.3	Algorithm	7-55
7.13.1	Maximum Transfer Unit (MTU)	7-38			
7.13.2	Fields Related to Fragmentation	7-39			



7.22.4	Assigned or Reserved Blocks	7-55
7.22.5	Unspecified Address	7-55
7.22.6	Loopback Address	7-55
7.22.7	Difference between Loopback Address of IPv4 and IPv6	7-56
7.22.8	Embedded IPv4 Addresses	7-56
7.22.9	Compatible Address	7-56
7.22.10	A Mapped Address	7-56
7.22.11	Calculation of Checksum	7-56
7.23	Migrating to IPv6 (Compatibility to IPv4)	7-56
7.24	Transition from IPv4 to IPv6	7-57
7.24.1	Transition Strategies	7-57
7.24.2	Use of IP Addresses	7-58
7.24.3	Comparison between IPv4 and IPv6	7-58
7.25	University Questions and Answers	7-61
•	Review Questions	7-61

Unit V

Chapter 8 : Routing Algorithms	8-1 to 8-46
---------------------------------------	--------------------

Syllabus : Routing : Metric, Static vs dynamic routing tables, Routing protocol, Unicast routing protocols - Optimality principle, Intra and inter domain routing, Shortest path routing, Flooding, Distant vector routing, Link state routing, Path vector routing, Interior gateway routing protocol - OSPF, EIGRP, RIP, Exterior gateway routing protocol – BGP.

Case study : Case study on network simulation tools such as packet tracer.

8.1	Routing	8-2
8.1.1	Types of Routing	8-2
8.1.2	Intra and Interdomain Routing	8-2
8.1.3	Unicast Routing	8-3
8.1.4	Broadcast Routing	8-3
8.1.5	Multicast Routing	8-4
8.2	Routing Algorithms	8-4
8.2.1	Desired Properties of a Routing Algorithm	8-4
8.2.2	Types of Routing Algorithms	8-4
8.2.3	Optimality Principle	8-5
8.3	Static Algorithms.....	8-5
8.3.1	Shortest Path Routing	8-5
8.3.2	Flooding	8-6
8.3.3	Flow Based Routing	8-6

8.4	Dynamic Routing Algorithms	8-7
8.5	Distance Vector Routing Algorithm	8-7
8.5.1	Disadvantages	8-8
8.5.2	Looping in Distance Vector Routing Protocol	8-9
8.5.3	Count to Infinity Problem	8-9
8.5.4	Split Horizon Algorithm	8-11
8.6	Link State Routing	8-11
8.6.1	Comparison of Link State Routing and Distance Vector Routing	8-12
8.7	Hierarchical Routing	8-12
8.7.1	Two Level Hierarchical Routing	8-13
8.8	Least Cost Algorithms	8-14
8.8.1	Bellman-Ford Algorithm	8-14
8.8.2	Dijkstra's Algorithm	8-18
8.9	Path Vector Routing	8-21
8.9.1	Path Vector Messages	8-21
8.9.2	Loop Prevention	8-22
8.9.3	Path Attributes	8-22
8.10	Unicast Routing Protocols	8-22
8.10.1	Routing	8-22
8.10.2	Cost or Metric	8-22
8.10.3	Routing Tables	8-22
8.11	Routing Protocols	8-23
8.11.1	Unicast Routing Protocols	8-23
8.12	RIP (Routing Information Protocol)	8-23
8.12.1	RIP Updating Algorithm	8-24
8.12.2	Initializing the Routing Table	8-24
8.12.3	Updating the Routing Table	8-24
8.12.4	RIP Operation	8-24
8.12.5	RIP Message Format	8-25
8.13	Request and Response Messages (RIP)	8-25
8.13.1	Request Message	8-25
8.13.2	Response Message	8-26
8.13.3	Timers in RIP	8-26
8.14	RIP Version 2	8-27
8.14.1	Message format (RIPv2)	8-27
8.14.2	Authentication	8-28
8.14.3	Multicasting	8-28
8.14.4	Encapsulation	8-28
8.14.5	Problems in RIP	8-28
8.15	OSPF	8-29
8.15.1	Features of OSPF	8-30



8.15.2 Metric	8-31
8.15.3 Types of Links	8-31
8.15.4 Virtual Link	8-32
8.15.5 Graphical Representation	8-32
8.15.6 Link State Advertisements (LSAs)	8-32
8.15.7 OSPF Packet Types	8-33
8.15.8 Link State Update Packet	8-34
8.15.9 General LSA Header	8-34
8.15.10 Router Link LSA	8-35
8.15.11 Router Link Packet	8-35
8.15.12 Network Link LSA	8-35
8.15.13 Summary Link to Network LSA	8-36
8.15.14 Summary Link to AS Boundary Router LSA	8-36
8.15.15 External Link LSA	8-37
8.15.16 Other Packets	8-37
8.15.17 Encapsulation	8-37
8.15.18 Comparison between RIP and OSPF	8-38
8.16 Border Gateway Protocol (BGP)	8-38
8.16.1 Types of Autonomous Systems	8-38
8.16.2 CIDR	8-39
8.16.3 Path Attributes	8-39
8.16.4 Types of Attributes	8-39
8.17 BGP Sessions	8-39
8.17.1 External and Internal BGP	8-39
8.17.2 Types of Messages	8-40
8.17.3 Packet Format	8-40
8.17.4 Open Message	8-40
8.17.5 The Update Message	8-41
8.17.6 Keepalive Message	8-41
8.17.7 Notification Message	8-41
8.17.8 Encapsulation	8-42
8.17.9 How does BGP Solve the Count to Infinity Problem ?.....	8-42
8.18 Interior Gateway Routing Protocol (IGRP)	8-42
8.18.1 Characteristics of IGRP Protocol	8-42
8.18.2 Stability Features of IGRP	8-43
8.18.3 IGRP Timers	8-43
8.19 Enhanced IGRP (EIGRP)	8-43
8.19.1 Features of Enhanced IGRP (EIGRP) ..	8-43
8.19.2 Enhanced IGRP Technologies	8-44
8.19.3 Routing Concepts in EIGRP	8-44
8.19.4 Packet Types in Enhanced IGRP	8-45

8.19.5 Comparison between IGRP and EIGRP	8-46
• Review Questions	8-46

Unit VI**Chapter 9 : Transport Layer-Services and Protocols****9-1 to 9-60**

Syllabus : Transport layer services (Duties), TCP : COTS, TCP header, Services, Segments, Connection establishment, Flow control, Congestion control, Congestion control algorithms, Leaky bucket, Token bucket and QoS, Timers, UDP : CLTS, UDP header, Datagram, Services, Applications, Socket : Primitives, TCP & UDP sockets.

Case study : Client server model using simple socket programming,

Case study on transport layer security - Firewall (Stateless (Packet filtering), Stateful, Application).

9.1 Introduction	9-2
9.2 Transport Layer Duties and Functionalities	9-2
9.3 Transport Layer Services	9-3
9.3.1 Process-to-Process Communication	9-3
9.3.2 Addressing Port Number	9-3
9.3.3 Encapsulation and Decapsulation	9-5
9.3.4 Multiplexing and Demultiplexing	9-5
9.3.5 Flow Control	9-5
9.3.6 Flow Control at Transport Layer	9-6
9.3.7 Error Control	9-7
9.3.8 Combination of Flow and Error Control	9-8
9.3.9 Congestion Control	9-9
9.3.10 Connectionless and Connection Oriented Services(CLTS& COTS)	9-10
9.3.11 Reliability at Transport Layer Versus Reliability at DLL	9-12
9.3.12 Quality of Service (QoS)	9-12
9.4 Transport Layer Protocols	9-13
9.4.1 The Internet Transport Protocols (TCP and UDP)	9-13
9.5 User Datagram Protocol (UDP)	9-13
9.5.1 Responsibilities of UDP	9-14
9.5.2 Advantages of UDP	9-14
9.5.3 User Datagram	9-14



9.5.4	UDP Pseudo Header	9-15	9.13.2	Connection Termination Protocol [Connection Release]	9-29
9.6	UDP Services	9-16	9.13.3	TCP Connection Management	9-30
9.6.1	Process to Process Communication	9-17	9.13.4	TCP Connection Release	9-30
9.6.2	Connectionless Services	9-17	9.14	Flow Control	9-31
9.6.3	Flow and Error Control	9-17	9.14.1	Opening and Closing Windows	9-32
9.6.4	Checksum	9-17	9.14.2	Shrinking of Windows	9-32
9.6.5	Congestion Control	9-18	9.14.3	An Example of Flow Control	9-32
9.6.6	Encapsulation and Decapsulation	9-18	9.14.4	Silly Window Syndrome	9-33
9.6.7	Queuing	9-18	9.14.5	Nagle's Algorithm	9-33
9.6.8	Multiplexing and Demultiplexing	9-19	9.15	Congestion Control	9-34
9.6.9	Comparison of UDP and Generic Simple Protocol	9-20	9.15.1	Need of Congestion Control	9-34
9.7	UDP Applications	9-20	9.15.2	Causes of Congestion	9-35
9.8	UDP Features	9-20	9.15.3	Effects of Congestion	9-35
9.8.1	Connectionless Service	9-20	9.15.4	Difference between Congestion Control and Flow Control	9-36
9.8.2	Lack of Error Control	9-20	9.15.5	Principle of Congestion Control	9-36
9.8.3	Lack of Congestion Control	9-20	9.15.6	Congestion Prevention Policies	9-37
9.8.4	Typical Applications of UDP	9-20	9.15.7	Congestion Control in Virtual Circuit Subnets	9-38
9.9	Transmission Control Protocol (TCP)	9-21	9.15.8	Approaches to Congestion Control	9-38
9.9.1	Relationship Between TCP and IP	9-21	9.16	Congestion Control in Datagram Subnets	9-40
9.9.2	Ports and Sockets	9-22	9.16.1	Choke Packets	9-40
9.10	TCP Services	9-23	9.16.2	Load Shedding	9-41
9.10.1	Process to Process Communication	9-23	9.17	Quality of Service (QoS)	9-41
9.10.2	Stream Delivery Service	9-23	9.17.1	Techniques for Achieving Good QoS ...	9-42
9.10.3	Sending and Receiving Buffers	9-23	9.17.2	Traffic Shaping	9-42
9.10.4	Bytes and Segments	9-24	9.17.3	Leaky Bucket Algorithm	9-43
9.10.5	Full Duplex Service	9-24	9.17.4	Token Bucket Algorithm	9-44
9.10.6	Connection Oriented Service	9-24	9.17.5	Combination of Token Bucket and Leaky Bucket	9-45
9.10.7	Reliable Service	9-24	9.17.6	Resource Reservation	9-45
9.11	Features of TCP	9-24	9.17.7	Admission Control	9-45
9.11.1	Numbering System	9-25	9.17.8	Queuing Disciplines	9-45
9.11.2	Flow Control	9-25	9.17.9	FIFO Queuing	9-46
9.11.3	Error Control	9-25	9.17.10	Fair Queuing	9-46
9.11.4	Congestion Control	9-25	9.17.11	Weighted Fair Queuing	9-47
9.12	The TCP Protocol	9-25	9.18	TCP Congestion Control	9-47
9.12.1	TCP Segment	9-26	9.18.1	Slow Start Algorithm	9-49
9.12.2	The TCP Segment Header	9-26	9.18.2	Internet Congestion Control Algorithm	9-49
9.12.3	Checksum	9-28	9.18.3	Congestion Avoidance (Additive Increase)	9-50
9.12.4	Encapsulation	9-28			
9.13	A TCP Connection	9-28			
9.13.1	TCP Connection Establishment	9-28			



9.19	TCP Timer Management	9-50	9.21.4	Connection Oriented Concurrent Server	9-56
9.19.1	Jacobson's Algorithm	9-51	9.22	Case Study : Socket Programming with TCP	9-56
9.19.2	Karn's Algorithm	9-51	9.22.1	Socket Programming with TCP	9-57
9.19.3	Other Timers in TCP	9-51	9.22.2	Socket Programming with UDP	9-58
9.20	Comparison of UDP and TCP	9-52	9.23	University Questions and Answers	9-59
9.21	Sockets	9-53		• Review Questions	9-58
9.21.1	Socket Types	9-53			
9.21.2	Socket Primitives	9-54			
9.21.3	Connectionless Iterative Server	9-55			

TechKnowledge
Publications

Unit I

Chapter 1

Introduction to Communication Theory

Syllabus

Basics of data communication, Types of signals, A/D, D/A, A/A, D/D signal conversion methods, Bandwidth utilization and data rate limits, Multiplexing techniques, Data rate limits, Topologies, Noise, Types of noise, Shannon Hartley theorem, Channel capacity, Nyquist and Shannon theorem, Bandwidth S/N trade off.

Chapter Contents

- 1.1 Introduction
- 1.2 Basics of Data Communication
- 1.3 Components of Data Communication System
- 1.4 Data Communication System
- 1.5 Analog and Digital Signals
- 1.6 Analog Signals
- 1.7 Digital Signals



Chapter Contents

- 1.8 Signal Conversion Methods
- 1.9 A to D Conversion
- 1.10 Pulse Code Modulation (PCM)
- 1.11 Delta Modulation (D.M.)
- 1.12 D to A Conversion
- 1.13 Amplitude Shift Keying (ASK)
- 1.14 Frequency Shift Keying (FSK)
- 1.15 Phase Shift Keying (PSK)
- 1.16 A to A Conversion
- 1.17 Amplitude Modulation (AM)
- 1.18 Frequency Modulation (FM)
- 1.19 Phase Modulation (PM)
- 1.20 Digital to Digital Conversion
- 1.21 Bandwidth Utilization
- 1.22 Some Important Definitions
- 1.23 Data Rate Limits
- 1.24 Introduction to Multiplexing
- 1.25 Frequency Division Multiplexing (FDM)
- 1.26 Synchronous Time Division Multiplexing
- 1.27 Statistical (Asynchronous) TDM
- 1.28 Wavelength Division Multiplexing (WDM)
- 1.29 A Network
- 1.30 Noise
- 1.31 Types of Internal Noise
- 1.32 Theorems in Data Communication



1.1 Introduction :

SPPU : Dec. 12

University Questions

- Q. 1** Explain the data communication system with its five components and discuss the fundamental characteristics of data communication system. Give the different forms in which data can be represented. **(Dec. 12, 8 Marks)**

Definition of Data :

- Data is defined as information which is stored in the digital form. A single data unit is called as datum.
- Data communication is the process of exchanging the digital information between two points.

Type of Data :

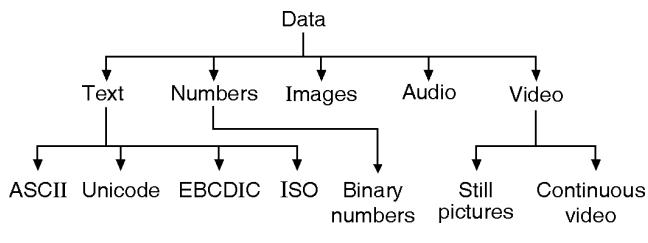
- Data can correspond to alphabets, numeric or symbols and it consists of any one or the combination of the following : microprocessor OPcodes, control codes, user addresses, program data or data base information.
- At the source or destination the data is in digital form but during the transmission, it may be in the form of analog or digital signals.
- A data communication network can be simply consisting of two computers connected to each other a public telecommunication network as shown in Fig. 1.1.1.



(G-1425) Fig. 1.1.1 : A simplest possible data communication network

Data Representation :

- Data can be represented using different forms as shown in Fig. 1.1.2.



(L-4) Fig. 1.1.2 : Data representation

1.2 Basics of Data Communication :

- Data communication system are used for interconnecting all types of digital computing equipments, internet etc.
- The aim of data communication and networking is to allow the exchange of data such as audio, text and video between any points in world.
- The transfer of data takes place over a computer network.
- A network provides path over which the data can travel to the desired destination.

Definition of Data Communication :

- **Data communication** can be defined as the exchange of data between a source and destination over some kind of transmission medium, such as a co-axial cable, (wired communication) or air (wireless communication).
- Before exchanging information, creators and the users of data should agree upon how the information should be presented.
- An information that is presented in such a form is called as **data**.

1.2.1 Characteristics of Data Communication System :

SPPU : Dec. 12

University Questions

- Q. 1** Explain the data communication system with its five components and discuss the fundamental characteristics of data communication system. Give the different forms in which data can be represented. **(Dec. 12, 8 Marks)**

- The three important characteristics of a data communication system are :

1. Delivery 2. Accuracy 3. Timeliness

1. Delivery :

- A data communication system (DCS) must deliver data only to the user who is intended to use it and not to any one else.

2. Accuracy :

- Due to noise the data may get altered or corrected when it is travelling over a communication medium.



- Errors will be introduced and the accuracy of the received data is adversely affected.
- The data communication system (DCS) must be designed in such a way that the delivered data is accurate and free from any errors.

3. Timeliness :

- The time delay is unacceptable for the audio and video data as it introduces errors in the reproduced sound or picture.
- So the DCS should deliver the data without any time delay.
- Such a data delivery is called as real-time transmission of data.

1.3 Components of Data Communication System :

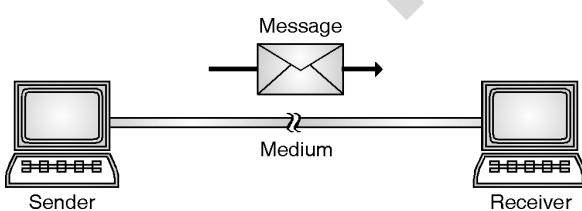
SPPU : Dec. 12

University Questions

- Q. 1** Explain the data communication system with its five components and discuss the fundamental characteristics of data communication system. Give the different forms in which data can be represented. **(Dec. 12, 8 Marks)**

Block diagram :

- If we specifically consider the communication between two computers then the data communication system is as shown in Fig. 1.3.1.
- It has the following five components :
 1. Message
 2. Sender
 3. Medium
 4. Receiver and
 5. Protocol



(L-2) Fig. 1.3.1 : Five components of a data communication system

1. Message :

- Message is nothing but information or data which is to be sent from sender to the receiver.
- A message can be in the form of sound, text, number, pictures, video or combination of them.

2. Sender :

- Sender is a device such as a host, video camera, telephone, work station etc which sends the message over the medium.

3. Medium :

- The message originating from the sender needs a path over which it can travel to the receiver. Such a path is called as the medium or channel.
- The examples of transmission medium are coaxial cable, twisted pair wire, fiber optic cable, radio waves (used in terrestrial or satellite communication) etc.

4. Receiver :

- It is the device which receives the message and reproduces it.
- A receiver can be in the form of a workstation, telephone handset, a TV receiver, etc.

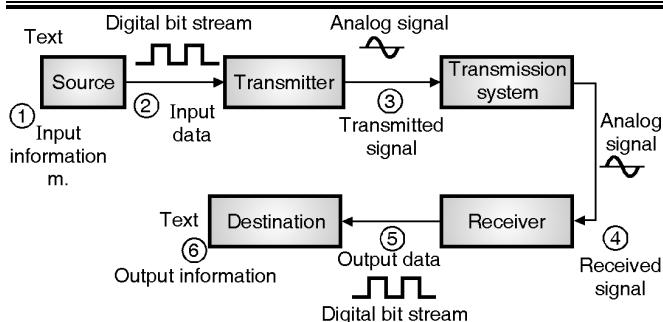
5. Protocol :

- Protocol is defined as the set of rules agreed by the sender and receiver.
- There can be different protocols defined for different functions. Protocols govern the exchange of data in true sense.
- A set of such rules is known as a "protocol" of the data communication system.
- Many different protocols are used in the modern data communication system.
- The interconnection of one station to many stations is called as networking.
- A network is any interconnection of two or more stations that wish to communicate.

1.4 Data Communication System :

Block diagram :

- Fig. 1.4.1 shows the simplified block diagram of data communication system.
- Suppose that the source and transmitter are the components of a personal computer. The user of this PC wants to send a message "m" to another PC.
- Then the message "m" will be in the form of a digital bit stream and called as **input data** as shown in Fig. 1.4.1.



(L-3) Fig. 1.4.1 : Data communication system

- The sender's PC is connected to some **transmission medium** such as a local network or a telephone line, by an input/output device (transmitter) such as a modem.
- The input data is applied to the transmitter as a sequence of digital bits on a transmission cable or communication bus.
- The transmitter is connected directly to the medium and converts the incoming digital bit stream into an analog signal suitable for transmission over the communication cable.
- The analog transmitted signal travels on the transmission medium and is subjected to a number of impairments (noise, attenuation etc.), before reaching the receiver.
- Due to these impairments, the received signal may appear completely different from the transmitted signal.
- The receiver tries to estimate the original signal based on the distorted received signal, and the knowledge of transmission medium.
- A sequence of digital bits is produced at the output of the receiver.
- These bits are then sent to the destination which is another PC.
- The signal "m" represents the output information which is presented to the user and can be seen on the computer screen for display or printed using a printer.

1.5 Analog and Digital Signals :

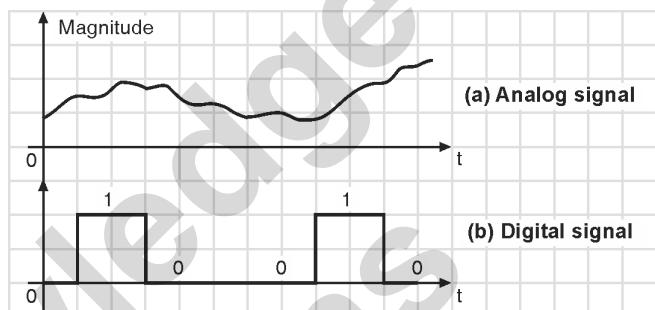
- Signals can be of two types :
 1. Analog signals.
 2. Digital signals.

1. Analog signal :

- It is the signal in which the signal magnitude varies in a smooth fashion without any break with respect to time, as shown in Fig. 1.5.1(a).

2. Digital signal :

- It is the signal in which the signal magnitudes has a constant level for some period of time, then it changes suddenly to another constant level as shown in Fig. 1.5.1(b).
- The examples of digital signal are binary signal, hexadecimal signal etc.



(L-24) Fig. 1.5.1 : Types of signals

1.5.1 Analog and Digital Data :

- Data are the entities which convey meaning, or information such as temperature, pressure etc.
- Signals are electric or electromagnetic representation of data.
- Thus signal is the representation of data.
- Data can be of two types :
 1. Analog data
 2. Digital data.

1. Analog data :

- Analog data is the type of data that varies continuously (smoothly) with respect to time.
- Voice and video are the best examples of analog data. The other examples are temperature, pressure etc.

2. Digital data :

- Digital data is the type of data that can take on discrete values i.e. it is discrete in nature.
- The examples of digital data are text and integers.

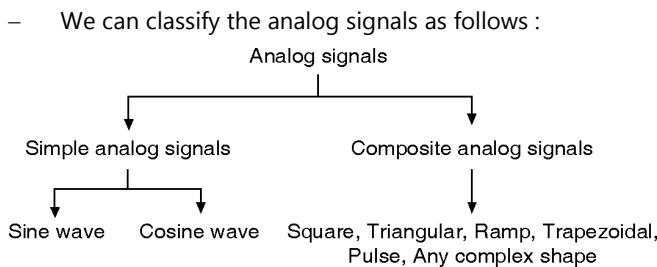
1.6 Analog Signals :

SPPU : Dec. 14, Dec. 15

University Questions

- Q. 1** Write short note on analog signals and digital signals with the help of waveforms.

(Dec. 14, Dec. 15, 6 Marks)



(L-770) Fig. 1.6.1 : Classification of analog signals

1.6.1 Simple Analog Signal :

- It is the analog signal which cannot be decomposed into simpler signals.
- So this is the most basic analog signal which can be used as basic building block to build other composite signals.
- Examples of simple analog signal are sine and cosine waves.

1.6.2 Composite Analog Signal :

- A composed analog signal is made of multiple sine or cosine waves of different amplitudes added to / subtracted from each other.
- Examples of composite analog signals are square wave, triangular wave, ramp, trapezoidal signal, pulse etc.

1.7 Digital Signals : SPPU : Dec. 14, Dec. 15

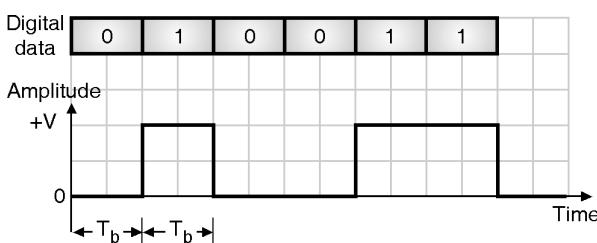
University Questions

Q. 1 Write short note on analog signals and digital signals with the help of waveforms.
(Dec. 14, Dec. 15, 6 Marks)

- The input data which is either analog or digital can also be represented by a digital signal.

Definition :

- A digital signal is a discrete time signal having finite number of amplitudes.
- For example see the digital signal shown in Fig. 1.7.1. 0 is represented by zero volt and a 1 by some positive voltage.



(G-823) Fig. 1.7.1 : Digital signal

1.7.1 Sources of Digital Signal :

- The digital signals can be obtained directly from the computers. All the data used by the computers is digital.
- We can also use an A to D converter (Analog to digital converter) so as to convert analog signals into digital signals.

1.7.2 Advantages of Digital Signals :

SPPU : May 06, May 11

University Questions

Q. 1 What are the advantages of digital signals over analog signals ? **(May 06, May 11, 4 Marks)**

- 1 Digital signals can be processed and transmitted more efficiently and reliably than analog signals.
- 2 It is possible to store the digital data.
- 3 Play back or further processing of the digital data is possible.
- 4 The effect of "noise" (unwanted voltage fluctuations) is less. So digital data does not get corrupt.
- 5 It is possible to separate signal and noise and use repeaters between the transmitter and receiver.
- 6 Use of microprocessor and digital systems is possible.

1.7.3 Bit Interval :

Definition :

- The bit interval is the time corresponding to one single bit (0 or 1).
- As shown in Fig. 1.7.2, time corresponding to a 0 or a 1 is T_b hence it is the bit interval or bit length.

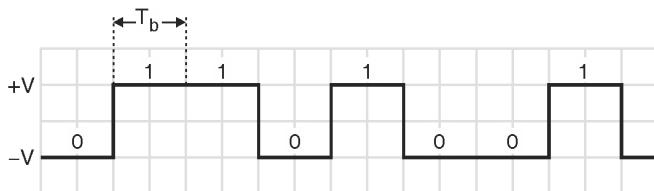
1.7.4 Bit Rate (Data Rate) :

Definition :

- Bit rate is defined as the number of bits transmitted or sent in one second. It is expressed in bits per second (bps).
 - Relation between bit rate and bit interval is as follows :
- $$\text{Bit rate} = \frac{1}{\text{Bit interval}}$$
- Bit rate is also called as **signaling rate** and is defined as the number of bits which can be transmitted in a second.



- If the bit duration is " T_b " then bit rate will be $1/T_b$. Look at Fig. 1.7.2, you will see that the bit duration is necessarily equal to the pulse duration.
- In Fig. 1.7.2 the first pulse is of two bit duration.



(G-83) Fig. 1.7.2 : A bit stream

- Bit rate is also called as signaling rate and it should be as high as possible.
- However with increase in bit rate the bandwidth of transmission medium (channel bandwidth) must be increased, in order to ensure that the signal is received without any distortion.

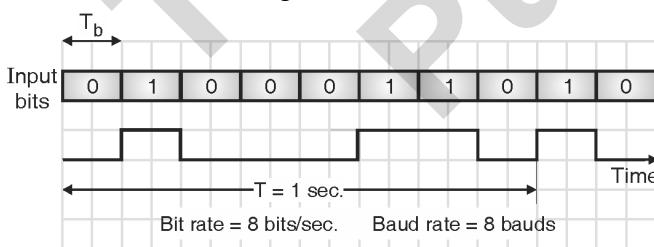
1.7.5 Bauds (or Baud Rate) :

Definition :

- Baud** is defined as the unit of signaling speed or modulation rate or the rate of symbol transmission.
- It indicates the rate at which a signal level changes over a given period of time.

Baud rate of binary transmission :

- When binary bits are transmitted as an electrical signal with two levels "0" and "1" the bit rate and the modulation rate i.e. baud rate are same.
- This is as shown in Fig. 1.7.3(a).



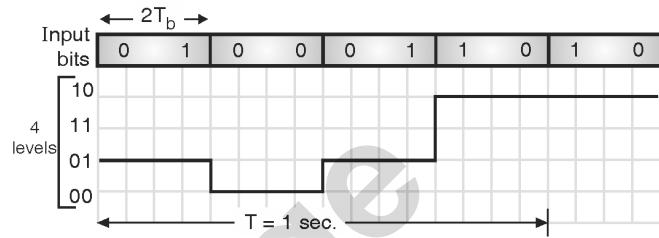
(G-84) Fig. 1.7.3(a) : Baud rate for two level modulation

- Note that for a two level signal (binary signal) the bit rate and bauds are equal.

Baud rate of M-ary transmission :

- Now consider Fig. 1.7.3(b) where four different levels are used to represent the data.
- Each level is being represented by a combination of two bits i.e. 00 or 01 etc.

- The bit rate is therefore not equal to the baud rate.
- The bit rate is 8 bits/sec. but baud rate is only 4 bauds as there are 4-levels per second.



(G-85) Fig. 1.7.3(b) : Baud rate for a four level modulation

Ex. 1.7.1 : A system sends a signal that can assume 8 different voltage levels. It sends 400 of these signals per second. What are the baud and bit rates ?

Dec. 01, May 02, 4 Marks, May 03, 6 Marks

Soln. :

- As the signal assumes 8 different voltage levels we need 3 bit digital signal to have 8 different combinations.
- Hence the number of bits per voltage level is 3. Let each voltage level represent one symbol.

$$\therefore \text{Number of bits / symbol} = 3$$
- The system sends 400 signal / sec. Hence the number of symbols transmitted per second is also 400.

$$\begin{aligned}\therefore \text{Symbol rate} &= \text{Number of symbols / sec.} \\ &= 400 \text{ symbols / sec.}\end{aligned}$$
- The baud rate is defined as the number of symbols per second.

$$\therefore \text{Baud rate} = \text{Symbol rate.}$$

$$\therefore \text{Baud rate} = 400 \text{ symbols / sec.} \quad \dots\text{Ans.}$$
- We are using 3 bit to represent each symbol.

$$\begin{aligned}\text{So bit rate} &= 3 \times \text{symbol rate} = 3 \times 400 \\ &= 1200 \text{ bits / sec.} \quad \dots\text{Ans.}\end{aligned}$$

Ex. 1.7.2 : A system sends a signal that can assume 4 different voltage levels. It sends 200 of such signals per second. What is the baud rate ?

May 02, 4 Marks

Soln. :

- This example is similar to the previous example. A system has 4 different voltage levels and it sends 200 of such signals/sec.



- Hence number of voltage levels transmitted will be 200/sec. Therefore the symbol rate is 200 symbols / sec.
 \therefore Baud rate = 200 symbols / sec.Ans.

Ex. 1.7.3 : A system sends a signal that can assume two different voltage level. It sends 100 of signal per second, what is baud rate ?

Dec. 02, 2 Marks

Soln. :

1. As the signal assumes 2 different voltage levels we need. 1 bit digital signal to have 2 different combinations. Hence the number of bits per voltage is 1. Let each voltage level represent one symbol.
 \therefore Number of bits / symbol = 1
2. The system sends 100 signals / sec. Hence the number of symbols transmitted per second is also 100.
 \therefore Baud rate = 100 symbols / sec.

1.7.6 Bit Length :

- The bit length for a digital signal is similar to the term wavelength for an analog signal.
- Bit length of a digital signal is defined as the distance corresponding to one bit on the transmission medium. It is measured in meters or cm.

$$\begin{aligned}\therefore \text{Bit length} &= \text{Propagation speed} \times \text{Bit duration.} \\ &= \frac{\text{meters}}{\text{sec}} \times \text{sec}\end{aligned}$$

1.8 Signal Conversion Methods :

- A computer network is designed to send information from one point to the other.
- It is necessary to convert this information to either digital signal or analog signal for transmission depending on the transmission medium and application.

1.8.1 Encoding and Modulation :

- It is possible to encode any type of data into any type of signal as shown in Fig. 1.8.1.

Digital Signalling :

- Fig. 1.8.1(a) illustrates the concept of **digital signalling** in which the input data (analog or digital) is encoded into a digital signal.

Analog or digital data → Encoder → Digital signal

(a)

Analog or digital data → Modulator → Analog signal

(b)

(L-25) Fig. 1.8.1 : Conversion from analog / digital data to analog / digital signal

Analog Signalling :

- Fig. 1.8.1(b) illustrates the concept of **analog signalling** in which the analog / digital source is used for modulating a continuous time carrier signal to produce an analog signal called modulated signal.

1.8.2 Signal Conversion Methods :

- There are four different signal conversion methods as follows :

1. Digital data, digital signal (D to D conversion)
2. Analog data, digital signal (A to D conversion)
3. Digital data, analog signal (D to A conversion)
4. Analog data, analog signal (A to A conversion)

1.9 A to D Conversion :

Principle :

- The process of converting the analog data to digital signal is known as digitisation.
- It is also called as A to D conversion.
- In this conversion process, the input analog data is converted into equivalent digital signal as shown in Fig. 1.9.1.
- In order to carry out this transformation, one has to follow a sequence of operations such as sampling, quantization and encoding.



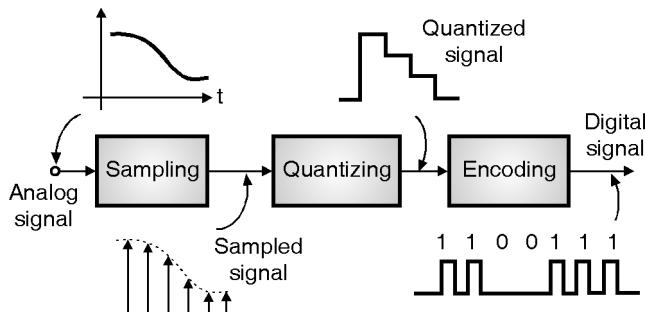
(L-218) Fig. 1.9.1 : Transformation from Analog signal to digital signal

Examples :

- This process is essential in all the digital communication systems such as Pulse Code Modulation (PCM) or Delta Modulation (D.M).

1.9.1 Block Diagram :

- The analog to digital conversion (A/D) can be achieved by using the system shown in Fig. 1.9.2.



(E-1) Fig. 1.9.2 : Analog-to-digital conversion

- This system consists of three blocks namely sampler, quantizer and encoder.
- The message signal can be analog or digital type. An analog signal can always be converted into a digital signal.

Sampler :

- The analog signal is applied at the input of the sampler.
- The sampler is a switch which samples the input signal at regular intervals of time and produces the discrete version of the input signal.

Quantizer :

- Quantization is a process of approximation or rounding off.
- Quantization process approximates each sample to its nearest standard voltage level called quantization level. We get the approximated version of the sampled signal at the output of the quantizer.
- The number of quantization levels is finite and generally it is a power of 2 i.e. 2, 4, 8, 16, 32

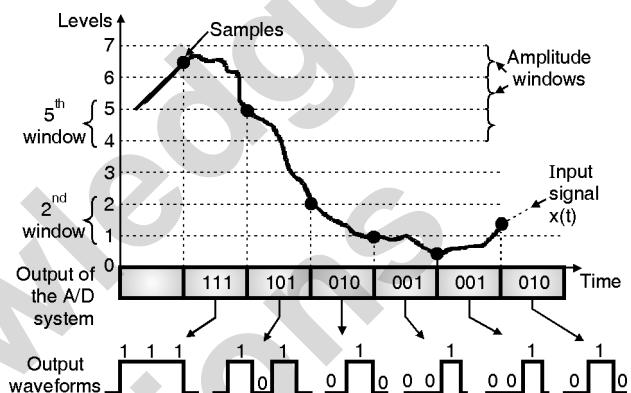
Encoder :

- An encoder converts each quantized sample into a separate code word of length say N bits.
- Thus at the output of the encoder we get digital code words.

1.9.2 Graphical Representation of A/D Conversion Process :

- Fig. 1.9.3 illustrates the A to D conversion process graphically.

- It is important to understand that the output is in the form of binary codes.
- Each transmitted binary code represents a particular amplitude of the input signal.
- Hence the "information" is represented in the form of a "code" which is being transmitted.
- The range of input signal magnitudes is divided into 8-equal levels (Y axis in Fig. 1.9.3).



(E-2) Fig. 1.9.3 : Input and output waveforms of an A to D converter

- Each level is denoted by a three bit digital word between 000 and 111.
- Input signal $x(t)$ is sampled. If the sample is in the 5th - window of amplitude then a digital word 101 is transmitted. If the sample is in the 2nd - window then the transmitted word is 010 and so on.
- In this illustration we have converted the sampled amplitudes into 3 bit codes, but in practice the number of bits per word can be as high as 8, 9 or 10.
- The codewords shown in Fig. 1.9.3 are three bit numbers. It is possible to introduce one more bit to indicate the "sign."

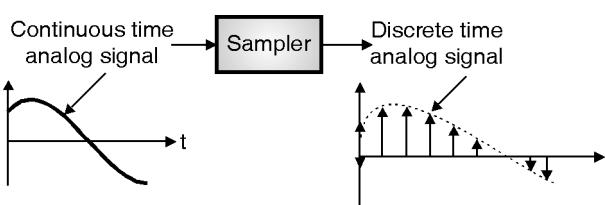
Error :

- Due to the approximation taking place in the quantization process, the A to D conversion introduces some error in the digital signal.
- Such errors cannot be reversed and it is not possible to produce an exact replica of the original analog signal at the receiver.
- However it is possible to minimize these errors by selecting a proper sampling rate and number of quantization levels.



1.9.3 Sampling Process :

- In the pulse modulation and digital modulation systems, the signal to be transmitted must be in the discrete time form.
- The sampling process is used to convert the analog input signal into a discrete time signal.
- For the sampling process to be of practical utility it is necessary to choose the sampling rate properly.
- Fig. 1.9.4 summarizes the sampling process.



(L-156) Fig. 1.9.4 : Sampling process

Definition :

- Thus sampling is the process of converting a continuous analog signal to a discrete analog signal and the sampled signal is the discrete time representation of the original analog signal.

Nyquist Rate :

- The minimum sampling rate of "2W" samples per second for a signal $x(t)$ having maximum frequency of "W" Hz is called as "Nyquist rate".

$$\text{Nyquist rate} = 2W \text{ Hz.}$$

Importance of Sampling Theorem :

- The first step in any digital communication system is conversion of a continuous time signal into a discrete time signal.
- This is achieved by sampling the given continuous time signal.
- The sampling rate f_s is an important parameter to ensure that the sampled signal represents the original signal faithfully.
- The sampling theorem helps us to decide the value of the minimum sampling frequency $f_{s(\min)}$ to avoid distortion.
- The minimum sampling frequency $f_{s(\min)}$ is called as the Nyquist rate.

1.9.4 Quantization Process :

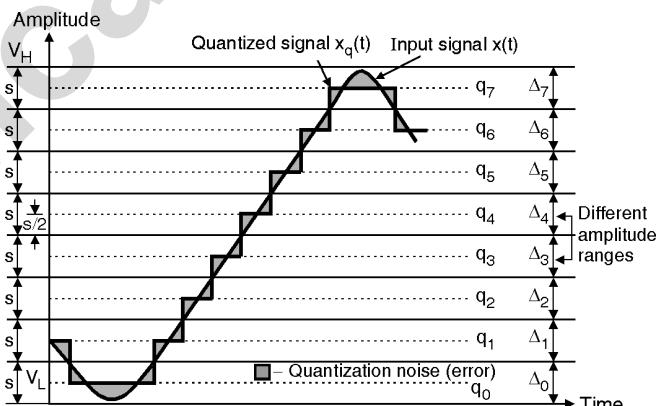
- In the analog to digital (A to D) conversion process, the first block is sampler and the next block is quantizer.

Definition :

- Quantization is a process of approximating or rounding off a sampled value to a nearest predetermined level called as quantization level.

Quantization process :

- The sampled signal in an A to D converter is applied to the quantizer block.
- Quantizer converts the sampled signal into an approximate quantized signal which consists of only a finite number of predecided voltage levels.
- Each sampled value at the input of the quantizer is approximated or rounded off to the nearest standard predecided voltage level.
- These standard levels are known as the "quantization levels".
- Refer to Fig. 1.9.5 to understand the process of quantization.



(L-225) Fig. 1.9.5 : Process of quantization

- The input signal $x(t)$ is assumed to have a peak to peak swing of V_L to V_H volts.
- This entire voltage range has been divided into "Q" equal intervals each of size "s".
- "s" is called as the step size and its value is given as,

$$s = \frac{V_H - V_L}{Q} \quad \dots(1.9.1)$$

- In Fig. 1.9.5, the value of $Q = 8$
- At the center of these ranges, the quantization levels q_0, q_1, \dots, q_7 are placed.



- Thus the number of quantization levels is $Q = 8$. The quantization levels are also called as decision thresholds.
- $x_q(t)$ represents the quantized version of $x(t)$. We obtain $x_q(t)$ at the output of the quantizer.
- When $x(t)$ is in the range Δ_0 , then corresponding to any value of $x(t)$, the quantizer output will be equal to " q_0 ".
- Similarly for all the values of $x(t)$ in the range Δ_1 , the quantizer output is constant equal to " q_1 ".
- Thus in each range from Δ_0 to Δ_7 , the signal $x(t)$ is rounded off to the nearest quantization level and the quantized signal is produced.
- The quantized signal $x_q(t)$ is thus an approximation of $x(t)$.
- The difference between them is called as quantization error or quantization noise.
- This error should be as small as possible.
- To minimize the quantization error we need to reduce the step size "s" by increasing the number of quantization levels Q.

1.9.5 Quantization Error or Quantization

Noise ϵ :

SPPU : Dec. 12

University Questions

- Q. 1** Explain with diagram pulse code modulation.
Define the term quantization error.

(Dec. 12, 8 Marks)

Definition :

- The difference between the instantaneous values of the quantized signal and input signal is called as **quantization error or quantization noise**.

$$\epsilon = x_q(t) - x(t) \quad \dots(1.9.2)$$

- The quantization error is shown by shaded portions of the waveform in Fig. 1.9.5.
- The maximum value of quantization error is $\pm s/2$ where s is step size.
- Therefore to reduce the quantization error we have to reduce the step size by increasing the number of quantization levels i.e. Q.

1.10 Pulse Code Modulation (PCM) :

SPPU : May 10, Dec. 10, Dec. 11, May 12, Dec. 12, Dec. 14, May 15, May 16, May 17, Dec. 17, May 18

University Questions

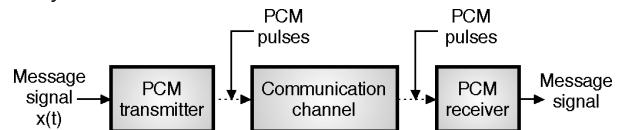
- Q. 1** Explain pulse code modulation. **(May 10, May 15, 4 Marks)**
- Q. 2** What is PCM ? Describe it in detail with the help of diagram. **(Dec. 10, 4 Marks)**
- Q. 3** Explain pulse code modulation. State the advantages of delta modulation over pulse code modulation. **(Dec. 11, 8 Marks)**
- Q. 4** What is PCM ? Describe with the help of diagram. **(May 12, 4 Marks, May 16, 6 Marks)**
- Q. 5** Explain with diagram pulse code modulation. Define the term quantization error. **(Dec. 12, 8 Marks)**
- Q. 6** Draw and explain PCM and DM. **(Dec. 14, May 17, Dec. 17, May 18, 7 Marks)**

Definition :

- Pulse Code Modulation (PCM) is an example of A to D conversion scheme.
- PCM is a type of pulse modulation system which converts the analog information at its input into a digital information at its output.
- The information is transmitted in the form of "code words".

Block diagram :

- Fig. 1.10.1 shows the simplified block diagram of a PCM system. It consists of a transmitter and receiver.



(E-1072) Fig. 1.10.1 : Simplified block diagram of PCM system

- The transmitter converts the message signal $x(t)$ into a series of coded pulses and sends it over the communication channel.
- The transmitter is also called as an encoder.
- The receiver performs exactly in the reverse way as compared to the transmitter.
- It will convert the received encoded PCM pulses back into the message signal.



1.10.1 PCM Transmitter (Encoder) :

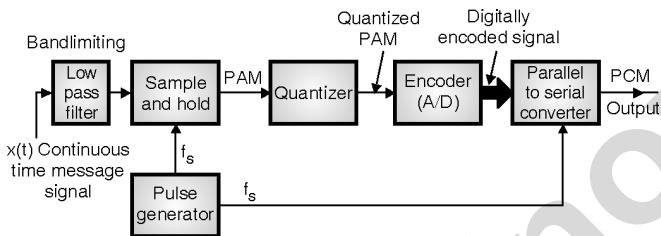
SPPU : Dec. 10, May 12, Dec. 14, May 16

University Questions

- Q. 1** What is PCM ? Describe it in detail with the help of diagram. **(Dec. 10, 4 Marks)**
- Q. 2** What is PCM ? Describe with the help of diagram. **(May 12, 4 Marks)**
- Q. 3** Draw and explain PCM and DM. **(Dec. 14, 6 Marks)**
- Q. 4** Explain pulse code modulation with suitable diagram. **(May 16, 6 Marks)**

Block diagram :

- Block diagram of the PCM transmitter is as shown in Fig. 1.10.2.



(L-221) Fig. 1.10.2 : PCM transmitter (Encoder)

Operation of PCM transmitter :

Operation of the PCM transmitter is as follows :

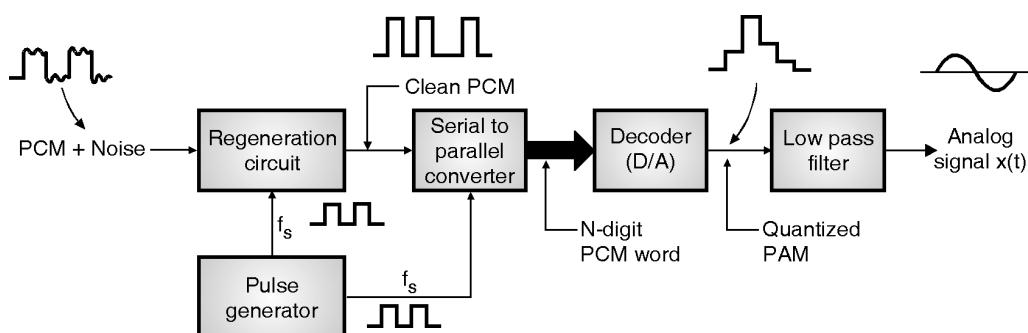
- The analog signal $x(t)$ is passed through a bandlimiting low pass filter, which has a cut-off frequency $f_c = W$ Hz.
- The band limited analog signal is then applied to a sample and hold circuit where it is sampled at adequately high sampling rate. Output of sample and hold block is a flat topped PAM signal.

- These samples are then subjected to the operation called "Quantization" in the "Quantizer".
- The quantization is used to reduce the effect of noise. The combined effect of sampling and quantization produces the quantized PAM at the quantizer output.
- The quantized PAM pulses are applied to an encoder which is basically an A to D converter.
- Each quantized level is converted into an N bit digital word by the A to D converter. The value of N can be 8, 16, 32, 64 etc.
- The encoder output is converted into a stream of pulses by the parallel to serial converter block.
- Thus at the PCM transmitter output we get a train of digital pulses.
- A pulse generator produces a train of rectangular pulses with each pulse of duration " τ " seconds.
- The frequency of this signal is " f_s " Hz. This signal acts as a sampling signal for the sample and hold block.
- The same signal acts as "clock" signal for the parallel to serial converter. The frequency " f_s " is adjusted to satisfy the Nyquist criteria.

1.10.2 PCM Receiver (Decoder) :

Block diagram :

- Fig. 1.10.3 shows the block diagram of a PCM receiver.



(L-224) Fig. 1.10.3 : PCM receiver (Decoder)



Operation of PCM receiver :

- A PCM signal contaminated with noise is available at the receiver input.
- The regeneration circuit at the receiver will separate the PCM pulses from noise and will reconstruct the original PCM signal.
- The pulse generator has to operate in synchronization with that at the transmitter.
- Thus at the regeneration circuit output we get a "clean" PCM signal.
- The reconstruction of PCM signal is possible due to the digital nature of PCM signal.
- The reconstructed PCM signal is then passed through a serial to parallel converter.
- Output of this block is then applied to a decoder.
- The decoder is a D to A converter which performs exactly the opposite operation of the encoder.
- The decoder output is the sequence of a quantized multilevel pulses.
- The quantized PAM signal is thus obtained, at the output of the decoder.
- This quantized PAM signal is passed through a low pass filter to recover the analog signal, $x(t)$.
- The low pass filter is called as the reconstruction filter and its cut off frequency is equal to the message bandwidth W .

1.10.3 Applications of PCM :

- Some of the applications of PCM are as follows :
1. In digital telephone systems.
 2. In the space communication, space craft transmits signals to earth. Here the transmitted power is very low (10 to 15W) and the distances are huge (a few million km). Still due to the high noise immunity, only PCM systems can be used in such applications.

1.10.4 Advantages of PCM :

1. Very high noise immunity.

2. Due to digital nature of the signal, repeaters can be placed between the transmitter and the receivers. The repeaters actually regenerate the received PCM signal. This is not possible in analog systems. Repeaters further reduce the effect of noise.
3. It is possible to store the PCM signal due to its digital nature.
4. It is possible to use various coding techniques so that only the desired person can decode the received signal. This makes the communication secure.
5. The increased channel bandwidth requirement for PCM is balanced by the improved SNR.

1.10.5 Disadvantages of PCM :

1. The encoding, decoding and quantizing circuitry of PCM is complex.
2. PCM requires a large bandwidth as compared to the other systems.

1.11 Delta Modulation (D.M.) :

SPPU : May 17, Dec. 17, May 18

University Questions

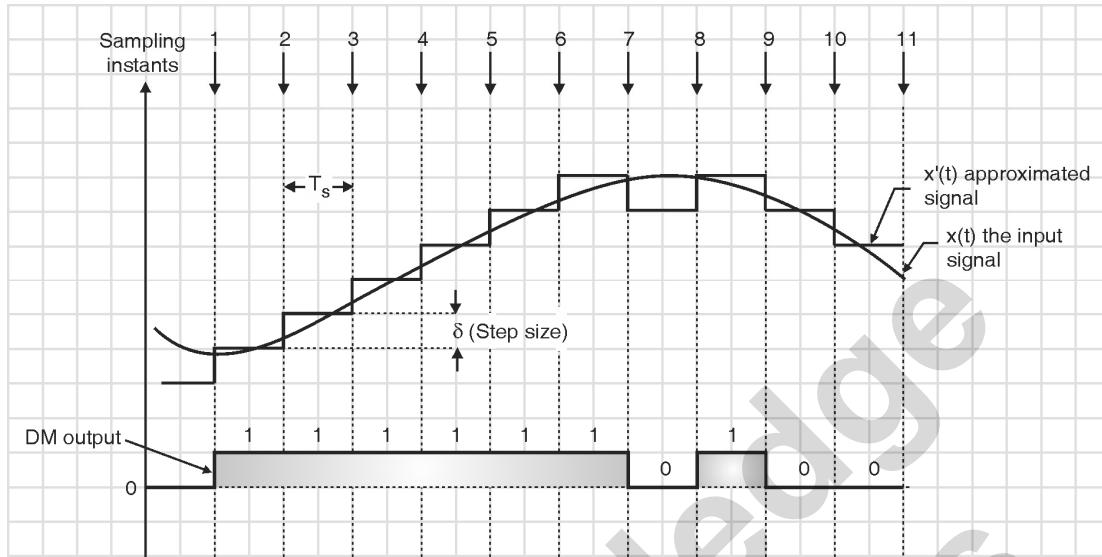
Q. 1 Draw and explain PCM and DM.

(May 17, Dec. 17, May 18, 7 Marks)

- In PCM system, N number of binary digits are transmitted per quantized sample.
- Hence the signaling rate and transmission channel bandwidth of the PCM system are very large.
- These disadvantages can be overcome by using the delta modulation.

Principle of operation :

- Delta modulation transmits only one bit per sample instead of N bits transmitted in PCM. This reduces its signaling rate and bandwidth requirement to a great extent.
- In the basic or linear D.M., a staircase approximated version of the sampled input signal is produced as shown in Fig. 1.11.1.
- The original signal and its staircase representation are then compared to produce a difference signal.



(L-235) Fig. 1.11.1 : D.M. waveforms

- And this difference signal is quantized into only two levels namely $\pm \delta$ corresponding to positive and negative difference respectively.
- That means if the approximated signal $x'(t)$ lies below $x(t)$ at the sampling instant, then the approximated signal is increased by " δ ". (See instants 1, 2, 3, 4, 5 and 6 in Fig. 1.11.1.)
- Whereas if $x'(t)$ is greater than $x(t)$ at the sampling instant, then $x'(t)$ is decreased by " δ " (see instants 7, 9 and 10 in Fig. 1.11.1.)

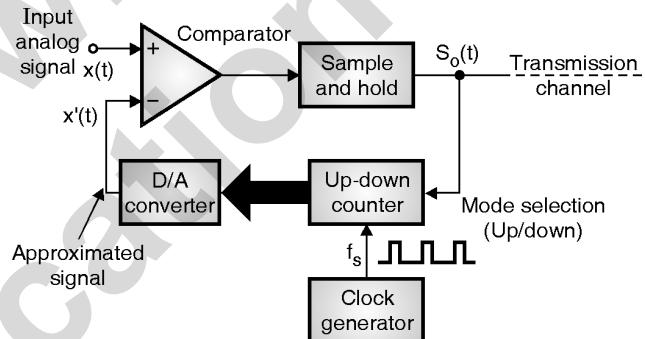
D.M. output :

- As shown in Fig. 1.11.1, the D.M. output is 1 if the staircase signal $x'(t)$ is increased by " δ " i.e. at sampling instants 1, 2, 3, 4, 5 and 6.
- Whereas D.M. output is 0 if $x'(t)$ is decreased by " δ " i.e. at sampling instants 7, 9 and 10.
- In delta modulation, the present sample value $x(t)$ is compared with the approximate value $x'(t)$ and the result of this comparison is transmitted.
- Thus we are sending the information of whether the present sample value is higher than or lower than the approximate value. Note that the actual sampled value is not being transmitted.

1.11.1 Delta Modulator Transmitter :

Block diagram :

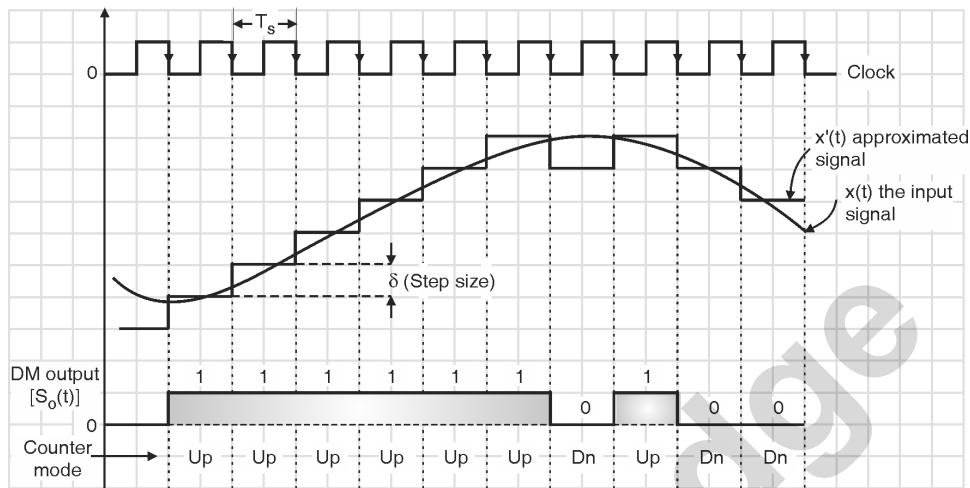
- The block diagram of a delta modulator transmitter is as shown in the Fig. 1.11.2.



(L-236) Fig. 1.11.2 : D.M. transmitter

Operation :

- The operation of the transmitter is as follows :
- $x(t)$ is the analog input signal and $x'(t)$ is the quantized (approximated) version of $x(t)$. Both these signals are applied to a comparator.
- The comparator output goes high if $x(t) > x'(t)$ and it goes low if $x(t) < x'(t)$.
- Thus the comparator output is either 1 or 0. The sample and hold circuit will hold this level (0 or 1) for the entire clock cycle period.
- The output of the sample and hold circuit is transmitted as the output of the DM system.
- Thus in DM, the information which is transmitted is only whether $x(t) > x'(t)$ or vice versa.
- Also note that one bit per clock cycle is being sent. This will reduce the bit rate and hence the BW.
- The transmitted signal is also used to decide the mode of operation of an up/down counter.



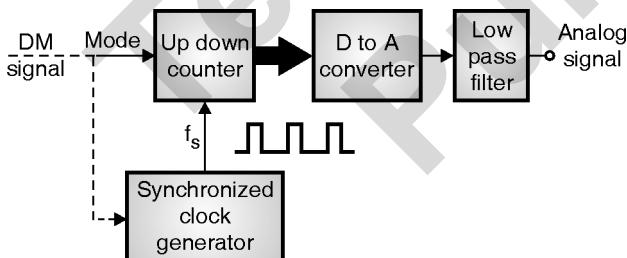
(L-237) Fig. 1.11.3 : D.M. waveforms

- The counter output increments by 1 if $S_o(t) = 1$ and it decrements by 1 if $S_o(t) = 0$, at the falling edge of each clock pulse. This is as shown in the waveform in the Fig. 1.11.3.
- The counter output is converted into analog signal by a D to A converter.
- Thus we get the approximated signal $x'(t)$ at the output of the D to A converter.

1.11.2 D.M. Receiver :

Block diagram :

- The block diagram of the D.M. receiver is as shown in Fig. 1.11.4.



(L-238) Fig. 1.11.4 : D.M. receiver

- Compare it with the transmitter block diagram, you will find that it is identical to the chain of blocks producing the signal $x'(t)$ i.e. the approximated signal.
- The original modulating signal can be recovered back by passing this signal through a low pass filter.

1.11.3 Applications of D.M. :

- For some types of digital communications.

- For digital voice storage.

1.11.4 Distortions in the DM System :

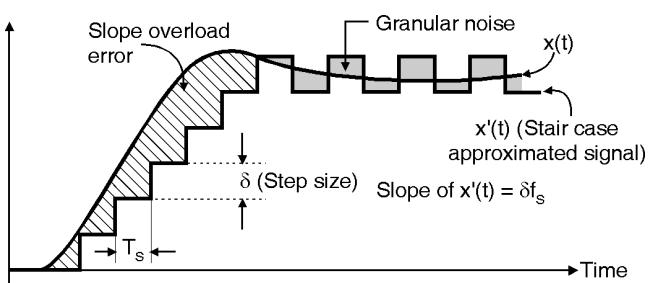
SPPU : Dec. 18

University Questions

Q. 1 What is meant by delta modulation ? Explain distortions in delta modulation. (Dec. 18, 7 Marks)

- The DM system is subjected to two types of quantization error or distortions :

1. Slope overload distortion and
2. Granular noise.



(L-239) Fig. 1.11.5 : Distortions in D.M.

1. Slope overload distortion :

- Look at the Fig. 1.11.5. Due to small step size (δ), the slope of the approximated signal $x'(t)$ will be small.

$$\text{The slope of } x'(t) = \frac{\delta}{T_s} = \delta f_s \quad \dots(1.11.1)$$

- If slope of the input analog signal $x(t)$ is much higher than that of $x'(t)$ over a long duration then $x'(t)$ will not be able to follow the variations in $x(t)$, at all.
- The difference between $x(t)$ and $x'(t)$ is called as the slope overload distortion.



- Thus the slope overload error occurs when slope of $x(t)$ is much larger than slope of $x'(t)$.
- The slope overload error can be reduced by increasing slope of the approximated signal $x'(t)$.
- Slope of $x'(t)$ can be increased and hence the slope overload error can be reduced by either increasing the step size " δ " or by increasing the sampling frequency f_s .
- However with increase in δ the granular noise increases and if f_s is increased, signaling rate and bandwidth requirements will go up. Thus reducing the slope overload error is not easy.

2. Granular noise :

- When the input signal $x(t)$ is relatively constant in amplitude, the approximated signal $x'(t)$ will fluctuate above and below $x(t)$ as shown in Fig. 1.11.5.
- The difference between $x(t)$ and $x'(t)$ is called as granular noise.
- The granular noise is similar to the quantization noise in the PCM system.
- It increases with increase in the step size δ . To reduce the granular noise, the step size should be as small as possible.
- However this will increase the slope overload distortion.
- In the linear delta modulator the step size δ is not variable. If it is made variable then the slope overload distortion and granular noise both can be controlled.
- A system with a variable step size is known as the adaptive delta modulator (ADM).

1.11.5 Advantages of Delta Modulation :

SPPU : Dec. 11

University Questions

Q. 1 Explain pulse code modulation. State the advantages of delta modulation over pulse code modulation. **(Dec. 11, 8 Marks)**

1. Low signalling rate and low transmission channel bandwidth, because in delta modulation, only one bit is transmitted per sample.
2. The delta modulator transmitter and receiver are less complicated to implement as compared to PCM.

1.11.6 Disadvantages of Delta Modulation :

1. The two distortions discussed earlier i.e. slope overload error and granular noise are present.
2. Practically the signalling rate with no slope overload error will be much higher than that of PCM.
- The slope overload error can be reduced by using another type of delta modulation, called as adaptive delta modulation (ADM).

1.12 D to A Conversion :

- In the process of D to A conversion the digital data at the input is converted into an analog signals. These analog signals are transmitted over the transmission medium.
- The most familiar application of D to A conversion is for transmitting digital data through the public telephone network.
- The D to A conversion is done by the modems to convert the digital data from the computers into the analog signals that are sent on the telephone lines for the Internet.



(L-791) Fig. 1.12.1 : Digital data to analog signal

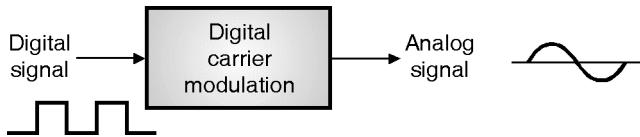
- As shown in Fig. 1.12.1 the digital data is converted into analog signal which is generally a continuous time sinusoidal signal.
- Hence the output of a D to A converter is also known as digital carrier wave modulated signal.

Need of Digital Carrier Wave Modulation :

- This type of digital to analog conversion is essential when the digital message signal is to be sent over a band limited channel such as the telephone line.

Application :

- The best application of digital carrier modulation is MODEM.
- The modem modulates the digital data signal from the DTE (computer) into an analog signal.
- This analog signal is then transmitted on the telephone lines.



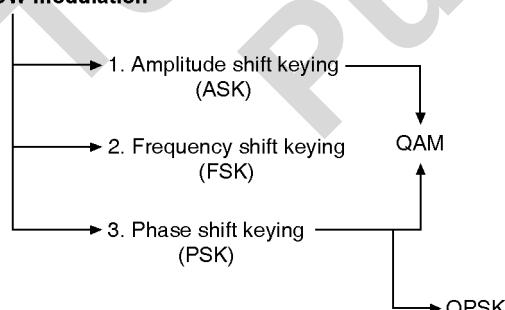
(L-61) Fig. 1.12.2 : Digital carrier modulation

- The digital data consists of binary 0s and 1s, therefore the waveform changes its value abruptly from high to low or low to high.
- In order to carry such a signal without any distortion being introduced, the communication medium needs to have a large bandwidth.
- Unfortunately the telephone lines do not have high bandwidth.
- Therefore we have to convert the digital signal first into an analog signal which needs lower bandwidth by means of the modulation process.

1.12.1 Types of Digital CW Modulation :

- There are three basic types of modulation techniques for the transmission of digital signals.
- These methods are based on the three characteristics of a sinusoidal signal; amplitude, frequency and phase.
- The corresponding modulation methods are then called as :
 1. Amplitude Shift Keying (ASK)
 2. Frequency Shift Keying (FSK)
 3. Phase Shift Keying (PSK)

Digital CW modulation



(L-62) Fig. 1.12.3 : Classification of digital CW modulation

- Digital CW modulation schemes are demonstrated in Fig. 1.12.4.

1. Amplitude Shift Keying (ASK) :

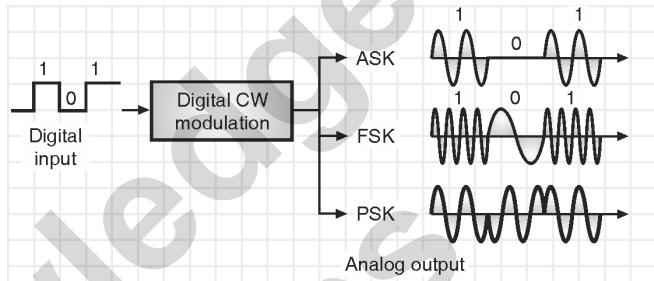
- In ASK the amplitude of the sinusoidal carrier is changed in proportion with the value of binary input data (0 or 1).

2. Frequency Shift Keying (FSK) :

- In FSK the frequency of the sinusoidal carrier is changed in proportion with the value of binary input data (0 or 1).

3. Phase Shift Keying (PSK) :

- In PSK the phase of the sinusoidal carrier is changed in proportion with the value of binary input data (0 or 1).



(L-63) Fig. 1.12.4 : Various digital CW modulation schemes

1.13 Amplitude Shift Keying (ASK) :

SPPU : May 12, Dec. 12, May 17, Dec. 17,
May 18, Dec. 19

University Questions

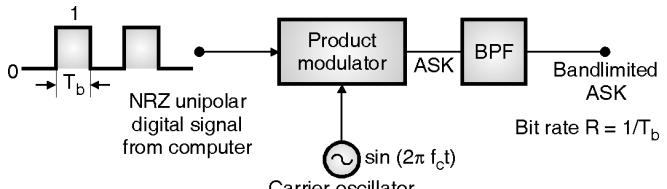
- Q. 1** Explain the shift keying technique with suitable diagram : ASK. **(May 12, 8 Marks)**
- Q. 2** Explain the methods of Digital to Analog conversion : ASK. **(Dec. 12, 8 Marks)**
- Q. 3** Explain the following shift keying techniques with suitable examples :
1. ASK
 2. FSK
 3. PSK
- (May 17, Dec. 17, May 18, Dec. 19, 7 Marks)**

Definition :

- ASK is the digital carrier modulation in which the amplitude of the sinusoidal carrier will take one of the two predetermined values in response to 0 or 1 value of digital input signal.

1.13.1 ASK Generation (Transmitter) :

- The ASK modulator is nothing but a multiplier followed by a band pass filter as shown in Fig. 1.13.1(a).



(L-64) Fig. 1.13.1(a) : ASK generator

- Here the carrier is a sinewave of frequency f_c .



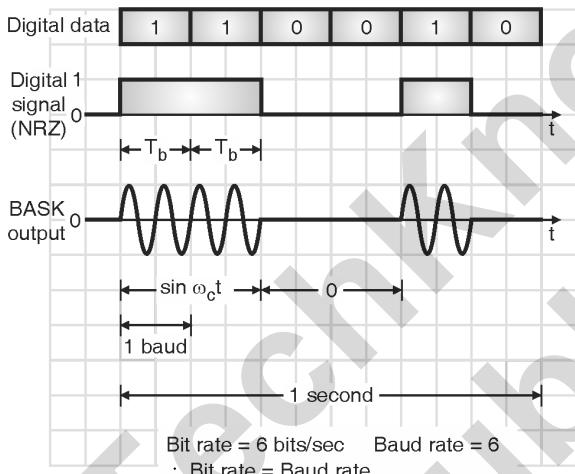
- We can represent the carrier signal mathematically as follows :

$$e_c = \sin(2\pi f_c t) \quad \dots(1.13.1)$$

- The digital signal from the computer is a unipolar NRZ signal which acts as the modulating signal.
- Due to the multiplication, the ASK output will be present only when a binary "1" is to be transmitted.

Waveforms :

- The ASK output waveforms are as shown in Fig. 1.13.1(b).
- The ASK output corresponding to a binary "0" is zero as shown in Fig. 1.13.1(b).
- From the waveforms of Fig. 1.13.1(b) we can conclude that the carrier is transmitted when a binary 1 is to be sent and no carrier is transmitted when a binary 0 is to be sent.



(L-901(a)) Fig. 1.13.1(b) : ASK waveforms

Mathematical representation :

- The ASK signal can be mathematically expressed as follows :

$$V_{ASK}(t) = d \sin(2\pi f_c t) \quad \dots(1.13.2)$$

where d = Data bit which can take values 1 or 0.

$$\left. \begin{array}{l} V_{ASK}(t) = \sin(2\pi f_c t) \text{ when } d = 1 \\ V_{ASK}(t) = 0 \text{ when } d = 0 \end{array} \right\} \quad \dots(1.13.3)$$

1.13.2 Transmission Bandwidth of the ASK Signal :

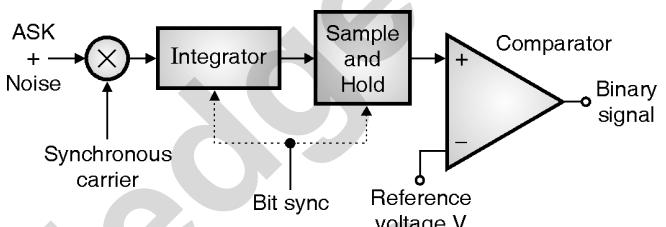
- The bandwidth of ASK signal is dependent on the bit rate f_b . Where bit rate $f_b = 1/T_b$.
- For a bit rate of " f_b " bits/sec. the maximum bandwidth required for an ASK signal is,

$$BW_{(max)} = 2 f_b \text{ Hz} \quad \dots(1.13.4)$$

1.13.3 ASK Receiver :

Block diagram :

- The coherent receiver for an ASK signal is shown in Fig. 1.13.2 in which a locally produced synchronized carrier is applied to a multiplier.



(E-363) Fig. 1.13.2 : Coherent ASK receiver

Operation :

- The ASK signal alongwith noise is also applied to the multiplier.
- The multiplier output is then applied to an integrator which integrated over one bit duration T_b .
- The integrator output is sampled at a particular instant corresponding to the maximum possible value of output and the sampled value is held by the sample and hold circuit.
- The output of sample and hold circuit is compared with a reference voltage V by a comparator.
- If the S/H output is less than V , then comparator output is low which indicates that the received ASK signal is 0.
- If the S/H output is greater than V , then comparator output is high which indicates that the received ASK signal corresponds to 1.
- Thus at the receiver output we recover the original binary signal.

1.13.4 Constellation Diagram :

SPPU : May 08, May 09, Dec. 10

University Questions

Q. 1 Explain different analog to digital modulation techniques with suitable diagram and constellation patterns. (ASK, FSK, PSK, QAM)

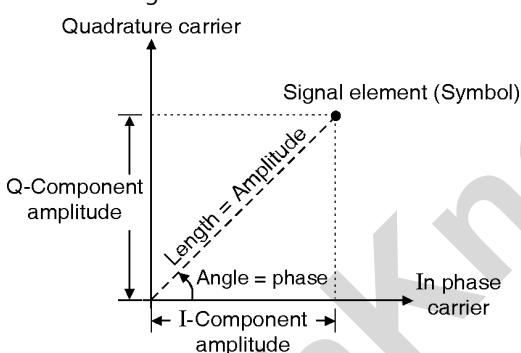
(May 08, 6 Marks, May 09, 10 Marks)

Q. 2 What is constellation pattern ? Describe it in detail with representation technique details. Draw constellation patterns for the ASK, PSK, QPSK and 4-QAM.

(Dec. 10, 10 Marks)

**Definition :**

- A constellation diagram is a diagram which can help us to define the amplitude and phase of each symbol or signal element in a given system (ASK, FSK, PSK, etc.).
- In this diagram each signal element (i.e. symbol) is represented by a dot as shown in Fig. 1.13.3.
- This diagram has two axes i.e. it is a two dimensional graphical representation of a symbol.
- On the X-axis we plot the **in phase carrier** while on the Y-axis we plot the **quadrature (90° phase shifted) carrier**. The concept of constellation diagram has been illustrated in Fig. 1.13.3.



(L-786) Fig. 1.13.3 : Concept of constellation diagram

1.13.5 Constellation Diagram of ASK :

SPPU : May 08, May 09, Dec. 10

University Questions

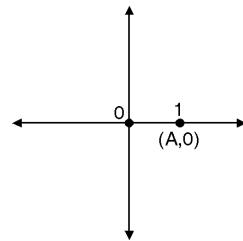
Q. 1 Explain different analog to digital modulation techniques with suitable diagram and constellation patterns. (ASK, PSK)

(May 08, 6 Marks, May 09, 10 Marks)

Q. 2 What is constellation pattern ? Describe it in detail with representation technique details. Draw constellation patterns for the ASK, PSK.

(Dec. 10, 10 Marks)

- Fig. 1.13.4 shows the constellation diagram of ASK. For ASK only one in-phase carrier is used. Hence both the signal points appear on the X-axis.
- There are two symbols (signal elements) in ASK namely 0 and 1.



(L-787) Fig. 1.13.4 : Constellation diagrams of ASK

- The amplitude of binary 0 is zero so it is located at the origin.
- The amplitude of binary 1 is say A volts and has zero phase shift.
- So binary 1 appears at point (A, 0) in Fig. 1.13.4.

1.13.6 Application :

- ASK is not used in many applications. One of its applications is very low speed telemetry circuits.

1.14 Frequency Shift Keying (FSK) :SPPU : May 12, Dec. 12, May 17,
Dec. 17, May 18, Dec. 19**University Questions**

Q. 1 Explain the shift keying techniques with suitable diagram : FSK. (May 12, Dec. 12, 8 Marks)

Q. 2 Explain the following shift keying techniques with suitable examples :

1. ASK
2. FSK
3. PSK

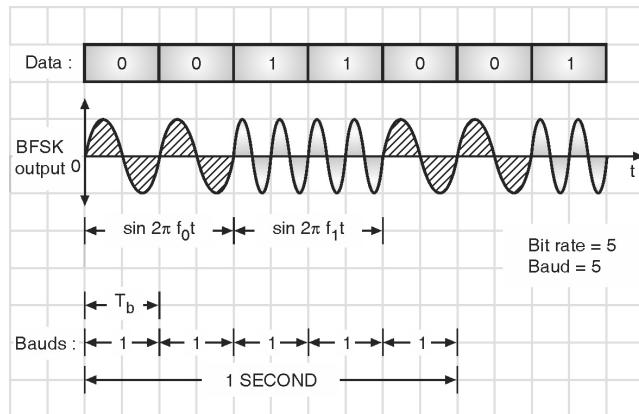
(May 17, Dec. 17, May 18, Dec. 19, 7 Marks)

Definition :

- FSK is a digital modulation system in which, the frequency of a sinusoidal carrier is shifted between two discrete values in response to the value of the digital input signal (0 or 1).
- One of these frequencies (f_1) represents a binary "1" and the other value (f_0) represents a binary "0".

Waveforms :

- The representation of digital data using FSK is as shown in Fig. 1.14.1(a). Note that there is no change in the amplitude of the carrier.

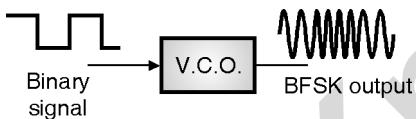


(L-902) Fig. 1.14.1(a) : Representation of digital signal using FSK

1.14.1 FSK Generation :

Block diagram and working :

- Refer to the FSK generator shown in Fig. 1.14.1(b). It is basically a voltage controlled oscillator (VCO) which produce sinewaves at frequencies f_1 and f_0 , respectively.



(L-785) Fig. 1.14.1(b) : FSK generation

- Corresponding to binary 0 input, the VCO produces a sinewave of frequency f_0 whereas corresponding to binary 1 input, the VCO produces a sinewave of frequency f_1 . ($f_1 > f_0$).
- Thus we obtain the binary FSK (BFSK) signal at the output of VCO corresponding to the input digital data bits.

Mathematical expression :

- The FSK is mathematically expressed as follows :

$$\begin{aligned} V_{FSK}(t) &= \sin 2\pi f_0 t \dots \text{for 0 input} \\ &= \sin 2\pi f_1 t \dots \text{for 1 input} \end{aligned}$$

1.14.2 Bandwidth of FSK Signal :

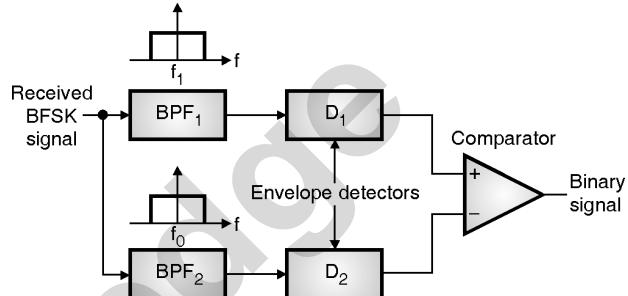
- The bandwidth of FSK signal is dependent on the pulse width T_b or bit rate $f_b = 1/T_b$ and the separation between the frequencies f_0 and f_1 .
- The maximum bandwidth of FSK system is given by,

$$\begin{aligned} B_{max} &= \left(f_1 + \frac{f_b}{2} \right) - \left(f_0 - \frac{f_b}{2} \right) \\ &= (f_1 - f_0 + f_b) \quad \dots(1.14.1) \end{aligned}$$

1.14.3 FSK Receiver :

Block diagram :

- The FSK receiver block diagram is as shown in Fig. 1.14.2.



(E-1092) Fig. 1.14.2 : FSK receiver

- It is supposed to regenerate the original digital data signal from the FSK signal at its input.

Working :

- The receiver consists of two band pass filters one with center frequency " f_0 " and the other with a center frequency of " f_1 ".
- The envelope detectors are simple diode detectors which rectify and filter their inputs, to generate a dc voltage proportional to the ac input.
- Suppose a binary "1" is received. That means the received signal will be,

$$V_{BFSK}(t) = \sin(2\pi f_1 t) \quad \dots(1.14.2)$$

- Thus the BPF₁ will pass this signal to D₁. The output of BPF₂ will be 0, hence the output of D₂ is zero.
- Therefore the comparator output will be positive representing a logic "1".
- Similarly if a binary "0" is received, the received FSK signal will have a frequency " f_0 ".
- The output of BPF₁ will be zero. The BPF₂ will pass this signal to D₂ to produce a proportional dc voltage. Output of D₁ is zero.
- Therefore comparator output will be zero which represents a logic "0". Thus the original data is recovered by the receiver.

1.14.4 Application :

FSK is used for the low data rate MODEMs.



1.15 Phase Shift Keying (PSK) :

**SPPU : May 12, Dec. 12, May 13, May 17, Dec. 17,
May 18, Dec. 19**

University Questions

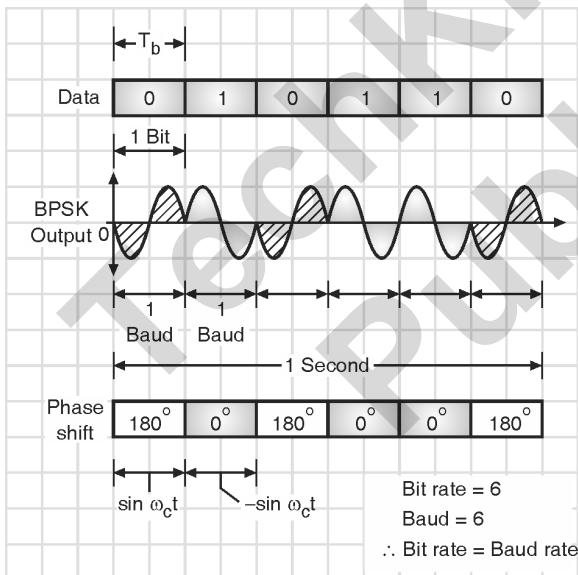
- Q. 1** Explain the shift keying techniques with suitable diagram : PSK **(May 12, Dec. 12, 8 Marks)**
- Q. 2** Explain BPSK. Draw constellation diagram of it. **(May 13, 8 Marks)**
- Q. 3** Explain the following shift keying techniques with suitable examples : 1. ASK 2. FSK 3. PSK **(May 17, Dec. 17, May 18, Dec. 19, 7 Marks)**

Definition :

- Binary phase shift keying is the digital modulation system in which the phase shift of the sinusoidal carrier is shifted between two values (0° and 180°) in response to the value of digital input signal (0 or 1).

Waveforms :

- Fig. 1.15.1(a) shows the simplest form of PSK called Binary PSK (BPSK).



(E-2004) Fig. 1.15.1(a) : Binary phase shift keying (BPSK)

- The carrier phase is changed between 0° and 180° by the bipolar digital signal.
- A bipolar NRZ signal is used to represent the digital data at the input.

Mathematical expression :

- The BPSK signal can be represented mathematically as :

$$V_{\text{BPSK}}(t) = \sin(2\pi f_c t)$$

– when binary "0" is to be represented and $V_{\text{BPSK}}(t) = -\sin(2\pi f_c t)$

$$= \sin(2\pi f_c t + \pi)$$

– when binary "1" is to be represented.

– Combining the two conditions we can write

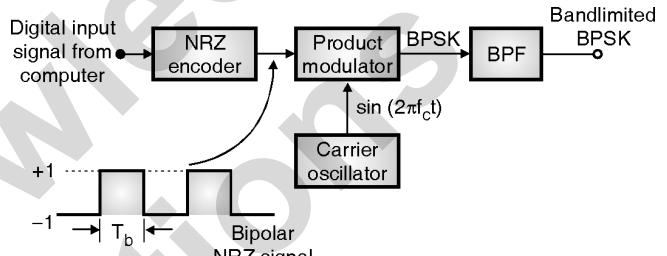
$$V_{\text{BPSK}}(t) = d \sin(2\pi f_c t) \quad \dots(1.15.1)$$

$$\text{where } d = \pm 1$$

1.15.1 BPSK Transmitter :

Block diagram :

- The BPSK generation takes place as shown in Fig. 1.15.1(b).



(L-81) Fig. 1.15.1(b) : BPSK generation

Operation :

- The binary data signal (0s and 1s) is converted into a NRZ bipolar signal by an NRZ encoder, which is then applied to a multiplier (balanced modulator).
- The other input to the multiplier is the carrier signal ($2\pi f_c t$).
- The data bits 0s and 1s are converted into a bipolar NRZ signal "d" as shown in the following table.

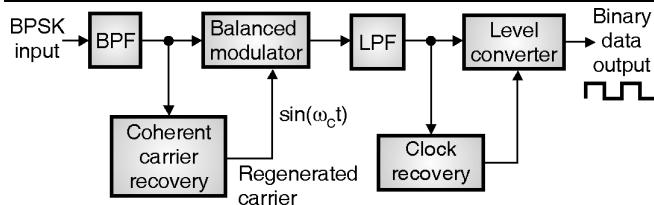
Digital signal	Bipolar NRZ signal	BPSK output
Binary 0	$d = 1$	$V_{\text{BPSK}}(t) = \sin(2\pi f_c t)$
Binary 1	$d = -1$	$V_{\text{BPSK}}(t) = -\sin(2\pi f_c t)$

- The BPSK output corresponding to the "0" binary input i.e. $\sin(2\pi f_c t)$ has a phase shift of 0° , whereas the BPSK output corresponding to a "1" binary input i.e. $(-\sin(2\pi f_c t))$ has a phase shift of 180° .

1.15.2 BPSK Receiver :

Block diagram :

- The block diagram of a BPSK receiver is shown in Fig. 1.15.2.



(E-373) Fig. 1.15.2 : BPSK receiver

- The input BPSK signal can be either $+\sin \omega_c t$ or $-\sin \omega_c t$ representing either logic 1 or 0 respectively.

Operation :

- The coherent carrier recovery circuit detects and regenerates a carrier signal $\sin \omega_c t$.
- This regenerated carrier has the same frequency and phase as the carrier used at the transmitter.
- So the regenerated carrier is known as coherent carrier, which is phase and frequency synchronized with the transmitter.
- The filtered BPSK signal alongwith the regenerated carrier is applied to a balanced modulator which acts as a product detector.

$$\therefore \text{B.M. output} = \text{BPSK} \times \text{Regenerated carrier} \\ = (\pm \sin \omega_c t \times \sin \omega_c t = \pm \sin^2 \omega_c t)$$

But $\sin^2 \theta = \frac{1}{2} - \frac{1}{2} \cos 2\theta$

$$\therefore \text{B.M. output} = \frac{1}{2} \mp \frac{1}{2} \cos 2\omega_c t$$

(E-1459)

↓
 Second harmonic
 ↓
 DC term

- The BM output consist of a dc term and a term having frequency twice the carrier frequency (Second harmonic term).
- The BM output is passed through LPF which allows only the second harmonic term to pass through and blocks the dc component.

$$\therefore \text{LPF output} = \mp \frac{1}{2} \cos 2\omega_c t$$

- The LPF output is applied to the level detector and clock recovery circuit. At the output of level detector we get the following output.

$$-\frac{1}{2} \cos \omega_c t \rightarrow \frac{1}{2} V \text{ (logic 1)}$$

$$-\frac{1}{2} \cos \omega_c t \rightarrow -\frac{1}{2} V \text{ (logic 0)}$$

Thus the binary signal is obtained at the output.

1.15.3 Bandwidth of BPSK :

- The bandwidth of a BPSK signal is given by,

$$\text{BW} = \text{Highest frequency}$$

$$= \text{Lowest frequency in main lobe}$$

$$= (f_c + f_b) - (f_c - f_b)$$

$$\therefore \text{BW} = 2f_b \quad \dots(1.15.2)$$

where $f_b = 1/T_b$

1.15.4 Constellation Diagram of BPSK :

SPPU : May 08, May 09, Dec. 10, Dec. 11, May 13

University Questions

- Q. 1** Explain different analog to digital modulation techniques with suitable diagram and constellation patterns. (ASK, FSK, PSK, QAM)

(May 08, 6 Marks, May 09, 10 Marks)

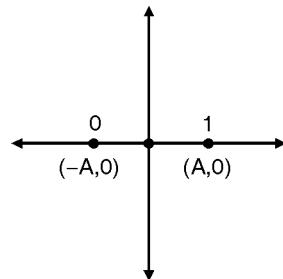
- Q. 2** What is constellation pattern ? Describe it in detail with representation technique details. Draw constellation patterns for the ASK, PSK.

(Dec. 10, 10 Marks)

- Q. 3** Explain BPSK.. Draw constellation diagram of it.

(Dec. 11, May 13, 8 Marks)

- Fig. 1.15.3 shows the constellation diagram of Binary PSK (BPSK).



(L-787(a)) Fig. 1.15.3 : Constellation diagram of BPSK

- BPSK also uses only one in phase carrier. The two symbols in the BPSK system are represented as follows :
 - Binary 1 : Amplitude A, phase 0
 - Binary 0 : Amplitude A, phase 180°
- Hence these two signal points are located at points $(A, 0)$ and $(-A, 0)$ respectively as shown in Fig. 1.15.3.
- Thus BPSK created two signal elements. One with amplitude A and in phase and the other with amplitude A and out of phase.

1.15.5 Applications :

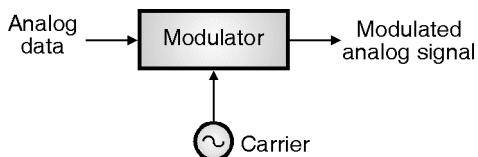
- Phase shift keying (PSK) is the most efficient of the three modulation methods.



- Therefore it is used for high bit rate modems.
- Due to low bandwidth requirement the BPSK modems are preferred over the FSK modems, at higher operating speeds.

1.16 A to A Conversion :

- In some applications we have to transform analog data such as voice, video etc. into analog signal.
- This process is known as modulation. The analog data at the input is called as modulating signal.
- It modulates a high frequency sinusoidal signal called carrier to produce another analog signal called modulated signal.



(L-31) Fig. 1.16.1 : Transformation from analog data to analog signals

Types of A to A Conversion :

- The three basic types of analog to analog conversion are AM, FM and PM.

1.17 Amplitude Modulation (AM) :

SPPU : May 07, May 10, May 11, Dec. 12

University Questions

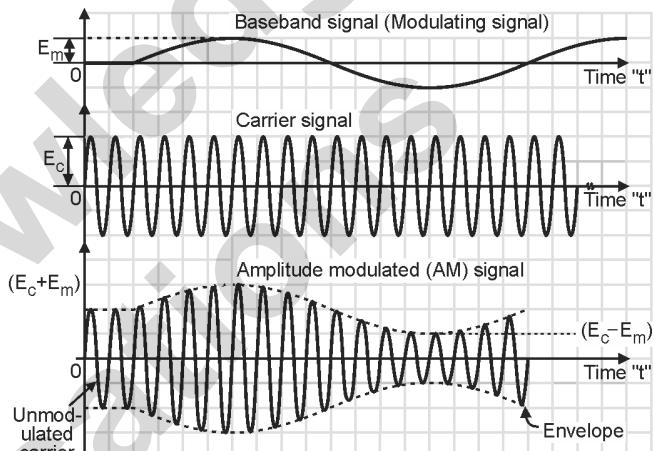
- Q. 1** Define modulation and draw the typical diagram for modulated signals for frequency and amplitude modulation. **(May 07, 4 Marks)**
- Q. 2** With the help of diagram explain amplitude modulation. Write mathematical representation of Amplitude modulated signal. **(May 07, 6 Marks)**
- Q. 3** Explain with diagram amplitude modulation and frequency modulation and compare them. **(May 10, 8 Marks)**
- Q. 4** Draw a neat waveform for amplitude modulation :
 1. Modulating signal
 2. Carrier signal
 3. Amplitude modulated signal
 4. Frequency spectrum of AM wave.**(May 11, 8 Marks)**
- Q. 5** Explain the amplitude modulation. **(Dec. 12, 8 Marks)**

Definition :

- **Amplitude modulation (AM)** or Amplitude Modulation with Full Carrier (AM-FC) is the process of changing the amplitude of a high frequency sinusoidal carrier signal in proportion with the instantaneous value of modulating signal.

Waveforms :

- Fig. 1.17.1 shows the amplitude modulated wave when the modulating signal is a sinusoidal signal.



(D-12) Fig. 1.17.1 : AM waveform (Time domain representation) for sinusoidal modulating signal

Observations :

1. The frequency of the sinusoidal carrier is much higher than that of the modulating signal.
2. In AM the instantaneous amplitude of the sinusoidal high frequency carrier is changed continuously in proportion with the instantaneous amplitude of the modulating signal. This is the principle of AM.
3. The waveforms in Fig. 1.17.1 are also called as the time domain display of AM signal.
4. The information in the AM signal is contained in the amplitude variations of the carrier of the envelope shown by dotted lines in Fig. 1.17.1.
5. Note that the frequency and phase of the carrier remain constant.

Note : The modulating signal in practice may or may not be purely sinusoidal. Most of the times it will have a complex shape.



1.17.1 Expression of AM wave :

SPPU : Dec. 06, May 07

University Questions

- Q. 1** Write the mathematical representation of A.M. Explain the various components in the same. **(Dec. 06, 4 Marks)**
- Q. 2** With the help of diagram explain amplitude modulation. Write mathematical representation of amplitude modulated signal. **(May 07, 6 Marks)**

- Let the modulating signal be sinusoidal and be represented as,
- $$e_m = E_m \cos \omega_m t \quad \dots(1.17.1)$$
- where "e_m" is the instantaneous amplitude of the modulating signal, E_m is the peak amplitude, $\omega_m = 2\pi f_m$ and f_m = Frequency of the modulating signal.
 - Let the carrier signal also be sinusoidal at a much higher frequency than that of the modulating signal. The instantaneous carrier signal e_c is given by,

$$e_c = E_c \cos \omega_c t \quad \dots(1.17.2)$$

where E_c = Peak carrier amplitude,

f_c = Carrier frequency and

$$\omega_c = 2\pi f_c.$$

- The AM wave is expressed by the following expression,

$$e_{AM} = A \cos (2\pi f_c t) \quad \dots(1.17.3)$$

where A = Envelope of AM wave

- Where A represents the instantaneous value of the envelope.
- Then the AM wave is given by,

$$\begin{aligned} e_{AM} &= A \cos (2\pi f_c t) \\ &= [E_c + E_m \cos (2\pi f_m t)] \cos (2\pi f_c t) \\ \therefore e_{AM} &= E_c \left[1 + \frac{E_m}{E_c} \cos (2\pi f_m t) \right] \cos (2\pi f_c t) \end{aligned}$$

- Let m = E_m / E_c be the modulation index.
- $$\therefore e_{AM} = E_c [1 + m \cos (2\pi f_m t)] \cos (2\pi f_c t) \quad \dots(1.17.4)$$
- This expression represents the time domain representation of an AM signal.

Note : It is not necessary to always consider the cosine waves to obtain the mathematical expression. We can even use the sine waves to obtain the mathematical expression for AM.

$$\therefore e_{AM} = E_c [1 + m \sin (2\pi f_m t)] \sin (2\pi f_c t) \quad \dots(1.17.5)$$

- This is the required expression for AM wave in terms of sine wave.

1.17.2 Modulation Index :

SPPU : Dec. 06, May 07, Dec. 11

University Questions

- Q. 1** Define modulation index. **(Dec. 06, 2 Marks)**
- Q. 2** Define modulation and draw the typical diagram for modulated signals for frequency and amplitude modulation. **(May 07, 4 Marks)**
- Q. 3** Define modulation index for frequency and amplitude modulation. **(May 07, 3 Marks)**
- Q. 4** Define modulation and modulation index. **(Dec. 11, 8 Marks)**

Definition :

- In AM wave the modulation index (m) is defined as the ratio of amplitudes of the modulating and carrier waves as follows :

$$M = \frac{E_m}{E_c} \quad \dots(1.17.6)$$

1.17.3 Frequency Spectrum of the AM Wave:

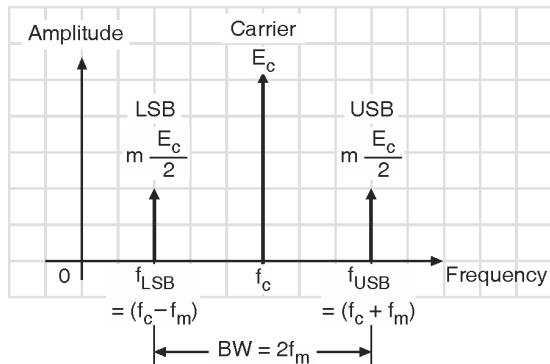
SPPU : Dec. 07, Dec. 10, May 11, Dec. 12

University Questions

- Q. 1** Draw a neat waveform for amplitude modulation :
 1. Modulating signal
 2. Carrier signal
 3. Amplitude modulated signal
 4. Frequency spectrum of AM wave. **(Dec. 07, May 11, 8 Marks)**
- Q. 2** Draw and explain the amplitude modulation generation. Draw frequency domain representation of AM. State the formula for bandwidth calculation of AM and list out advantages of AM. **(Dec. 10, 10 Marks)**
- Q. 3** Explain the following :
 Draw the frequency domain representation of AM and FM wave. **(Dec. 12, 8 Marks)**

Definition :

- The frequency spectrum is a graph of amplitude on Y axis versus frequency on X axis.
- The frequency spectrum of an AM wave is as shown in Fig. 1.17.2.



(D-37)Fig. 1.17.2 : Frequency spectrum of AM wave

- It consists of the carrier and two sidebands. The sidebands are the frequency components at frequencies $(f_c + f_m)$ and $(f_c - f_m)$.

Bandwidth Requirement :

- The bandwidth of the AM signal is equal to the difference between the highest and the lowest frequency component in the frequency spectrum.
- Therefore :

$$\begin{aligned} BW &= f_{USB} - f_{LSB} = (f_c + f_m) - (f_c - f_m) \\ BW &= 2f_m \text{ Hz or kHz} \end{aligned} \quad \dots(1.17.7)$$

1.17.4 Disadvantages of AM (DSBFC) :

- The AM signal is also called as "Double Sideband Full Carrier (DSBFC)" signal. The three main disadvantages of this technique are :
- Power wastage takes place (Carrier does not contain any information).
- AM needs larger bandwidth.
- AM wave gets affected due to noise.

1.17.5 Advantages of AM :

SPPU : Dec. 10

University Questions

- Q. 1** Draw and explain the amplitude modulation generation. Draw frequency domain representation of AM. State the formula for bandwidth calculation of AM and list out advantages of AM.

(Dec. 10, 10 Marks)

- AM transmitters are less complex.
- AM receivers are simple, detection is easy.
- AM receivers are cost efficient. Hence even a common person can afford to buy it.
- AM waves can travel a longer distance.
- Low bandwidth.

1.17.6 Applications of AM :

- Radio broadcasting.
- Picture transmission in a TV system.

Ex. 1.17.1 : An audio frequency signal $10 \sin 2\pi \times 500 t$ is used to amplitude modulate a carrier of $50 \sin 2\pi \times 10^5 t$. Calculate :

- Modulation index
- Sideband frequencies
- Amplitude of each sideband frequencies
- Bandwidth requirement
- Total power delivered to a load of 600Ω .

May 03, 11 Marks, May 06, 10 Marks

Soln. :

- The modulating signal $e_m = 10 \sin (2\pi \times 500 t)$

Comparing it with standard modulating signal given by,

$$e_m = E_m \sin (2\pi f_m t) \text{ we get,}$$

$$E_m = 10 \text{ V}, f_m = 500 \text{ Hz}$$

- The carrier signal $e_c = 50 \sin (2\pi \times 10^5 t)$

Comparing it with the standard carrier signal given by,

$$e_c = E_c \sin (2\pi f_c t) \text{ we get,}$$

$$E_c = 50 \text{ V}, f_c = 1 \times 10^5 \text{ Hz} = 100 \text{ kHz}$$

Step 1 : Modulation index :

$$m = \frac{E_m}{E_c} = \frac{10}{50} = 0.2$$

Step 2 : Sideband frequencies :

- $f_{USB} = f_c + f_m = 100.5 \text{ kHz}$
- $f_{LSB} = f_c - f_m = 99.5 \text{ kHz}$

Step 3 : Amplitude of sidebands :

$$\text{Amplitude of sidebands} = \frac{m E_c}{2} = \frac{0.2 \times 50}{2} = 5 \text{ V}$$

Step 4 : Bandwidth :

$$BW = 2f_m = 2 \times 500 \text{ Hz} = 1 \text{ kHz}$$

Step 5 : Power delivered to load :

$$\begin{aligned} \text{Carrier power, } P_c &= \frac{(E_c/\sqrt{2})^2}{R_L} = \frac{E_c^2}{2 R_L} = \frac{(50)^2}{2 \times 600} \\ &= 2.0833 \text{ W} \end{aligned}$$



$$\text{Total power, } P_t = P_c \left[1 + \frac{m^2}{2} \right]$$

$$= 2.0833 \left[1 + \frac{(0.2)^2}{2} \right] = 2.125 \text{ W}$$

Ex. 1.17.2 : A carrier wave of frequency 1 MHz and peak value 10 V is amplitude modulated by a 5 kHz sine wave of amplitude 6 V. Determine the modulation index and draw spectrum.

Dec. 03, 6 Marks

Soln. :

Given : $f_c = 1 \text{ MHz}$, $E_c = 10 \text{ V}$, $f_m = 5 \text{ kHz}$, $E_m = 6 \text{ V}$

Step 1 : Modulation index :

$$m = \frac{E_m}{E_c} = \frac{6}{10} = 0.6 \quad \dots\text{Ans.}$$

Step 2 : Spectrum :

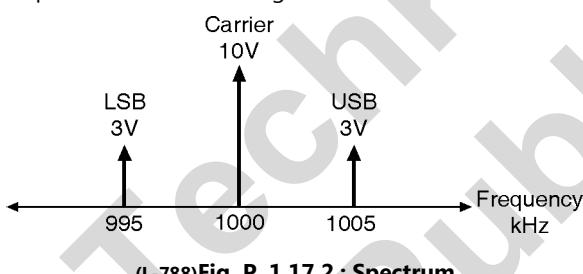
1. $f_{USB} = f_c + f_m = 1000 \text{ kHz} + 5 \text{ kHz} = 1005 \text{ kHz}$

2. $f_{LSB} = f_c - f_m = 1000 \text{ kHz} - 5 \text{ kHz} = 995 \text{ kHz}$

3. Amplitude of each sideband,

$$\frac{m E_c}{2} = \frac{0.6 \times 10}{2} = 3 \text{ Volts}$$

4. Spectrum is shown in Fig. P. 1.17.2.



Ex. 1.17.3 : For given data, find modulation index, frequencies of the sideband components and their amplitudes and plot the frequency spectrum of Amplitude modulated wave :

Modulating signal $e_m = 5 \cos 2\pi 10^3 t$

Carrier signal $e_c = 10 \cos 2\pi 10^4 t$

May 07, 8 Marks

Soln. :

Given : Modulating signal $e_m = 5 \cos 2\pi 10^3 t$

Carrier signal $e_c = 10 \cos 2\pi 10^4 t$

To find :

1. Modulation index
2. Sideband frequencies and amplitudes

3. Frequency spectrum.

1. Modulation index (m) :

From the expressions of e_m and e_c we get,

$$E_m = 5 \text{ V}, f_m = 1000 \text{ Hz}$$

$$E_c = 10 \text{ V}, f_c = 10 \text{ kHz}$$

$$\therefore m = \frac{E_m}{E_c} = \frac{5}{10} = 0.5 \quad \dots\text{Ans.}$$

2. Sideband frequencies :

$$f_{USB} = f_c + f_m = 10 + 1 = 11 \text{ kHz} \quad \dots\text{Ans.}$$

$$f_{LSB} = f_c - f_m = 10 - 1 = 9 \text{ kHz} \quad \dots\text{Ans.}$$

3. Amplitude of sidebands :

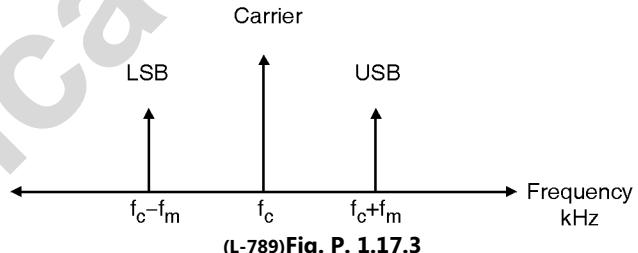
Amplitude of both the sidebands

$$= \frac{m E_c}{2}$$

$$= \frac{0.5 \times 10}{2} = 2.5 \text{ V} \quad \dots\text{Ans.}$$

4. Frequency spectrum :

Fig. P. 1.17.3 shows the frequency spectrum of AM wave.



1.18 Frequency Modulation (FM) :

SPPU : May 10, Dec. 12

University Questions

Q. 1 Explain with diagram amplitude modulation and frequency modulation and compare them.

(May 10, 8 Marks)

Q. 2 Explain the frequency modulation.

(Dec. 12, 8 Marks)

Definition :

- FM is a system of modulation in which the instantaneous frequency of the carrier is continuously varied in proportion with the instantaneous amplitude of the modulating signal.
- The amplitude of the carrier signal remains constant. Thus the information is conveyed via frequency changes.

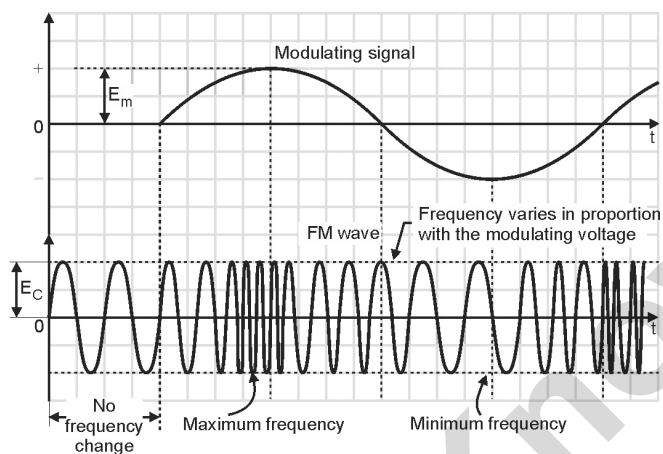


Carrier and Modulating frequency :

- In sinusoidal Frequency Modulation (FM), the modulating signal $x(t) = E_m \cos(2\pi f_m t)$ is a pure sinusoidal signal. The carrier signal $c(t)$ is also a sine wave at much higher frequency.

Waveforms :

- FM transmission is more resistant to noise than A.M. The time domain display of FM wave is as shown in the Fig. 1.18.1.



(B-709) Fig. 1.18.1 : Time domain display of FM wave

- The rate at which these frequency variations or oscillations takes place in the FM wave is equal to the modulating frequency (f_m).
 - The amplitude of the FM wave always remains constant. This is the biggest advantage of FM.
 - For the F.M. wave the modulating signal $x(t)$ be a sinusoidal signal of amplitude E_m and frequency f_m .
- $$\therefore x(t) = E_m \cos(2\pi f_m t) \quad \dots(1.18.1)$$
- The unmodulated carrier is represented by the expression,
- $$e_c = A \sin(\omega_c t + \phi) \quad \dots(1.18.2)$$
- It is a sinusoidal signal with amplitude A and frequency f_c .

1.18.1 Frequency Deviation (δ) :

SPPU : May 19

University Questions

- Q. 1** With respect to FM discuss following terms :

1. Frequency deviation
2. Deviation ratio
3. Bandwidth of FM

(May 19, 6 Marks)

Definition :

- **Frequency deviation δ** is defined as the maximum departure of the instantaneous frequency $f_i(t)$ of the FM wave from the carrier frequency f_c .
- The unit of frequency deviation is Hz or kHz.

Maximum and minimum frequency of FM wave :

- The **maximum** frequency of FM wave is,

$$f_{\max} = f_c + \delta$$

- The **minimum** frequency of a FM wave is,

$$f_{\min} = (f_c - \delta).$$

1.18.2 Mathematical Expression for F.M. :

- We know that the FM wave is a sinewave having a constant amplitude and a variable instantaneous frequency.

- The equation for the FM wave is as follows,

$$e_{FM} = s(t) = E_c \sin \left[\omega_c t + \frac{\delta}{f_m} \sin \omega_m t \right] \dots(1.18.3)$$

- But $\frac{\delta}{f_m} = m_f$ i.e. the **modulation index** of FM wave.

Hence the equation for FM wave is given as,

$$e_{FM} = E_c \sin [\omega_c t + m_f \sin \omega_m t] \dots(1.18.4)$$

- This is the expression for a FM wave, where m_f represents the modulation index.

1.18.3 Modulation Index of FM : SPPU : May 07

University Questions

- Q. 1** Define modulation index for frequency and amplitude modulation. (May 07, 3 Marks)

Definition :

- The modulation index of an FM wave is defined as :

$$m_f = \frac{\text{Maximum frequency deviation}}{\text{Modulating frequency}} \quad \dots(1.18.5)$$

$$\therefore m_f = \frac{\delta}{f_m} \quad \dots(1.18.6)$$

1.18.4 Deviation Ratio :

SPPU : May 19

University Questions

- Q. 1** With respect to FM discuss following terms :

1. Frequency deviation
2. Deviation ratio
3. Bandwidth of FM

(May 19, 6 Marks)



- In FM broadcasting the maximum value of deviation is limited to 75 kHz.
- The maximum modulating frequency is also limited to 15 kHz.
- The modulation index corresponding to the maximum deviation and maximum modulating frequency is called as the "deviation ratio".

$$\text{Deviation ratio} = \frac{\text{Maximum deviation}}{\text{Maximum modulating frequency}}$$

...(1.18.7)

1.18.5 Frequency Spectrum of FM Wave :

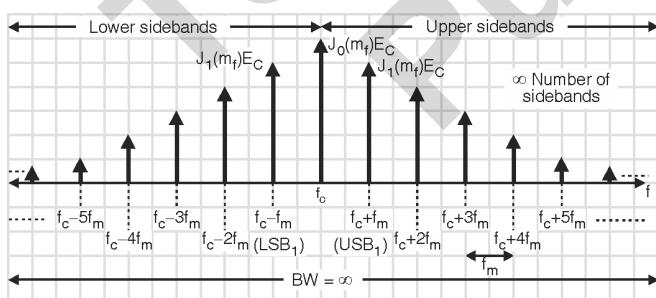
SPPU : Dec. 12

University Questions

- Q. 1** Explain and draw the frequency domain representation of AM and FM wave.

(Dec. 12, 8 Marks)

- Frequency spectrum of FM wave is a graph of amplitude of FM wave plotted on y axis versus the frequency plotted on the x axis.
- Fig. 1.18.2 shows the ideal frequency spectrum of a FM wave.
- It consists of the carrier and infinite sidebands.
- Ideally there are infinite number of sidebands, but practical bandwidth depends on the number of significant sidebands and hence on the modulation index value.
- However the amplitude of FM wave will remain constant.



(D-166) Fig. 1.18.2 : Ideal frequency spectrum of FM wave

1.18.6 Ideal Bandwidth of FM : **SPPU : May 19**

University Questions

- Q. 1** With respect to FM discuss following terms :
1. Frequency deviation
 2. Deviation ratio
 3. Bandwidth of FM

(May 19, 6 Marks)

Ideal Bandwidth of FM :

- **Ideally the bandwidth of FM is infinite**, because its spectrum consists of infinite number of upper and lower sidebands.

Practical Bandwidth :

- The simplest method to calculate the practical bandwidth is as follows :

$$BW = 2 f_m \times \text{Number of significant sidebands} \quad ... (1.18.8)$$

Carson's Rule :

- The second method to find the practical bandwidth is a rule of thumb (Carson's rule).
- It states that the bandwidth of FM wave is equal to twice the sum of the deviation and the highest modulating frequency.

$$BW = 2 [\delta + f_{m(\max)}] \quad ... (1.18.9)$$

1.18.7 Applications of FM :

- Some of the applications of FM are :
 1. Radio broadcasting (VividhBharti, Radio Mirchi).
 2. Sound broadcasting in T.V.
 3. Satellite communication.
 4. Police wireless.
 5. Point to point communication.

- Ex. 1.18.1 :** What is the bandwidth required for FM in which the modulating frequency is 2 kHz and maximum deviation is 10 kHz. Assume highest needed sidebands are 8.

May 18, 6 Marks

Soln. :

$$f_m = 2 \text{ kHz}, \delta = 10 \text{ kHz}$$

Method I :

$$\begin{aligned} \text{Bandwidth} &= 2 f_m \times \text{Number of significant sidebands} \\ &= 2 \times 2 \text{ kHz} \times 8 = 32 \text{ kHz} \end{aligned}$$

Method II :

$$\text{Bandwidth} = 2 [\delta + f_{m(\max)}] = 2 [10 + 2] = 24 \text{ kHz}$$

- Ex. 1.18.2 :** Calculate bandwidth required for FM in which the modulating frequency is 1 kHz and maximum possible deviation is 15 kHz. Assume highest needed sidebands 5. Also calculate bandwidth using Carson's rule ?

Dec. 18, 6 Marks



Soln. :

Given : $f_m = 1 \text{ kHz}$, $\delta = 15 \text{ kHz}$

To find : Bandwidth required.

Method I :

$$\begin{aligned} \text{Bandwidth} &= 2 f_m \times \text{Number of significant sidebands} \\ &= 2 \times 1 \times 5 = 10 \text{ kHz} \end{aligned} \quad \dots \text{Ans.}$$

Method II (Carson's rule) :

$$\text{Bandwidth} = 2 [\delta + f_m] = 2 [15 + 1] = 32 \text{ kHz} \quad \dots \text{Ans.}$$

1.19 Phase Modulation (PM) : SPPU : May 13

University Questions

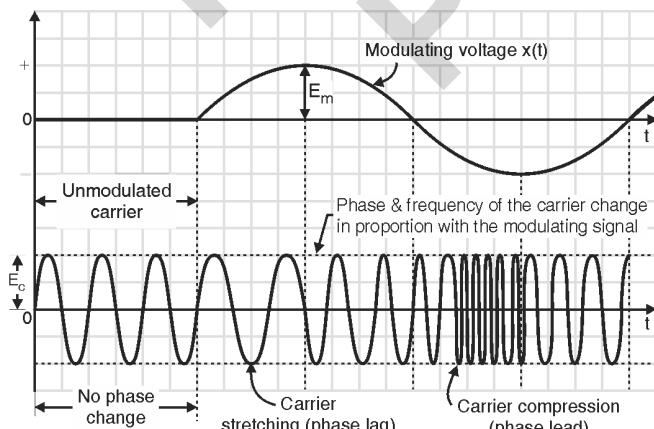
Q. 1 Explain phase modulation. (May 13, 4 Marks)

Definition :

- PM is a system of modulation in which the instantaneous phase of the carrier is continuously varied in proportion with the instantaneous amplitude of the modulating signal.
- Phase modulation is very similar to the frequency modulation.
- The only difference is that the phase of the carrier is varied instead of varying the frequency. The amplitude of the carrier remains constant.

Waveforms :

- Fig. 1.19.1 shows the waveforms for phase modulation.
- As shown in Fig. 1.19.1, as the modulating signal goes positive, the amount of phase lag increases with the amplitude of the modulating signal.



(L-45) Fig. 1.19.1 : Waveforms of PM wave

- The effect of this is that the carrier signal is stretched or its frequency is reduced.

- When the modulating signal goes negative, the phase shift becomes leading.
- This causes the carrier wave to be effectively compressed. The effect of this is as if the carrier frequency is increased.
- Thus phase modulation is always associated with frequency modulation and vice versa.

Mathematical representation of PM :

- The phase modulation is another type of angle modulation. PM and FM are closely related.
- The PM wave is obtained by varying the phase angle ϕ of a carrier in proportion with the amplitude of the modulating voltage.
- If the carrier voltage is expressed as,

$$e_c = A \sin (\omega_c t + \phi) \quad \dots (1.19.1)$$

- Then the PM wave can be expressed as,

$$e_{PM} = A \sin (\omega_c t + \phi_m \sin \omega_m t) \quad \dots (1.19.2)$$

- Here ϕ_m = Maximum phase change corresponding to the maximum amplitude of the modulating signal.
- For the sake of uniformity let us modify the Equation (1.19.2) as,

$$e_{PM} = A \sin [\omega_c t + m_p \sin \omega_m t] \quad \dots (1.19.3)$$

Where $m_p = \phi_m$ = Modulation index of PM.

- The FM and PM waves look identical when their modulation index are identical. However if we change the modulating frequency f_m then m_f will change but there is no change in the value of m_p .

1.19.1 Bandwidth of PM :

- The formula for bandwidth of PM is same as that for FM. But the actual bandwidth of PM is less than that for FM.
- The bandwidth of a PM signal can be calculated from the maximum modulating frequency and the maximum amplitude of the modulating signal.

1.19.2 Comparison of AM, FM and PM :

SPPU : May 10, Dec. 11

University Questions

Q. 1 Explain with diagram amplitude modulation and frequency modulation and compare them. (May 10, 8 Marks)

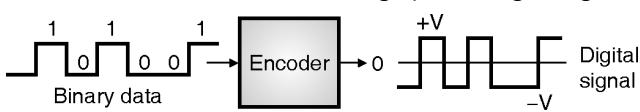
Q. 2 Compare AM, FM and PM. (Dec. 11, 4 Marks)



Sr. No.	Parameter	AM	FM	PM
1.	Variable parameter of the carrier	Amplitude	Frequency	Phase
2.	Mathematical equation		$s(t) = E_c \sin [\omega_c t + m_p \sin \omega_m t]$	$s(t) = E_c \sin [\omega_c t + m_p \sin \omega_m t]$
3.	Variable parameter proportional to modulating voltage	Peak signal amplitude	Frequency deviation	Phase deviation
4.	Amplitude of modulated signal	Varies continuously	Constant	Constant
5.	Bandwidth	Constant $2 f_m$	$2 [\delta + f_m]$	-
6.	Noise immunity	Very poor	Best of all schemes	Better than AM, worse than FM
7.	Transmission and reception equipments	Simple	Complex	Complex
8.	The information is contained in	Amplitude variation	Frequency variation	Phase deviation
9.	Usefulness of transmitted power	Carrier power and one S.B. power are not useful.	All the power is useful.	All the power is useful.
10.	Usage	Widely used.	Widely used.	Limited use.
11.	Applications	Radio and TV broadcasting	Radio, TV, police wireless, point to point communication.	Data communications.

1.20 Digital to Digital Conversion :

- In this type of encoding, the digital data which is normally binary in nature is converted into a sequence of discrete, discontinuous voltage pulses (digital signal).



(L-254) Fig. 1.20.1 : Digital to digital conversion

- The digital data at the input of the encoder may not be suitable for transmission over a longer distance.
- Hence it is converted into the digital signal which is more suitable for long distance communication.
- The digital signals at the output of the encoder are known as the **line codes**.

Definition of Line Coding :

- The line coding is defined as the process of converting binary data, a sequence of bits to a digital signal.
- The digital data such as text, numbers, graphical images, audio and video are stored in computer memory in the form of sequences of bits.
- Line coding converts these sequences into digital signals as shown in Fig. 1.20.2.



(L-255) Fig. 1.20.2 : Line coding

1.20.1 Classification of Line Codes :

SPPU : May 10, May 14, May 15, May 19

University Questions

- Q. 1** List the line coding schemes in digital transmission. Explain polar NRZ scheme. **(May 10, May 15, 4 Marks)**
- Q. 2** List the line coding schemes in digital transmission. Explain polar NRZ and unipolar NRZ schemes. **(May 14, May 19, 6 Marks)**

- The line codes are basically divided into the following three categories :
 - Unipolar codes
 - Polar codes
 - Bipolar codes

1. Unipolar codes :

- Unipolar codes use only one voltage level other than zero. So the encoded signal will have either + A volts value or 0.
- These codes are very simple and primitive and are not used now a days.

2. Polar codes :

- Polar coding using two voltage levels other than zero such as + A/2 and - A/2 volts.



- This will bring the dc level for some codes to zero which is a desired characteristics.

3. Bipolar codes :

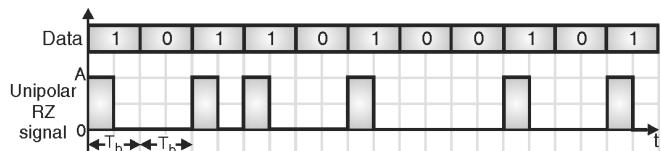
- Bipolar coding uses three voltage levels positive, negative and zero which is similar to polar codes.
- But here the zero level is always used for representing the "0" in the data stream at the input.

1.20.2 Properties of Line Codes :

- Following are some of the important properties of line codes :
- 1. All the cable systems and other communication systems, do not allow transmission of a dc signal. Therefore the line signal must have a zero average (dc) value. NRZ bipolar formats usually satisfy this requirement. For this reason, long strings of element sequences having same polarity should not be transmitted.
- 2. As the code adds redundancy, the code efficiency should be as high as possible.
- 3. To ensure synchronization at the receiver, the line signal should undergo a sufficient number of zero crossings that means the transmitted signal should always undergo transitions.
- 4. The crosstalk between channels should be minimized. To do so the amount of energy in the signal at low frequencies should be small.

1.20.3 Unipolar RZ Format :

- The return to zero (RZ) unipolar format is as shown in Fig. 1.20.3.



(L-262) Fig. 1.20.3 : Unipolar RZ format

- In this format each "0" is represented by an off pulse (0) and each "1" by an on pulse with amplitude A and a duration of $T_b/2$, followed by a return to zero level.
- Therefore this is called as return to zero (RZ) format. As the voltage level is either + A or zero, this is a unipolar format. (Unipolar means only one polarity).

- Due to the unipolar nature, the unipolar RZ format has a nonzero dc value. The dc value does not contain any information.

1.20.4 Unipolar NRZ Format :

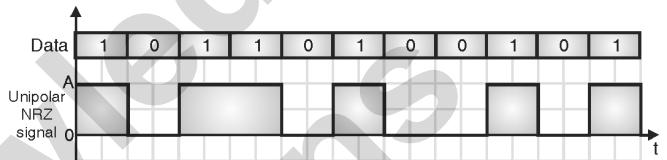
SPPU : May 14, May 19

University Questions

- Q. 1** List the line coding schemes in digital transmission. Explain polar NRZ and unipolar NRZ schemes

(May 14, May 19, 6 Marks)

- A non-return to zero (NRZ) format is as shown in Fig. 1.20.4.

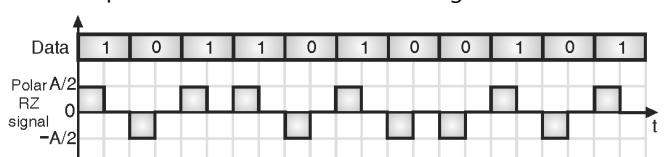


(L-263) Fig. 1.20.4 : Unipolar NRZ format

- In this format a logic "1" is represented by a pulse of full bit duration T_b and amplitude + A while a logic "0" is represented by an off pulse or zero amplitude.
- During the on time, the pulse does not return to zero after half bit period. Therefore the name NRZ format.
- As the pulses have either + A or 0 amplitude it is called as a unipolar format.
- Internal computer waveforms are usually of this type. Due to the unipolar nature, the unipolar NRZ format also will have a nonzero average (dc) value which does not carry any information.
- Due to longer pulse duration, the NRZ pulses carry more "energy" than the RZ pulses.
- But they need synchronization at the receiver as there is no separation between the adjacent pulses.

1.20.5 Polar RZ Format :

- The disadvantage of the two unipolar formats discussed earlier is that they result in a dc component that does not carry any information and wastes power.
- The polar RZ format is as shown in Fig. 1.20.5.



(L-264) Fig. 1.20.5 : Polar RZ format



- It shows that opposite polarity pulses of amplitude $\pm A/2$ are used to represent logic "1" and "0".
- Therefore it is called as a "polar" format. As the pulses return to zero after half the bit duration " $T_b/2$ " this format is a RZ format.

1.20.6 Polar NRZ Format :

SPPU : May 10, May 14, May 15, May 19

University Questions

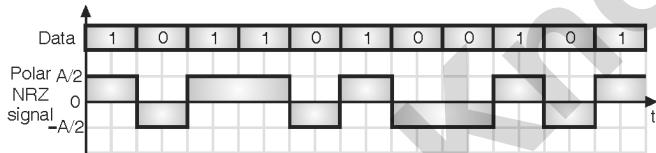
Q. 1 List the Line coding schemes in Digital transmission. Explain polar NRZ scheme.

(May 10, May 15, 4 Marks)

Q. 2 List the line coding schemes in digital transmission. Explain polar NRZ and unipolar NRZ schemes.

(May 14, May 19, 6 Marks)

- In the polar NRZ format, as shown in Fig. 1.20.6 a pulse of amplitude "+ A/2" of duration T_b is used to represent a logic "1" and a pulse of amplitude "- A/2" of the same duration represents a logic "0".

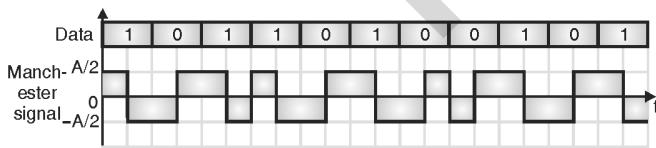


(L-265) Fig. 1.20.6 : Polar NRZ format

- Unlike the unipolar waveform, a polar waveform has no dc component if the 0s and 1s in the input data occur in equal proportion.

1.20.7 Split Phase Manchester Format :

- The split phase Manchester format is as shown in Fig. 1.20.7.



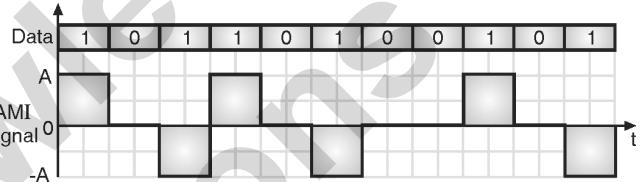
(L-266) Fig. 1.20.7 : Split phase Manchester format

- In this format, symbol "1" is represented by transmitting a positive pulse of "+ A/2" amplitude for one half of the symbol duration, followed by a negative pulse of amplitude "- A/2" for remaining half of the symbol duration.
- For symbol "0" these two pulses are transmitted in reverse order.
- This waveform does not have any dc component.

- The Manchester format has a built in synchronization capability as it crosses zero at regular intervals.
- But this capability is attained at the expense of a bandwidth requirement of twice that of the NRZ unipolar, polar and bipolar formats.
- Local Area Networks (LAN) such as Ethernet and CheaperNet are increasingly using the Manchester code for signal transmission over the network.

1.20.8 Bipolar NRZ Format (AMI) :

- The bipolar NRZ format is as shown in Fig. 1.20.8. Here the successive "1s" are represented by pulses with alternating polarity, and no pulse is transmitted for a logic "0".

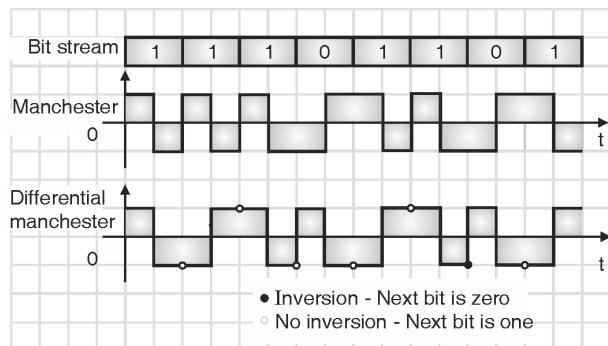


(L-268) Fig. 1.20.8 : Bipolar NRZ format (AMI)

- Note that in this representation there are three levels : + A, 0 and - A.
- Therefore this is also known as "pseudoternary or Alternative Mark Inversion (AMI)" format.
- An attractive feature of the bipolar format is the absence of a dc component even though the input binary data may contain long strings of "0s" and "1s".
- Moreover the bipolar format eliminates ambiguity that may arise because of polarity inversion during the course of transmissions.

Ex. 1.20.1 : Show the Manchester and differential Manchester encoding pattern for the bit stream 11101101.

Soln. :

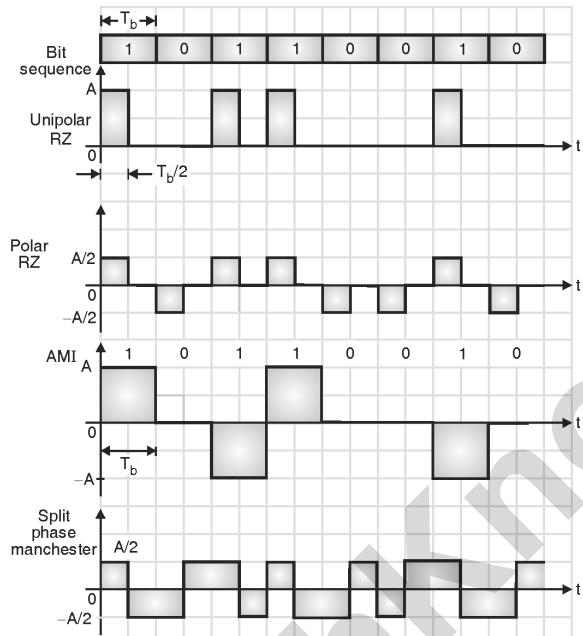


(L-287) Fig. P. 1.20.1

- Ex. 1.20.2 :** Consider that the bit sequence given below is to be transmitted. Bit sequence = 10110010. Draw the resulting waveform if the sequence is transmitted using :
1. Unipolar RZ
 2. Polar RZ
 3. AMI
 4. Split Phase Manchester

Soln. :

The required waveforms are as shown in Fig. P. 1.20.2.

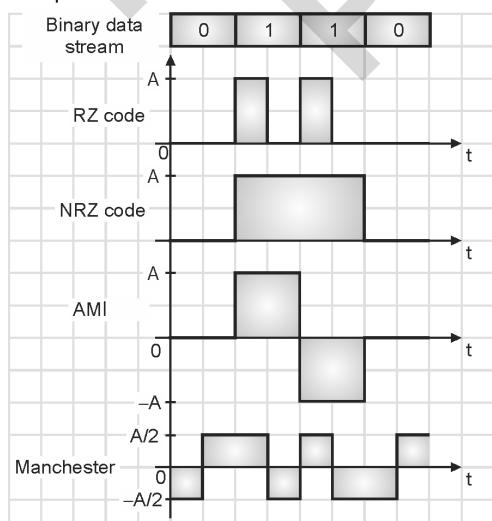


(L-279) Fig. P. 1.20.2

- Ex. 1.20.3 :** List popular line codes alongwith their waveforms for digital code word 0110.

Soln. :

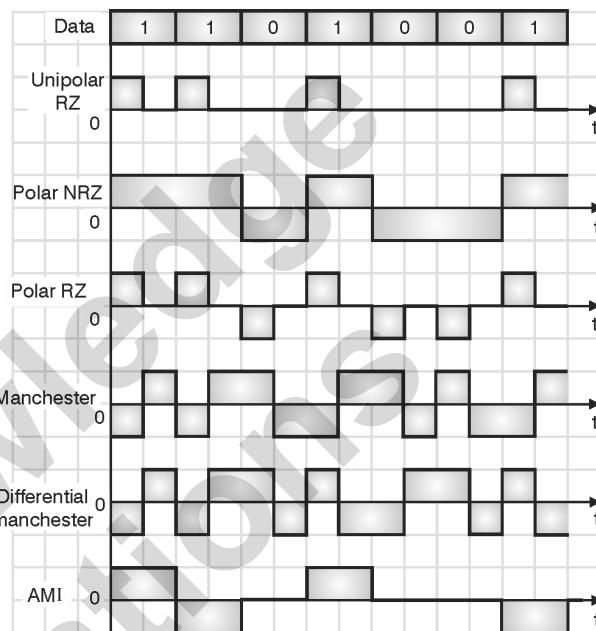
- Refer section 1.20 for the codes.
- The required waveforms are as follows.



(E-1183) Fig. 1.20.3

- Ex. 1.20.4 :** Draw unipolar RZ, polar NRZ, polar RZ, Manchester, differential Manchester and AMI waveforms of line codes for data stream : 1101001.

Soln. :



(E-1856) Fig. P. 1.20.4

1.21 Bandwidth Utilization :

- Bandwidth is a very important characteristics of a network, which can be used for measuring the network performance.
- Bandwidth can have two different values :
 1. BW in hertz and 2. BW in bits per second.

BW in Hz :

- It is the range of frequencies present in a composite signal. It can also be defined as a range of frequencies that a channel can pass through without much attenuation.

BW in bits per second :

- We can also define bandwidth as the number of bits per second (bps) that a channel or network can transmit.
- For example the BW of Fast Ethernet is 100 Mbps i.e. that network can transmit 100 Mbps.

Relationship :

- There is a clear relationship between the bandwidth in Hz and BW in bps. With increase in BW in Hz, there is an increase in bps bandwidth.



- The relation between them depends on whether baseband transmission is being used or transmission with modulation is being used.

1.21.1 Signal and Channel Bandwidths :

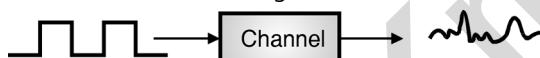
- We can define two different bandwidths :
 - Signal bandwidth
 - Channel bandwidth

Signal bandwidth :

- Signal bandwidth B_s is defined as the range of frequencies contained in the signal.

Channel bandwidth :

- Whereas the bandwidth of a channel B_c is the range of frequencies that is passed by a channel.
- If the bandwidth of the input signal is larger than the channel bandwidth, then the output of the channel will not contain all the frequencies of the input signal.
- Fig. 1.21.1 shows a typical digital signal at the input and the output is of different shape than input, if the channel BW is less than signal BW.



(G-698) Fig. 1.21.1 : Effect of $B_c < B_s$

- If the signaling rate of input signal is increased, then the channel bandwidth has to be increased so as to pass the signal without any change in shape of the signal.
 - The maximum rate at which pulses can be transmitted through the channel is given by,
- $$r_{\max} = 2W \text{ pulses/sec.}$$
- where, $W = 1/2\tau$ and τ = Smallest pulse width of input signal.
- The bandwidth is also important in deciding the channel capacity C of a transmission system.

1.22 Some Important Definitions :

1.22.1 Channel Capacity :

SPPU : May 05, Dec. 05, May 06, Dec. 07

University Questions

- Q. 1** What is channel capacity ? How is it related to channel bandwidth ? Explain with an appropriate formula. (May 05, Dec. 05, Dec. 07, 4 Marks)
- Q. 2** What do you understand by signal to noise (S/N) ratio ? Explain Shannon's channel capacity. (May 06, 4 Marks)

Definition :

- The **channel capacity C** of a transmission system is the maximum rate at which bits can be transferred reliably.
- The relation between C and channel bandwidth B_c is given by,

$$C = B_c \log_2 \left(1 + \frac{S}{N} \right) \text{ bits/sec.} \quad \dots(1.22.1)$$

- The channel capacity should be as high as possible and to increase C , we have to increase the channel bandwidth B_c .

1.22.2 Error Rate :

It is defined as the rate at which errors occur in the received (or detected) signal.

1.22.3 Signal to Noise Ratio :

SPPU : May 05, Dec. 05, May 06, Dec. 07

University Questions

- Q. 1** What is channel capacity ? How is it related to channel bandwidth ? Explain with an appropriate formula. (May 05, Dec. 05, Dec. 07, 4 Marks)
- Q. 2** What do you understand by signal to noise (S/N) ratio ? Explain Shannon's channel capacity. (May 06, 4 Marks)

Definition :

- The signal to noise ratio (SNR) is defined as :

$$\text{SNR} = \frac{\text{Average Signal Power}}{\text{Average Noise Power}}$$

- SNR can be used to find the theoretical bit rate limit of a given communication medium. SNR is the ratio of the desired portion (signal) and the undesired portion (noise) in the transmitted or received waveform.
- Its value should be as high as possible.
- SNR is a ratio of two powers. So it is often defined in decibels (dB).

$$[\text{SNR}]_{\text{dB}} = 10 \log_{10} \text{SNR}$$

- Ex. 1.22.1 :** The power of a signal is 10 mW and the power of the noise is 1 μ W. What are the values of SNR and SNR_{dB} ?

Dec. 17, 6 Marks

Soln. :

Given : Signal power = 10 mW, Noise power = 1 μ W

To find : SNR and SNR in dB



$$\begin{aligned} \text{SNR} &= \frac{\text{Average signal power}}{\text{Average noise power}} = \frac{10 \times 10^{-3}}{1 \times 10^{-6}} \\ &= 10000 \quad \dots \text{Ans.} \\ [\text{SNR}]_{\text{dB}} &= 10 \log_{10} \text{SNR} = 10 \log_{10} [10000] \\ &= 40 \text{ dB} \quad \dots \text{Ans.} \end{aligned}$$

1.23 Data Rate Limits :**SPPU : Dec. 07****University Questions**

- Q. 1** Explain the three factors on which achievable data rate limits are dependent with appropriate formulas. **(Dec. 07, 6 Marks)**

Definition :

- Data rate of a communication system is defined as the amount of data that it transmits per second. The unit of data rate is bits/ sec.
- In data communication a large data is required to be transferred from one place to the other.
- It is necessary to transfer it as quickly as possible. In other words the data rate in bits per second over a channel should be as high as possible.

Factors determining the data rate :

- The data rate is decided by the following factors :
 1. The maximum bandwidth.
 2. The signal level.
 3. The noise presented by the channel.
- Two theorems were developed to calculate the data rate and we can use them on the basis of the type of channel as follows :
 1. A noiseless channel : Nyquist theorem
 2. A noisy channel : Shannon's theorem

1.24 Introduction to Multiplexing :**SPPU : May 05, Dec. 11, Dec. 12, May 13****University Questions**

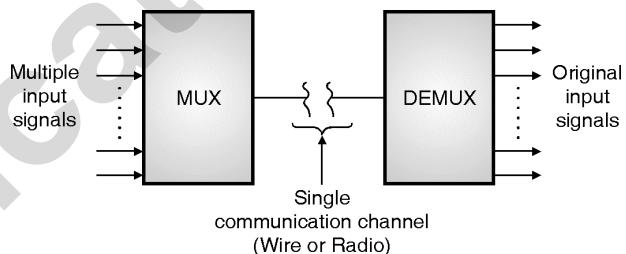
- Q. 1** What is multiplexing ? What are its types in the context of communication ? Write two applications of each type. **(May 05, 4 Marks)**
- Q. 2** Explain the concept of multiplexing. Explain TDM, FDM and WDM. **(Dec. 11, May 13, 8 Marks)**
- Q. 3** Define multiplexing and de-multiplexing. Explain frequency division multiplexing and wavelength-division multiplexing. **(Dec. 12, 8 Marks)**

Definition :

- Multiplexing is the process of simultaneously transmitting two or more individual signals over a single communication channel.
- Due to multiplexing it is possible to increase the number of communication channels so that more information can be transmitted.
- The typical applications of multiplexing are in telemetry and telephony or in the satellite communication.

Multiplexer :

- A multiplexer is an electronic circuit that performs multiplexing of the signals applied at its input to produce one combined signal.
- The concept of a simple multiplexer is illustrated in Fig. 1.24.1.
- The multiplexer receives a large number of different input signals.
- It has only one output which is connected to the single communication channel.

**(L-105) Fig. 1.24.1 : Concept of multiplexing**

- Sometimes the composite signal is used for modulating a carrier before transmission.

Demultiplexing :

- Demultiplexing is defined as the process of separating out the signals from a multiplexed signal.

De-multiplexer :

- A de-multiplexer is an electronic circuit that performs demultiplexing of the multiplexed signals applied at its input to separate out the individual signals..
- The concept of a simple demultiplexer is illustrated in Fig. 1.24.1.

Demultiplexer :

- A demultiplexer is an electronic circuit that performs demultiplexing of the signal applied at its input to separate out the individual signals.



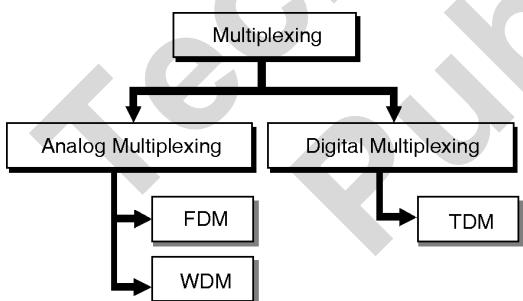
- At the receiving end, of communication link, a demultiplexer is used to separate out the signals into their original form.
- The operation of demultiplexer is exactly opposite to that of a multiplexer..

1.24.1 Types of Multiplexing : SPPU : May 05

University Questions

Q. 1 What is multiplexing ? What are its types in the context of communication ? Write two applications of each type. (May 05, 4 Marks)

- There are three basic types of multiplexing. They are :
 - Frequency division multiplexing (FDM)
 - Time division multiplexing (TDM).
 - Wavelength division multiplexing (WDM).
- The multiplexing techniques can be broadly classified into two categories namely analog and digital.
- Analog multiplexing can be either FDM or WDM and digital multiplexing is TDM.
- Fig. 1.24.2 shows the classification of multiplexing techniques.



(L-106) Fig. 1.24.2 : Classification of multiplexing techniques

- Generally the FDM and WDM systems are used to deal with the analog information whereas the TDM systems are used to handle the digital information.
- In FDM many signals are transmitted simultaneously where each signal occupies a different frequency slot within a common bandwidth.
- In TDM the signals are not transmitted at a time, instead they are transmitted in different time slots.

1.25 Frequency Division Multiplexing (FDM) :

SPPU : May 12, Dec. 12, May 13, May 15, May 16, May 17, Dec. 19

University Questions

Q. 1 Explain FDM and statistical TDM. (May 12, 8 Marks)

Q. 2 Define multiplexing and de-multiplexing. Explain frequency division multiplexing and wavelength-division multiplexing. (Dec. 12, 8 Marks)

Q. 3 Explain the concept of multiplexing. Explain TDM, FDM and WDM. (May 13, 8 Marks)

Q. 4 Draw and explain FDM and TDM. (May 15, 6 Marks)

Q. 5 Explain FDM and TDM multiplexing techniques. (May 16, 6 Marks)

Q. 6 Explain FDM and statistical TDM. (May 17, 6 Marks)

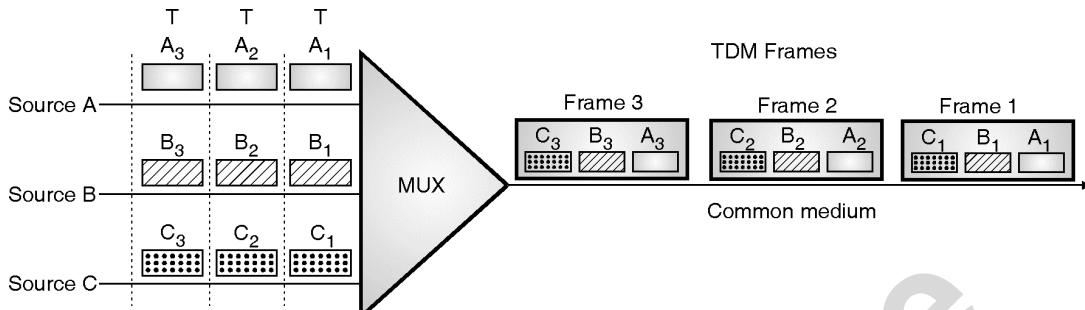
Q. 7 Explain FDM and TDM multiplexing with their advantages and disadvantages. (Dec. 19, 6 Marks)

Definition :

- FDM is a type of multiplexing in which all the signals or channels to be multiplexed are transmitted at the same time with each channel occupying a distinct non overlapping frequency band.
- The operation of FDM is based on sharing the available bandwidth of a communication channel among the signals to be transmitted.
- That means many signals are transmitted simultaneously with each signal occupying a different frequency slot within the total available bandwidth.
- Each signal to be transmitted modulates a different carrier. The modulation can be AM, SSB, FM or PM.
- The modulated signals are then added together to form a composite signal which is transmitted over a single channel.

Spectrum of FDM :

- The spectrum of composite FDM signal is shown in Fig. 1.25.1.

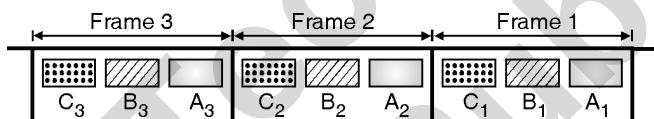


(L-123) Fig. 1.26.2 : TDM system

- As shown in the Fig. 1.26.1 one transmission of each channel completes one cycle of operation called as a "Frame".
- The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
- The concept of TDM will be more clear if you refer to Fig. 1.26.2.
- The data flow of each source (A, B or C) is divided into units (say A₁, A₂ or B₁, C₁ etc.)
- Then one unit from each source is taken and combined to form one frame. The size of each unit such as A₁, B₁ etc. can be 1 bit or several bits.

A TDM Frame :

- Fig. 1.26.3 shows the frames of TDM signal.



(L-124) Fig. 1.26.3 : TDM frames

- For 3 inputs being multiplexed, a frame of TDM will consist of 3 units i.e. one unit from each source.
- Similarly for n number of inputs, each TDM frame will consist of n units.
- The TDM signal in the form of frames is transmitted on the common communication medium.

Data rate :

- For a TDM, the data rate of the multiplexed signal is always n times the data rate of individual sources, where n is the number of sources.
- So if three sources are being multiplexed, then the data rate of the TDM signal is three times higher than the individual data rate.

- Naturally the duration of every unit (A₁ or B₁ etc.) in TDM signal is n times shorter than the unit duration before multiplexing.

1.26.1 Advantages of TDM :

SPPU : Dec. 10, Dec. 19

University Questions

- Q. 1** Explain in detail TDM and statistical TDM. Mention advantages and disadvantages.
(Dec. 10, 8 Marks)
- Q. 2** Explain FDM and TDM multiplexing with their advantages and disadvantages.
(Dec. 19, 6 Marks)

- Full available channel bandwidth can be utilized for each channel.
- Intermodulation distortion is absent.
- TDM circuitry is not very complex.
- The problem of crosstalk is not severe.

1.26.2 Disadvantages of TDM :

SPPU : Dec. 10, Dec. 19

University Questions

- Q. 1** Explain in detail TDM and statistical TDM. Mention advantages and disadvantages.
(Dec. 10, 8 Marks)
- Q. 2** Explain FDM and TDM multiplexing with their advantages and disadvantages.
(Dec. 19, 6 Marks)

- Synchronization is essential for proper operation.
- Due to slow narrowband fading, all the TDM channels may get wiped out.

1.26.3 Applications of TDM :

SPPU : May 05

University Questions

- Q. 1** What is multiplexing ? What are its types in the context of communication ? Write two applications of each type.
(May 05, 4 Marks)



1. Multiplexing of digital signals.
2. Digital telephony.
3. Satellite communications.
4. Fiber optic communication.
5. Wireless communication applications.

1.27 Statistical (Asynchronous) TDM :

SPPU : May 09, Dec. 10, May 11, May 12, Dec. 17

University Questions

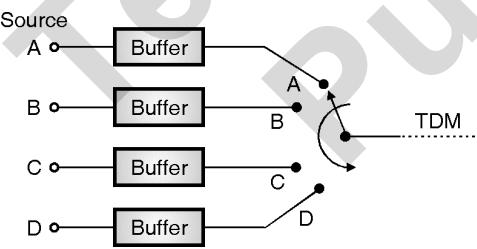
- Q. 1** Explain FDM and statistical TDM.
(May 09, May 11, May 12, 8 Marks)
- Q. 2** Explain in detail TDM and statistical TDM. Mention advantages and disadvantages.
(Dec. 10, 8 Marks)
- Q. 3** Explain Statistical TDM and Synchronous TDM techniques.
(Dec. 17, 6 Marks)

Concept :

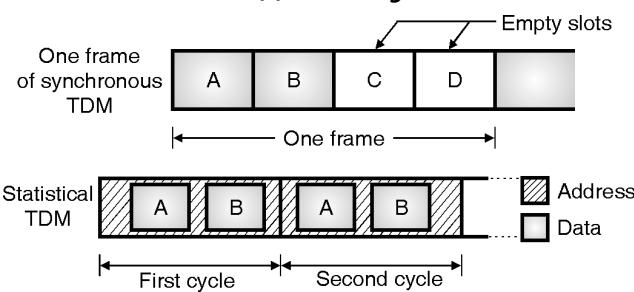
- The TDM system that we have discussed earlier is known as the synchronous TDM. This system has a major drawback.
- In synchronous TDM, many of the time slots in a frame are wasted due to absence of data on some of the time slots.
- Therefore an alternative system called as statistical TDM or asynchronous TDM or intelligent TDM is used.

Block diagram :

- The block diagram of the statistical TDM system is as shown in Fig. 1.27.1(a) and its frame format is as shown in Fig. 1.27.1(b).



(L-138)(a) Block diagram



(b) Frame format

(L-139) Fig. 1.27.1 : Statistical TDM

Operating principle :

- In statistical TDM, the time slots are not permanently assigned to all the available users (like synchronous TDM).
- Instead, the time slots are allocated dynamically on demand only to those channels holding data for transfer.
- Each TDM channel is called as an I/O line.
- Thus the statistical TDM has many I/O lines and one high speed multiplexed line.
- Each I/O line has a buffer associated with it. As shown in Fig. 1.27.1, there are N number of I/O lines.
- Out of these only K channels are transmitted which hold data for transfer.
- The remaining (N - K) channels are not considered for transmission.
- In statistical TDM, the multiplexer will "scan" the input buffers of all the channels, sequentially.
- During the scan time, it collects the data until a frame is filled. As soon as a frame is filled, it is transmitted.
- The data is transferred on the transmission medium. The received frame is then distributed among the output buffers by the output multiplexer.

1.27.1 Data Rate of Statistical TDM :

- In statistical TDM system, all the channels are not transmitted in every frame.
- Hence the data rate on the multiplexed line will be less than the sum of the data rates of all the sources.
- Thus a statistical multiplexer can use a transmission medium of lower data rate to support the same number of sources as the synchronous multiplexer.
- That means if we have a synchronous and statistical TDM with equal data rates, then the statistical TDM will support more number of sources.

1.27.2 Slot Size :

- The slot carries both data and address, the ratio of the data size to address size should be reasonable to ensure high efficiency.



- In statistical TDM, the data block contains many bits while address bits are very few.

No Synchronization Bit :

- The statistical TDM frames need not be synchronized. So it is not necessary to use the synchronizing bit.

1.27.3 Bandwidth :

- In statistical TDM, the capacity of multiplexed link is generally less than the sum of capacities of individual channels.
- Therefore the bandwidth requirement of the multiplexed link is less than that for the synchronous TDM.

1.27.4 Comparison of FDM, Synchronous TDM and Statistical TDM : SPPU : May 13

University Questions

Q. 1 Compare FDM and TDM. (May 13, 8 Marks)

Table 1.27.1 : Comparison of data multiplexer techniques

Sr. No.	Parameter	FDM	Synchronous TDM	Statistical TDM
1.	Line utilization efficiency	Poor	Good	Very good
2.	Flexibility	Poor	Good	Very good
3.	Channel capacity	Poor	Good	Excellent
4.	Error control	Not possible	Not possible	Possible
5.	Multidrop capacity	Very good	Difficult to achieve	Possible
6.	Transmission delay	Does not exist	Low	Random
7.	Cost	High	Low	Moderate

1.28 Wavelength Division Multiplexing (WDM) : SPPU : Dec. 11, Dec. 12, May 13

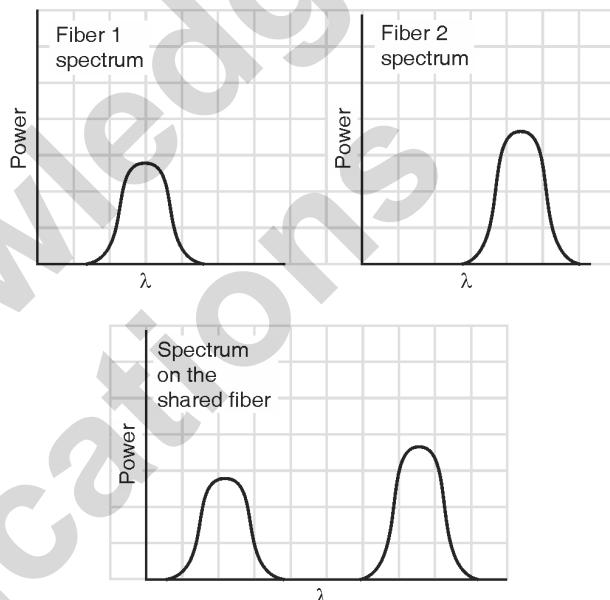
University Questions

Q. 1 Explain the concept of multiplexing. Explain TDM, FDM and WDM. (Dec. 11, May 13, 8 Marks)

Q. 2 Define multiplexing and de-multiplexing. Explain frequency division multiplexing and wavelength-division multiplexing. (Dec. 12, 8 Marks)

Concept :

- WDM is the variation of FDM. It is especially used for fiber optic channels.
- As shown in Figs. 1.28.1(a) and (b), 2 fibres come together at a prism, each having energy in a different frequency band.

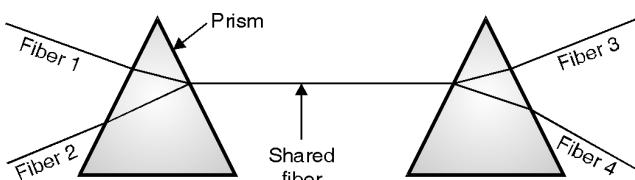


(L-119) Fig. 1.28.1(a)

- After passing through the prism, beams are combined onto a single shared fiber, for transmission to a distant destination, where they are split again.
- Channels having different frequency ranges can be multiplexed on a single long fiber.
- The only difference between WDM and electrical FDM is that an optical system is completely passive and thus highly reliable.
- Reason WDM is popular, is that the energy on a single fiber is a few gigahertz wide because it is impossible to convert between electrical and optical media any faster.
- Since BW of a single fiber band is about 25,000 GHz, there is great potential for multiplexing many optical channels together over long routes. Necessary condition is that incoming channels use different frequency bands.
- Potential application of WDM is in the FTTC (Fiber To The Curb) systems or in SONET networks.

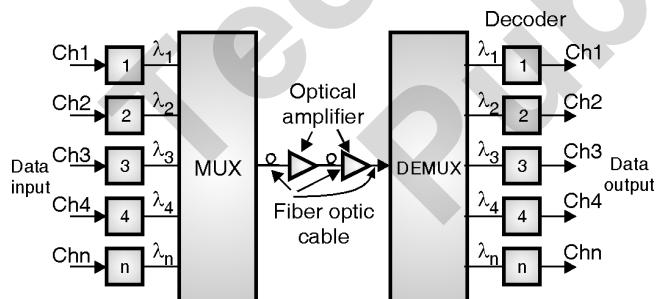


- In the Fig. 1.28.1(b) we have a fixed wavelength system bits from fiber 1 go to fiber 3 and bits from fiber 2 go to fiber 4.



(L-120) Fig. 1.28.1(b)

- It is not possible to have bits going from fiber 1 to fiber 4.
- It is also possible to build WDM systems that are switched, which contain many input and output fibers, switching data among themselves.
- Although spreading energy over n outputs dilutes it by a factor n , such systems are practical for hundred of channels.
- If light from one of the incoming fibers have to go to any output fiber, all the output fibers need tunnable filters.
- Alternatively, input fibers could be tunnable and output ones fixed. Having both to be tunnable is unnecessary expense.
- A simple block diagram of WDM transmitter and receiver system with different channels is as shown in Fig. 1.28.1(c).



(L-121) Fig. 1.28.1(c) : WDM system

1.28.1 Application of WDM : SPPU : May 05

University Questions

Q. 1 What is multiplexing ? What are its types in the context of communication ? Write two applications of each type. (May 05, 4 Marks)

- One important application of WDM is the SONET network in which a large number of optical fiber lines are multiplexed and demultiplexed.

1.29 A Network :

Network :

- Network is a broad term similar to "system". Network is a communication system which supports many users.
- The interconnection of one station to many stations is called as networking.
- A network is any interconnection of two or more stations that wish to communicate.

1.29.1 Network Topologies :

SPPU : May 07

University Questions

Q. 1 What is the significance of using various networking topologies ? Justify your answer with suitable examples. (May 07, 8 Marks)

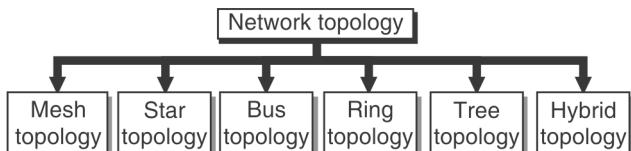
- It is possible to connect the computer in many different ways in a network.
- The way of connecting the computers is called as the topology.
- So depending on the manner of connecting the computers we can have different network topologies.

Definition :

- Topology is defined as the logical arrangement of the nodes (computers).
- The word physical network topology is used to explain the manner in which a network is connected.
- Devices or nodes in a network get connected to each other via communication links and all these links are related to each other in one way or the other.
- The geometric representation of such a relationship of links and nodes is known as the topology of that network.

Types :

- The six basic network topologies are as shown in Fig. 1.29.1.



(G-14(b)) Fig. 1.29.1 : Classification of network topology

- These topologies can be classified into two types :
 1. Peer to peer
 2. Primary – secondary



- Peer to peer is the relationship where the devices share the link equally. The examples are ring and mesh topologies.
- In primary – secondary relationship, one device controls and the other devices have to transmit through it. For example star and tree topology.

1.29.2 Bus Topology :

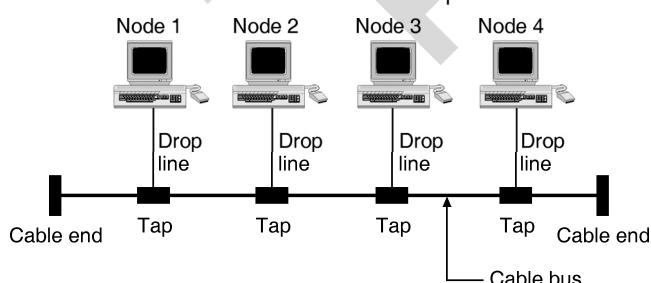
SPPU : May 07, May 09, May 19

University Questions

- Q. 1** Explain network topologies with neat diagrams :
Bus topology. **(May 07, 6 Marks)**
- Q. 2** Explain the merits and demerits of star, bus, ring and mesh topologies. **(May 09, 8 Marks)**
- Q. 3** Explain any three network topology with advantages and disadvantages. **(May 19, 6 Marks)**

Definition :

- The bus topology is a network topology in which nodes are directly connected to the common linear or branched half duplex link called as bus.
- The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 1.29.2.
- On a typical bus network a simple cable is used without additional electronics to amplify the signal or pass it along from computer to computer. Therefore bus is a **passive topology**.
- This long cable called bus is used as backbone to all the nodes. The tap is connector that connects the node to the metallic core of the bus via a drop line.



(G-15) Fig. 1.29.2 : Bus topology

Working :

- When one computer sends a signal on the cable; all the computers on the network receive the information.
- However only the one with the address that matches with the destination address stored in the message

accepts the information while all the others reject the message.

- The speed of the bus topology is **slow** because only one computer can send a message at a time.
- A computer must wait until the bus is free before it can transmit.
- The bus topology requires a proper termination at both the ends of the cable in order to avoid reflections.
- Since the bus is a passive topology, the electrical signal from a transmitting computer is free to travel over the entire length of the cable.
- Without termination when the signal reaches the end of the cable, it returns back and travels back on the cable.
- The transmitted waves and reflected waves, if they are in phase add and if they are out of phase cancel.
- Thus addition and cancellation of wave results in a standing wave.
- The standing waves can distort the normal signals which are travelling along the cable. This can be avoided by terminating the bus on both ends in 50Ω load.
- The terminators absorb the electrical energy and avoid reflections.
- As the signal travels across the bus, some of the energy is converted into heat. This will weaken the signal. This will limit the number of taps and the distance between them.
- Hence the bus topology cannot be used for very large networks that contain a number of computers.
- The bus topology is easy to install and uses less cable than the mesh, star or tree topology.
- Addition of a new node to the bus topology is difficult because this will change the number of taps and average distance between them.
- The number of taps and the distance between them is optimized so it is not supposed to be changed. Thus Bus topology is inflexible.
- It is very difficult to isolate a fault or faulty node. One more drawback is that even if a part of bus breaks down, the whole bus stops functioning.

Performance of Bus Topology :

- Adding more computers in bus topology affects performance of the network because :



- With increase in number of computers, the waiting time for each computer increases which makes the network traffic slow.
- The number of packet collisions increases which results in high amount of packet loss.

When to Use the Bus Topology ?

- The bus topology is preferred if :

 - The given network is small, simple or temporary.
 - Number of computers to be connected is small.
 - The cost involved are to be kept low.

Advantages of Bus Topology :

- The bus topology is easy to understand, install, and use for small networks.
- The cabling cost is less as the bus topology requires a small length of cable to connect the computers.
- The bus topology is easy to expand by joining two cables with a BNC barrel connector.
- In the expansion of a bus topology repeaters can be used to boost the signal and increase the distance.

Disadvantages of Bus Topology :

- Heavy network traffic slows down the bus speed. In bus topology only one computer can transmit and others have to wait till their turn comes and there is no coordination between computers for reservation of transmitting time slot.
- The BNC connectors used for expansion of the bus attenuates the signal considerably.
- A cable break or loose BNC connector will cause reflections and bring down the whole network causing all network activity to stop.

Note : A bus network behaves erratically if it is not terminated or improperly terminated.

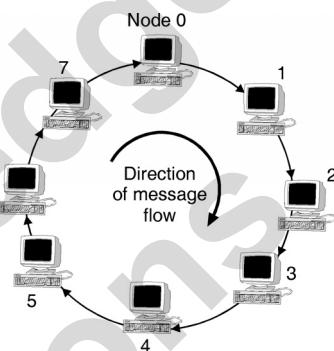
1.29.3 Ring Topology : SPPU : May 09, May 19

University Questions

- Q. 1** Explain the merits and demerits of star, bus, ring and mesh topologies. (May 09, 8 Marks)
- Q. 2** Explain any three network topology with advantages and disadvantages. (May 19, 6 Marks)

Definition :

- A ring topology is a network topology in which each node connects exactly to two other nodes, to form a single closed pathway for signal through each node.
- Data travels from node to node with each node having an access to every packet.
- In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 1.29.3.



(G-16) Fig. 1.29.3 : Ring topology

- Rings are used in high-performance networks where large bandwidth is necessary e.g. time sensitive features such as video and audio.
- Every computer is connected to the next computer in the ring and each retransmits what it receives from the previous computer hence the ring is an active network.
- The messages flow around the ring in one direction. There is no termination because there is no end to the ring.

Token passing :

- Some ring networks do **token passing**. A short message called a **token** is passed around the ring until a computer wishes to send information to another computer.
- That computer modifies the token, adds an electronic address and data and sends it around the ring.
- Each computer one by one receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin.
- The receiving computer returns a message to the sender to indicate that the message has been received.
- The sending computer then creates another token and places it on the network, so as to allow another computers to grab the token and begin their transmission.



- The token circulates until a station is ready to send and capture the token. Faster networks circulate several tokens at once.
- Some ring networks have two counter-rotating rings that help them recover from network faults.
- A ring is very easy to reconfigure and install and the signal keeps circulating over the ring all the time.
- A node which does not receive a signal for a long time indicates that it is faulty. This makes the fault detection easy.
- But if a node in a ring network fails, then the whole ring becomes inoperative. To overcome this problem, sometimes a ring topology with **dual rings** is used.
- Another disadvantage of ring is that the flow of information is only in one direction.
- So the ring topology is not used if a large number of nodes are to be connected in a network.

Active or passive ?

- Ring topology is an active topology, because each station has to recreate the packet.

Problems Faced in the Ring Topology :

1. If any link breaks or if any repeater fails then the entire network will be disabled.
2. To install a new repeater for supporting a new device, it is necessary to have the identification of two nearby, topologically adjacent repeaters.
3. It is necessary to take preventive measures to deal with the time jitter.
4. Due to the closed nature of the ring topology it is necessary to remove the circulating packets.

These problems except for the fourth one can be rectified by refinements of the ring topology.

Advantages of Ring Topology :

1. Every computer gets an equal access to the token.
2. There are no standing waves produced.
3. It is very easy to reconfigure and install.
4. Ring performs better than a bus under heavy network load.
5. Point to point configuration makes it easy to identify and isolate faults.

Disadvantages of Ring Topology :

1. Failure of one computer on the ring can affect the whole network.
2. It is difficult to trouble shoot the ring topology.
3. Adding or removing the computers in an existing ring is difficult. It disturbs the network.
4. Communication delay is directly proportional to the number of nodes, connected in the network
5. Bandwidth is shared on all links between devices.
6. Ring is more difficult to configure than star.

Note : Token ring networks are defined by the IEEE 802.5 standard. Fibre Distributed Data Interface (FDDI) is a fast fibre-optic network based on the ring topology.

1.29.4 Star Topology :

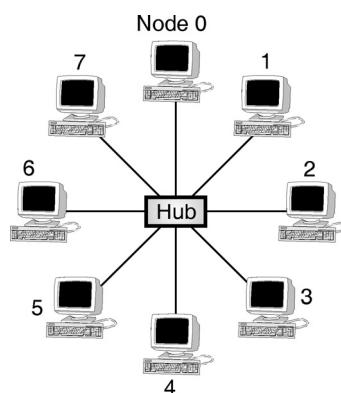
SPPU : May 07, May 19

University Questions

- Q. 1** Explain network topologies with neat diagrams : Star topology. **(May 07, 6 Marks)**
- Q. 2** Explain any three network topology with advantages and disadvantages. **(May 19, 6 Marks)**

Definition :

- Star topology is a network topology, in which each individual piece of a network is connected to a central node called as a hub or switch.
- In a star topology all the computers (nodes) are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 1.29.4.



(G-18)Fig. 1.29.4 : Star topology

- There is no direct connections among the computers. All the connections are made via the central hub.



- Stars are used in concentrated networks, where the endpoints are directly reachable from a central location; when network expansion is expected and when the greater reliability of a star topology is needed.
- The telephone system also uses the star topology.
- Each computer on a star network communicates with a central hub. The hub then resends the message either to all the computers in a broadcast star network.
- It will resend the message only to the destination computer in a switched star network.
- The hub in a broadcast star network can be active or passive.
- An active hub generates the electrical signal and sends it to all the computers connected to it.
- This type of hub is usually called a multiport repeater. Active hubs require external power supply.
- A passive hub is a wiring panel or punch down block which acts as a connection point. It does not amplify or regenerate the signal.
- Passive hubs do not require electrical power supply.
- Several types of cables can be used to implement a star network. A hybrid hub can use different types of cable in the same star network.

Expansion of star :

- A star network can be expanded by placing another star hub.
- This arrangement allows several more computers or hubs to be connected to that hub. This creates a hybrid star network.

Active or passive topology ?

- Star topology networks can be either active or passive depending on the following factors.
- If the central node performs processes like amplification or regeneration then it is an **active** topology. Otherwise it is a **passive** topology.
- If the network actively controls the data transit, then it is **active** otherwise **passive**.
- If the network requires electrical power sources then it is **active** otherwise **passive**.

When is star topology suitable ?

- The star topology is preferred under the following circumstances :

1. If the centralized network control is expected.
2. If high reliability is more important than cost.
3. If the network is to be expanded frequently.

Devices used for star topology :

- The devices used for establishing a star topology network are : twisted pair cable, or optical fiber cable, a hub or switch, suitable connectors etc.

Advantages of Star Topology :

1. It is easy to add new computers to a star network without disturbing the rest of the network.
2. The star network is easy to install and maintain.
3. The fault diagnosis is easy.
4. If a computer or link fails it does not bring down the whole star network.
5. Different types of cables can be used in the same network with a hub that can accommodate multiple cable types.

Disadvantages of Star Topology :

1. If the central hub fails, the whole network fails to operate.
2. Many star networks require a device at the central point to rebroadcast or switch the network traffic.
3. The cabling cost is more since cables must be pulled from all computers to the central hub.

Note : Ethernet 10 base T is a popular network based on the star topology. Intelligent hubs with microprocessor that implement features in addition to repeating network. Signals provide for centralized monitoring and management of the network. It is the most flexible and the easiest to diagnose when there is a network fault.

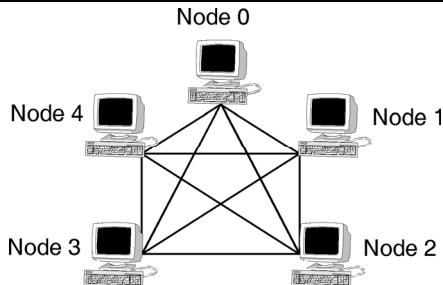
1.29.5 Mesh Topology :

SPPU : May 09

University Questions

Q. 1 Explain the merits and demerits of star, bus, ring and mesh topologies. **(May 09, 8 Marks)**

- In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 1.29.5.



(G-21)Fig. 1.29.5 : Mesh topology

- The term dedicated means that the link carries data only between two devices connected on it.
- The mesh topology is also called as **complete topology**.
- The mesh topology does not have the traffic congestion problem, because dedicated lines are being used to connect the nodes.
- These links are not being shared. So the special protocol called Media Access Control (MAC) protocol is not required to be used.
- This topology has an advantage of **data security** due to the use of dedicated links. It is robust. If one link fails, the rest of the network can continue to function. The fault diagnosis and isolation of fault also is easy.
- The only disadvantages of this topology are the cable length, the cost of the cable and the associated complexity.
- A fully connected mesh network therefore has $n(n-1)/2$ physical cables to connect n devices. To accommodate that many links every device on the network must have $n-1$ input/output ports.
- So too many cables are required to be used for the mesh topology.
- Using this formula for a network of 1000 nodes, we will require $1000 (1000 - 1)/2 = 499500$ cables or links. So this topology is suitable only for small networks.

Advantages :

1. The use of dedicated links guarantees that each connection can carry its own data reliably.
2. A mesh topology is robust because the failure of any one computer does not bring down the entire network.
3. It provides security and privacy because every message sent travels along a dedicated line.
4. Point to point links make fault diagnose easy.

5. MAC protocol need not be used due to the use of dedicated links.

Disadvantages :

1. Since every computer must be connected to every other computer installation and reconfiguration is difficult.
2. Cabling cost is more.
3. The hardware required to connect each link input/output and cable is expensive.
4. It is suitable only for smaller networks.

Note : Mesh topology is usually implemented as a backbone connecting the main computers of a hybrid network that can include several other topologies.

1.29.6 Tree Topology :

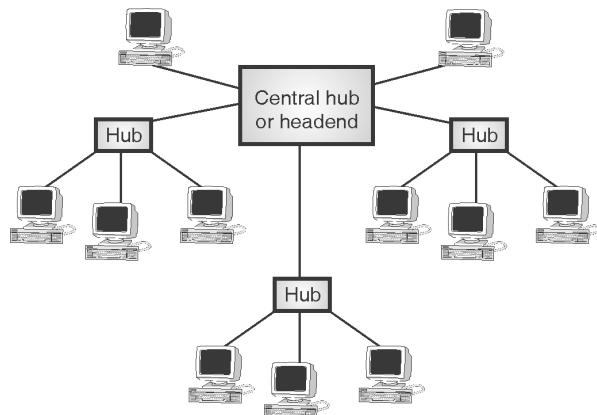
SPPU : May 07

University Questions

Q. 1 Explain network topologies with neat diagrams : Hierarchical topology. (May 07, 6 Marks)

Definition :

- Tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree.
- A tree topology is a variation of a star. As in a star, nodes in a tree are connected to a central hub/headend that controls the entire network.
- However, every computer is not plugged into the central hub. Most of them are connected to a secondary hub which in turn is connected to the central hub as shown in Fig. 1.29.6.



(G-22) Fig. 1.29.6 : Tree topology



- The central hub in the tree is an active hub which contains repeater. The repeater amplify the signal and increase the distance a signal can travel.
- The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.
- In this topology, there can be only one connection between any two nodes. Therefore it is also called as a parent-child topology.

Advantages :

1. It allows more devices to be attached to a single hub and can therefore increase the distance that a signal can travel between devices.
2. It allows the network to isolate and attach priorities to the communications from different computers.

Disadvantages :

1. If the central hub fails the system breaks down.
2. The cabling cost is more.

Note : The advantages and disadvantages of a tree topology are generally the same as those of a star.

1.29.7 Logical Topology :

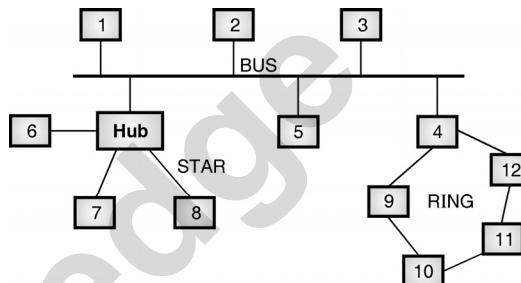
- Logical topology describes the manner in which the stations are logically connected to each other for the purpose of data unit exchange.
- Physical topology discussed earlier can be different from the logical topology, of the network.
- As an example consider the bus topology. The bus acts as a central controller. It receives data and forwards it to the various nodes.
- Thus the stations have a logical connection to the bus which acts as a centralized controller.
- Therefore the logical topology of a bus is star topology, even though the physical topology is bus.

1.29.8 Hybrid Topology :

Definition :

- We have discussed various basic topologies such as bus, ring, mesh, star etc.
- Hybrid topology is the one which makes use of two or more basic topologies mentioned above, together.

- There are different ways in which a hybrid network is created. Fig. 1.29.7 shows the hybrid topology in which bus, star and ring topologies are used simultaneously.
- In Fig. 1.29.7, the nodes 1, 2, 3, 4 and 5 are connected in the bus topology, node 6, 7 and 8 form a star and the nodes 4, 9, 10, 11, 12 are arranged in a ring topology.



(G-23) Fig. 1.29.7 : Hybrid topology

- The practical networks generally make use of hybrid topology. Many complex networks can be reduced to some form of hybrid topology.
- The hybrid topology which is to be used for a particular application depends on the requirements of that application.

Advantages of Hybrid Topology :

1. High reliability.
2. Easy to detect fault.
3. It can be expanded very easily.
4. It can be used for both wired and wireless networks.
5. Low security risk.
6. Greater flexibility and speed.

Disadvantages :

1. It is difficult to design and manage.
2. Its design is expensive.
3. It needs to use the MAU (Multistation Access Unit).

Applications :

- Hybrid topology is often used in the wide area networks (WANs).

1.30 Noise :

Definition :

- Noise is an unwanted electrical disturbance which gives rise to audible or visual disturbances in the communication systems, and errors in the digital communication.

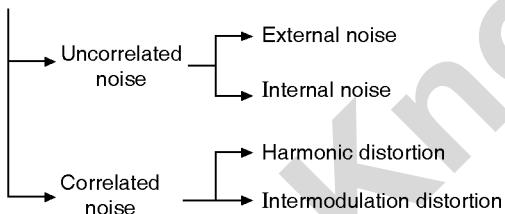


- The noise energy always falls within the passband of the signal.
- The noise gets superimposed on the signal and makes it impossible to separate the signal from noise.

1.30.1 Sources of Noise :

- Noise can be divided into two categories :
 1. Correlated noise
 2. Uncorrelated noise.
- The word "correlation" is used to indicate that there is a relation between signal and noise.
- Therefore the **correlated noise** can exist only when the signal is present, whereas the **uncorrelated noise** always exists independent of the signal.
- The uncorrelated noise is further classified into two types : External noise and Internal noise as shown in the classification of noise sources (Fig. 1.30.1).

Noise sources



(D-1661) Fig. 1.30.1 : Classification of noise sources

1.30.2 External Noise :

Definition :

- It is defined as the noise that is generated outside the device or circuit.
- The external noise can be of three types :
 1. Atmospheric noise
 2. Extraterrestrial and
 3. Man made noise

1. Atmospheric noise :

- This type of noise gets produced within the Earth's atmosphere.
- The common source of this type of noise is lightning.
- This type of noise is in the form of impulses or spikes which covers a wide frequency band typically upto 30 MHz.
- The sputtering, cracking etc heard from the loud speakers of radio is due to atmospheric noise.
- This type of noise becomes insignificant above 30 MHz.

2. Extraterrestrial noise :

- This type of noise originates from the sources which exist outside the Earth's atmosphere. Hence this noise is also called as deep space noise.
- The noise originating from the sun and the outer space is known as **Extraterrestrial Noise**.
- The extraterrestrial noise can be sub-divided into two groups : (a) Solar noise (b) Cosmic noise.

Solar Noise :

- Our sun, being a very large hot body radiates a lot of noise. The noise radiated by the sun varies according to its surface temperature variations.
- This temperature changes follow a cycle of 11 years hence the cycle of great electrical disturbances (noise) also repeats after every 11 years.

Cosmic Noise :

- The cosmic noise comes from the stars. This is identical to the noise radiated by sun because stars also are large hot bodies.
- This noise is called as black body noise or thermal noise and it is distributed uniformly over the entire sky.
- The noise also gets originated from the center of our galaxy, other galaxies and special type of stars such as "Quasars" and "Pulsars".

3. Man made noise (Industrial noise) :

- The man made noise is generated due to the make and break process in a current carrying circuit.
- The examples are the electrical motors, welding machines, ignition system of the automobiles, thyristorized high current circuits, fluorescent lights, switching gears etc.
- This type of noise is also called as industrial noise.

1.30.3 Fundamental or Internal Noise :

- The fundamental sources of noise are within the electronic equipment.
- They are called fundamental sources because they are the integral part of the physical nature of the material used for making electronic components.



- This type of noise follows certain rules. Therefore it can be eliminated by properly designing the electronic circuits and equipments.

1.31 Types of Internal Noise :

- The fundamental noise sources produce different types of noise.
- They are as follows :
 1. Thermal noise
 2. Shot noise
 3. Partition noise
 4. Low frequency or flicker, noise.
 5. High frequency or transit time, noise.
 6. Avalanche noise.
 7. Burst noise.

1.31.1 Shot Noise :

- The shot noise is produced due to shot effect. Due to the shot effect, shot noise is produced in all the amplifying devices or for that matter in all the active devices.
- The shot noise is produced due to the random variations in the arrival of electrons (or holes) at the output electrode of an amplifying device.
- Therefore it appears as a randomly varying noise current superimposed on the output.
- The shot noise "sounds" like a shower of lead shots falling on a metal sheet if amplified and passed through a loud speaker.
- The shot noise has a uniform spectral density like thermal noise.
- The exact formula for the shot noise can be obtained only for diodes.
- For all other devices an approximate equation is stated.

1.31.2 Partition Noise :

- Partition noise is generated when the current gets divided between two or more paths.
- It is generated due to the random fluctuations in the division. Therefore the partition noise in a transistor will be higher than that in a diode.

- The devices like gallium arsenide FET draw almost zero gate bias current, hence keeping the partition noise to its minimum value.

1.31.3 Low Frequency or Flicker Noise :

- The flicker noise will appear at frequencies below a few kilohertz. It is sometimes called as "1/f" noise.
- In the semiconductor devices, the flicker noise is generated due to the fluctuations in the carrier density (i.e. density of electrons and holes).
- These fluctuations in the carrier density will cause the fluctuations in the conductivity of the material.
- This will produce a fluctuating voltage drop when a direct current flows through a device. This fluctuating voltage is called as flicker noise voltage.
- The mean square value of flicker noise voltage is proportional to the square of direct current flowing through the device.

1.31.4 Thermal Noise or Johnson Noise :

- The free electrons within a conductor are always in random motion.
- This random motion is due to the thermal energy received by them.
- The distribution of these free electrons within a conductor at a given instant of time is not uniform.
- It is possible that an excess number of electrons may appear at one end or the other of the conductor.
- The average voltage resulting from this non-uniform distribution is zero but the average power is not zero.
- As this power has appeared as a result of the thermal energy, it is called as the "thermal noise power".

Average thermal noise power:

- The average thermal noise power is given by,
$$P_n = kTB \text{ Watts} \quad \dots(1.31.1)$$
where, $k = \text{Boltzmann's constant} = 1.38 \times 10^{-23}$ Joules/Kelvin.
 $B = \text{Bandwidth of the noise spectrum (Hz)}$.
 $T = \text{Temperature of the conductor, } {}^\circ\text{Kelvin}$
- Equation (1.31.1) indicates that a conductor operated at a finite temperature can work as a generator of electrical energy.



- The thermal noise power P_n is proportional to the noise BW and conductor temperature.

1.31.5 High Frequency or Transit Time Noise :

- If the time taken by an electron to travel from the emitter to the collector of a transistor becomes comparable to the time period of the signal which is being amplified then the transit time effect will take place.
- This effect is observed at very high frequencies typically in the VHF range.
- Due to the transit time effect some of the carriers may diffuse back to the emitter.
- This gives rise to an input admittance, the conductance component of which increases with frequency.
- The very small currents induced in the input of the device by means of the random fluctuations in the output current will create random noise at high frequencies.
- Once this noise appears, it goes on increasing with frequency at a rate of 6 dB per octave.

1.32 Theorems in Data Communication :

1.32.1 Channel Capacity :

Definition :

- The channel capacity is denoted by C and in simple terms defined as the maximum possible bit rate a channel can support without introducing errors.
- The unit of channel capacity is bits/sec.

$$\therefore C = R_{\max} \text{ bits/sec}$$

1.32.2 Nyquist Theorem : SPPU : Dec. 10, May 13

University Questions

- Q. 1** State the Nyquist theorem and explain Shannon capacity with an example. **(Dec. 10, 4 Marks)**
- Q. 2** Explain Nyquist bit rate and Shannon capacity theorem. **(May 13, 8 Marks)**

- As we know a transmission channel is a medium over which the electrical signals from a transmitter travel to the receiver.
- Two important characteristics of a transmission channel are :
 1. Signal to Noise ratio (SNR) and
 2. Channel bandwidth.

- These two characteristics will ultimately decide the maximum capacity of a channel to carry information.
- Nyquist and Shannon worked on finding the maximum channel capacity of a bandlimited channel.

Statement :

- Nyquist's theorem states that if the bandwidth of a transmission channel is "B" which carries a signal having "L" number of levels, then the maximum data rate "R" on this channel is given by.

$$R = 2 B \log_2 L \quad \dots(1.32.1)$$

- As maximum data rate for reliable transmission is defined as channel capacity C , the above expression gets modified as :

$$C = 2 B \log_2 L \quad \dots(1.32.2)$$

- This expression indicates that the data rate can be increased by increasing the number of different signal elements (L).

1.32.3 Shannon's Theorem :

SPPU : May 09, May 10, Dec. 10, May 11, May 13

University Questions

- Q. 1** State Shannon's channel capacity theorem. **(May 09, 6 Marks)**
- Q. 2** State and explain Shannon's channel capacity theorem. **(May 10, May 11, 4 Marks)**
- Q. 3** State the Nyquist theorem and explain Shannon capacity with an example. **(Dec. 10, 4 Marks)**
- Q. 4** Explain Nyquist bit rate and Shannon capacity theorem. **(May 13, 8 Marks)**

Statement :

- Given that a source of M equally likely messages with $M >> 1$, which is generating information at a rate R . Given that a channel of capacity " C " exists.
- Then if, $R \leq C$ then there exists a "coding" technique such that the output of the source may be transmitted over the channel with a probability of error in the received message which may be made arbitrarily small.

Meaning :

1. The theorem is concerned with the rate of transmission of information (R) over a communication channel.
2. The channel capacity " C " is a rate of transmission in bits/sec. According to the theorem for $R \leq C$ transmission can be accomplished with coding without error in the presence of noise.



- There is a negative statement associated with the Shannon's theorem. It's statement is as follows.

Negative statement of Shannon's theorem :

- Given a source of equally likely messages with $M \gg 1$, which is generating an information at a rate R , and if

$$R > C$$

- then the probability of error is close to unity for every possible set of M transmitted signals.

Meaning :

1. If the information rate R exceeds a specific value "C", then the error probability will increase towards unity as M increases.
2. When $R > C$, complexity of coding is increased which results in an increase in the probability of error.

1.32.4 Shannon Hartley Theorem :

Statement :

- The channel capacity of a white, bandlimited gaussian channel is given by,

$$C = B \log_2 \left(1 + \frac{S}{N} \right) \text{ bits/sec} \quad \dots(1.32.3)$$

where, B = Channel bandwidth

S = Signal power

N = Noise within the channel bandwidth

Explanation :

- By Shannon Hartley theorem we get the channel capacity as,

$$C = B \log_2 \left[1 + \frac{S}{N} \right]$$

- Let us try to find out the maximum possible value of C . From the equation for "C" it is evident that it depends on two factors, which are the bandwidth "B" and the S/N ratio.
- Let us find their effect on "C" one by one.

Effect of S/N on C :

- If the communication channel is noiseless then $N = 0$. Therefore $(S/N) \rightarrow \infty$ and so "C" also will tend to ∞ . Thus the noiseless channel will have an infinite capacity.

Effect of bandwidth on channel capacity :

- Now consider that some white gaussian noise is present hence (S/N) is not infinite.

- Now as the bandwidth approaches infinity the channel capacity does not become infinite since $N = N_o B$ will also increase with the bandwidth B .
- This will reduce the value of (S/N) with increase in B , assuming the signal power S to be constant.
- Thus we conclude that an ideal system with infinite bandwidth has a finite channel capacity.
- It is denoted by " C_∞ " and given by,

$$C_\infty \equiv 1.44 \frac{S}{N_o} \quad \dots(1.32.4)$$

1.32.5 S/N Bandwidth Trade off :

- The Shannon-Hartley theorem also indicates that we can trade off between the (S/N) ratio and the bandwidth and vice versa.
- This can be explained as follows :
- Assume that $(S/N) = 7$ and $B = 4$ kHz. The corresponding value of C is calculated as,

$$C = 4 \times 10^3 \log_2 (1 + 7)$$

$$\therefore C = 12 \times 10^3 \text{ bits/sec}$$

- Now (S/N) is increased to 15 and bandwidth is decreased to 3 kHz

$$\text{We get, } C = 3 \times 10^3 \log_2 (1 + 15)$$

$$\therefore C = 12 \times 10^3 \text{ bits/sec}$$

So C has remained constant.

- To increase the (S/N) ratio to 15 from 7 we need to increase the signal power by a factor of 1.6.
- This is 60% increase in the signal power, for a 25% reduction in the bandwidth (from 4 kHz to 3 kHz).
- Therefore 25 percent reduction in bandwidth requires a 60 percent increase in the signal power.

Ex. 1.32.1 : Calculate the maximum bit rate for a channel having bandwidth 3100 Hz and S/N ratio 20 dB. **Dec. 01, 5 Marks**

Soln. :

Given : $B = 3100$ Hz

$$\frac{S}{N} = 20 \text{ dB.}$$

But $20 \text{ dB} = 10 \log (S/N)$

$$\therefore S/N = 100$$

- The maximum bit rate is given by,

$$R_{\max} = B \log_2 \left[1 + \frac{S}{N} \right] = 3100 \log_2 [1 + 100]$$



$$= \frac{3100 \log_{10} 101}{\log_{10} 2} = 20,640 \text{ bits/sec. ...Ans.}$$

Ex. 1.32.2 : Calculate the maximum bit rate for a channel having bandwidth 3100 Hz and S/N ratio 10 dB.

May 02, 5 Marks

Soln. :

Given : $B = 3100 \text{ Hz}$

$$\left(\frac{S}{N}\right)_{\text{dB}} = 10$$

$$\therefore 10 = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\therefore \frac{S}{N} = 10$$

$$\begin{aligned} \therefore \text{Maximum bit rate} &= R_{\max} = B \log_2 \left[1 + \frac{S}{N} \right] \\ &= 3100 \log_2 (1 + 10) = \frac{3100 \log_{10} 11}{\log_{10} 2} \\ &= 10,724 \text{ bits/s} \quad \dots\text{Ans.} \end{aligned}$$

Ex. 1.32.3 : Calculate the maximum bit rate for a channel having bandwidth 1600 Hz if :

- (a) S/N ratio is 0 dB (b) S/N ratio is 20 dB.

Dec. 02, 6 Marks

Soln. :

Given : $B = 1600 \text{ Hz}$

1. R_{\max} for S/N = 0 dB :

$$\left(\frac{S}{N}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\therefore \frac{S}{N} = 1$$

$$\begin{aligned} \therefore R_{\max} &= B \log_2 (1 + S/N) \\ &= 1600 \log_2 (1 + 1) \\ &= 1600 \text{ bits/sec} \quad \dots\text{Ans.} \end{aligned}$$

2. R_{\max} for S/N = 20 dB :

$$\left(\frac{S}{N}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\therefore 20 = 10 \log_{10} (S/N)$$

$$\therefore \frac{S}{N} = 100$$

$$\begin{aligned} \therefore R_{\max} &= B \log_2 \left(1 + \frac{S}{N} \right) = 1600 \log_2 (101) \\ &= \frac{1600 \log_{10} (101)}{\log_{10} (2)} \end{aligned}$$

$$R_{\max} = 10,654 \text{ bits/sec} \quad \dots\text{Ans.}$$

Using both the limits :

- In practice we have to use both the methods to calculate the required bandwidth and signal level. consider the following example for the same.

Ex. 1.32.4 : Calculate the maximum bit rate of channel having bandwidth 1200 Hz if :

1. S/N ratio is 0 dB
2. S/N ratio is 20 dB

Dec. 03, May 17, 6 Marks

Soln. :

Given : $B = 1200 \text{ Hz}$.

1. R_{\max} for S/N = 0 dB :

$$\left(\frac{S}{N}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\frac{S}{N} = 1$$

$$\begin{aligned} \therefore R_{\max} &= B \log_2 \left(1 + \frac{S}{N} \right) \\ &= 1200 \log_2 (1 + 1) \\ &= 1200 \text{ bits/sec} \quad \dots\text{Ans.} \end{aligned}$$

2. R_{\max} for S/N = 20 dB :

$$\left(\frac{S}{N}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$20 = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\therefore \frac{S}{N} = 100$$

$$\begin{aligned} \therefore R_{\max} &= B \log_2 \left(1 + \frac{S}{N} \right) = 1200 \log_2 (101) \\ &= 1200 \frac{\log_{10} (101)}{\log_{10} (2)} \\ &= 7990 \text{ bits/sec} \quad \dots\text{Ans.} \end{aligned}$$

Maximum bit rate = 1200 bits/sec for 0 dB

Maximum bit rate = 7990 bits/sec for 20 dB

Ex. 1.32.5 : Find the number of coding or symbol levels if $C = 31000 \text{ bits/s}$ and B is 3100 Hz .

May 06, 3 Marks

Soln. :

- C is the channel capacity while B is the bandwidth.

$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

where S/N is the signal to noise ratio.

$$\therefore 31000 = 3100 \log_2 \left(1 + \frac{S}{N} \right)$$



$$\begin{aligned}\therefore \log_2 \left(1 + \frac{S}{N}\right) &= 10 \\ \therefore \frac{S}{N} &= 1023 \text{ or } 30\text{dB} \\ \left(\frac{S}{N}\right) \text{dB} &= 1.8 + 6 \text{ NdB} \\ \therefore 30 &= 1.8 + 6N \\ \text{where } N &= \text{Number of bits per word.} \\ \therefore N &= 4.72 \approx 5\end{aligned}$$

Number of symbol levels

$$Q = 2^N = 2^5 = 32 \quad \dots\text{Ans.}$$

Ex. 1.32.6 : Calculate the channel capacity for a noisy channel having bandwidth = 5 kHz and SNR = 0 using appropriate formula.

Dec. 10, 4 Marks

Soln. :

Given : $B = 5 \text{ kHz}$, $\frac{S}{N} = 0$

To find : Channel capacity.

$$\begin{aligned}C &= B \log_2 \left[1 + \frac{S}{N} \right] \\ &= 5 \times 10^3 \log_2 [1 + 0] \\ C &= 0 \text{ bits/sec.} \quad \dots\text{Ans.}\end{aligned}$$

Ex. 1.32.7 : An analog signal has a bit rate of 8000 bps and a baud rate of 1000 baud. How many data elements are carried by each signal element ? How many signal elements do we need ?

May 12, 8 Marks

Soln. :

Given : Bit rate (n) = 8000 bps, Baud rate = 1000 baud.

To find : 1. Data elements carried by each signal element (R)
2. Total signal elements (L)

Step 1 : Calculate R :Bit rate = Numbers of data elements per signal \times baud rate

$$\therefore \text{Number of data elements per signal (R)} = \frac{\text{Bit rate (n)}}{\text{Baud rate}}$$

$$\therefore R = \frac{8000}{1000} = 8 \text{ bits/baud} \quad \dots\text{Ans.}$$

Step 2 : Calculate L :

$$\text{Total signal elements (L)} = 2^R = 2^8 = 256 \quad \dots\text{Ans.}$$

Ex. 1.32.8 : State and explain the Nyquist theorem and Shannon capacity and solve the following example :

Example : Calculate the maximum bit rate for noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels.

May 14, 6 Marks, Dec. 15, May 16, 7 Marks

Soln. :

Given : $B = 3000 \text{ Hz}$, $L = 2$

To find : Maximum bit rate

$$\text{Maximum bit rate (R)} = 2B \log_2 L = 2 \times 3000 \log_2 (2)$$

$$= 2 \times 3000 \times \left(\frac{\log_{10} (2)}{\log_{10} 2} \right)$$

$$\therefore R = 6000 \text{ bits/sec.} \quad \dots\text{Ans.}$$

Ex. 1.32.9 : Calculate the bandwidth of noiseless channel having maximum bit rate of 24 Kbps and 8 signal levels.

May 16, 7 Marks

Soln. :

$$R = 2B \log_2 L \quad \dots \text{Nyquist's theorem}$$

$$\therefore 24 \times 10^3 = 2B \log_2 8$$

$$\therefore 24 \times 10^3 = 2B \log_2 2^3$$

$$\therefore 24 \times 10^3 = 6B$$

$$\therefore B = 4 \times 10^3 \text{ or } 4 \text{ kHz} \quad \dots\text{Ans.}$$

Review Questions

- Q. 1 Discuss the fundamental characteristics of data communication system.
- Q. 2 Explain the data communication system with its five components.
- Q. 3 Define : Bit rate and baud rate.
- Q. 4 What are the importance of sampling theorem ?
- Q. 5 Explain with block diagram pulse code modulation encoder.
- Q. 6 What are the advantages and disadvantages of PCM?
- Q. 7 With neat block diagram explain transmitter and receiver of delta modulation.
- Q. 8 Explain distortions in delta modulation.
- Q. 9 Explain the two different methods of Digital to Analog conversion.
- Q. 10 Write the bandwidth requirement for ASK, FSK, BPSK, QPSK.



- | | | | |
|-------|---|-------|---|
| Q. 11 | Explain the frequency shift keying techniques with suitable diagram. | Q. 20 | What is multiplexing ? What are its types of multiplexing explain any one? |
| Q. 12 | Explain the phase shift keying techniques with suitable diagram. | Q. 21 | Explain FDM multiplexing with their advantages and disadvantages. |
| Q. 13 | Explain the BPSK transmitter and receiver with suitable diagram. | Q. 22 | Explain TDM and statistical TDM multiplexing with their advantages and disadvantages. |
| Q. 14 | Explain the amplitude modulation. | Q. 23 | Give the comparison of statistical and synchronous TDM. |
| Q. 15 | Write the mathematical representation of A.M. | Q. 24 | Define and explain network topology. |
| Q. 16 | Define modulation index. | Q. 25 | Explain any two network topology with advantages and disadvantages. |
| Q. 17 | With respect to FM discuss following terms :
1. Frequency deviation, 2. Deviation ratio. | Q. 26 | Define noise. Give the sources of noise. |
| Q. 18 | Compare AM, FM and PM. | Q. 27 | State the Nyquist theorem and explain Shannon capacity theorem. |
| Q. 19 | Define signal to noise ratio. | | |

□□□

TechKnowledge
Publications

Unit I

Chapter 2

Network Models and Addressing

Syllabus

OSI model, TCP/IP model (Data format, Addressing mechanisms, Devices).

Case study : Study of Physical layer components such as Cable, NIC, hub, etc. available in the computers / laboratories of your department.

Chapter Contents

2.1	Introduction	2.6	Detailed Description of Each Layer in TCP/IP
2.2	Network Software	2.7	Encapsulation and Decapsulation
2.3	Reference Models	2.8	Addressing in TCP/IP
2.4	OSI Model	2.9	Multiplexing and Demultiplexing in TCP / IP
2.5	TCP/IP Model	2.10	Comparison of OSI and TCP/IP

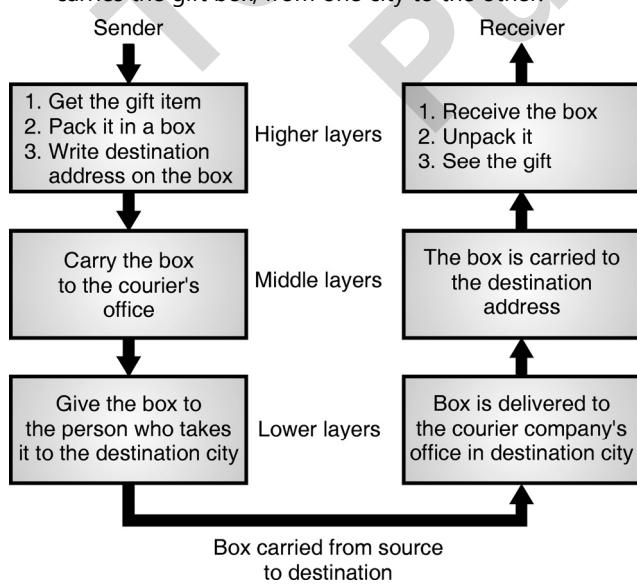


2.1 Introduction :

- A network is a combination of hardware and software that sends data from one computer to the other.
- The hardware is defined as the part of network which contains the physical equipment to carry signals from one point of network to the other.
- The software is defined as the other part of the network which consists of the instruction sets and program which makes it possible to carry out the expected services from the networks.
- Any task that is to be performed by a computer network can be divided into several smaller tasks each performed by a separate software package.
- Each software package uses services of another software package to carry out the task assigned to it.
- We can think of this process as a stack of layers as described in the subsection below.

2.1.1 Layered Tasks :

- The concept of layers is used in our daily life. Take an example of two friends with one friend wants to send a gift to the other via courier service. Fig. 2.1.1 shows the steps involved in this process.
- In Fig. 2.1.1 we have three important persons involved namely the sender, the receiver and the carrier who carries the gift box, from one city to the other.



Hierarchy of tasks :

- The point to be noted is that in order to complete a task in day to day life small actions are being done in a hierarchical way or layered manner.

1. At the sender :

Upper layers :

- The tasks of higher layers :
 1. Get the gift item
 2. Pack it in a box
 3. Write the destination address on the box.

- **Middle layer :** Carry the addressed box to the office of a courier company.

- **Lower layer :** Give the box to a person who will take it to the destination city.

2. At the receiver :

- **Tasks of lower layers :** The box is delivered to the courier company office in the destination city.
- **Middle layers :** The box is carried by another person to the destination address and the box is delivered.

Upper layers :

1. Receive the box
2. Unpack it
3. See the gift

Hierarchy and layered tasks :

- This discussion demonstrates that the important tasks are carried out by the higher layers whereas the simpler tasks are carried out by the middle and lower layers.
- In the network protocols as well the layered architecture is used.

2.1.2 Protocol :

SPPU : Dec. 06

University Questions

- Q. 1** What is the need of protocols in communication networks ? **(Dec. 06, 2 Marks)**

Definition :

- Protocol is defined as a set of rules which governs the format and meaning of frames, packets or messages that are being exchanged between the peer entities.
- These rules are decided and agreed upon by both the communicating entities.



- The entities use protocols so as to implement their services. They can choose any suitable protocol as long as their pre-decided services are being taken care of.

2.1.3 Network Architecture :

Definition :

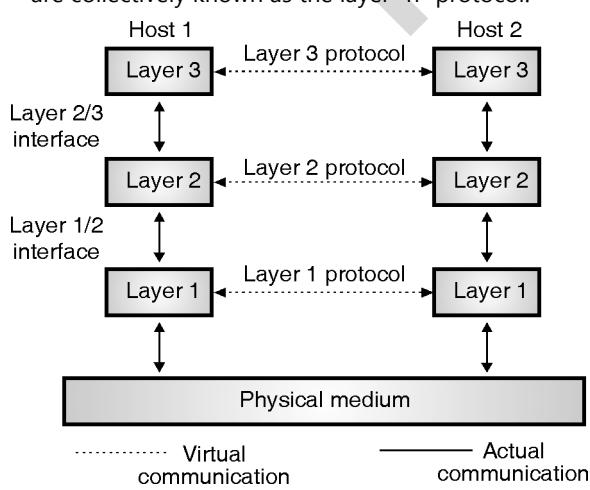
- A set of layers and protocols is called as network architecture.
- Protocol stack is defined as a list of protocols used for a certain system, one protocol per layer.

2.2 Network Software :

- The software used in networks is equally important as the hardware. The network software is highly structured now a days.

2.2.1 Protocol Hierarchies (Layered Architecture) :

- Most networks are organized in the form of a series of layers or levels as shown in Fig. 2.2.1 to reduces the design complexity.
- The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (source) will communicate with layer n on another machine (destination).
- The rules and conventions used in this communication are collectively known as the layer "n" protocol.



(G-49) Fig. 2.2.1 : Layers, protocols and interfaces

- Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.
- Violation of the protocol will lead to the communication difficulties or failure.

Peer :

- A three layer network is shown in Fig. 2.2.1. The entities comprising the corresponding layers on different machines are called as **peers**.
- The communication actually takes place between the peers using the protocol.
- The dotted lines in Fig. 2.2.1 shows the virtual communication and physical communication is shown by solid lines.

2.2.2 Reasons for having Layered Protocols and its Benefits :

- The process of establishing a link between two devices to communicate and share information is complicated.
- There are many functions which are to be taken into consideration to allow an effective communication to take place.
- To organize all these functions in an organized way the designers felt the need to develop network architecture.
- In the network architecture various tasks and functions are grouped into related and manageable sets called **LAYERS**.
- A network architecture can be defined as a set of protocols that tell how every layer is to function.
- The reasons and advantages of using the network architecture are as follows :

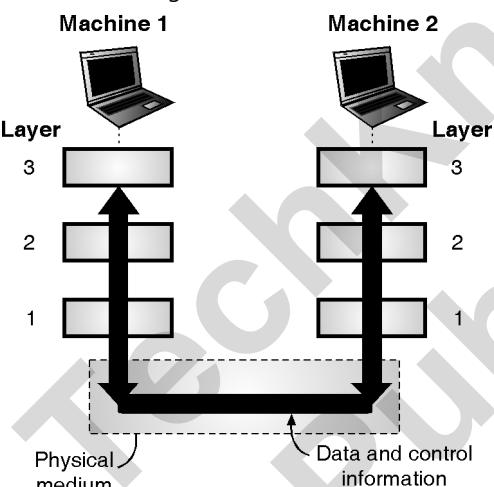
 1. It simplifies the design process as the functions of each layers and their interactions are well defined.
 2. The layered architecture provides flexibility to modify and develop network services.
 3. The number of layers, names of the layers, and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers some services to its upper layer.
 4. The concept of layered architecture is a new way of looking at the networks.



5. Addition of new services and management of network infrastructure becomes easy.
6. Due to segmentation (layered structure), it is possible to break difficult problems into smaller and more manageable tasks.
7. Logical segmentation allows parallel working by different teams on different tasks simultaneously.

2.2.3 How does Data Transfer Take Place ?

- Data does not get transferred directly from layer n of one machine to layer n of the other machine. Instead the data transfer takes place as explained below.
- The data and control information is passed on to the lower layers until the lowest layer (layer 1) is reached. Below layer 1 lies the physical medium such as coaxial cable, through which the actual transfer of data and control information takes place.
- This is shown in Fig. 2.2.2.



(G-50) Fig. 2.2.2 : Data transfer

Interface :

- An interface defines the operations and services offered by lower layer to the upper layer.
- There is an interface between each pair of adjacent layers.

2.3 Reference Models :

- After discussing about the layered networks, now we will discuss two work architectures or reference models.
- The two most important reference models are :
 1. The OSI reference model and

2. The TCP/IP reference model.
- The International Standards Organisation (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model.
 - An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
 - The purpose of each layer is to offer certain services to the higher layers.
 - Layer n on one machine (source) will communicate with layer n on another machine (destination).
 - The rules and conventions used in this communication are collectively known as the layer n protocol.
 - Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.

2.4 OSI Model :

SPPU : May 06

University Questions

Q. 1 What is an open system ? (May 06, 3 Marks)

- The users of a computer network are located over a wide physical range i.e. all over the world.
- Therefore to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed.
- These standards will fit into a framework which has been developed by the "International organization of standardization (ISO)".
- This framework is called as "Model for open system interconnection (OSI)" and it is normally referred to as "OSI reference model".

2.4.1 Layered Architecture :

SPPU : May 10, May 11, Dec. 12, May 13,
May 14, May 15

University Questions

Q. 1 Explain ISO-OSI model in detail.

(May 10, May 14, May 15, 8 Marks)

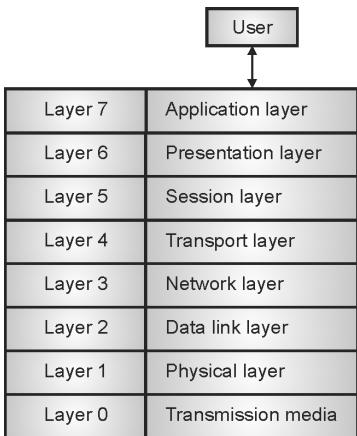
Q. 2 Explain ISO-OSI reference model in detail.

(May 11, 8 Marks)



- Q. 3** Draw the diagram of OSI model. Discuss briefly the functions of each layer. **(Dec. 12, 8 Marks)**
- Q. 4** Draw ISO-OSI reference model. What are the responsibility of : 1. Physical layer 2. Data link layer 3. Network layer. **(May 13, 8 Marks)**

- Fig. 2.4.1 shows the seven layer architecture of ISO-OSI reference model.



(G-59) Fig. 2.4.1 : A seven layer ISO-OSI reference model

- It defines seven levels or layers in a complete communication system.
- The lowest layer is physical layer and highest one is called as the application layer.
- Each computer on a network uses a series of protocols to perform the functions assigned to each layer.
- These layers collectively form the protocol stack or networking stack.
- At the top of the stack we have the application and at the bottom is the physical medium which actually connects the computers to form a network.

Who developed the OSI model ?

- The OSI model was developed in two different and completely independent projects by the International Organization for Standardization (ISO) and the Consultative Committee for International Telephone and Telegraphy (CCITT) which is now known as ITU-T.
- Both these organizations developed their own seven layer models. Then in 1983 the two projects were combined together.

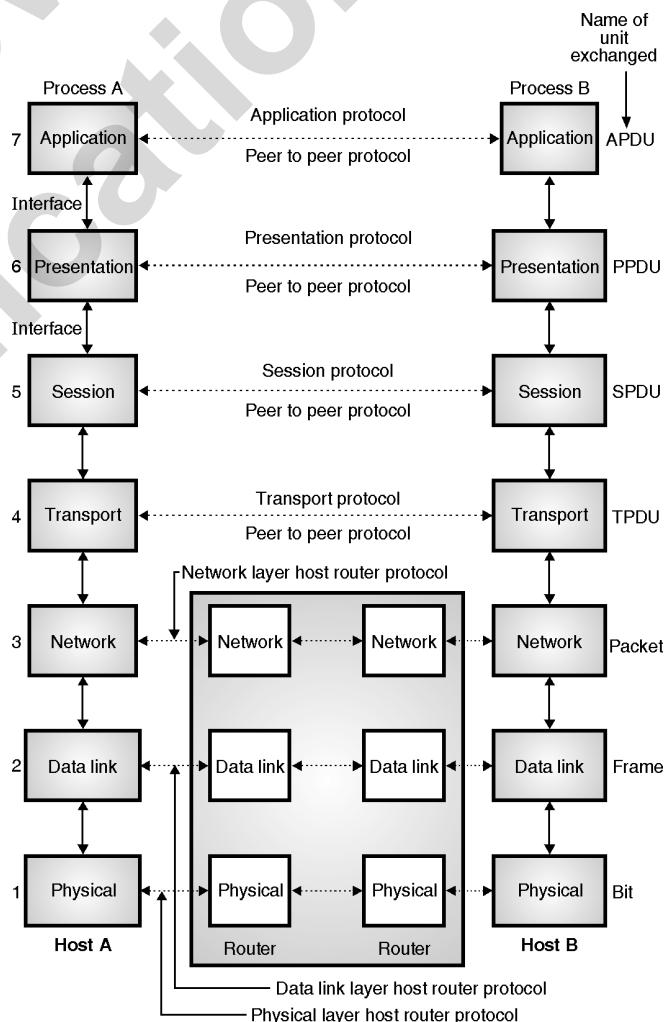
OSI protocol suite :

- The OSI model was originally developed as a model for creating a 7 layer protocol suite. But this seven layer protocol suite never came into existence.

- In fact none of the protocol suites existing today exactly match the seven layer structure of the OSI model.
- But still the OSI reference model is so simple yet powerful that it is being used as a teaching, reference and communications tool.
- The reason why real protocol stacks differ from the OSI model is that many protocols used today were developed before the OSI model was developed.
- The TCP/IP protocols which are used extensively in practice have their own layered model. The TCP/IP reference model is discussed later on.

2.4.2 A More Detailed OSI Model :

- Fig. 2.4.2 shows a more detailed OSI model with two hosts A and B communicating with each other.



(G-60) Fig. 2.4.2 : The OSI reference model

**Interface :**

- An interface defines the operations and services offered by lower layer to the upper layer.
- There is an interface between each pair of adjacent layers as shown in Fig. 2.4.2.

Peer :

- The active elements present in each layer are known as **entities**. The entities can be hardware entities or software entities.
- The entities comprising the corresponding layers on different machines are called as **peers**.
- The communication actually takes place between the peers using the protocol.
- The dotted lines in Fig. 2.4.2 show the virtual communication and physical communication is shown by solid lines.
- Within a single machine, each layer uses the services of the layer just below it.
- However between two machines A and B of Fig. 2.4.2 layer x on machine A will communicate with layer x on machine B.
- This communication is based on some mutually agreed rules called **protocols**.
- The processes on each machine which communicate at a given layer are called as **peer-to-peer processes**.

2.4.3 Peer to Peer Processes :

- All the applications need not use all the seven layers shown in Fig. 2.4.1.
- The lower three layers are enough for most of the applications.
- Each layer is built from electronic circuits and/or software and has a separate existence from the remaining layers.
- Each layer is supposed to handle message or data from the layers which are immediately above or below it.
- This is done by following the protocol rules. Thus each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

Interlayer Communication :

- In order to get an idea of interlayer communication, let us take a simple example first.
- We want the data to get transferred from layer-3 of machine-A to layer 3 of machine-B.
- But the data does not get transferred directly from layer 3 of one machine to layer 3 of the other machine.
- The data and control information is passed on from the topmost layer to the lower layers until the lowest layer (layer 1) is reached. Below layer 1 lies the physical medium such as coaxial cable, through which the actual communication takes place.
- This is shown in Fig. 2.4.2. This is called as the actual communication between the layers.

2.4.4 Organization of the Layers :

- The seven layers in the OSI model can be considered to belong to three subgroups as follows :
- 1. Subgroup 1 : Physical, data link and network-network support layers. (layers 1, 2 and 3)
- 2. Subgroup 2 : Session, Presentation and application-user support layers. (layers 5, 6 and 7)
- 3. Subgroup 3 : Transport layer-linking of subgroups 1 and 2.
- The first subgroup consists of layers 1, 2 and 3 i.e the physical, data link and network layers.
- They are important for the physical aspects of moving data from one computer to the other.
- The second subgroup is made up of the upper three layers (5, 6 and 7) i.e. session, presentation and application layers. This is called as the user support layers.
- They allow the interaction between unrelated software systems.
- The third subgroup consists of only the fourth layer i.e. the transport layer. It links the subgroups 1 and 2.
- The upper layers are implemented using software only whereas the lower layers are a combination of hardware and software.
- The physical layer is implemented by only hardware.
- Table 2.4.1 shows various layers and its functions.

**Table 2.4.1 : Functions of the layers of ISO-OSI model**

Level	Name of the layer	Functions
1.	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2.	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4.	Transport layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session management.
6.	Presentation layer	It works as a translating layer.
7.	Application layer	Retransferring files of information, LOGIN, password checking etc.

2.4.5 Functions of Different Layers :

SPPU : Dec. 05, Dec. 11, Dec. 12, May 13, Dec. 18

University Questions

Q. 1 Describe the functions of all the layers of the OSI reference model in short. **(Dec. 05, 8 Marks)**

Q. 2 Draw ISO-OSI reference model. What are the responsibilities of :

1. Physical layer
2. Data link layer
3. Network layer

(Dec. 11, May 13, Dec. 18, 8 Marks)

Q. 3 Draw the diagram of OSI model. Discuss briefly the functions of each layer. **(Dec. 12, 8 Marks)**

Layer 1 : The physical layer :

- Functions of the physical layer are as follows :

1. To activate, maintain and deactivate the physical connection.
 2. To define voltages and data rates needed for transmission.
 3. To convert the digital data bits into electrical signal.
 4. To decide whether the transmission is simplex, half duplex or full duplex.
 5. A physical layer does not perform the following operations :
 6. It does not detect or correct errors.
 7. It does not decide the medium or modulation.
- The examples of the physical layer protocols are RS-232 or RS-449 standards.

Layer 2 : Data link layer :

- Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.
- To enable the error detection, it adds error detection bits to the data which is to be transmitted.
- The encoded data is then passed to the physical layer.
- These error detection bits are used by the data link layer on the other side to detect and correct the errors.
- At this level the outgoing messages are assembled into frames, and the system waits for the acknowledgements to be received after every frame transmitted.
- Correct operation of the data link layer ensures reliable transmission of each message. Examples of data link layer protocols are HDLC, SDLC and X.25 protocols.

Layer 3 : The network layer :

- The functions of network layer are as follows :
- 1. To route the signals through various channels to the other end.
- 2. To act as the network controller by deciding which route data should take.
- 3. To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.
- In short the network layer acts as a network controller for routing data.



Layer 4 : Transport layer :

- As the name suggests this layer provides the transport services. The functions of the transport layer are as listed below :

 1. It decides if the data transmission should take place on parallel paths or single path.
 2. It does the functions such as multiplexing, splitting or segmenting on the data.
 3. Transport layer guarantees transmission of data from one end to the other.
 4. It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

Layer 5 : The session layer :

- This layer manages and synchronizes conversations between two different applications. This is the level at which the user will establish system to system connection.
- It controls logging on and off, user identification, billing and session management.
- In the transmission of data from one system to the other, at session layer streams of data are marked and resynchronized properly so that the ends of messages are not cut prematurely and data loss is avoided.

Layer 6 : The presentation layer :

- The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.
- The form and syntax (language) of the two communicating systems can be different. Example, one system is using the ASCII code for file transfer and the other one uses IBM's EBCDIC.
- Under such conditions the presentation layer provides the "translation" from ASCII to EBCDIC and vice versa.

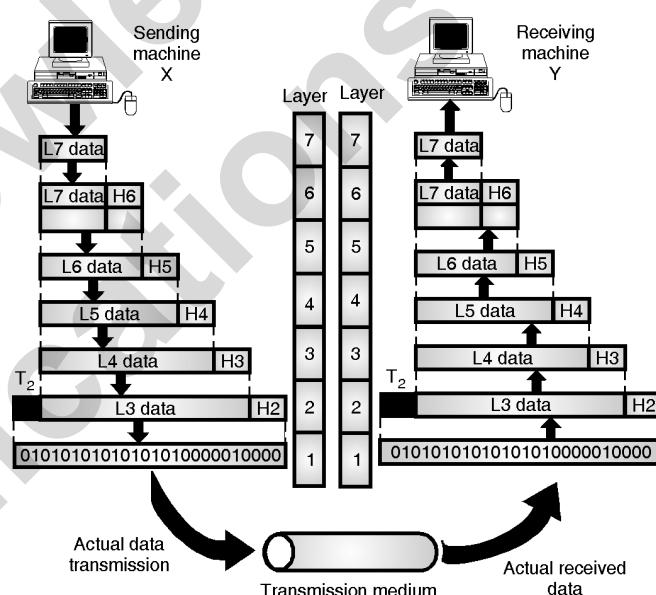
Layer 7 : Application layer :

- Application layer is at the top of all as shown in Fig. 2.4.2.
- It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results etc. to the user who is sitting above this layer.

- The functions such as LOGIN, or password checking are also performed by the application layer.
- Let us now go into the details of each and every layer.

2.4.6 Exchange of Information using the OSI Model :

- At the physical layer, communication is direct i.e. machine X sends a stream of bits to machine Y.
- At higher layers, each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it as shown in Fig. 2.4.3.



(G-61) Fig. 2.4.3 : An exchange using the OSI model

- The information added by each layer is in the form of headers or trailers. Headers are added to the message at the layers 6, 5, 4, 3, and 2. A trailer is added at layer 2.
- At layer 1 the entire package is converted to a form that can be transferred to the receiving machine.
- At the receiving machine, the message is unwrapped layer by layer with each process receiving and removing the data meant for it.
- The upper OSI layers are always implemented in software (4, 5, 6 and 7) and lower layers are a combination of hardware and software (2, 3) except for the physical layer which is mostly hardware.
- Layers 1, 2 and 3 (i.e. physical, data link and network) are the network support layers.



- They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing and transport timing and reliability.
- Layer 4, the transport layer ensures end to end reliable data transmission.
- Layers 5, 6 and 7 (i.e. session, presentation and application) they allow interoperability among unrelated software systems.

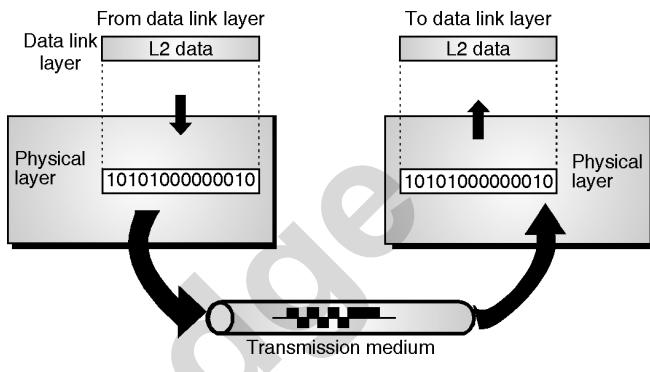
Protocols Associated With OSI reference Model :

Layer Name	Protocol Supported
Physical Layer	RS-232, RS-449, V.35, V.34, I.430, I.431, T1, E1, POTS, SONET/SDH, OTN, DSL, 802.11a/b/g/n, 802.15.x, USB · Bluetooth, Firewire (IEEE 1394)
Data Link Layer	ARP, CSLIP, SLIP, PPP
Network Layer	VLAN, IP (IPv4, IPv6), ICMP, IPsec, IGMP, IPX, AppleTalk
Transport Layer	TCP, UDP, SCTP, DCCP
Session Layer	NetBIOS, SAP, SIP, L2TP, VPN
Presentation Layer	MIME, XDR, TLS, SSL
Application Layer	NNTP = Usenet, SIP = VOIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP = TIME, SMPP, SMTP = email, DHCP, SNMP, Telnet

2.4.7 Physical Layer :

- The physical layer is responsible for sending bits from one computer to another.
- The physical layer is not concerned with the meaning of the bits, but it deals with physical connection to the network and with transmission and reception of signals.
- The physical layer is used to define physical and electrical details such as what will represent a 1 or a 0, how many pins a network will have, how data will be synchronized and when the network adapter may or may not transmit the data.

- The position of the physical layer with respect to the transmission medium and the data link layer is shown in Fig. 2.4.4.



(G-62)Fig. 2.4.4 : Physical layer

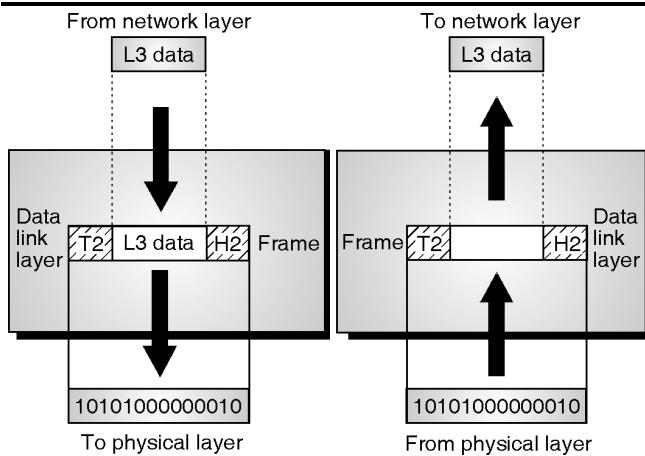
Functions of the physical layer :

1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
2. To define the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point to point connections.
5. To deal with physical topologies i.e. bus, star, ring, or mesh.
6. To deal with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. To define the characteristics between the device and the transmission medium.
9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

Note : Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.

2.4.8 Data Link Layer :

- It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown in Fig. 2.4.5.



(G-63) Fig. 2.4.5 : Data link layer

Functions of DLL :

Following are the functions of data link layer :

1. Framing :

- The bits received from the network layer are divided into another type of data units called frames at the data link layer.

2. Flow control :

- It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

3. Physical addressing :

- It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. Error control :

- A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. Access control :

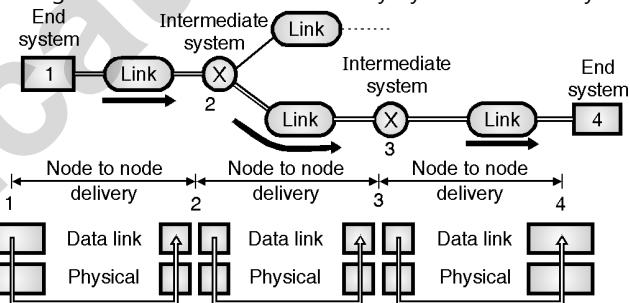
- The data link layer protocol performs an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institute of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :

1. Logical Link Control (LLC) :

- It establishes and maintains links between the communicating devices.

2. Media Access Control (MAC) :

- It controls the way multiple devices share the same media channel.
- The logical link control sub-layer provides Service Access Points (SAPs) that the other computers can refer to and use to transfer information from LLC to the network layer.
- The MAC sub-layer provides for shared access to the network adapter and communicates directly with the network interface cards.
- Network Interface Cards (NIC) have a unique 12-digit hexadecimal MAC address assigned before they leave the factory where they are manufactured.
- The MAC addresses are used to establish logical link between two computers on the same LAN. Bridges, intelligent hubs and network interface cards are devices associated with the data link layer.
- The data link layer is responsible for moving frames from one hop (node) to the next.
- Fig. 2.4.6 shows the node delivery by the data link layer.

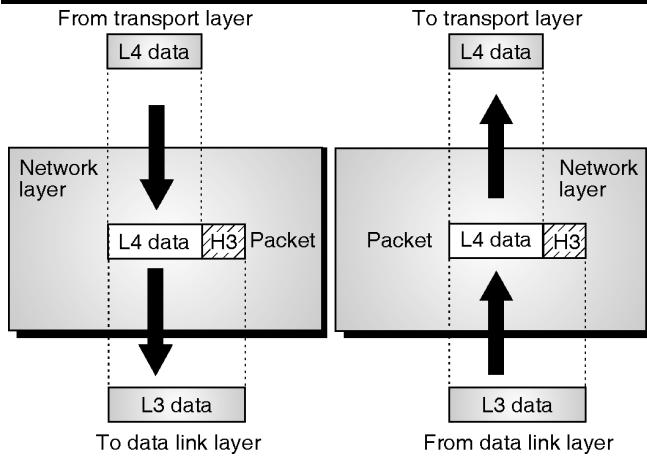


(G-64) Fig. 2.4.6 : Node to node delivery

- Fig. 2.4.6 illustrates that the communication at data link layer takes place between two adjacent nodes.
- The data is being sent from end system-1 to end system-4. To do so, partial data deliveries are made three times, from 1 to 2 from 2 to 3 and then from 3 to 4.

2.4.9 Network Layer :

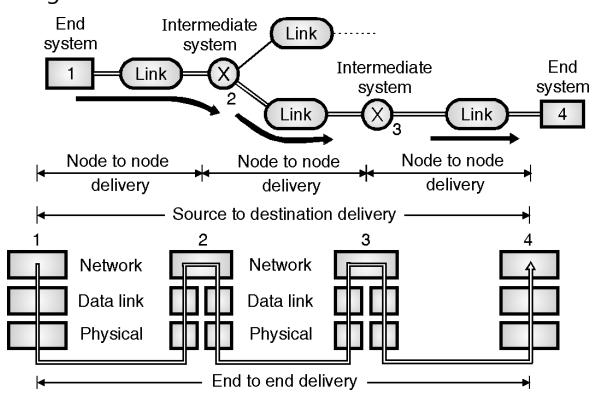
- The main function of this layer is to deliver packets from source to destination across multiple networks (links).
- If two systems are connected on the same link, then the network layer may not be needed.
- The relationship of the network layer to the data link and transport layer is shown in Fig. 2.4.7.



(G-65) Fig. 2.4.7 : Network layer

Functions of the network layer :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.
- The network layer carries out the end to end (source to destination) delivery and routing. This is illustrated in Fig. 2.4.8.



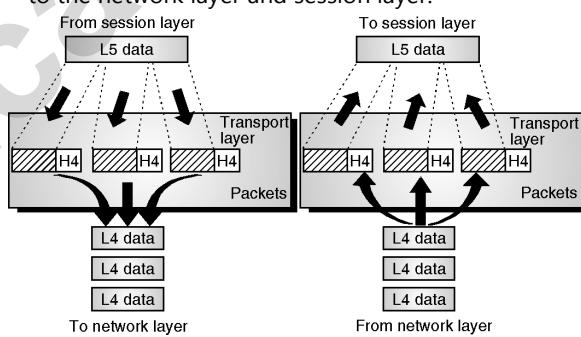
(G-66) Fig. 2.4.8

- The sequence of events takes place as follows :

1. Network layer of end system-1 (source) sends the packet to the network layer of intermediate system-2 which is a router.
2. The router (2) decides the next node to which this packet should be sent on the basis of the final destination. The next hop is the router (3). The network layer of 2 forward the packet to the network layer of router 3.
3. The network layer of 3 (which is again a router) will direct the packet to the network layer of end system-4.

2.4.10 Transport Layer :

- The function of the transport layer is the process to deliver the entire message.
- It ensures that the whole message reaches the destination intact and in order, with both error control and flow control incorporated at the source and destination.
- Fig. 2.4.9 shows the relationship of the transport layer to the network layer and session layer.



(G-67) Fig. 2.4.9 : Transport layer

Functions of transport layer :

- The transport layer performs the following functions :
- 1. It divides each message into packets at the source and re-assembles them at the destination.
- 2. The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.
- 3. The transport layer is capable of either connectionless or connection-oriented transfer of data.
- 4. It performs end to end flow control. Flow control is an important function of the transport layer.
- 5. It makes sure that the entire message arrives at the receiving transport layer without error.



2.4.11 The Session Layer :

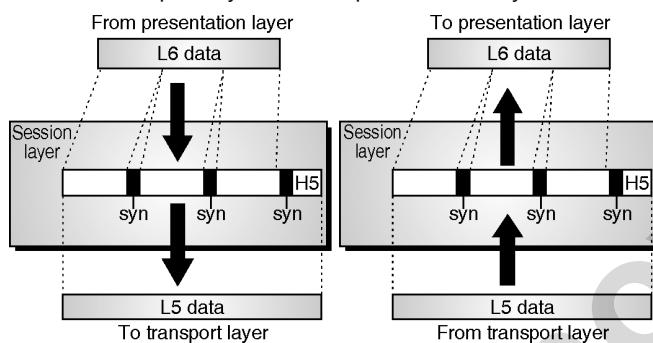
SPPU : Dec. 06

University Questions

- Q. 1** What are the functions of the session and the presentation layer of the OSI model ?

(Dec. 06, 6 Marks)

- The main function of this layer is to establish, maintain and synchronize the communication between interested systems.
- Fig. 2.4.10 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) Fig. 2.4.10 : Session layer

Functions of sessions layer :

- The session layer performs the following functions :
- It allows two systems to start a dialog. The communication between two processes will take place either in half duplex or full duplex mode.
- The other function of this layer is synchronization.
- The session layer is not inherently concerned with security and the network logon process.
- The primary functions of this layer is exchange of messages between two interested systems called as a **dialog**.
- Infact 22 different services are provided by the session layer. These are grouped into subsets such as the Kernel Function Unit, the Basic Activity Subset and the Basic Synchronization Subset.
- However the two most important services provided by the session layer are :
 1. Dialog control and 2. Dialog separation

1. Dialog control :

- Dialog control is the means by which a sending and receiving systems initiate a dialog, exchange messages and finally end the dialog.

2. Dialog separation :

- It is a process of inserting a reference marker called as a checkpoint into the data stream travelling between the sending and receiving systems.
- This allows the checking of status of both the machines at the same point in time.
- This will avoid any possible confusion and collision situation.

2.4.12 Presentation Layer :

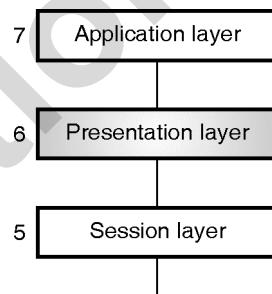
SPPU : Dec. 06

University Questions

- Q. 1** What are the functions of the session and the presentation layer of the OSI model ?

(Dec. 06, 6 Marks)

- The presentation layer is the 6th layer the OSI model as shown in Fig. 2.4.11.



(G-707) Fig. 2.4.11 : Position of presentation layer

- Above it there is the application layer and below it there is the sessions layer.
- The presentation layer is related to the **syntax** and **semantics** of the information being exchanged between the interested systems.
- Some of the important responsibilities of the presentation layer are :
 1. Translation
 2. Encryption
 3. Compression.

1. Translation :

- The communication systems usually exchange the information in the form of strings of characters, numbers etc.
- This information needs to be changed into bit streams before transmission.



- This is essential because different systems use different encoding techniques. The presentation layer does the job of translation.
- The presentation layer at the sending end converts the information into a common format and the presentation layer at the receiving end will convert this common format into the one which is compatible to the receiver.

2. Encryption :

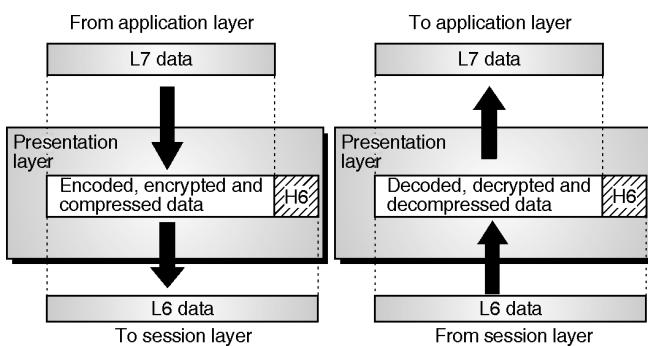
- For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential.
- Encryption is carried out at the sending end. In the encryption process, the sender transforms the original information to another form, and sends the transformed information.
- At the receiving end, an exactly opposite process called Decryption is carried out in which the received information is transformed back to its original form.
- Encryption and Decryption are carried out by the presentation layer.

3. Compression :

- The data compression technique is used for reducing the number of bits required to send an information.
- Data compression is essential for transmission of multimedia such as text, audio and video.

Relation with application and session layers :

- The relation of presentation layer with the application layer and session layer is illustrated in Fig. 2.4.12.



(G-69) Fig. 2.4.12 : Relation of presentation layer with the application layer and session layer

- The data from the application layer (L7 data) is encrypted, encoded and compressed at the presentation layer. A presentation layer header H-6 is also added as shown in Fig. 2.4.12.
- This is then sent to the session layer as L-6 data. These processes take place at the sending end of the system.
- While receiving the data from session layer, the operations carried out by the presentation layer are exactly opposite to those carried out while transmitting.
- The received data from the session layer undergoes decryption, decompression and decoding at the presentation layer.
- The header H-6 is detached from the data and then the L-7 data is sent to the application layer.

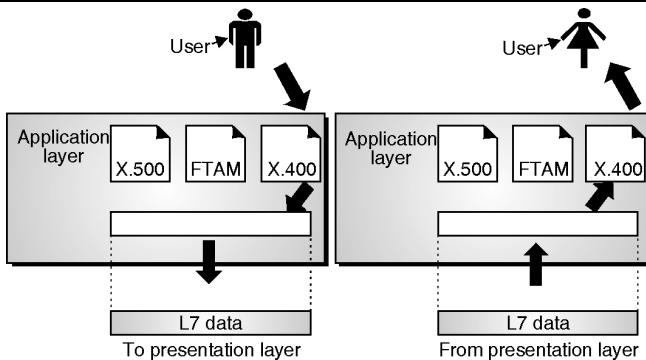
Functions of presentation layer :

The presentation layer performs the following function :

1. It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIC).
2. It does the protocol conversion.
3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
4. It carries out data compression to reduce the bandwidth of the data to be transmitted.
- Unlike the session layer, which provides many different functions, the presentation layer has only one function.
- It basically functions as a pass through device. It receives primitives from the application layer and issues duplicate primitives to the session layer below it, using the Presentation Service Access Point (PSAP) and Session Service Access Point (SSAP).

2.4.13 Application Layer :

- It is the topmost layer of OSI model. It provides services that directly support user application such as database access, e-mail and file transfer.
- It allows applications on one computer to communicate with applications on other computers as though they were on the same computer.
- The relationship of the application layer to the user and the presentation layer is shown in Fig. 2.4.13.



(G-70) Fig. 2.4.13 : Application layer

Functions of application layer :

- The application layer performs the following functions :

 1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
 2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
 3. It creates a basis for forwarding and storage of e-mails.

2.4.14 Merits of OSI Reference Model :

1. It distinguishes very clearly between the services, interfaces and protocols.
2. The protocols in OSI model are better hidden. So they can be easily replaced by new protocols as the technology changes.
3. OSI model is truly a general model.
4. This model supports connection oriented as well as connectionless services.

2.4.15 Demerits of OSI Model :

1. Sessions and presentation layers are not of much use.
2. This model was devised before the protocols were invented. So in real life there is a problem of fitting protocol into a model.

2.5 TCP/IP Model :

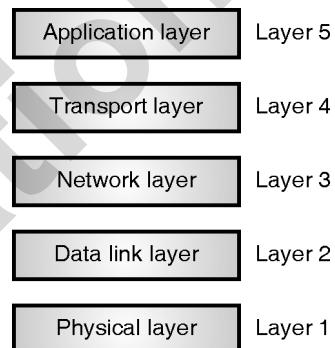
SPPU : Dec. 10, Dec. 15

University Questions

- Q. 1** Describe in brief the TCP/IP protocol stack along with the layered representation. (Dec. 10, 4 Marks)

Q. 2 Explain TCP/IP protocol suite with layered architecture. (Dec. 15, 6 Marks)

- TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol.
- A **protocol suite** is defined as the set of protocols organized in different layers.
- The TCP/IP protocol suite is used in Internet today.
- TCP/IP is a hierarchical protocol suite means that each upper layer protocol receives support and services from either one or more lower level protocols.
- In the original TCP/IP protocol suite, there were four software layers built upon the hardware.
- But today's TCP/IP protocol suite uses a five layer model as shown in Fig. 2.5.1.



(G-2065) Fig. 2.5.1 : Layers in TCP/IP protocol suite

2.5.1 Introduction to TCP/IP :

- The Internet protocol is like any other communication protocol is a set of rules which will govern every possible communication over the internet.
- TCP/IP together has emerged as the controlling body. It is being used in computers of not only in the U.S. but all over the world for all the types and sizes of computers.
- It has become the language of the Internet.
- TCP/IP are two protocols : Transmission control protocol and Internet protocol.
- These two protocols describe the movement of data between the host computers on Internet.
- The protocol however is a suite of many other protocols which provide for reliable communications across the Internet and the web.



- In the TCP/IP protocol suite, there are various layers, with each layer being responsible for different facets of communication.
- The Internet Protocol (IP) and Transmission Control Protocol (TCP) are together known as TCP/IP protocol.
- TCP/IP offers a simple naming and addressing scheme whereby different resources on Internet can be easily located.
- Information on Internet is carried in "packets". The IP protocol is used to put a message into a "packet".
- Each packet has the address of the sender and the recipient's address. These addresses are known as the IP addresses.
- Using the TCP protocol, a single large message is divided into a sequence of packets and each is put into an IP packet.
- The packets are passed from one network to another until they reach their destination.
- At the destination the TCP software reassembles the packets into a complete message.
- It is not necessary for all the packets in a single message to take the same route each time it is sent.

2.5.2 Overview of TCP/IP Architecture :

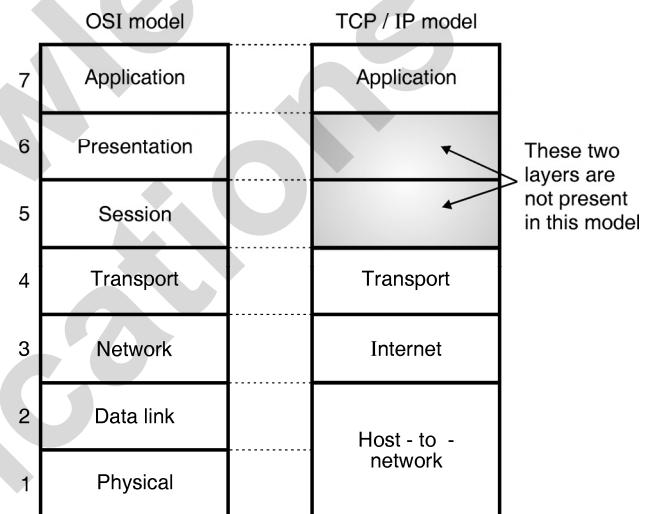
SPPU : Dec. 10, Dec. 15

University Questions

- Q. 1** Describe in brief the TCP/IP protocol stack along with the layered representation. (Dec. 10, 4 Marks)
- Q. 2** Explain TCP/IP protocol suite with layered architecture. (Dec. 15, 6 Marks)

- Transmission Control Protocol and the Internet Protocol (TCP/IP) was developed by the Department of Defence's Projects Research Agency (ARPA, later DARPA) under its project on network interconnection.
- It is a set of protocols that allow communication across multiple diverse network.
- TCP/IP was originally developed to connect military networks together, but later on this protocol was also given to government agencies and universities free of cost.
- Since the TCP/IP was developed for military use, it became robust to failures and flexible to different types of networks.

- TCP/IP is the most widely used protocol for interconnecting computers and it is the protocol of the Internet.
- TCP/IP became the standard for interoperating Unix Computers, especially in military and university environments.
- With the development of the Hypertext Transfer Protocol (HTTP) for sharing Hypertext Markup Language (HTML) documents freely on the internet, the World Wide Web (WWW) was born and soon TCP/IP came into much use.
- Fig. 2.5.2 shows the TCP/IP reference model along with the OSI model used for comparison.



(G-71)Fig. 2.5.2 : TCP/IP reference model

2.5.3 Description of TCP/IP Model :

SPPU : May 09, Dec. 10, May 11, May 13, May 14, May 15, May 18

University Questions

- Q. 1** Explain the TCP/IP protocol stack. (May 09, 8 Marks)
- Q. 2** Describe in brief the TCP/IP protocol stack along with the layered representation. (Dec. 10, 4 Marks)
- Q. 3** Explain TCP/IP protocol suites. (May 11, 8 Marks)
- Q. 4** Explain TCP/IP protocol suit in detail. (May 13, 8 Marks)
- Q. 5** Explain TCP/IP protocol suite. (May 14, 7 Marks)
- Q. 6** Write a short note on TCP/IP protocol stack. (May 15, May 18, 5 Marks)



- As shown in Fig. 2.5.3, the TCP/IP model has only four layers.

Application layer	Telnet, FTP, SMIP, DNS, HTTP NNTP
Transport	TCP UDP
Internet (network)	IP
Host-to-network	Arpanet, satnet lan, paket radio

(G-2706) Fig. 2.5.3

Internet layer :

- This layer is called as the internet layer and it holds the whole architecture together.
- The task of this layer is to allow the host to insert packets into any network and then make them travel independently to the destination.
- The order in which the packets are received can be different from the sequence in which they were sent.
- Then the higher layers are supposed to arrange them in the proper order.
- Note that "internet" is being used as a generic term.
- The internet layer defines (specifies) a packet format and a protocol called Internet Protocol (IP).
- The internet layer is supposed to deliver IP packets to their destinations.
- So routing of packets and congestion control are important issues related to this layer.
- Hence TCP/IP internet layer is very similar to the network layer in OSI model as shown in Fig. 2.5.2.

Transport layer :

- This is the layer above the internet layer. Its functions are same as those of a transport layer in OSI model.
- This layer allows the peer entities of the source and destination machines to converse with each other.
- The end to end protocols used here are TCP and UDP (User Datagram Protocol).
- TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine without introducing any errors.

- TCP also handles the flow control.
- UDP (User Datagram Protocol) is the second protocol used in the transport layer.
- It is an unreliable, connectionless protocol and used for the applications which do not want the TCP's sequencing or flow control.
- UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting speech or video.

Application layer :

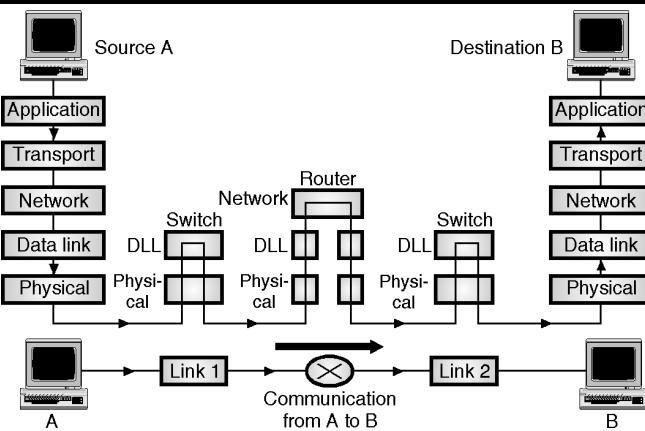
- TCP/IP model does not have session or presentation layers, because they are of little importance in most applications.
- The layer on top of transport layer is called as application layer.
- The protocols related to this layer are all high level protocols such as virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP) as shown in Fig. 2.5.3.
- Many other protocols have been added to these, over the years such as Domain Name Service (DNS), NNTP and HTTP etc.

Host-to-network layer :

- This is the lowest layer in TCP/IP reference model.
- The host has to connect to the network using some protocol, so that it can send the IP packets over it.
- This protocol varies from host to host and network to network.

2.5.4 Communication through Internet :

- In order to understand how the communication takes place between various layers of TCP/IP protocol suite, we have considered a small internetwork consisting of three LANs (links) with all LANs connected to each other via a router as shown in Fig. 2.5.4.
- In Fig. 2.5.4, there are two computers A and B communicating with each other and three more devices namely : the link layer switch in link-1, the router and the link layer switch in link-2.
- Computer A is called as the **source host** and computer B is called as the **destination host**.



(G-2176) Fig. 2.5.4 : Communication through an Internet

- Each device in the Internet has a specific role to play, depending on which each device uses a set of layers as shown in Fig. 2.5.4.
- All the five layers are involved in communication for the source and destination hosts A and B respectively.
- At the source host, a message is created at the application layer and then it is sent in down the layers in order to physically send it to the destination host.
- At the destination host this message is received at the physical layer and then it is delivered to the application layer via the other layers between the physical and application layers.
- At the router, as shown in Fig. 2.5.4 only three layers of TCP/IP protocol suite are needed to be involved.
- Thus a router does not need the transport or application layers when it is being used only for routing.
- The router is connected to multiple links. At each link we use a switch which involves only two layers of the TCP/IP protocol suite as shown in Fig. 2.5.4.
- However note that the link layer and physical layer protocols used by each link can be completely different.
- Thus the router may have to receive a packet from link-1 based on one pair of protocol and may have to deliver a packet to link-2 based on a totally different pair of protocols.
- Now consider a switch in Fig. 2.5.4 which shows that it has two different connections.
- But both of them belong to the same link. Therefore two different protocol pairs will not be involved.
- A switch has to deal with only one pair of DLL and physical layer protocols.

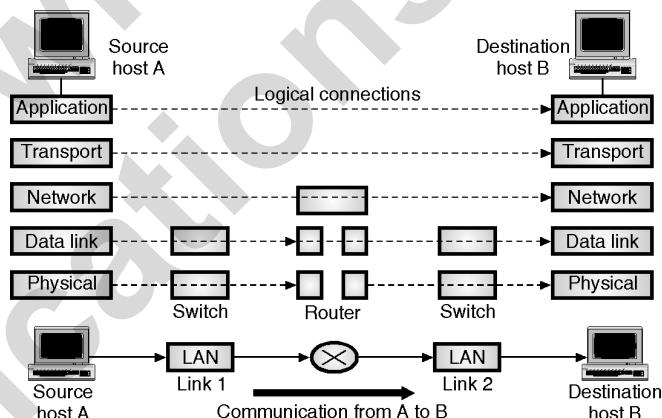
2.5.5 Logical Connections :

SPPU : Dec. 10, Dec. 15

University Questions

- Q. 1** Describe in brief the TCP/IP protocol stack along with the layered representation. (Dec. 10, 4 Marks)
- Q. 2** Explain TCP/IP protocol suite with layered architecture. (Dec. 15, 6 Marks)

- Now we are going to discuss the functions and duties of various layers in the TCP/IP protocol suite.
- In this section, we will think about the logical connections between various layers, so as to clearly understand the duties of each layer.
- The logical connections in a simple internetwork have been shown in Fig. 2.5.5.



(G-2177) Fig. 2.5.5 : Logical connections between the layers of TCP/IP suite

- Each layer has some specific duties and we can use the logical connections to think about them easily.
- From Fig. 2.5.5 it is clear that the network, transport and application layers have an **end-to-end** duty.
- But the data link and physical layers have the **hop to hop** duty. (Hop is a host or router).
- In this way the upper three layers have a **domain of duty** of the entire Internet while the lower two have a domain of duty of only link.

Data unit created by every layer :

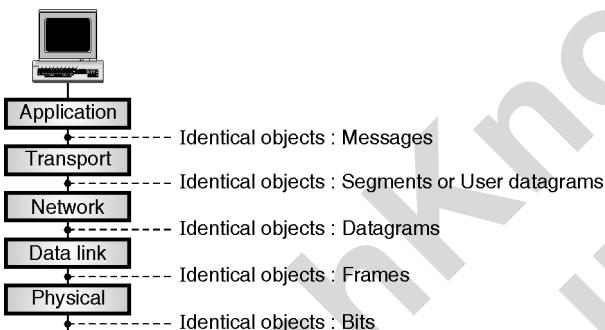
- We can think about the logical connections in a different way i.e. in terms of the **data unit** created by each layer.
- The names of data units (packets) created by different layers are as follows :



Layer	Data unit
Application	Message
Transport	Segment
Network	Datagram
Layer	Data unit
Datalink	Frame
Physical	Bits

(G-2714)

- The data unit (packet) created by the top three layers, should not be changed by a router or a link layer switch.
- However the data unit created at the lower two levels can be changed only by the router. The link layer switches cannot modify it.
- The second principle that we discussed for the protocol layering has been shown in Fig. 2.5.6. Note that the objects shown below each layer related to each device are identical.



2.6 Detailed Description of Each Layer in TCP/IP :

- In this section we are going to discuss the duties of various layers in TCP/IP.

2.6.1 Physical Layer :

- Physical layer is the lowest layer in the TCP/IP protocol suite. The communication at the physical layer level is still **logical** because of the presence of a hidden layer (transmission media) under the physical layer.
- The **primary responsibility** of the physical layer is to carry the individual bits present in a frame across the link.
- The transmission media (wired or wireless) is used for connecting two devices to each other. Here it is

important to understand that the transmission media does not actually carry the bits.

- Instead it carries the electrical or optical signals which represents the bits which are to be carried from one device to the other.
- That means the bits received in a frame from the data link layer are transformed into an electrical or optical signal and sent over the transmission media.
- Still we consider **bit** as the data unit for communication between physical layers of two communicating devices.
- For the transformation of bits to signal, several physical layer protocols are available.

Functions :

- Following are the functions of the physical layer :
- 1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
- 2. To define the transmission rate i.e. the number of bits transmitted per second.
- 3. To deal with the synchronization of the transmitter and receiver.
- 4. To deal with network connection types, including multipoint and point-to-point connections.
- 5. To deal with physical topologies i.e. bus, star, ring, or mesh.
- 6. To deal with the media bandwidth i.e. baseband and broadband transmission.
- 7. Multiplexing which deals with combining several data channels into one.
- 8. To define the characteristics between the device and the transmission medium.
- 9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

Devices :

- Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.



2.6.2 Data Link Layer :

- An internetwork consists of many LANs and WANs, connected to each other by routers.
- While travelling from source to destination a datagram has to travel through many overlapping sets of links.
- It is the responsibility of router to choose the best possible link for a datagram to travel.
- When a router does so, it is the responsibility of the data link layer to take the datagram across the link.
- The said link can be anything such as a wired LAN, a wireless LAN, or a link layer switch etc.
- Every type of link will use different types of protocols. The data link layer should be able to handle all the different types of protocols and move the packet through the link.
- The data link layer receives a datagram from the network layer and encapsulates it into a packet called as **frame**.
- There are no specific data link layer protocols defined by the TCP/IP suite.
- Instead it supports all the standard protocols that can carry the datagram successfully over the link.
- The services provided by each data link layer protocol are different.

Functions :

- Following are the functions of data link layer :
 1. **Framing :**
 - The bits received from the network layer are divided into another type of data units called frames at the data link layer.
 2. **Flow control :**
 - It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.
 3. **Physical addressing :**
 - It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. Error control :

- A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. Access control :

- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :
 1. Logical Link Control (LLC).
 2. Media Access Control (MAC).

2.6.3 Network Layer :

- The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication.
- The several routers present between the source and destination hosts choose the best route for each travelling packet.
- Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.
- The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP.
- The routing of datagrams from their source to destination is also the responsibility of IP.
- It achieves this by making each router forward the datagrams to the next router in its path towards the destination.
- IP is a **connectionless** protocol. It does not provide services like **flow control**, **error control** or even the **congestion control**.
- Therefore it is dependent on the transport layer in case if an application needs these services.
- The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.



- These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.
- There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks.
- The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.

Functions :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

2.6.4 Transport Layer :

- The primary responsibility of the transport layer is also to provide an end to end connection.
- At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.
- In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination.
- For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.

- The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol.
- The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data.
- Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :
 1. Flow control
 2. Error control and
 3. Congestion control
- The other commonly used transport layer protocol is UDP (User Datagram Protocol).

Functions :

- The transport layer performs the following functions :
 1. It divides each message into packets at the source and re-assembles them at the destination.
 2. The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.
 3. The transport layer is capable of either connectionless or connection-oriented transfer of data.
 4. It performs end to end flow control. Flow control is an important function of the transport layer.
 5. It makes sure that the entire message arrives at the receiving transport layer without error.

2.6.5 Application Layer :

- The logical connection between the application layers of source and destination hosts is **end-to-end** type.
- The communication between the application layers of source and destination hosts takes place through all the layers.
- The application layer communication is between **two processes**. A process is nothing but a program running at the application layer.
- Thus the primary responsibility of the application layer is the **process to process communication**.
- There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc.



Functions :

- The application layer performs the following functions :

 1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
 2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
 3. It creates a basis for forwarding and storage of e-mails.

2.6.6 TCP/IP Model with Protocol :

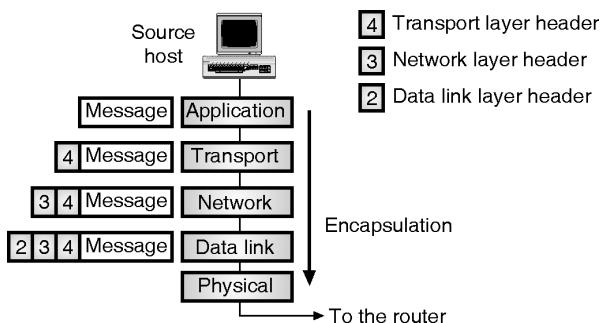
Layer Name	Protocol Supported
Application Layer	DNS, HTTP, Telnet, SSH, FTP, TFTP, SNMP, SMTP, DHCP, X Windows, RDP.
Transport Layer	TCP and UDP
Internet Layer	IP, ICMP, ARP, RARP andIGMP
Link or Network Access Layer	Ethernet, Token Ring, FDDI, X.25, Frame Relay

2.7 Encapsulation and Decapsulation :

- The encapsulation / decapsulation is one of the most important concepts in the protocol layering in Internet.
- This concept applied to a small Internet has been illustrated in Fig. 2.7.1.
- In this figure, the layers of data link switches have not been shown because encapsulation or decapsulation does not take place in the data link layer switches.
- In Fig. 2.7.1, the encapsulation takes place at the source host, decapsulation takes place at the destination host while both encapsulation and decapsulation takes place at the router.

2.7.1 Encapsulation at the Source Host :

- Refer Fig. 2.7.1(a) to understand the process of encapsulation at the source host.



(G-2066) Fig. 2.7.1(a) : Encapsulation at the source host

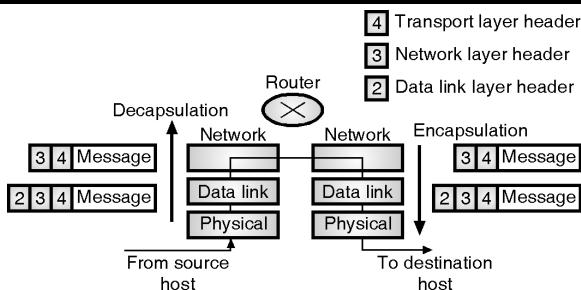
- The data to be exchanged at the application layer is called as **message**.
- Normally a message does not contain any header or trailer. This message is passed on to the transport layer.
- The transport layer takes this message which is also called as the **payload** and adds a transport layer header to it to produce the **segment of user datagram**.
- It is then passed on to the network layer.
- The transport layer header consists of the identifiers of the application programs at the source and destination and some additional information needed for the flow control, error control and congestion control.
- The packet from transport layer is accepted by the network layer as its payload and adds its own header to it to produce a **datagram** as shown in Fig. 2.7.1(a).
- The network layer header contains the source and destination host's addresses and some additional information needed for checking errors in the header.
- This network layer packet (datagram) is then passed on to the data link layer.
- The packet from the network layer is taken by the data link layer as its payload and adds its own header to it to produce a **frame** (packet at the data link layer).
- The link layer header contains the link layer addresses of the host or the next hop i.e. the router. This **frame** is then passed on to the physical layer for transmission.

2.7.2 Decapsulation and Encapsulation at the Router :

- Refer Fig. 2.7.1(b) which illustrates the processes of decapsulation and then encapsulation occurring at a router connected to two or more links.

1. Decapsulation :

- The router receives a set of bits at its input port.
- When these bits are delivered to the data link layer at the router, it decapsulates the datagram from the frame as passes it on to the network layer.

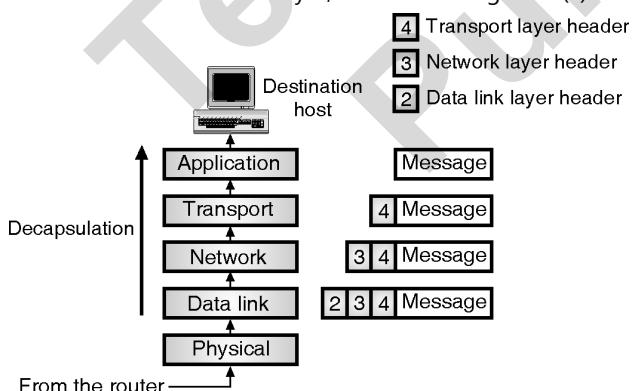


(G-2067) Fig. 2.7.1(b) : Decapsulation / Encapsulation at the router

- The router checks the header for source and destination addresses.
- Then it refers to its forwarding tables and finds out the next hop to which this datagram is to be forwarded.
- Note here that the network layer at the router should not change the contents of the datagram unless fragmentation of the datagram is needed.
- Fragmentation is done if the datagram is too large in size. After all this, the datagram is passed to the data link layer.
- At the data link layer, the datagram received from the network layer is encapsulated again into a frame and the frame is passed on to the physical layer which transmits it to the destination host.

2.7.3 Decapsulation at the Destination Host :

- At the destination host, only the decapsulation process is carried out at each layer, as shown in Fig. 2.7.1(c).



(G-2068) Fig. 2.7.1(c) : Decapsulation at the destination host

- At each layer, the payload is removed from the packet and the payload is delivered to the higher layer, by removing the headers at each stage.
- Finally after removing all the headers, the message is delivered to the application layer.

- It is important to note that the **error checking** is involved in the process of decapsulation at the destination host.

2.8 Addressing in TCP/IP :

SPPU : Dec. 11, May 12, Dec. 12, Dec. 14, Dec. 15, May 17, Dec. 18 Dec. 19

University Questions

- Q. 1** Explain various addresses in TCP/IP protocol suite. **(Dec. 11, May 12, 8 Marks)**
- Q. 2** Explain four levels of addresses used in an Internet. Draw the diagram to show the relationship of layers and addresses in TCP/IP. **(Dec. 12, 8 Marks)**
- Q. 3** Explain different addressing schemes in TCP/IP model. **(Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19, 6 Marks)**

- Addressing is another important concept related to the protocol layering in the Internet.
- There is a logical connection between the pair of layers as discussed earlier.
- For any communication to take place between a source and a destination, two addresses namely source address and destination address are needed.
- Thus we will need four pairs of such addresses corresponding to the data link, network, transport and application layers.
- There is no need of addresses at the physical layer because communication at the physical layer takes place in bits which cannot have an address.
- Fig. 2.8.1 shows the addressing at each layer.

Packet name	Layers	Address
Message	Application	Names
Segment/User datagram	Transport	Port numbers
Datagram	Network	Logical addresses
Frame	Data link	Link layer addresses
Bits	Physical	No address needed

(G-2069) Fig. 2.8.1 : Addressing in TCP/IP protocol suite

- Fig. 2.8.1 also shows the relationship between various layers, the addresses used in each layer and the name of the packet at each layer.



- When the computers wish to communicate with one another, they need to know the address of each other. Each computer has its own address.
- The addresses can be of different types such as physical addresses or logical address.
- In an internet employing the TCP/IP protocols, four levels of addresses are used by the computers.
 - Physical address
 - Logical address (IP)
 - Port address and
 - Specific address

2.8.1 MAC Address (Physical Address) :

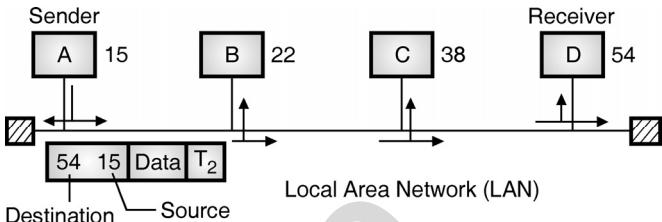
**SPPU : Dec. 11, May 12, Dec. 14, Dec. 15,
May 17, Dec. 18, Dec. 19**

University Questions.

- Q. 1** Explain various addresses in TCP/IP protocol suite. **(Dec. 11, May 12, 8 Marks)**
- Q. 2** Explain different addressing schemes in TCP/IP model. **(Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19, 6 Marks)**

- The packets from source to destination hosts pass through physical networks.
- At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time.
- Similarly a packet may pass through different physical networks.
- So to deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.
- The size and format of the physical address varies depending on the nature of network.
- The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is imprinted on the network interfacing card (NIC).

- Refer Fig. 2.8.2 which explains the concept of physical addressing.



(G-77) Fig. 2.8.2 : Physical addresses

- The sender computer with a physical address of 15 wants to communicate with the receiver computer with a physical address 54.
- The frame sent by the sender consists of the destination address, sender's address, encapsulated data and a trailer (T₂) that contains the error control bit.
- When this frame travels over the bus topology, every computer receives it and tries to match it with its own physical address.
- If the destination address in the frame header does not match with the physical address it will simply drop the frame.
- At receiver computer (D), the destination address matches with its physical address (54). So the frame is accepted and decapsulation is carried out to recover the data.
- The example of a 48 bit or 6 byte physical address is as follows. It contains 12-hexadecimal digits.

08 : 63 : 4C : 81 : 08 : 1D

2.8.2 Logical Addresses (IP Addresses) :

**SPPU : Dec. 11, May 12, Dec. 14, Dec. 15,
May 17, Dec. 18, Dec. 19**

University Questions

- Q. 1** Explain various addresses in TCP/IP protocol suite. **(Dec. 11, May 12, 8 Marks)**
- Q. 2** Explain different addressing schemes in TCP/IP model. **(Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19, 6 Marks)**

- Logical addresses are required to facilitate universal communications in which different types of physical networks can be involved.
- The logical address is also called as the IP (Internet Protocol) address.



- The internet consists of many physical networks interconnected via devices like routers.
- Internet is a packet switched network that means the data from the source computer is sent in the form of small packets carrying the destination address upon them.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognised by their **IP addresses** or logical addresses.
- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.
- The logical address used in internet is currently a 32-bit address. The same IP address can never be used by more than one computer on the Internet.

2.8.3 Port Address :

SPPU : Dec. 11, May 12, Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19

University Questions

- Q. 1** Explain various addresses in TCP/IP protocol suite. **(Dec. 11, May 12, 8 Marks)**
- Q. 2** Explain different addressing schemes in TCP/IP model. **(Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19, 6 Marks)**

- The modern computers are designed to run multiple processes on it simultaneously.
- The main objective of internet is the process to process communication. For this purpose it is necessary to label or name the processes.
- Thus the processes need addresses. The label assigned to a process is called as a **port address**. It is a 16 bit address.

2.8.4 Specific Addresses :

SPPU : Dec. 11, May 12, Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19

University Questions.

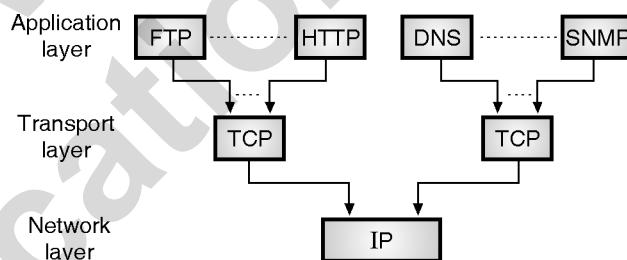
- Q. 1** Explain various addresses in TCP/IP protocol suite. **(Dec. 11, May 12, 8 Marks)**

Q. 2 Explain different addressing schemes in TCP/IP model. **(Dec. 14, Dec. 15, May 17, Dec. 18, Dec. 19, 6 Marks)**

- Some applications have user friendly addresses. The examples of specific addresses are the e-mail addresses or the University Resource Locators (URL).

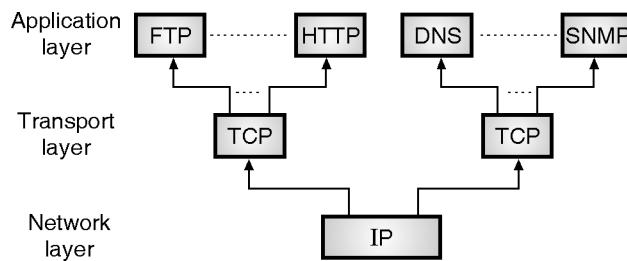
2.9 Multiplexing and Demultiplexing in TCP / IP :

- In TCP/IP protocol, many protocols are being used at the same layer.
- Therefore multiplexing is needed at the source and demultiplexing is needed at the destination.
- In the process of **multiplexing** as shown in Fig. 2.9.1(a), a protocol at one layer in TCP/IP can encapsulate a packet (one at a time) from several protocols corresponding to the next higher layer in TCP/IP suite.



(G-2070) Fig. 2.9.1(a) : Multiplexing in TCP/IP

- In the process of **demultiplexing**, a protocol will decapsulate and deliver a packet one at a time to several protocols belonging to the next higher layer in TCP/IP protocol suite as shown in Fig. 2.9.1(b).



(G-2071) Fig. 2.9.1(b) : Demultiplexing in TCP/IP

- As shown in Fig. 2.9.1(a), at the transport layer two protocols TCP and UDP are capable of multiplexing the messages coming from various protocols at the application layer.
- Next the segments from TCP or user datagrams from UDP are accepted and multiplexed by IP at the network layer.



- IP can also multiplex the packets from some other protocols such as ICMP or IGMP etc.
- The frames at the data link layer level can carry the payload coming from the network layer protocols such as IP or ARP etc.

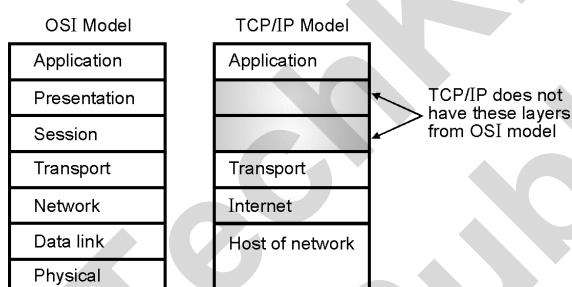
2.10 Comparison of OSI and TCP/IP :

2.10.1 Similarities between OSI and TCP/IP Models :

- Following are some of the similarities between OSI and TCP/IP models :

 1. In both the models the functions of layers is approximately same.
 2. Both models use the concept of layered architecture.
 3. The transport layers and the layers below it provide transport services independent of networks.
 4. In both the models, the layers above transport layer are application oriented.

- Refer to Fig. 2.10.1 and Table 2.10.1 for the comparison of the two reference models.



(G-73) Fig. 2.10.1 : Relationship between OSI and TCP/IP models

2.10.2 Difference between OSI & TCP/IP :

Table 2.10.1 : Difference between OSI and TCP/IP model

OSI	TCP/IP
Has 7 layers	Has 4 layers
Transport layer guarantees delivery of packets.	Transport layer does not guarantee delivery of packets.
Horizontal approach.	Vertical approach.
Separate session layer.	No session layer, characteristics are provided by transport layer.

OSI	TCP/IP
Separate presentation layer.	No presentation layer, characteristics are provided by application layer.
Network layer provides both connectionless and connection oriented services.	Network layer provides only connection less services.
It defines the services, interfaces and protocols very clearly and makes a clear distinction between them.	It does not clearly distinguish between service, interfaces and protocols.
The protocols are better hidden and can be easily replaced as the technology changes.	It is not easy to replace the protocols.
OSI is truly a general model.	TCP/IP cannot be used for any other application.
It has a problem of protocol fitting into a model.	The model does not fit any other protocol stack.

2.10.3 Demerits of TCP/IP Model :

1. TCP/IP model does not clearly distinguish the concepts of service, interface and protocol.
2. This model is not at all general and it cannot describe any protocol stack other than TCP/IP.
3. The host-to-network layer is not a layer at all in the normal sense. It is simply an interface.
4. The TCP/IP model does not even mention the physical and data link layers. A proper model should include both as separate layers.

2.10.4 Hybrid (Internet) Reference Model :

- In spite of many problems associated with the OSI model, it has proved to be very useful one practically.
- But the OSI protocols have not become popular.
- On the other hand the TCP/IP model is practically non existing but the TCP/IP protocols are used widely.
- So sometimes a modified OSI model with primary concentration on TCP/IP is used which is called as the hybrid model.
- The hybrid model is shown in Fig. 2.10.2. It is also called as the Internet model.



5	Application layer
4	Transport layer
3	Network layer
2	Data link layer
1	Physical layer

(G-2704) Fig. 2.10.2 : Hybrid model

Review Questions

- Q. 1 Draw the OSI reference model and explain the functions of different layers.
- Q. 2 Explain the duties of network layer.
- Q. 3 What is routing ?
- Q. 4 Explain the functions of transport layer.
- Q. 5 Explain flow control at transport layer.
- Q. 6 What are the main duties of the session layer ?
- Q. 7 What is dialog control and dialog separation ?
- Q. 8 Explain the role of presentation layer.
- Q. 9 What is protocol layering ?

- Q. 10 Explain the concept of logical connections.
- Q. 11 Draw the layers of TCP/IP model.
- Q. 12 Explain the layered architecture of TCP/IP model.
- Q. 13 Explain in detail the physical layer in TCP/IP model.
- Q. 14 Explain in detail the data link layer in TCP/IP model.
- Q. 15 Explain in detail the network layer in TCP/IP model.
- Q. 16 Explain in detail the transport layer in TCP/IP model.
- Q. 17 Explain in detail the application layer in TCP/IP model.
- Q. 18 Name any three network layer protocols.
- Q. 19 Explain the TCP / IP reference model
- Q. 20 Compare the OSI and TCP / IP reference models.
- Q. 21 Explain the concept of addressing.
- Q. 22 What is the IP address ?
- Q. 23 What is the difference between IP and MAC address ?
- Q. 24 What is the difference between IP address and port numbers ?

□□□

Unit II

Chapter 3

Error Control Coding

Syllabus

Data link layer : Data link layer services, Error detection and correction : Introduction, Error detection, Error correction, Linear block codes : Hamming code, Hamming distance, Parity check code, Cyclic codes : CRC (Polynomials), Advantages of cyclic codes, Other cyclic codes (Examples : Checksum : Ones complement, Internet checksum).

Chapter Contents

3.1 Introduction	3.8 Error Correction using Block Codes
3.2 Error Detection and Correction	3.9 Linear Block Codes
3.3 Forward Error Correction Versus Retransmission	3.10 Hamming Codes
3.4 Error Correction	3.11 Cyclic Codes
3.5 Coding	3.12 Cyclic Redundancy Check (CRC)
3.6 Linear Block Codes	3.13 Other Cyclic Codes
3.7 Error Detection in Block Coding	

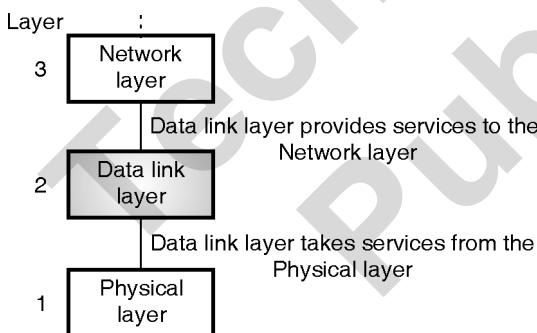


3.1 Introduction :

- The physical layer deals with the transmission of signals over different transmission medias.
- A reliable and efficient communication between two adjacent machines can be achieved via the data link layer.
- This layer basically deals with frame formation, flow control, error control, addressing and link management.
- While sending data from source to destination errors may get introduced.
- The data communication circuits have only a finite data rate and there is non-zero propagation delay between the instant a bit is sent and the instant at which it is received.
- These limitations affect the efficiency of data transfer. The data link layer protocols used for communication take care of all these problems.
- Data link layer is the second layer in OSI reference model. It is above the physical layer.

3.1.1 Position of Data Link Layer :

- Fig. 3.1.1 shows the position of data link layer in the five layer Internet model. It is the second layer.

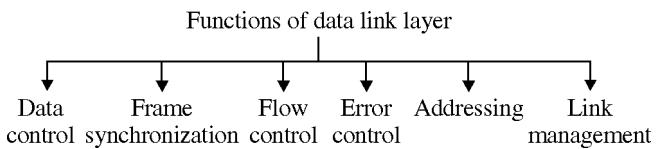


(L-663) Fig. 3.1.1 : Position of data link layer

- It receives services from the physical layer and provides services to the network layer.

3.1.2 Functions of Data Link Layer :

- The data link layer is supposed to carry out many specified functions.
- For effective data communication between two directly (physically) connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows :



(L-664) Fig. 3.1.2 : Functions of data link layer

1. Services provided to the network layer :

- The data link layer provides a well defined service interface to the network layer.
- The principle service is transferring data from the network layer on sending machine to the network layer on destination machine.
- This transfer always takes place via the DLL.

2. Frame synchronisation :

- The source machine sends data in the form of blocks called frames to the destination machine.
- The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. Flow control :

- The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. Error control :

- The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. Addressing :

- When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames.
- This is known as addressing.

6. Control and data on same link :

- The data and control information is combined in a frame and transmitted from the source to destination machine.
- The destination machine must be able to separate out the control information from the data being transmitted.

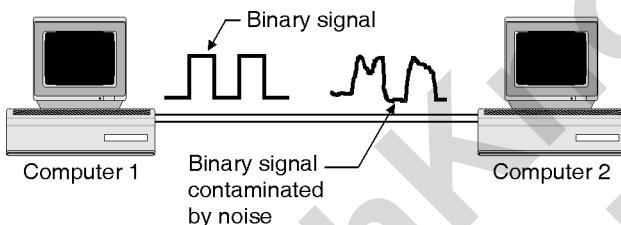


7. Link management :

- The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data.
- It requires co-ordination and co-operation among all the involved stations.
- Protocols or procedures are required to be designed for the link management.

3.1.3 Introduction to Error Control :

- In the real time operating conditions, it is not possible to send a signal from source to destination without introducing any error.
- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 3.1.3, the signal get contaminated due to the addition of "Noise" to it.



(L-302)Fig. 3.1.3 : Noise contaminates the binary signal

- The noise can introduce an error in the binary bits travelling from one system to the other. That means a 0 may change to 1 or a 1 may change to 0.
- These errors can become a serious threat to the accuracy of the digital system. Therefore it is necessary to detect and correct the errors.

3.1.4 Need of Error Control Coding :

- In data communication, errors are introduced during the transmission of data from the transmitter to receiver due to noise or some other reasons.
- The reliability of data transmission will be severely affected due to these errors.
- In order to improve the reliability of data transmission, the designer will have to increase the signal power or reduce the noise spectral density N_o so as to maximize the ratio E_b / N_o .

- But practically there is a limitation on the maximum value of the ratio E_b / N_o . We cannot increase the ratio beyond this limit.
- Hence for a fixed value of E_b / N_o , we have to use some kind of "coding" in order to improve the quality of the transmitted signal.
- Another advantage of using coding is that we can reduce the required value of E_b / N_o if the error rate is predefined and remains fixed at that value.
- This will intern reduce the required transmitted power and the size of antenna.

How to detect and correct errors ?

- For the detection, and / or correction of these errors, one or more than one extra bits are added to the data bits at the time transmitting.
- These extra bits are called as **parity** bits. They allow the detection or sometimes correction of the errors.
- The data bits alongwith the parity bits form a code word.

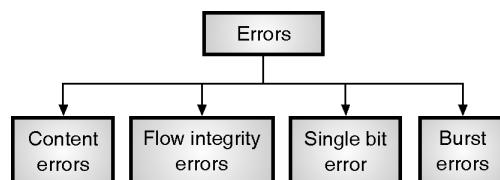
Error control techniques :

- The error control techniques can be divided into two types :
 1. Error detection techniques
 2. Error correction techniques.
- The error detecting techniques are capable of only detecting the errors. They cannot correct the errors.
- The error correcting techniques are capable of detecting as well as correcting the errors.

3.1.5 Types of Errors :

Types of errors :

- Different types of errors have been listed in Fig. 3.1.4.



(L-911) Fig. 3.1.4 : Classification of errors

- The errors introduced in the data bits during their transmission can be categorised as :



1. Content errors
2. Flow integrity errors.

1. Content error :

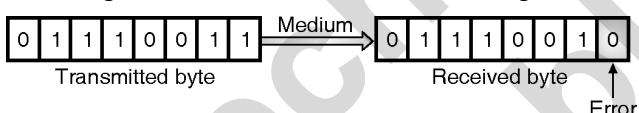
- The content errors are nothing but errors in the contents of a message e.g. a "0" may be received as "1" or vice versa.
- Such errors are introduced due to noise added into the data signal during its transmission.

2. Flow integrity error :

- Flow integrity errors means missing blocks of data. It is possible that a data block may be lost in the network possibly because it has been delivered to a wrong destination.
- Depending on the number of bits in error we can classify the errors into two types as :
 1. Single bit error
 2. Burst errors.

1. Single bit error :

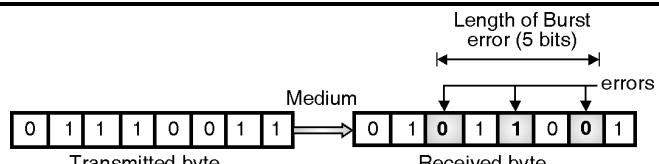
- The term single bit error suggests that only one bit in the given data unit such as byte is in error.
- That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 3.1.5.



(G-188) Fig. 3.1.5 : Single bit error

2. Burst errors :

- If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.
- Refer Fig. 3.1.6 in which the shaded bits in the received byte have been the erroneous bits.
- These are 3 bits but the length of the burst is shown to be of 5 bits.
- The length of the burst error extends from the first erroneous bit to the last erroneous bit.
- Even though some of the bits in between have not been corrupted. The length of the burst error is shown to be 5 bits.
- Burst errors are illustrated in Fig. 3.1.6.



(G-189) Fig. 3.1.6 : Burst errors

3.1.6 Disadvantages of Coding :

- Some of the disadvantages of the coding technique are:
 1. An increased transmission bandwidth is required in order to transmit the encoded signal. This is due to the additional bits (redundancy) added by the encoder.
 2. Use of coding make the system complex.

3.1.7 Redundancy :

SPPU : Dec. 11, May 15, Dec. 15

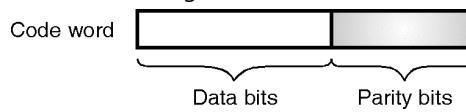
University Questions

- Q. 1** Discuss the concept of redundancy in error detection and correction.

(Dec. 11, May 15, 8 Marks, Dec. 15, 7 Marks)

Definition :

- Redundancy involves transmission of extra bits alongwith the data bits. These extra bits actually do not contain any data or information but they ensure the detection and correction of errors introduced during the data travel from sender to receiver.
- As these extra bits do not contain any information, they are known as redundant bits.
- The redundant bits are also known as **parity check** bits. They are produced from the data bits using some predecided rules.
- The data bits and redundant bits together form a code word as shown in Fig. 3.1.7.



(L-303)Fig. 3.1.7 : Structure of a transmitted code word

Use of redundancy in error detection and correction :

- In the error detection technique such as parity checking we add parity bits so as to make the error detection at the receiver possible.
- In the error correction techniques such as block codes or cyclic codes, $(n-k)$ parity bits are added to k message bits to produce an n bit codeword.



3.2 Error Detection and Correction :

- Detection and correction of errors are the two most important aspects of error control in data communication.
- The correction of errors is more difficult as compared to their detection.
- The process of error detection is much easier because we have to simply find if error is present or absent in the received code word.
- In **error detection** we are not interested even in the number of errors.
- The only question to be answered is whether an error has occurred or not.
- In **error correction**, multiple processes are involved such as detecting the errors, knowing their number, the location of errors and then correcting the erroneous bits.

3.3 Forward Error Correction Versus Retransmission :

- The two most important techniques used for error correction are as follows :
 1. Forward Error Correction (FEC)
 2. Automatic request for retransmission (ARQ).

3.3.1 The ARQ Technique :

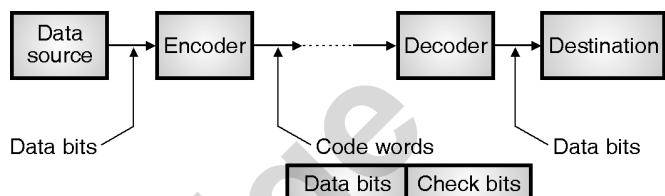
- In the ARQ system, the receiver can request for the retransmission of the complete or a part of message if it finds some error in the received message.
- This needs an additional channel called feedback channel to send the receiver's request for retransmission.

3.3.2 FEC :

- In the FEC technique there is no such feedback path and request for retransmission.
- So error correction has to take place at the receiver.
- In this technique, the receiver tries to guess the transmitted message with the help of the redundant bits (parity bits or code bits).
- This technique is useful only when the number of errors is small.

3.3.3 Error Correction Technique :

- In the error correction techniques, codes are generated at transmitter by adding a group of parity bits or check bits as shown in Fig. 3.3.1.



(L-306) Fig. 3.3.1 : Error correction technique

- The source generates the data (message) in the form of binary symbols.
- The encoder accepts these bits and adds the check (parity) bits to them to produce the code words.
- These code words are transmitted towards the receiver. The check bits are used by the decoder to detect and correct the errors.
- The encoder of Fig. 3.3.1, adds the check bits to the data bits, **according to a prescribed rule**.
- This rule will be dependent on the type of code being used.
- The decoder separates out the data and check bits.
- It uses the parity bits to detect and correct errors if they are present in the received code words.
- The data bits are then passed on to the destination.

3.3.4 FEC (Forward Error Correction) :

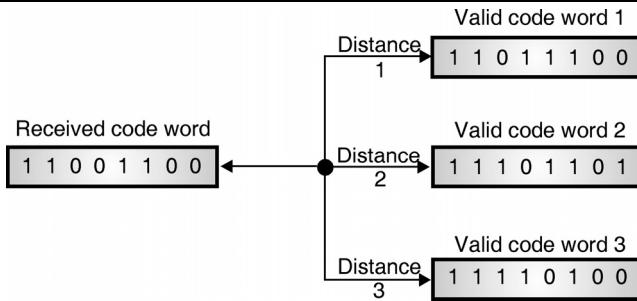
SPPU : May 07

University Questions

- Q. 1** Discuss forward error correction and give an example of 1 bit error correcting code.

(May 07, 4 Marks)

- In FEC the receiver searches for the most likely correct code word.
- When an error is detected, the distance between the received invalid code word and all the possible valid code word is obtained.
- The nearest valid code word (the one having minimum distance) is the most likely the correct version of the received code word as shown in Fig. 3.3.2.



(L-307) Fig. 3.3.2 : Concept of FEC

- In Fig. 3.3.2, the valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

3.4 Error Correction :

- In this section we will discuss the following two error correction techniques :
 - Automatic repeat request (ARQ).
 - Hamming codes.

3.4.1 ARQ Technique (Retransmission) :

SPPU : May 10

University Questions

Q. 1 Explain different ARQ techniques.

(May 10, 8 Marks)

- There are two basic systems of error detection and correction.
- The first one being the Forward Error Correction (FEC) system and the second one is the automatic repeat request (ARQ) system.
- In the ARQ system of error control, when an error is detected, the receiver makes a request for the retransmission of that signal.
- Therefore a feedback channel is required for sending the request for retransmission.

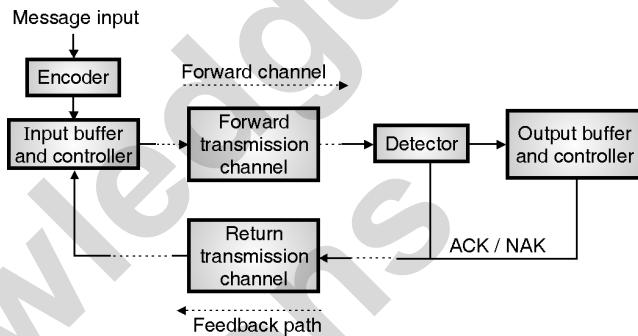
Difference between FEC and ARQ :

- The ARQ systems differ from the FEC systems in three important aspects. They are as follows :
- In ARQ system less number of check bits (parity bits) are required to be sent. This will increase the (k/n) ratio for an (n, k) block code if transmitted using the ARQ system.

- A return transmission path and additional hardware in order to implement repeat transmission of codewords will be needed.
- The bit rate of forward transmission must make allowance for the backward repeat transmission.

Basic ARQ system :

- The block diagram of the basic ARQ system is as shown in Fig. 3.4.1.



(L-372) Fig. 3.4.1 : Block diagram of the basic ARQ system

Operation of ARQ system :

- The encoder produces codewords for each message signal at its input.
- Each codeword at the encoder output is stored temporarily and transmitted over the forward transmission channel.
- At the destination a decoder will decode the code words and search for errors.
- The decoder will send a "positive acknowledgment" (ACK) if no errors are detected and it will output a negative acknowledgment (NAK) if errors are detected, to the transmitter on the return transmission channel.
- On receiving a negative acknowledgment (NAK) signal via the return transmission path the "controller" will retransmit the appropriate word from the words stored by the input buffer.
- A particular word may be retransmitted only once or it may be retransmitted twice or more number of times.
- The output controller and buffer on the receiver side assemble the output bit stream from the code words accepted by the decoder.

Error probability on the return path :

- The bit rate of the return transmission which involves the return transmission of ACK/NAK signal is low as



compared to the bit rate of the forward transmission. Therefore the error probability of the return transmission is negligibly small.

3.4.2 Types of ARQ System :

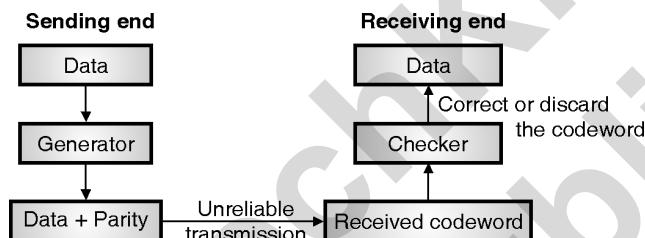
- The three types of ARQ systems are :
 1. Stop-and-wait ARQ system
 2. Go back n ARQ and
 3. Selective repeat ARQ.

Note : Error control in the data link layer is based on the principle of request for automatic retransmission (ARQ) of the missing, lost or damaged frames.

3.5 Coding :

Block diagram :

- Redundancy can be implemented by using various coding schemes.
- The block diagram explaining the coding and decoding processes is shown in Fig. 3.5.1.



(G-1448(a))**Fig. 3.5.1 : Structure of encoding and decoding process**

- At the sending end, redundant bits are added to data word using a well defined process.
- The receiver detects and corrects the errors and makes a decision on whether to accept or discard the received message.
- The two most important factors in any coding scheme are as follows :
 1. Ratio of parity bits to data bits.
 2. How robust the process is.
- The coding schemes can be divided into two types as follows :
 1. Block coding
 2. Convolution coding.

3.5.1 Modular Arithmetic :

- In modular arithmetic only a limited range of integers is used.
- The upper limit is defined as **modulus N**. Then the number of integers used are in the range 0 to $(N - 1)$ inclusive of both.
- Addition and subtraction in modulo arithmetic are simple as there is no carry when you add or subtract two digits in a column.

3.5.2 Modulo – 2 Arithmetic :

- In modulo – 2 arithmetic $N = 2$ so we can use numbers 0 and 1 only. Arithmetic operations in modulo – 2 arithmetic are simple and as given below.

Addition	$0 + 0 = 0$	$0 + 1 = 1$	$1 + 0 = 1$	$1 + 1 = 0$
Subtraction	$0 - 0 = 0$	$0 - 1 = 1$	$1 - 0 = 1$	$1 - 1 = 0$

- Note that addition and subtraction gives the same result.
- In this arithmetic we use the XOR (exclusive OR) gate in order to implement both addition and subtraction.
- The XOR operation produces a 0 output if both the inputs are same (0 or 1) and it produces a 1 output if the inputs are different from each other.

3.6 Linear Block Codes :

SPPU : May 15

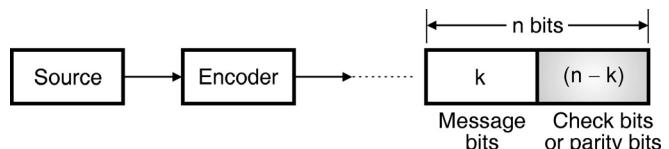
University Questions

Q. 1 Explain linear code block. (May 15, 5 Marks)

- The linear codes are the codes for which addition of any two valid code words in modulo-2 adder to produce a third valid code word in the code.

Generation :

- The generation of block codes is illustrated in Fig. 3.6.1.



(L-316)**Fig. 3.6.1 : Generation of an n bit linear block code**

- To generate an (n, k) block code, the encoder accepts the information in the form of block of successive “ k ” bits.

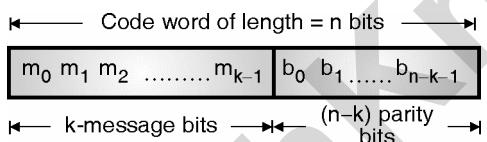
- At the end of each such block (of k message bits) it adds $(n - k)$ parity bits as shown in Fig. 3.6.1.
 - As these bits do not contain any information, they are called as "redundant" bits.
 - It is important to note that the $(n - k)$ parity bits are related algebraically related to the " k " message bits.
 - The n bit code word is thus produced as shown in Fig. 3.6.1.

Why are these codes called linear codes ?

- These codes have an important property that any two code words of a linear code can be added in modulo-2 adder to produce a third code word in the code.
 - Non-linear codes do not exhibit such a property. All the practically used codes are linear codes.

3.6.1 Code Word Structure :

- The code word structure of a linear block code is as shown in Fig. 3.6.2.



(L-317)Fig. 3.6.2 : Structure of the code word for a linear block code

- A code word consists of "k" message bits which are denoted by m_0, m_1, \dots, m_{k-1} and $(n - k)$: parity bits denoted by $b_0, b_1, \dots, b_{n-k-1}$.
 - The sequence of message bits is applied to a linear block encoder to produce an "n" bit code word. The elements of this code word are x_0, x_1, \dots, x_{n-1} .
 - As shown in Fig. 3.6.2, the first k bits of the code word are identical to the corresponding message bits (m_0, m_1, \dots) and the next $(n - k)$ bits are identical to the corresponding parity bits (b_0, b_1, \dots). We can express this mathematically as :

$$\begin{aligned} x_i &= m_i \quad \left\{ \begin{array}{l} i = 0, 1, \dots, k-1 \\ i = k, k+1, \dots, n-1 \end{array} \right. \\ b_{i-k} & \quad \dots \quad (3.6.1) \end{aligned} \quad (\text{G-2325})$$

- The $(n - k)$ parity bits are “linear sums” of the k message bits as will be discussed later on.
 - The code word represented by Equation (3.6.1) can be mathematically represented as :

$$X = [M : B] \quad \dots(3.6.2)$$

where $M = k$ - message bits

and $B = (n - k)$, parity bits

3.7 Error Detection in Block Coding :

SPPU : May 14, Dec. 14, May 18

University Questions.

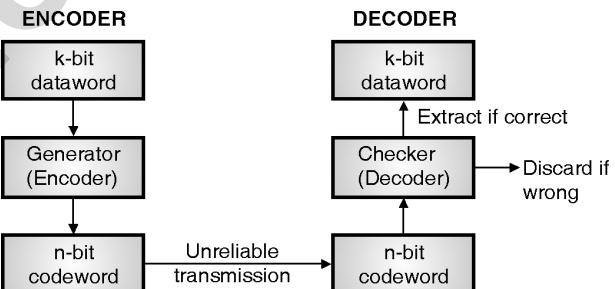
- Q. 1** Explain error detection and correction in block coding. **(May 14, Dec. 14, 6 Marks)**

Q. 2 What are different error detection techniques ? Explain any one with suitable example.

- We can detect errors using **Block coding** if the following conditions are satisfied :
 1. The receiver has a list of all valid codewords with it.
 2. The received code word is different than these valid codewords i.e. if the received codeword is an invalid codeword.

Process of error detection :

- Fig. 3.7.1 explains the process of error detection using the block codes.



(G-1449)Fig. 3.7.1 : Process of error detection in block coding

- The k-bit data words are applied to a generator or encoder.
 - It applies the rules and procedures to encode these bits and generates an n-bit codeword.
 - These code words are transmitted using an unreliable transmission to the receiver.
 - Each transmitted code word may change due to noise while travelling from transmitter to receiver.
 - If the received codeword is same as one of the valid codewords then the receiver extracts the data word and uses it without any change.



- But if the received codeword is not valid, it is discarded. However if a corrupted received codeword matches with a valid codeword then the errors go unnoticed as the receiver treats this codeword as a valid codeword.
- This type of coding can detect only single errors. Multiple errors may remain undetected.

Error detection techniques :

- Some of the error detection techniques are as given below:
 1. Redundancy.
 2. Parity.
 3. Checksum.
 4. VRC, LRC.
 5. CRC.

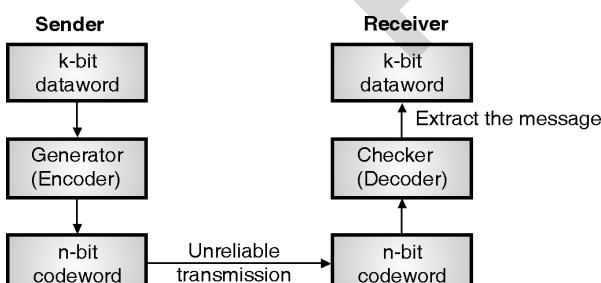
3.8 Error Correction using Block Codes :

SPPU : May 14, Dec. 14

University Questions

Q. 1 Explain error detection and correction in block coding. **(May 14, Dec. 14, 6 Marks)**

- The process of error correction is much more difficult as compared to the error detection.
- In error correction the receiver has to detect the presence of error in the received codeword and correct it too.
- Therefore more redundant bits are required to be sent for error correction than those required for error detection.
- Fig. 3.8.1 explains how block coding can be used for error correction.



(G-1554) **Fig. 3.8.1 : Structure of encoder and decoder in error correction**

- Note that the block schematic of the sender and receiver for error correction is same as that for the error detection but the role of **checker** block is much more complex in error correction process.

3.8.1 Hamming Weight of a Code Word :

Definition :

- The Hamming weight of a code word X is defined as the number of non zero elements in the code word.
- Hamming weight of a code vector (code word) is the distance between that code word and an all zero code vector. (a code having all elements equal to zero).

3.8.2 Hamming Distance :

SPPU : Dec. 11, May 12, May 14

University Questions

Q. 1 What is hamming distance ? What is the minimum hamming distance ? **(Dec. 11, May 12, 4 Marks)**

Q. 2 What is Hamming distance ? Explain it with an example. Explain simple parity check code. **(May 14, 7 Marks)**

Definition :

- Consider two code vectors (or code words) having the same number of elements.
- The “Hamming distance” or simply distance between the two code words is defined as the number of locations in which their respective elements differ. For example consider the two code words given below :

Codeword - 1 :	1	1	1	1	0	1	0	0
	↑	↑	↑	↑	↑	↑	↑	↑
(E-1705)								
Codeword - 2 :	0	1	0	1	1	1	1	0

- Note that the bits 2, 4, 7 and 8 are different from each other. Hence Hamming distance is 4.

Ex. 3.8.1 : Find the Hamming weight of the following code vector :
 $x = 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0$

Soln. :

- As the number of non-zero elements in the above code word is 4, the Hamming weight $W(x) = 4$.

3.8.3 Minimum Hamming Distance d_{min} :

SPPU : May 10, Dec. 11, May 12

University Questions

Q. 1 What is hamming distance ? Explain with example. Explain simple parity check code. **(May 10, 8 Marks)**



- Q. 2** What is hamming distance ? What is the minimum hamming distance ?

(Dec. 11, May 12, 4 Marks)

Definition :

- The minimum distance " d_{min} " of a linear block code is defined as the smallest Hamming distance between any pair of code vectors in the code.
- Therefore the minimum distance is same as the smallest Hamming weight of difference between any pair of code vectors.
- It can be proved that the minimum distance of a linear block code is the smallest Hamming weight of the non-zero code vectors in the code.

Role of " d_{min} " in error detection and correction :

- The error detection is always possible when the number of transmission errors in a code word is less than the minimum distance d_{min} because then the erroneous word is not a valid code word.
- But when the number of errors equals or exceeds d_{min} , the erroneous code word may correspond to another valid code word and errors cannot be detected.
- The error detection and correction capabilities of a coding technique depend on the minimum distance d_{min} as shown in the Table 3.8.1.

Table 3.8.1 : Role of d_{min} for detection and correction of errors

Detect upto "s" errors per word.	$d_{min} \geq (s + 1)$
Correct upto "t" errors per word.	$d_{min} \geq (2t + 1)$
Correct upto "t" errors and detect $s > t$ errors per word.	$d_{min} \geq (t + s + 1)$

- Ex. 3.8.2 :** For a Hamming distance of 5 how many errors can be detected ? How many errors can be corrected ?

May 10, 2 Marks

Soln. :

- Refer to Table 3.8.1. Assuming minimum Hamming distance i.e. $d_{min} = 5$.
- 1. Number of errors that can be detected (s) can be obtained from

$$(s + 1) \leq d_{min}$$

$$\therefore s \leq 5 - 1$$

$$\therefore s \leq 4$$

...Ans.

- Thus at the most 4 errors can be detected.
- 2. Number of errors that can be corrected (t) can be obtained from

$$(2t + 1) \leq d_{min}$$

$$\therefore t \leq 2$$

...Ans.

- Thus at the most 2 errors can be corrected.

- Ex. 3.8.3 :** For a hamming distance of 6 how many errors can be detected ? How many can be corrected ?

Soln. :

- 1. Number of errors that can be detected is

$$s \leq d_{min} - 1$$

$$\therefore s \leq 6 - 1 = 5$$

...Ans.

- 2. Number of errors that can be corrected = $t \leq \frac{d_{min} - 1}{2}$,

$$\therefore t \leq 2.5.$$

- So at the most 2 errors can be corrected.

3.9 Linear Block Codes :

- Block codes can be of two types : Linear block codes and nonlinear block codes.
- Almost all the block codes used today are **linear block codes**.
- The non linear block codes are not used widely as their analysis and implementation is difficult.

Definition :

- A linear block code is defined as that code in which the exclusive OR (Modulo – 2 addition) of two valid codewords would produce an another valid codeword.

Minimum distance for linear block codes :

- For a linear block code, the minimum hamming distance is equal to the number of 1s present in that nonzero valid codeword which has the smallest number of 1s.

3.9.1 Some Linear Block Codes :

- Some of the important linear block codes are as follows
- 1. Simple parity check codes.
- 2. Hamming codes.



- Out of these the parity checking codes are designed for error detection purpose whereas hamming codes are designed for error correction.

3.9.2 Error Detection :

SPPU : Dec. 10

University Questions

Q. 1 Define error correction, error detection and hamming distance. **(Dec. 10, 2 Marks)**

- When a codeword is transmitted, one or more number of transmitted bits will be reversed (0 to 1 or vice versa) due to transmission impairments.
- Thus errors will be introduced.
- It is possible for the receiver to detect these errors if the received codeword (corrupted) is not one of the valid codewords.
- When the errors are introduced, the distance between the transmitted and received codewords will be equal to the number of errors as illustrated in Fig. 3.9.1.

Transmitted codeword :

1	0	1	0	1	1	0	0
---	---	---	---	---	---	---	---

1	1	1	0	1	0	1	0
---	---	---	---	---	---	---	---

Received codeword :

1	1	1	0	1	1	0	0
---	---	---	---	---	---	---	---

0	1	1	1	1	0	1	1
---	---	---	---	---	---	---	---

Number of Errors : 1 2
Distance : 1 2

(E-1730) Fig. 3.9.1 : Error detection

- Hence to detect the errors at the receiver, the valid codewords should be separated by a distance of more than 1.
- Otherwise the incorrect received codewords will also be treated as some other valid codewords and the error detection will be impossible.
- The number of errors that can be detected depends on the distance between any two valid codewords.

3.9.3 Parity Checking :

SPPU : May 10, May 14, Dec. 18

University Questions

Q. 1 What is hamming distance ? Explain with example. Explain simple parity check code.

(May 10, 8 Marks)

Q. 2 What is Hamming distance ? Explain it with an example. Explain simple parity check code.

(May 14, 7 Marks)

Q. 3 What is meant by parity check ? Explain two-dimensional parity check method in detail.

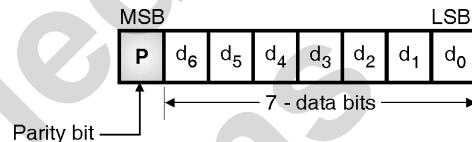
(Dec. 18, 6 Marks)

Definition of parity bit :

- A parity bit or a check bit is a bit added to a string of binary bits to ensure that the total number of 1-bit in the string including the parity bit is either even or odd.

Addition of parity bit :

- The simplest technique for detecting errors is to add an extra bit known as parity bit to each word being transmitted.
- As shown in Fig. 3.9.2, generally the MSB of an 8-bit word is used as the parity bit and the remaining 7 bits are used as data or message bits.

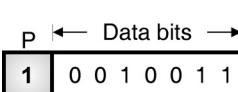
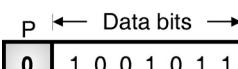


(L-309) Fig. 3.9.2 : Format of a transmitted word with parity bit

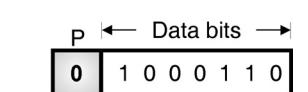
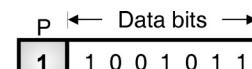
- The parity of the 8-bit transmitted word can be either even parity or odd parity.
- Even parity means the number of 1's in the given word including the parity bit should be even (2, 4, 6...).
- Odd parity means the number of 1's in the given word including the parity bit should be odd (1, 3, 5...).

3.9.4 Use of Parity Bit to Decide Parity :

- The parity bit can be set to 0 or 1 depending on the type of parity required.
- For odd parity this bit is set to 1 or 0 at the transmitter such that the number of "1 bits" in the entire word is odd.
- For even parity this bit is set to 1 or 0 such that the number of "1 bits" in the entire word is even. This is illustrated in Fig. 3.9.3.



(a) Inclusion of a parity bit to obtain an even parity



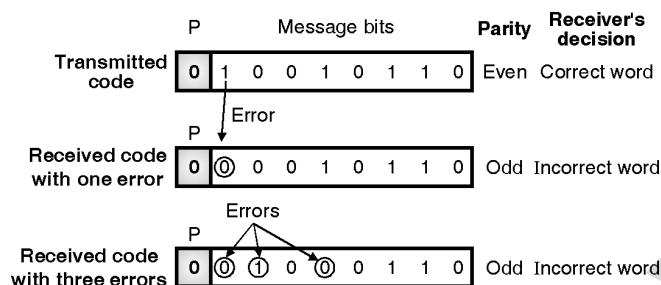
(b) Inclusion of a parity bit to obtain the odd parity

(L-310) Fig. 3.9.3



How does error detection take place ?

- The parity checking at the receiver can detect the presence of an error if the parity of the received signal is different from the expected parity.
- That means if it is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity then the receiver can conclude that the received signal is not correct.
- This is as shown in Fig. 3.9.4.

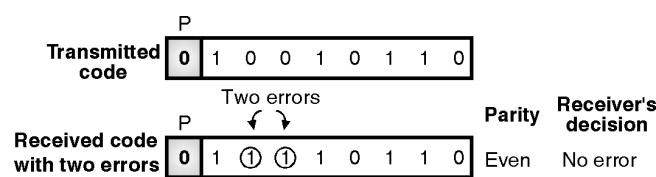


(L-311)Fig. 3.9.4 : The receiver detects the presence of error if the number of errors is odd i.e. 1, 3, 5

- If a single error or an odd number of bits change due to errors introduced during transmission the parity of the code word will change.
- Parity of the received code word is checked at the receiver and if there is change in parity then it is understood that error is present in the received word. This is as shown in Fig. 3.9.4.
- If presence of error is detected then the receiver will ignore the received byte and request for the retransmission of the same byte to the transmitter.

When does parity checking fail to detect errors ?

- If the number of errors introduced in the transmitted code is two or any even number, then the parity of the received code word will not change.
- It will still remain even as shown in Fig. 3.9.5 and the receiver will fail to detect the presence of errors.



(L-312)Fig. 3.9.5 : The receiver cannot detect the presence of error if the number of errors is even i.e. 2, 4, 6

Conclusions :

- Double or any even number of errors in the received word will not change the parity. Therefore even number of errors will be unnoticed.
- If one or odd number of errors occur then the parity of the received word will be different from the parity of transmitted signal. Thus error is noticed. However this error can neither be located nor be corrected.

Limitations of parity checking :

- Thus the simple parity checking method has its limitations. It is not suitable for detection of multiple errors (two, four, six etc).
- The other limitation of parity checking method is that it cannot reveal the location of erroneous bit. It cannot correct the error either.

3.9.5 Simple Parity Check Block Code :

- In the simple parity check code, we have a k-bit data word which is changed to an n-bit codeword with $n = k + 1$. That means we add one extra bit to each k bit data word.
- The extra bit added is known as the **parity bit**. It is selected in such a way that it makes the total number of 1s in the codeword, an even number.
- The minimum hamming distance for this code is $d_{min} = 2$ which shows that it is a single bit error detecting code. It cannot correct any errors.
- Table 3.9.1 shows the codewords for a parity check linear block code, with $k = 2$ and $n = 2 + 1 = 3$ with an even parity.

(G-1450) Table 3.9.1 : Codewords for a parity check code with $k = 2$ and $n = 3$

Dataword	Codeword
0 0	0 0 0
0 1	0 1 1
1 0	1 0 1
1 1	1 1 0

Note : Parity bit has been encircled

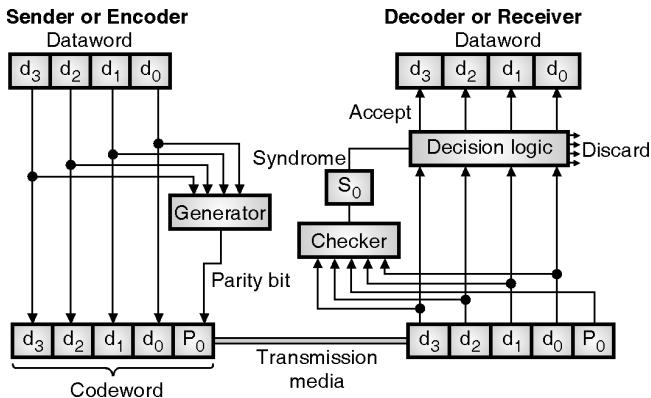
- Similarly it is possible to write codewords with $k = 3$ and $n = 4$ as shown in Table 3.9.2.

(G-1451) Table 3.9.2 : Codewords for a parity check code with $k = 3$ and $n = 4$

Dataword	Codeword	Dataword	Codeword
0 0 0	0 0 0 0	1 0 0	1 0 0 1
0 0 1	0 0 1 1	1 0 1	1 0 1 0
0 1 0	0 1 0 1	1 1 0	1 1 0 0
0 1 1	0 1 1 0	1 1 1	1 1 1 1

**Encoder (Sender) :**

- The encoder or sender for a parity check code is as shown in Fig. 3.9.6.



(G-1452)Fig. 3.9.6 : Encoder and decoder of a parity check code

- The generator uses the dataword as its input to generate a parity bit P₀.
 - The codeword contains the original data word alongwith the parity bit as shown.
 - The parity bit P₀ is generated by adding all the bits in the data word using the modulo – 2 addition.
- $$\therefore P_0 = d_0 \oplus d_1 \oplus d_2 \oplus d_3 \dots \text{Modulo} - 2.$$
- The codeword is then sent over the transmission medium over which it may get corrupted due to noise.

Decoder or receiver :

- The 5 bit codeword corrupted by noise is received by the decoder or receiver as shown in Fig. 3.9.6.
- The function of the checker is same as that of the generator with one change.
- It adds all the 5-bits (mod – 2 addition) in the received codeword and not four bits as in case of generator.
- The result of this addition is known as syndrome. It is a single bit produced at the output of the checker as shown.
- The syndrome S₀ = 0 if the received codeword has an even parity and S₀ = 1 if it has an odd parity.

$$S_0 = d_0 \oplus d_1 \oplus d_2 \oplus d_3 \oplus P_0 \dots \text{MOD 2 addition}$$

- This syndrome is then applied to the decision logic analyzer.
- If S₀ = 0 it indicates an even parity so there is no error in the received codeword.

- Hence the data bits of the received codeword would be accepted.
- But if S₀ = 1, it indicates an odd parity therefore an error is present in the received codeword.
- Hence, the data bits of this codeword are discarded.

3.9.6 Two Dimensional Parity Check (Block Parity) :

SPPU : May 16, May 18, Dec. 18

University Questions.

- Q. 1** Explain two dimensional parity check.

(May 16, 7 Marks)

- Q. 2** What are different error detection techniques ? Explain any one with suitable example.

(May 18, 7 Marks)

- Q. 3** What is meant by parity check ? Explain two-dimensional parity check method in detail.

(Dec. 18, 6 Marks)

Block of Data :

- When a large number of binary words are being transmitted or received in succession, the resulting collection of bits is considered as a **block of data**, with rows and columns as shown in Fig. 3.9.7.

Characters	C	O	M	P	U	T	E	R	
b ₁	1	1	1	0	1	0	1	0	1
b ₂	1	1	0	0	0	0	0	1	1
b ₃	0	1	1	0	1	1	1	0	1
(Message bits)	0	1	1	0	0	0	0	0	0
b ₄	0	0	0	1	1	1	0	1	0
b ₅	0	0	0	1	1	1	0	1	0
VRC bits	0	0	0	0	0	0	0	0	0
b ₇	1	1	1	1	1	1	1	1	0
(even parity) →	1	1	0	0	0	1	1	1	1

These bits will make the parity of each column even

These bits will make the parity of each row even ← LRC bits (even parity)

(L-315) Fig. 3.9.7 : Vertical and longitudinal parity check bits

LRC and VRC Bits :

- The parity bits are produced for each row and column of such block of data.
- The two sets of parity bits so generated are known as :
 1. Longitudinal Redundancy Check (LRC) bits



- Vertical Redundancy Check (VRC) bits.
- The LRC bits indicate the parity of rows and VRC bits indicate the parity of columns as shown in Fig. 3.9.7.

The Vertical Redundancy Check (VRC) Bits :

- As shown in Fig. 3.9.7 the VRC bits are parity bits associated with the ASCII code of each character.
- Each VRC bit will make the parity of its corresponding column "an even parity".
- For example consider column 1 corresponding to character "C". The ASCII code for the character C is,

Character	C
b ₁	1
b ₂	1
b ₃	0
b ₄	0
b ₅	0
b ₆	0
b ₇	1
VRC bit →	1

← Column - 1 of the data block

← VRC bit = 1 to make the parity of first column even

(G-1944)

- Therefore the 8th bit which is a VRC bit is made "1" to make the parity even. Similarly the other VRC bits are found as shown in Fig. 3.9.7.

The Longitudinal Redundancy Check (LRC) Bits :

- The LRC bits are parity bits associated with the rows of the data block of Fig. 3.9.7.
- Each LRC bit will make the parity of the corresponding row, an even parity. For example, consider row 1 of Fig. 3.9.7.

Row 1 :

b ₁	1	1	1	0	1	0	1	0	1
----------------	---	---	---	---	---	---	---	---	---

 ← LRC bit to make parity even

(G-1945)

How to locate the bit in error ?

- Even a single error in any bit will result in a noncorrect "LRC" in one of the rows and an incorrect VRC in one of the columns.
- The bit which is common to the row and column is the bit in error.
- However there is still a limitation on the Block parity code, which is that, multiple errors in rows and columns can be only detected but they cannot be corrected.

- This is because, it is not possible to locate the bits which are in error. This will be clear when you will solve the following example.

- Ex. 3.9.1 :** The following bit stream is encoded using VRC, LRC and even parity. Locate and correct the error if it is present.

1	1	0	0	0	1	1	1	1	0	0	1	1
1	0	1	1	0	0	1	0	1	0	0	1	0
0	0	1	0	1	0	1	0	1	0	1	0	1
1	0	1	0	0	1	1	0	0	1	0	1	1
1	1	1	0	0	0	0	0	0	1	0	0	1

Soln. :

- Fig. P. 3.9.1 shows the received data block alongwith the LRC and VRC bits.

bit in error											
byte byte byte			:	LRC bits (even parity)							
1	2	3	:	1	1	1	0	0	1	0	1
b ₁	1	1	1	0	0	0	0	0	1	0	1
b ₂	1	1	0	0	0	0	0	0	1	1	0
b ₃	0	1	1	0	1	1	1	0	1	0	1
b ₄	0	1	1	0	0	0	0	0	0	0	0
b ₅	0	0	0	1	1	1	0	1	0	1	0
b ₆	0	0	0	0	0	0	0	0	0	0	0
b ₇	1	1	1	1	1	1	1	1	1	0	0
VRC bits (even parity)	1	1	0	0	0	1	1	1	1	1	1

Data block →

↑ Wrong parity
First bit of the fifth byte is in error

(L-315(a))Fig. P. 3.9.1

- Note the parity bits corresponding to row 1 and column 5 indicate wrong parity.
- Therefore the fifth bit in the first row (encircled bit) is incorrect.
- Thus using VRC and LRC, it is possible to locate and correct the bits in error.

3.10 Hamming Codes :

SPPU : May 09, May 11, May 16

University Questions

- Q. 1** Discuss the hamming code technique. Calculate hamming code if data to be sent is 1001101.

(May 09, May 11, 8 Marks)

- Q. 2** What is hamming code ? Generate code words using hamming code for following data words :

1011, 0101.

(May 16, 7 Marks)

- Now let us discuss the other category of codes i.e. the error correcting codes known as the Hamming codes.



- Hamming codes are linear block codes. The family of (n, k) Hamming codes for $d_{min} = 3$ is defined by the following equations :

1. Block length : $n = 2^m - 1$
2. Number of message bits : $k = 2^m - m - 1$
3. Number of parity bits : $(n - k) = m$, where $m \geq 3$. i.e. minimum number of parity bits is 3.
4. The minimum distance : $d_{min} = 3$.
5. The code rate or code efficiency :

$$\eta = \frac{k}{n} = \frac{2^m - m - 1}{2^m - 1} = 1 - \frac{m}{2^m - 1}$$

If $m \gg 1$ then code rate $r \approx 1$.

Error detection and correction capabilities of Hamming code :

- For the minimum distance $d_{min} = 3$,
- 1. The number of errors that can be detected per word = 2.
But, $d_{min} \geq (s + 1)$
 $\therefore 3 \geq s + 1 \therefore s \leq 2$
- 2. The number of errors that can be corrected per word = 1. since $d_{min} \geq (2t + 1)$
 $\therefore 3 \geq (2t + 1) \therefore t \leq 2$
- Thus with $d_{min} = 3$ it is possible to detect upto 2 errors and it is possible to correct upto only 1 error.

3.10.1 Generation of Hamming Code :

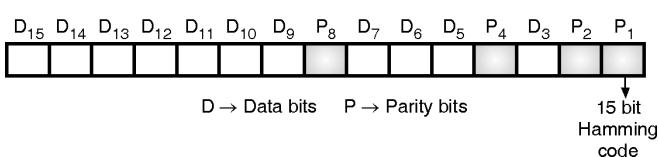
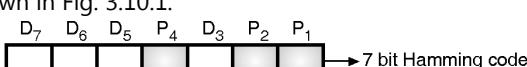
SPPU : May 19

University Questions.

Q. 1 Explain with suitable example generation of Hamming codes for 11 bit codeword.

(May 19, 7 Marks)

- Hamming code is basically a linear block code named after its inventor.
- It is an error correcting code.
- The parity bits are inserted in between the data bits as shown in Fig. 3.10.1.



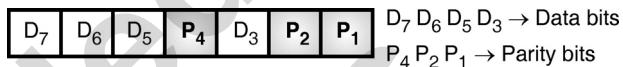
D → Data bits P → Parity bits 15 bit Hamming code

(G-1946) Fig. 3.10.1 : Hamming code words

- The 7-bit Hamming code is used commonly, but the concept can be extended to any number of bits.
- Note that the parity bits are inserted at each 2^n bit where $n = 0, 1, 2, 3, \dots$. Thus P_1 is at $2^0 = 1$, i.e. at first bit, P_2 is at $2^1 = 2$, P_4 is at $2^2 = 4$ and P_8 is at $2^3 = 8$ as shown in Fig. 3.10.1.

7-Bit Hamming Code :

- A scientist named R.W. Hamming developed a coding system which was easy to implement.
- Assuming that four data bits are to be transmitted, he suggested a code word pattern shown in Fig. 3.10.2.



(G-1947) Fig. 3.10.2 : Code word pattern for Hamming code

- The D bits in Fig. 3.10.2 are data bits, whereas P bits are parity bits. The parity bits P_1, P_2, P_4 are adjusted in a particular way as explained below.

Minimum number of parity bits :

- Table 3.10.1(a) gives a listing of minimum number of parity bits needed for various ranges of "m" information bits.

Table 3.10.1(a) : Number of parity bits to be used

Number of information bits	Number of parity bits
2 to 4	3
5 to 11	4
12 to 26	5
27 to 57	6
58 to 120	7

Deciding the values of parity bits :

- Table 3.10.1(b) indicates which bit positions are associated with each parity bit in order to establish required parity (even or odd) over the selected bits positions.

Table 3.10.1(b)

Parity Bit	Bits to be checked
P ₁	1,3,5,7,9,11,13,15,....
P ₂	2,3,6,7,10,11,14,15,....
P ₄	4,5,6,7,12,13,14,15,....
P ₈	8,9,10,11,12,13,14,15,....



3.10.2 Selection of Parity Bits :

Selection of P_1 :

- P_1 is adjusted to 0 or 1 so as to establish even parity over bits 1, 3, 5 and 7 i.e. P_1 , D_3 , D_5 and D_7 .

→ Consider bits 1,3,5,7 for P_1

→ Consider bits 2,3,6,7 for P_2

→ Consider bits 4,5,6,7 for P_4

(G-2291)

Selection of P_2 :

- P_2 is adjusted to 0 or 1 so as to set even parity over bits 2, 3, 6 and 7 (P_2 , D_3 , D_6 and D_7).

Selection of P_4 :

- P_4 is adjusted to 0 or 1 so as to set even parity over bits 4, 5, 6 and 7 (P_4 , D_5 , D_6 and D_7).
- The selection of parity bits will be clear after solving the following example.

Ex. 3.10.1 : A bit word 1 0 1 1 is to be transmitted. Construct the even parity seven-bit Hamming code for this data. **May 16, 7 Marks**

Soln. :

Step 1 : The code word format :

- The seven bit Hamming code format is shown in Fig. P. 3.10.1. Given bit word = 1 0 1 1

D₇ D₆ D₅ P₄ D₃ P₂ P₁

1 0 1 1

To be decided

(G-1948) **Fig. P. 3.10.1 : Seven bit Hamming code format**

Step 2 : Decide P_1 :

- P_1 sets the parity of bits P_1 , D_3 , D_5 and D_7 . As D_7 , D_5 , D_3 = 1 1 1 we have to set P_1 = 1 in order to have the even parity.

D₇ D₆ D₅ P₄ D₃ P₂ P₁

1 0 1 1

Set P_1 = 1 to have the even parity of P_1 D_3 D_5 D_7

(G-1949)

Step 3 : Decide P_2 :

- P_2 is set to have the even parity of P_2 D_3 D_6 and D_7 . But D_3 D_6 D_7 = 1 0 1 hence set P_2 = 0.

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1		1	0	1

↑ Set P_2 = 0 to have even parity of P_2 D_3 D_6 and D_7 (G-1950)

Step 4 : Decide P_4 :

- P_4 is set to have the even parity of P_4 D_5 D_6 and D_7 . But D_5 D_6 D_7 = 1 0 1, hence set P_4 = 0.

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1	0	1	0	1

↑ P₄ = 0 to have even parity of P_4 D_5 D_6 D_7 (G-1951)

Step 5 : Obtain the code word :

- Hence the complete 7-bit Hamming code word is as shown below.

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1	0	1	0	1

(G-2698) **Fig. P. 3.10.1(a) : Complete codeword**

Ex. 3.10.2 : Encode the data bits 0 1 0 1 into a seven bit even parity Hamming code. **May 16, 7 Marks**

Soln. :

Step 1 : The code word format :

- The seven bit Hamming code format is shown below. Given bit word = 0 1 0 1

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
0	1	0		1		

(G-1952)

Step 2 : Select P_1 for P_1 D_3 D_5 D_7 :

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
0	1	0		1		1

↑ P₁ = 1 for P_1 D_3 D_5 D_7 = 1 1 0 0 (G-1953)

Step 3 : Select P_2 for P_2 D_3 D_6 D_7 :

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
0	1	0		1	0	1

↑ P₂ = 0 for P_2 D_3 D_6 D_7 = 0 1 1 0 (G-1954)

Step 4 : Select P_4 :

D ₇	D ₆	D ₅	P ₄	D ₃	D ₂	D ₁
0	1	0	1	1	0	1

↑ Set P_4 = 1 to have P_4 D_5 D_6 D_7 = 1 0 1 0 (G-1955)

**Step 5 : Obtain the code word :**

- Hence the complete 7-bit Hamming code word is as shown below.

0	1	0	1	1	0	1
← Complete codeword						

(G-1956)

3.10.3 Detection and Correction of Errors :

- The Hamming coded data is now transmitted. At the receiver it is decoded to get the data back.
- The bits (1, 3, 5, 7), (2, 3, 6, 7) and (4, 5, 6, 7) are checked for even parity.
- If all the 4-bit groups mentioned above possess the even parity then the received code word is correct i.e. it does not contain errors.
- But if the parity is not even (i.e. it is odd) then error exists. Such an error can be located by forming a three bit number out of the three parity checks.
- This process becomes clear by solving the example given below.

Ex. 3.10.3 : If the 7-bit Hamming code word received by a receiver is 1 0 1 1 0 1 1. Assuming the even parity state whether the received code word is correct or wrong. If wrong, locate the bit in error.

Soln. :

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
Received codeword : 1	0	1	1	0	1	1

(G-1957)

Step 1 : Analyze bits 4, 5, 6 and 7 :

$$P_4 \ D_5 \ D_6 \ D_7 = 1 \ 1 \ 0 \ 1 \rightarrow \text{Odd parity.}$$

∴ Error exists here.

∴ Put P₄ = 1 in the 4's position of the error word.

Step 2 : Analyze bits 2, 3, 6 and 7 :

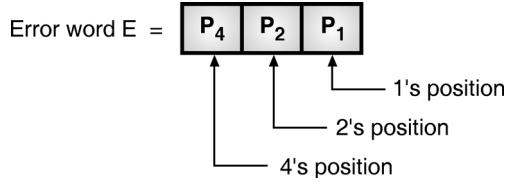
$$\therefore P_2 \ D_3 \ D_6 \ D_7 = 1 \ 0 \ 0 \ 1 \rightarrow \text{Even parity so no error.}$$

Hence put P₂ = 0 in the 2's position of the error word.

Step 3 : Check the bits 1, 3, 5, 7 :

$$\therefore P_1 \ D_3 \ D_5 \ D_7 = 1 \ 0 \ 1 \ 1 \rightarrow \text{Odd parity so error exists.}$$

Hence put P₁ = 1 in the 1's position of the error word.

Step 4 : Write the error word :

- Substituting the values of P₄, P₂ and P₁ obtained in steps 1, 2 and 3 we get

$$E = \boxed{1 \ 0 \ 1}$$

$$E = (5)_{10}$$

(G-1959)

- Hence bit 5 of the transmitted code word is in error.

7	6	5	4	3	2	1
1	0	1	1	0	1	1

↑
Incorrect bit

(G-1960)

Step 5 : Correct the error :

- Invert the incorrect bit to obtain the correct code word as follows :

$$\text{Correct code word} = [1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1] \quad \dots \dots \text{Ans.}$$

3.10.4 Solved Examples :

Ex. 3.10.4 : A seven bit even parity Hamming code is received as 1 1 1 0 1 0 1. What is the correct code ?

Soln. :

1.	7	6	5	4	3	2	1
	1	1	1	0	1	0	1

← Received codeword

(G-1961)

- Check bits 4, 5, 6, 7 = 0 1 1 1 odd parity, hence error ∴ Set P₄ = 1
- Check bits 2, 3, 6, 7 = 0 1 1 1 odd parity, hence error ∴ Set P₂ = 1
- Check bits 1, 3, 5, 7 = 1 1 1 1 even parity, hence no error ∴ Set P₁ = 0
∴ Error word E = 1 1 0 = P₄ P₂ P₁
- The decimal equivalent of the error word = 6. Hence the sixth bit is incorrect. Hence invert it to get the correct code word as follows :



D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1	0	1	0	1

Inverted bit

(G-1962)

Ex. 3.10.5 : Encode the data bits 1 1 0 0 into seven bit even parity Hamming code.

Soln. :

7	6	5	4	3	2	1
P ₄	P ₂	P ₁				
1	1	0		0		

← 7-bit Hamming code.

(G-2308)

Step 1 : Decide P₁ :

Check bits 1, 3, 5, 7 for P₁. D₃ D₅ D₇ = 0 0 1

∴ Make P₁ = 1 to have even parity.

Step 2 : Decide P₂ :

Check bits 2, 3, 6, 7 for P₂. D₃ D₆ D₇ = 0 1 1

∴ Make P₂ = 0

Step 3 : Decide P₄ :

Check bits 4, 5, 6, 7 for P₄. D₅ D₆ D₇ = 0 1 1

∴ Make P₄ = 0.

∴ Complete code word →	1	1	0	0	0	0	1
(G-2308(a))							

Ex. 3.10.6 : In a particular system the data received was 1 0 1 1 0 1 0. Using seven bit odd parity Hamming code, determine the correct code.

Soln. :

7	6	5	4	3	2	1	
Received codeword →	1	0	1	1	0	1	0

(G-1980(a))

1. Check bits 4, 5, 6, 7 = 1101 odd parity, no error

∴ P₄ = 0

2. Check bits 2, 3, 6, 7 = 1001 even parity, so error

∴ P₂ = 1

3. Check bits 1, 3, 5, 7 = 0011 even parity, so error

∴ P₁ = 1

∴ Error word E = 011

4. Decimal equivalent of E = (3)₁₀. Hence the third bit is incorrect. So change it to get the correct code word as follows :

Correct codeword →	7	6	5	4	3	2	1
	1	0	1	1	1	1	0

Inverted bit

(G-1980)

Ex. 3.10.7 : A seven bit even parity Hamming code is received as 1 1 0 0 1 1 0. Find and correct the error if any.

Soln. :

7	6	5	4	3	2	1	
Received codeword →	1	1	0	0	1	1	0

(G-2310)

1. Bits 4, 5, 6, 7 = 0 0 1 1 → even parity so no error.

2. Bits 2, 3, 6, 7 = 1 1 1 1 → even parity so no error.

3. Bits 1, 3, 5, 7 = 0 1 0 1 → even parity so no error.

∴ Received code word is correct, no error.

Ex. 3.10.8 : Data bits 1 0 1 1 have to be transmitted. Construct the odd parity seven bit Hamming code for the given data.

Soln. :

(G-2311)

Hamming codeword :	7	6	5	4	3	2	1
	1	0	1	P ₄	1	P ₂	P ₁

Check bits 1, 3, 5, 7 for P₁.

3, 5, 7 = 1 1 1, odd parity. ∴ P₁ = 0

Check bits 2, 3, 6, 7 for deciding P₂

3, 6, 7 = 1 0 1, even parity. So select P₂ = 1.

Check bits 4, 5, 6, 7 for deciding P₄

5, 6, 7 = 1 0 1, even parity. So select P₄ = 1.

∴ Required code word with odd parity is as follows :

1	0	1	1	1	1	0
---	---	---	---	---	---	---

← Answer

(G-2312)

Ex. 3.10.9 : A receiver received the following Hamming code 0011100101101 with odd parity. Find the error in the received code and give the corrected data.



Soln. : Received codeword : 0011100101101

Type of parity : odd

13	12	11	10	9	P ₈	7	6	5	P ₄	3	P ₂	P ₁
0	0	1	1	1	0	0	1	0	1	1	0	1

(C-1802)

Step 1 : Check bits 8, 9, 10, 11, 12, 13 :

The bits are 0 0 1 1 0 → odd parity so no error

$$\therefore P_8 = 0$$

Step 2 : Check bits 4, 5, 6, 7, 12, 13 :

The bits are 0 0 0 1 0 1 → odd parity. ∴ No error.

$$\therefore \text{Make } P_4 = 0$$

Step 3 : Check bits 2, 3, 6, 7, 10, 11 :

The bits are 1 1 0 1 1 0 → even parity. ∴ error exists.

$$\therefore \text{Make } P_2 = 1$$

Step 4 : Check bits 1, 3, 5, 7, 9, 11, 13 :

The bits are 0110011 → even parity. ∴ error exists.

$$\therefore \text{Make } P_1 = 1$$

Step 5 : Write the error word :

$$E = \begin{array}{|c|c|c|c|} \hline & 0 & 0 & 1 & 1 \\ \hline \text{P}_8 & \text{P}_4 & \text{P}_2 & \text{P}_1 \\ \hline \end{array} \quad (\text{C-1803})$$

Step 6 : Obtain correct codeword :

$$E = 0011 = (3)_{10}$$

- So the seventh bit in the received codeword is incorrect so invert it from 0 to 1.
- Hence the correct codeword is,

13	12	11	10	9	P ₈	7	6	5	P ₄	3	P ₂	P ₁
0	0	1	1	1	0	1	1	0	1	1	0	1

Inverted seventh bit

(G-2707)

Ex. 3.10.10 : What is the limitation of Hamming codes ?

Generate the Hamming code for the data 111011001 with even parity.

Soln. :

Limitation of Hamming code :

- The main limitation of hamming code is that it can detect and correct only one error.

Data number : 1 1 1 0 1 1 0 0 1

Step 1 :

- Number of message bits is 9. So we need to add 4 parity bits in the codeword.
- The parity bits will be at the positions 1, 2, 4, and 8 as shown below :

D ₁₃	D ₁₂	D ₁₁	D ₁₀	D ₉	D ₇	D ₆	D ₅	D ₃
1	1	1	0	1	P ₈	1	0	0

(C-1804)

Step 2 : Select P₁ for P₁ D₃ D₅ D₇ D₉ D₁₁ D₁₃ :

- Parity needs to be even parity

D ₁₃	D ₁₁	D ₉	D ₇	D ₅	D ₃
1	1	1	1	0	1

(C-1805)

- For even parity P₁ should be 1. ∴ P₁ = 1

Step 3 : Select P₂ :

- To select P₂ we have to consider the bits in positions 2, 3, 6, 7, 10 and 11
- ∴ 1 0 1 0 1 P₂ → odd parity ∴ P₂ = 1

Step 4 : Select P₄ :

- For P₄, we have to consider the bits in the following positions 4, 5, 6, 7, 12, 13 and select the value of P₄ for even parity.

$$\therefore 1 1 1 0 0 P_4 \rightarrow \text{odd parity} \quad \therefore P_4 = 1$$

Step 5 : Select P₈ :

- To select P₈, consider the bit in following positions 8, 9, 10, 11, 12, 13 and select P₈ for even parity

$$1 1 1 0 1 P_8 \rightarrow \text{even parity} \quad \therefore P_8 = 0$$

So the codeword is as follows :

Codeword	P ₈	P ₄	P ₂	P ₁
1	1	1	0	1

(L-341)

Ex. 3.10.11 : A receiver received the following Hamming code, 010101011 with even parity. Find the error in received code and give the corrected data.

Soln. :

Received codeword =	11	10	9	8	7	6	5	4	3	2	1
	0	1	0	1	0	1	0	1	0	1	1

(G-2313)

**Parity : Odd.****Step 1 : Check bits 8, 9, 10, 11 :**

- The bits are 0101 – even parity, so no error
 $\therefore \text{Set } P_8 = 0$

Step 2 : Check bits 4, 5, 6, 7 :

- The bits are 0101 – even parity, so no error.
 $\therefore \text{Set } P_4 = 0$

Step 3 : Check bits 2, 3, 6, 7, 10, 11 :

- The bits are 010101 – even parity, so no error.
 $\therefore \text{Set } P_2 = 0$

Step 4 : Check bits 1, 3, 5, 7, 9, 11 :

- The bits are 000001 – odd parity, so error exists
 $\therefore \text{Set } P_1 = 1$

Step 5 : Write the error word :

$$\begin{aligned} \text{Error word E} &= \boxed{0 \ 0 \ 0 \ 1} = P_8 P_4 P_2 P_1 \\ &= (1)_{10} \end{aligned} \quad (\text{E-1867})$$

Step 6 : Obtain the correct codeword :

$$E = (0001)_2 = (1)_{10}$$

- \therefore Error exists at the first position of the received codeword. So invert the first bit.
 $\therefore \text{Correct codeword} = 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0$

Inverted bit
(E-1863)

Ex. 3.10.12 : A receiver receives the Hamming code 101101010 with odd parity. Find the error in the received code and give corrected data.

Soln. :

- The received codeword = 1 0 1 1 0 1 0 1 0
- Type of parity = odd

9	8	7	6	5	4	3	2	1
P ₈			P ₄		P ₂	P ₁		
1	0	1	1	0	1	0	1	0

(L-342)

Step 1 : Check bits 8, 9 :

- The bits are 10 → odd parity. So error does not exist.
 $\therefore \text{Set } P_8 = 0$

Step 2 : Check bits 4, 5, 6, 7 :

- The bits are 1 1 0 1 → odd parity. So error does not exist.
 $\therefore \text{Set } P_4 = 0$

Step 3 : Check bits 2, 3, 6, 7 :

- The bits are 1 1 0 1 → odd parity. So error does not exist.
 $\therefore \text{Set } P_2 = 0$

Step 4 : Check bits 1, 3, 5, 7, 9 :

- The bits are 1 1 0 0 → even parity. So error exists.
 $\therefore \text{Set } P_1 = 1$

Step 5 : Write the error word :

$$\text{Error word E} = \boxed{0 \ 0 \ 0 \ 1} \quad (\text{L-343})$$

Step 6 : Obtain the correct codeword :

$$E = (0001)_2 = 1$$

- \therefore The error exists at the 1st position of the received codeword. So invert that bit.

$\therefore \text{Correct codeword} = 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1$

Inverted bit

(L-343(a))

Ex. 3.10.13 : Construct Hamming code for the data 11110011 with even parity.

Soln. :

- Data word : 11110011
- Number of parity bits : 4, parity : even
- \therefore Structure of codeword is as follows :

12	11	10	9	8	7	6	5	4	3	2	1
1	1	1	1	P ₈	0	0	1	P ₄	1	P ₂	P ₁

(L-344)

Step 1 : Select P₁ :

- Consider the bits 1, 3, 5, 7, 9, 11. The bits are 1 1 0 1 1 P₁
Select P₁ for even parity. $\therefore P_1 = 0$

Step 2 : Select P₂ :

- Consider bits 2, 3, 6, 7, 10, 11. The bits are 1 1 0 0 1 P₂
Select P₂ for even parity. $\therefore P_2 = 1$

**Step 3 : Select P_4 :**

- Consider bits 4, 5, 6, 7, 12. The bits are

1 0 0 1 P_4 Select P_4 for even parity. $\therefore P_4 = 0$ **Step 4 : Select P_8 :**

- Consider bits 8, 9, 10, 11, 12. The bits are,

1 1 1 1 P_8 Select P_8 for even parity. $\therefore P_8 = 0$ **Step 5 : Construct the codeword :**

- The required codeword is as shown below.

1	1	1	1	0	0	0	1	0	1	1	0
---	---	---	---	---	---	---	---	---	---	---	---

(L-345)

Ex. 3.10.14 : Discuss the Hamming code technique if the data to be sent is 1001101.

**Dec. 06, 6 Marks, May 09, 8 Marks,
May 11, 4 Marks**

Soln. :**Given :** Data = 1001 101.

- Number of data bits is $m = 7$
- Refer Table P. 3.10.14 to decide the number of parity bits.

Table P. 3.10.14

Number of data bits (m)	Number of parity bits (k)
2 to 4	3
5 to 11	4
12 to 26	5
27 to 57	6
58 to 120	7

- So we have to use 4 parity bits.

Step 1 : Codeword format :

11	10	9	8	7	6	5	4	3	2	1
1	0	0	P_8	1	1	0	P_4	1	P_2	P_1

(G-1469)Fig. P. 3.10.14 : Codeword format**Step 2 : Find : P_1, P_2, P_4, P_8 :**

- Assume even parity.

1. Find P_1 :

- Consider bits 1, 3, 5, 7, 9, 11. They are,

10101 P_1 \therefore For even parity $P_1 = 1$ **2. Find P_2 :**

- Consider bits 2, 3, 6, 7, 10, 11. They are,

10111 P_1 \therefore For even parity $P_2 = 0$ **3. Find P_4 :**

- Consider bits 4, 5, 6, 7. They are,

110 P_4 \therefore For even parity $P_4 = 0$ **4. Find P_8 :**

- Consider bits 8, 9, 10, 11. They are,

1 0 0 P_8 \therefore For even parity $P_8 = 1$ **Step 3 : Write the codeword :**

- The required codeword is as shown below.

Codeword =

1	0	0	1	1	1	0	0	1	0	1
---	---	---	---	---	---	---	---	---	---	---

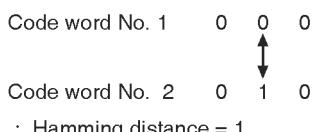
(G-1470)

Ex. 3.10.15 : Calculate hamming distance for following examples :

1. $d(000, 010)$
2. $d(011, 110)$
3. $d(101, 011)$
4. $d(000, 101)$

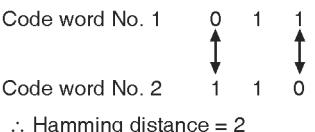
Dec. 10, 2 Marks**Soln. :** Hamming distance for

1. $d(000, 010)$ is,

 \therefore Hamming distance = 1

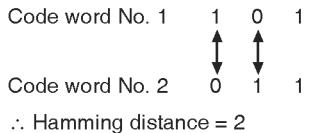
...Ans.

2. $d(011, 110)$ is,

 \therefore Hamming distance = 2

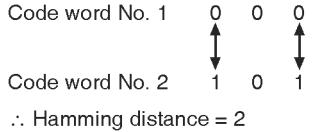
...Ans.

3. $d(101, 011)$ is,

 \therefore Hamming distance = 2

...Ans.

4. $d(000, 101)$ is,

 \therefore Hamming distance = 2

...Ans.

(G-2300)



3.11 Cyclic Codes :

- Binary cyclic codes are basically the linear block codes which actually satisfies all the restrictions that block code is supposed to satisfy.
- But the additional constraint on the binary cyclic codes is called as the **cyclic property**.

Properties of cyclic codes :

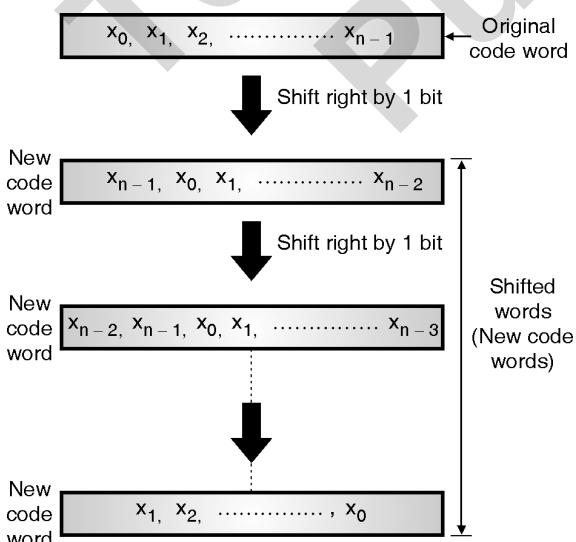
- A binary code is said to be a cyclic code if it exhibits the following properties :
 1. Linearity property
 2. Cyclic property

Linearity property :

- A code is said to be linear if sum of any two code words produces another valid code word. This property states that cyclic codes are linear block codes.

Cyclic property :

- A code is said to be cyclic if any cyclic shift of any code word results in the formation of another code word. This is as shown in Fig. 3.11.1.
- Let $(x_0, x_1, \dots, x_{n-1})$ be an n -bit (n, k) linear block codes. This code is shifted right 1 bit everytime in order to get the other code words as shown in Fig. 3.11.1.



(L-346)Fig. 3.11.1 : Cyclic property of the cyclic codes

- All the n bit words obtained by the circular right shifting are new code words. This is called as the cyclic property of the cyclic codes.

3.12 Cyclic Redundancy Check (CRC) :

SPPU : May 12, May 14, Dec. 15, May 17,

Dec. 17, Dec. 18, Dec. 19

University Questions

- Q. 1** What is CRC ? Explain with figure CRC encoder and decoder. **(May 12, 6 Marks)**
- Q. 2** What is CRC ? Explain CRC generator and CRC checker with suitable example. **(May 14, 6 Marks)**
- Q. 3** What is CRC ? Generate the CRC code for message 1101010101. Given generator polynomial $g(x) = x^4 + x^2 + 1$.

(Dec. 15, May 17, Dec. 17, Dec. 18,

Dec. 19, 7 Marks)

Definition :

- CRC is an error detection code which is included in each transmitted codeword as showing Fig. 3.12.1 and used by the receiver to detect the errors in the received codeword.
- This is a type of polynomial code in which a bit string is represented in the form of polynomials with coefficients of 0 and 1 only.
- Polynomial arithmetic uses a modulo-2 arithmetic i.e. addition and subtraction are identical to EXOR.
- For CRC code the sender and receiver should agree upon a generator polynomial $G(x)$. A codeword can be generated for a given data word (message) polynomial $M(x)$ with the help of long division.
- This technique is more powerful than the parity check and checksum error detection.

Procedure of error detection :

- CRC works on the principle of binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of the message. We will call this word as appended message word.



- The appended word thus obtained becomes exactly divisible by the generator word corresponding to $G(x)$.
- The sender appends the CRC to the message word to form a codeword.
- At the receiver, this codeword is divided by the same generator word which corresponds to $G(x)$.
- There is no error if the remainder of this division is zero. But a non-zero remainder indicates presence of errors in the received codeword.
- Such an erroneous codeword is then rejected.

3.12.1 CRC Encoder and Decoder :

SPPU : May 12, May 14

University Questions

- Q. 1** What is CRC ? Explain with figure CRC encoder and decoder. **(May 12, 6 Marks)**
- Q. 2** What is CRC ? Explain CRC generator and CRC checker with suitable example. **(May 14, 6 Marks)**

Block diagram :

- Fig. 3.12.1 shows the block diagrams of CRC encoder and decoder.

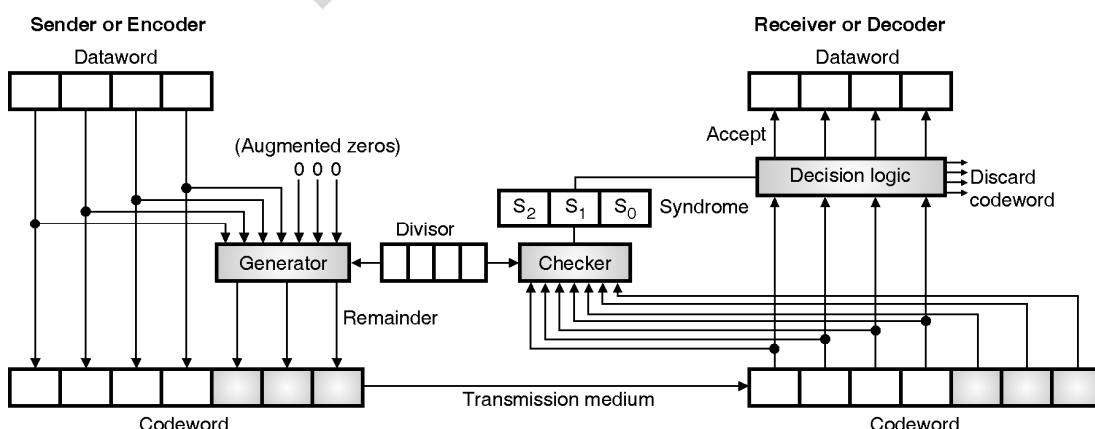
Encoder :

- The encoder shown in Fig. 3.12.1 has a 4 bit data word ($k = 4$) and 7 bit codeword ($n = 7$) with three parity check bits.

- The data bits are augmented by adding 3 zeros ($n - k$) to the R.H.S. of the word. This 7 bit resultant word is applied to the generator. This word acts as the dividend.
- The generator uses a 4 bit ($n - k + 1$) divisor which is predefined and used by the encoder as well as decoder to divide the augmented data word. This is a modulo – 2 division.
- The quotient of this division is discarded and the 3 bit remainder is appended to the data word to create a 7 bit codeword as shown in Fig. 3.12.1.

Decoder :

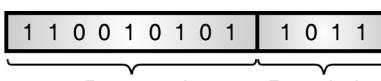
- A corrupted codeword is received by the decoder.
- All the 7 bits of the received codeword are applied to the checker alongwith the 4 bit divisor which is common to encoder and decoder. Checker is the replica of generator.
- A three bit syndrome is produced at the output of the checker which is actually a three bit remainder. The syndrome is applied to the decision logic block.
- If all the three syndrome bits are zero then the four leftmost bits of the received codeword are accepted ($S_2 S_1 S_0 = 000$ represents the no error situation).
- But if any of the syndrome bits are nonzero, then discard the 4 data bits because a non zero syndrome indicates presence of error in the received codeword.



(G-1454)Fig. 3.12.1 : CRC generator and checker

**Step 3 : Obtain the Codeword :**

- In CRC the required codeword is obtained by writing the data word followed by the remainder.

∴ Codeword = 
 Data word Remainder
 (G-1761)

3.12.5 CRC Checker :

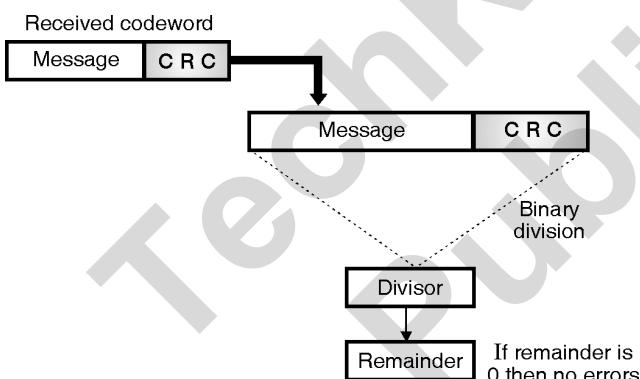
SPPU : May 12, May 14, May 19

University Questions

Q. 1 What is CRC ? Explain with figure CRC encoder and decoder. **(May 12, May 14, 6 Marks)**

Q. 2 Explain CRC generator and CRC checker with suitable example. **(May 19, 6 Marks)**

- Fig. 3.12.3 shows the CRC checker.
- The codeword received at the receiver consists of message and CRC. (Fig. 3.12.3)
- The receiver treats it as one unit and divides it by the same $(n + 1)$ bit divisor (generator word) which was used at the transmitter.



(L-820) Fig. 3.12.3 : CRC checker

- The remainder of this division is then checked.
- If the remainder is zero, then the received codeword is error free and hence should be accepted.
- But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

Detection of error :

- If the remainder is zero, then the received codeword is error free and hence should be accepted.
- But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

Ex. 3.12.2 : The codeword is received as 1100 1001 01011. Check whether there are errors in the received codeword, if the divisor is 10101. (The divisor corresponds to the generator polynomial).

Soln. :

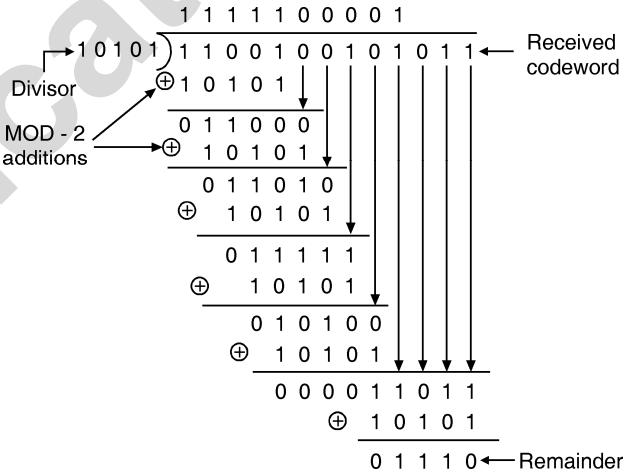
- As we know, the codeword is formed by adding the dividend and the remainder.
- This codeword will have an important property that it will be completely divisible by the divisor.
- Thus at the receiver we have to divide the received codeword by, the same divisor and check for the remainder.
- If there is no remainder then there are no errors. But if there is remainder after division, then there are errors in the received codeword.

- Let us use this technique and find if there are errors.

Code word : 1100 1001 01011

Divisor : 10101

- Carry out the division as follows.



(G-201(a))

Conclusion :

- The non zero remainder shows that there are errors in the received codeword.

Ex. 3.12.3 : Write the steps to compute the checksum in CRC code. Calculate CRC for the frame 110101011 and the generator polynomial $= x^4 + x + 1$ and write the transmitted frame.

May 07, Dec. 07, 6 Marks, May 09, 8 Marks

Soln. :

- For checksum in CRC refer section 3.12.



- The generator polynomial actually acts as the divisor in the process of CRC generation.

∴ Data word : 1 1 0 1 0 1 0 1 1

$$\text{Divisor} : x^4 + x^3 + 0x^2 + x + 1 = 1 0 0 1 1$$

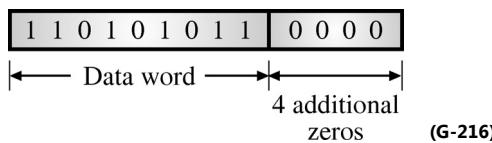
The number of data bits = m = 9

The number of bit in the divisor = N = 5

Step 1 : Obtain the dividend :

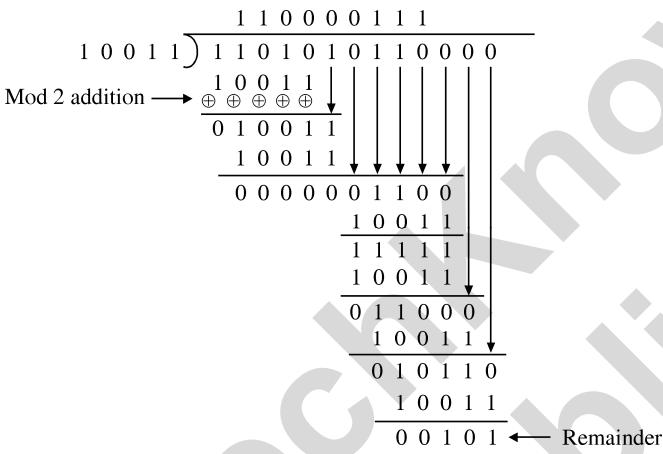
$$\text{Dividend} = \text{Data word} + (N - 1) \text{ number of zeros.}$$

- Therefore it is as shown below.



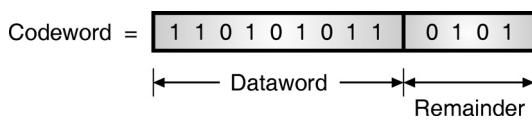
Step 2 : Carry out the division :

- Carry out the division as follows :



Step 3 : Obtain the Codeword :

- In CRC the required codeword is obtained by writing the data word followed by the remainder.
- The codeword is given by :



Ex. 3.12.4 : If the frame is 110101011 and generator is $x^4 + x + 1$ what would be the transmitted frame.

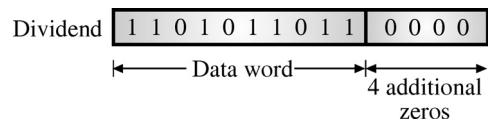
Soln. :

Given : Data word : 1 1 0 1 0 1 1 0 1 1

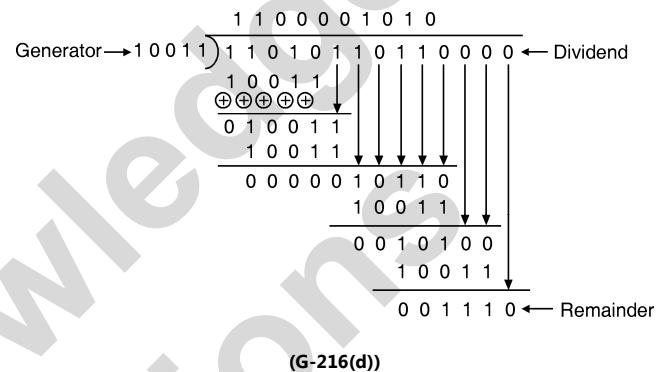
$$\begin{aligned} \text{Generator} : x^4 + x + 1 &= x^4 + 0x^3 + 0x^2 + x + 1 \\ &= 10011 = n \end{aligned}$$

Step 1 : Add four zeros at the end of the data word :

- Add four zeros ($n - 1$) at the end of data word to get the dividend as follows :

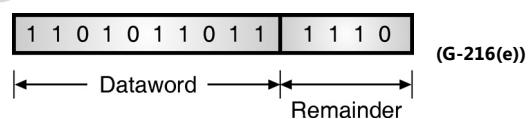


Step 2 : Carryout the long division :



Step 3 : Write the transmitted frame :

- The transmitted frame is obtained by writing the data word followed by the remainder.
- ∴ The transmitted codeword is as follows :



Ex. 3.12.5 : What is the remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

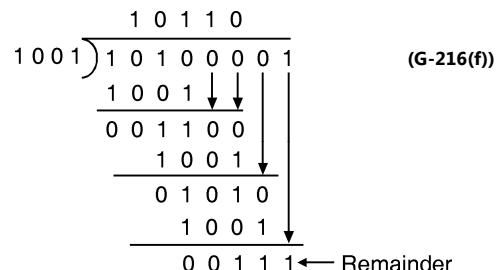
Soln. :

Given :

$$\begin{aligned} \text{Dividend} : x^7 + x^5 + 1 &= x^7 + 0x^6 + x^5 + 0x^4 \\ &\quad + 0x^3 + 0x^2 + 0x + 1 \\ &= 10100001 \end{aligned}$$

$$\text{Divisor} : x^3 + 1 = x^3 + 0x^2 + 0x + 1 = 1001$$

- The long division is as follows :





- The remainder is $00111 = x^2 + x + 1$ in the polynomial form.

Ex. 3.12.6 : A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string transmitted. Suppose the third bit from left is inverted during transmission. Show that this error is detected at the receiver's end.

Soln. :

Given :

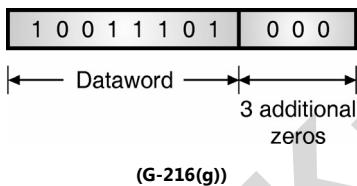
Data word (Bit string) : 1 0 0 1 1 1 0 1

$$\begin{aligned} \text{Generator polynomial} : x^3 + 1 &= x^3 + 0x^2 + 0x + 1 \\ &= 1 0 0 1 = n = 4 \end{aligned}$$

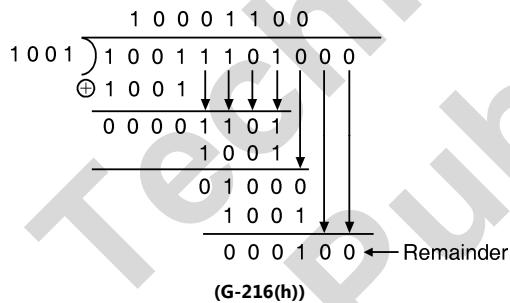
Step 1 : Obtain the dividend :

$$\text{Dividend} = \text{Data word} + 3 \text{ zeros.}$$

- The dividend is as follows :

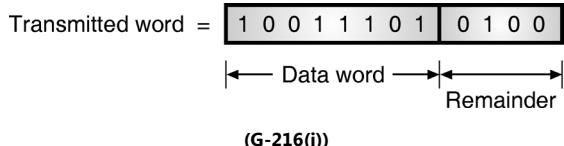


Step 2 : Carry out the division :



Step 3 : Obtain the actually transmitted bit stream :

- The transmitted word is obtained by writing the data word followed by the remainder as follows :



Error detection :

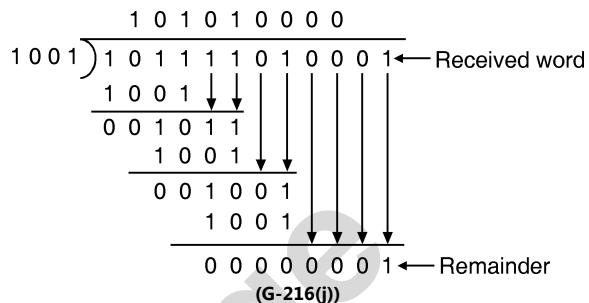
Step 4 : Write the erroneous received word :

$$\text{The received word} = 1 0 \textcircled{1} 1 1 0 1 0 0 0 1$$

↑ Error

(G-1982)

- At the receiver, this word is divided by the same divider used at the transmitter i.e. 1001.



Conclusion :

- A non zero remainder indicates that there is an error in the received codeword.

Ex. 3.12.7 : Generate the CRC code for message 1101010101. Given generator polynomial, $g(x) = x^4 + x^2 + 1$.

May 10, Dec. 14, 6 Marks, Dec. 15, 7 Marks,

May 17, Dec. 17, 4 Marks, Dec. 18, Dec. 19, 4 Marks

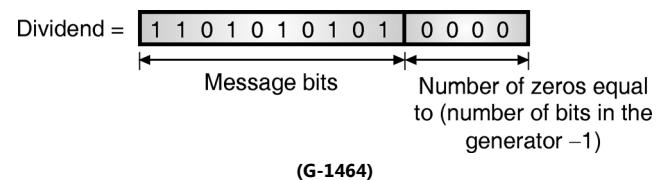
Soln. :

$$\text{Message} = 110101010101$$

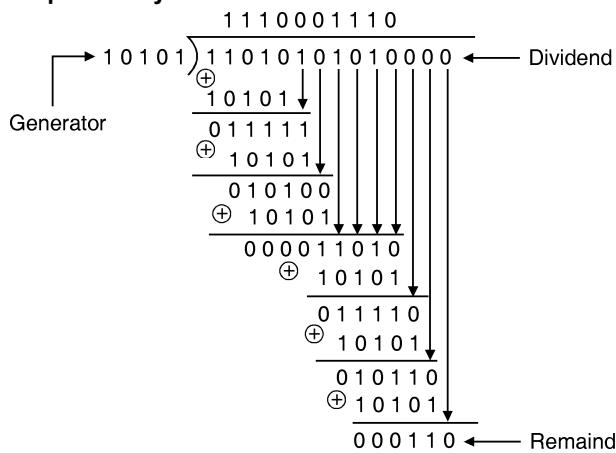
$$\begin{aligned} \text{Generator} &= x^4 + x^2 + 1 = x^4 + 0x^3 + x^2 + 0x + 1 \\ &= 1 0 1 0 1 \\ n &= 4 \end{aligned}$$

Step 1 : Obtain the dividend :

- Add four zeros ($n - 1$) at the end of data word to get the dividend as follows :



Step 2 : Carry out the division :



**Step 3 : Transmitted code word :**

Transmitted codeword : 1 1 0 1 0 1 0 1 0 1 0 1 1 0

Ex. 3.12.8 : Generate the CRC code for message 1001101010. Give generator polynomial.
 $g(x) = x^4 + x^2 + 1.$

May 02, 6 Marks, May 11, 4 Marks

Soln. :

Given :

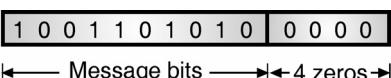
Message word : 1 0 0 1 1 0 1 0 1 0

Generator : $x^4 + x^2 + 1 = x^4 + 0x^3 + x^2 + 0x + 1 = 1 0 1 0 1$

$n = 4$

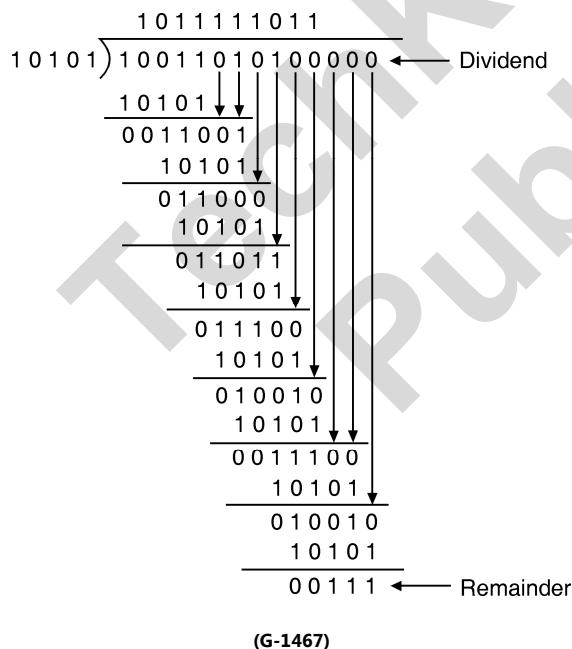
Step 1 : Obtain the dividend :

- Add four zeros ($n - 1$) at the end of data word to get the dividend as follows :

Dividend = 
(G-1466)

Step 2 : Carry out the division :

- Carry out the division as follows :

**Step 3 : Obtain the codeword :**

- In CRC the required codeword is obtained by writing the data word followed by the remainder.
- The codeword is given by :

Transmitted codeword : 1 0 0 1 1 0 1 0 1 0 0 1 1 1

Ex. 3.12.9 : Calculate the CRC if the data to be sent is 100100. The generator polynomial is

$$G(x) = x^3 + x^2 + 1$$

Dec. 06, 8 Marks

Soln. :

Step 1 : Obtain the dividend :

Data : 100100

Generator : $x^3 + x^2 + 1 = 1101$

Number of data bits = $m = 6$

Number of bits in the divisor or generator = n

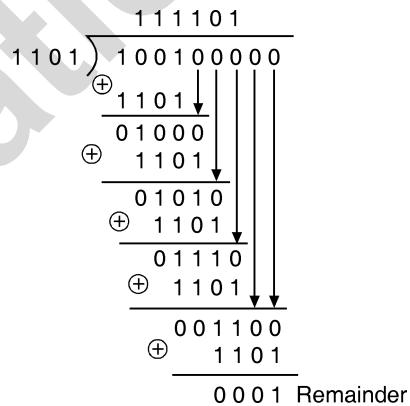
Dividend = Data word + ($n-1$) number of zeros.

So dividend is as follows:

1 0 0 1 0 0 0 0 0
Add 3 zeros
(G-1472)

Step 2 : Carry out the division :

- Carry out the long division as follows :

**Step 3 : Obtain the codeword :**

- In CRC the required codeword is obtained by writing the data word followed by the remainder.
- The codeword is given by :

Codeword : → 1 0 0 1 0 0 0 0 1

3.12.6 Advantages of Cyclic Codes :

- The advantages of cyclic codes over most of the other codes are as follows :
 - They are easy to encode.
 - They possess a well defined mathematical structure therefore a very efficient decoding schemes can be devised for them.



- 3. The methods that are to be used for error detection and correction are simpler and easy to implement.
- 4. These methods do not need look up table for decoding at the receiver.
- 5. It is possible to detect the error bursts using the cyclic codes.

3.12.7 Disadvantage of Cyclic Codes :

- Even though the error detection is simpler, the error correction is slightly more complicated.
- This is due to the complexity of the combinational logic circuit used for error correction.

3.13 Other Cyclic Codes :

- Some of the other cyclic codes are as follows :

 1. Checksum
 2. One's complement
 3. Internet checksum.

3.13.1 Checksum : SPPU : May 12, May 14, May 15

University Questions

Q. 1 What is checksum ? Describe in detail internet checksum method with suitable example.

(May 12, May 15, 8 Marks)

Q. 2 What is checksum ? Describe in detail internet checksum method with suitable example.

(May 14, 7 Marks)

Definition :

- A checksum is a small-sized datum derived from a block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage.
- Checksum is the last **error detection** method. It is used in the Internet by many protocols.

Concept :

- The concept of checksum is based on the principle of redundancy.
- This is very similar to linear block codes and cyclic codes.
- Some protocols still use checksum for error detection but now a days CRC is more preferred.

- Hence CRC is fast replacing the checksum.
- Checksum is used at the data link layer level and CRC is used in some layers other than the data link layer.
- Simple parity cannot detect two or even number of errors within the same word.
- One way to overcome this problem is to use a sort of two dimensional parity.

Calculation of checksum :

- As each word is transmitted, it is added to the previously sent word and the sum is retained at the transmitter as shown in Fig. 3.13.1.

$$\begin{array}{r} \text{Word A : } 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1 \\ + \\ \text{Word B : } 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0 \end{array}$$

$$\text{Sum : } 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1$$

(L-898) Fig. 3.13.1 : Calculation of checksum

- Each successive word is added in this manner to the previous sum.
- At the end of the transmission the sum (called a checksum) upto that time is sent.
- The errors normally occur in burst. The parity check method is not useful in detecting the errors under such conditions.
- The checksum error detection method can be used successfully in detecting such errors.
- In this method a "checksum" is transmitted along with every block of data bytes.
- In this method an eight bit accumulator is used to add 8 bit bytes of a block of data to find the "checksum byte".
- The carries of the MSB are ignored while finding out the checksum byte.

Steps for producing the checksum :

1. Transmit a word.
2. Add it to the previously transmitted word and retain the sum at the transmitter.
3. Add the next transmitted word to this sum and retain the new sum.
4. Continue till the last word in the data block is transmitted.
5. At the end of the block of data, transmit the final sum without considering the MSB carry.

- The generation of checksum will be clear if you refer to the following example.

Ex. 3.13.1 : Find the checksum of the following message.

10110001, 10101011,
00110101, 10100001

Soln. :

Carries	10 1 0 1 1 1 1 0
Data bytes	+ 1 0 1 1 0 0 0 1 + 1 0 1 0 1 0 1 1 + 0 0 1 1 0 1 0 1 + 1 0 1 0 0 0 0 1
Checksum byte	0 0 1 1 0 0 1 0

(G-1943)

- Note that the carries of MSB have been ignored while writing the checksum byte.

Detection of error using the checksum byte :

- After transmitting a block of data bytes (say 8-data bytes) the "checksum" byte is also transmitted.
 - The checksum byte is regenerated at the receiver separately by adding the received bytes.
 - The regenerated checksum byte is then compared with the transmitted one.
 - If both are identical then there is no error. If they are different then the errors are present in the block of received data bytes.
 - Sometimes the 2's complement of the checksum is transmitted instead of the checksum itself.
 - The receiver will accumulate all the bytes including the 2's complement of the checksum.
 - If there is no error, the contents of the accumulator should be zero after accumulation of the 2's complement of the checksum byte.

Advantage of the checksum method :

- The advantage of this method over the simple parity checking method is that the data bits are "mixed up" due to the 8 bit addition.
 - Therefore checksum represents the overall data block. In checksum therefore, there is 255 to 1 chance of detecting random errors.

Ex. 3.13.2 : What is the checksum of the following characters ?

0 1 0 1 1 0 1 0, 1 1 0 0 0 1 0 1,
1 1 0 1 1 0 0 1.

Soln. :

	0	1	0	1	1	0	1	0	← Byte 1
+									
	1	1	0	0	0	1	0	1	← Byte 2
+									
	1	1	0	1	1	0	0	1	← Byte 3
	1	1	1	1	1	1	1	1	← Byte 4
Discard final	1	1	1	1	1	1	0	0	← Checksum

(G-1986)

3.13.2 One's Complement Checksum :

- In one's complement arithmetic, we can represent the unsigned numbers between 0 and $2^n - 1$ using n bits.
 - If the number to be represented has more than n bits then the extra leftmost bits in this number need to be added to n rightmost bits. This is called as **wrapping**.
 - In 1's complement arithmetic a negative number is represented by inverting all its bits. This would have the same effect as subtracting that number from $(2^n - 1)$.

Ex. 3.13.3: Represent number 23 in one's complement arithmetic using only four bits.

Soln. :

Given number N = 23

Binary equivalent = (1 0 1 1 1)₂

- But the binary equivalent has 5 bits. So we use the wrapping technique.

$$\therefore \text{1's Complement equivalent} = \begin{array}{r} 1 \\ + \\ \hline 1 \end{array} \quad (G-1460)$$

(1 0 0 0)₂ = 8 ... Ans.

Ex. 3.13.4 : Represent the number -7 using one's complement arithmetic.

Soln. :

Given number	$N = -7$
Binary equivalent of	$7 = 0\ 1\ 1\ 1$
Invert all bits	$= 1\ 0\ 0\ 0$
So 1's complement of -7	$= 1\ 0\ 0\ 0 = 8$

Alternative method :

- Another method to find 1's complement is to subtract the given negative number from $(2^n - 1) = 2^4 - 1 = 15$.



- So in this example we subtract 7 from 15 to get 8.

Ex. 3.13.5 : The data items 7, 11, 12, 0 and 6 are to be sent with the help of 1's complement checksum technique. Calculate the value of checksum generated at the sending end. Demonstrate how error detection takes place at the receiver.

Soln. :

Step 1 : Generation of checksum :

- To generate the checksum, we add all the data items

$$7 + 11 + 12 + 0 + 6 = 36$$

- Represent 36 in the binary form.

$$36 = 100100$$

- Perform the wrapping in order to have a 4-bit checksum.

$$\begin{array}{r} 36 : \quad 1 \ 0 \ 0 \ 1 \ 0 \ 0 \\ \text{Wrapping :} \quad + \quad \quad \quad \quad \quad \quad \rightarrow 1 \ 0 \\ \hline 0 \ 1 \ 1 \ 0 = 6 \end{array}$$

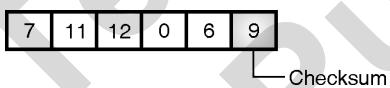
(G-1461)

- Now complement this number by subtracting it from $2^n - 1$ i.e. from 15.

$$\therefore \text{Checksum} = 15 - 6 = 9$$

Step 2 : Write the packet sent by the sender :

- The packet sent by the sender is as shown in Fig. P. 3.13.5(a).



(G-1462)Fig. P. 3.13.5(a) : Packet sent by the sender

Step 3 : At the receiver :

- At the receiver first all the received bits are added together.

$$7 + 11 + 12 + 0 + 6 + 9 = 45$$

- Binary equivalent of 45 = 101101

- The wrapping is carried out in the following manner.

$$\begin{array}{r} 45 : \quad 1 \ 0 \ 1 \ 1 \ 0 \ 1 \\ \text{Wrapping :} \quad + \quad \quad \quad \quad \quad \quad \rightarrow 1 \ 0 \\ \hline 1 \ 1 \ 1 \ 1 = 15 \text{ Wrapped sum} \end{array}$$

(G-1463)

- Subtract from 15 to get complemented wrapped sum.

$$15 - 15 = 0 \text{ complemented wrapped sum}$$

- Since the value of complemented wrapped sum or checksum is 0 at the receiver the received data is **NOT CORRUPTED**.
- So the receiver drops the checksum and keeps the other data items.
- But if the checksum at the receiver is not zero then the entire packet is dropped.

3.13.3 Internet Checksum :

SPPU : May 12, May 14, May 15, Dec. 15

University Questions

Q. 1 What is checksum ? Describe in detail internet checksum method with suitable example.

(May 12, May 15, May 14, 8 Marks)

Q. 2 Write a short note on internet checksum.

(Dec. 15, 6 Marks)

- The error detection in several Internet protocols such as IP, TCP, UDP etc. is done by using the check bits.
- For IP, a checksum is calculated for the contents of header and it is included in a special field.
- This checksum is recalculated at every router. Hence the algorithm for the checksum was selected for its ease of implementation in software.
- This algorithm assumes that the header consists of a certain number say L of 16 bits represented by $b_0, b_1, b_2, \dots, b_{L-1}$ and a checksum b_L
- These L words correspond to the information.
- The 16 bit checksum b_L corresponding to this information is calculated as follows.

Steps to calculate the checksum b_L :

Step 1 : Treat each 16 bit word as an integer and add the L words modulo $2^{16} - 1$.

$$\therefore x = b_0 + b_1 + b_2 + \dots + b_{L-1} \text{ modulo } 2^{16} - 1.$$

Step 2 : The checksum b_L then consists of the negative value of x as follows,

$$b_L = -x$$

Step 3 : The checksum b_L is then inserted in the dedicated field in the header.

- The contents of all headers, including the checksum field, must satisfy the following pattern.

$$0 = b_0 + b_1 + b_2 + \dots + b_{L-1} + b_L \text{ modulo } 2^{16} - 1.$$



- Each router can check for the errors present in the header.
- Table 3.13.1 shows the 16 possible codewords that result when the checksum calculating algorithm is applied to two bit words with $L = 2$.

Table 3.13.1 : Codewords resulting with $L = 2$

b₀	b₁	b₂	Codeword		
0	0	3	00	00	11
0	1	2	00	01	10
0	2	1	00	10	01
0	3	0	00	11	00
1	0	2	01	00	10
1	1	1	01	01	01
1	2	0	01	10	00
1	3	2	01	11	10
2	0	1	10	00	01
2	1	0	10	01	00
2	2	2	10	10	10
2	3	1	10	11	01
3	0	0	11	00	00
3	1	2	11	01	10
3	2	1	11	10	01
3	3	0	11	11	00

Error detecting capability :

- From Table 3.13.1 it is evident that the minimum distance $d_{min} = 2$.
- That means at least two bits are required to change one codeword to the other.
- The error patterns which cause the words $b_0 + b_1 + b_2 + \dots + b_{L-1} + b_L$ to change by a total of a multiple of $2^{16} - 1$ will not be detected.

3.13.4 Performance :

- The traditional checksum uses a small number of bits normally 16 for detecting errors in a message of any size.

- But the error checking capability of checksum method is not as good as that of the CRC method.
- So new protocols are designed in which the checksum is replaced by CRC.

Review Questions

- Q. 1 Explain the need, advantages and disadvantages of coding.
- Q. 2 How does the parity checking technique helps in detecting the presence of error ?
- Q. 3 When does the parity check technique fail ?
- Q. 4 Is it possible to correct errors using parity check ?
- Q. 5 Write a note on : Checksum error detection.
- Q. 6 Explain the VRC and LRC techniques.
- Q. 7 Write a short note on : Cyclic Redundancy Check (CRC).
- Q. 8 How are convolutional codes different from the block codes ?
- Q. 9 Define the following terms :
 1. Code rate
 2. Hamming distance
 3. Code efficiency.
- Q. 10 Define the minimum distance d_{min} and explain its role in deciding the number of detectable and correctable errors.
- Q. 11 Define and explain the properties of the cyclic codes.
- Q. 12 State the advantages and disadvantages of cyclic code.
- Q. 13 Write a short note on : Hamming codes.
- Q. 14 Write a short note on : Cyclic codes.
- Q. 15 What is the role of the parity bits in a code word ?
- Q. 16 Write a short note on : Internet checksum.

Unit II

Chapter

4

Data Link Control

Syllabus

Data link layer services, Framing : Fixed-size framing, Variable size framing, Flow control : Flow control protocols, Noiseless channels : Simplest protocol, Stop-and-wait protocol, Noisy channels : Stop-and-wait Automatic Repeat Request (ARQ), Go-back-n ARQ, Selective repeat ARQ, Piggybacking.
Case study : Draw PPPoE connection diagram with multiple devices, FFTH connection diagram.

Chapter Contents

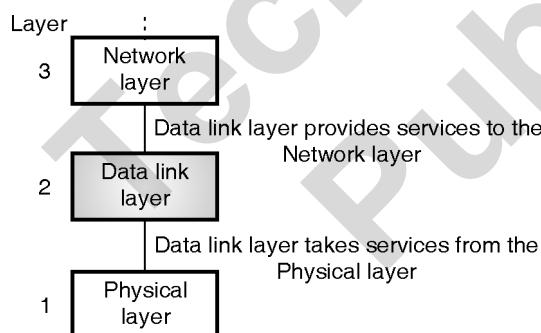
4.1 Introduction	4.7 Sliding Window Protocols
4.2 Services Provided to Network Layer	4.8 A One Bit Sliding Window Protocol (Stop and Wait ARQ)
4.3 Framing	4.9 A Protocol using GO Back n
4.4 Error Control	4.10 Selective Repeat ARQ
4.5 Flow Control	4.11 Protocol Performance
4.6 Elementary Data Link Protocols	4.12 Solved Examples

4.1 Introduction :

- The physical layer deals with the transmission of signals over different transmission medias.
- A reliable and efficient communication between two adjacent machines can be achieved via the data link layer.
- This layer basically deals with frame formation, flow control, error control, addressing and link management.
- While sending data from source to destination errors may get introduced.
- The data communication circuits have only a finite data rate and there is non-zero propagation delay between the instant a bit is sent and the instant at which it is received.
- These limitations affect the efficiency of data transfer. The data link layer protocols used for communication take care of all these problems.
- Data link layer is the second layer in OSI reference model. It is above the physical layer.

4.1.1 Position of Data Link Layer :

- Fig. 4.1.1 shows the position of data link layer in the five layer Internet model. It is the second layer.



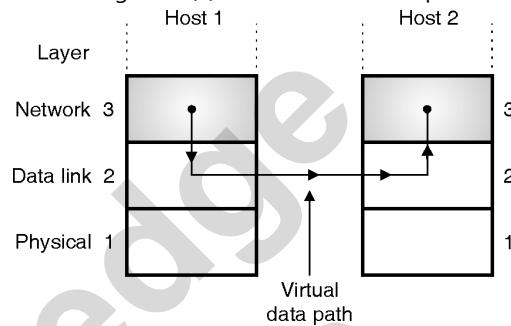
(L-663) Fig. 4.1.1 : Position of data link layer

- It receives services from the physical layer and provides services to the network layer.

4.2 Services Provided to Network Layer :

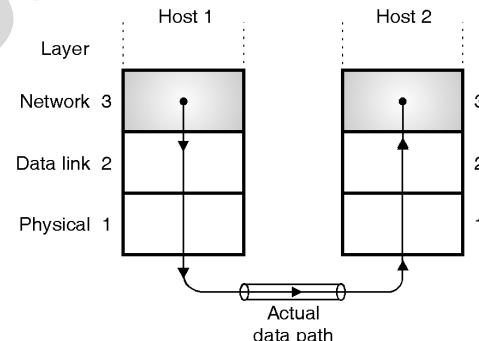
- Network layer is the layer above the data link layer in the OSI model.
- So it is supposed to provide services to the network layer.

- The main service to be provided is to transfer data from the network layer on the sending machine to the network layer of the receiving machine.
- The virtual path followed for such a communication is shown in Fig. 4.2.1(a). It is not the actual path.



(L-665) Fig. 4.2.1(a) : Virtual communication

- The actual path followed by the data from sending machine to destination is shown in Fig. 4.2.1(b) which is via all the layers below the network layer, then the physical medium, then layers 1, 2, 3 of receiving machine.
- However it is always easier to think that the communication is taking place through the data link layers (Fig. 4.2.1(a)) using a data link layer protocol.



(L-665) Fig. 4.2.1(b) : Actual data path

4.2.1 Types of Services Provided :

- Data link layer can be designed to offer different types of services. Some of them are as follows :
 1. Unacknowledged connectionless service.
 2. Acknowledged connectionless service.
 3. Acknowledged connection oriented service.

4.2.2 Unacknowledged Connectionless Service :

- In this type of service, the destination machine does not send back any acknowledgement after receiving frames.



- It is a connectionless service. So no connection is established before communication or released after it is over.
- If a frame is lost due to channel noise, then there are no attempts made to recover it.
- So this service is suitable only if the error rate is low. It is suitable for real time traffic such as speech. This type of service is highly unreliable.

4.2.3 Acknowledged Connectionless Service :

- This is the next step to improve reliability.
- In this service, there are no connections established for data transfer but for each frame received, the receiver sends an acknowledgement to the sender.
- If a frame is not received within some specified time it is assumed to be lost and the sender will retransmit it.
- This service is suitable for communication over unreliable channels such as wireless channels.

4.2.4 Acknowledged Connection Oriented Service :

- This is the most sophisticated one.
- The source and destination machines establish a connection before transferring the data.
- A specific number is given to each frame being sent and the data link layer guarantees that each transmitted frame is received.
- All the frames are guaranteed to be received in the same order as the order of transmission.
- Each received frame will be acknowledged individually by the destination machine.

Three phases of data transfer :

- The data transfer takes place by following three distinct phases given below :
 1. Connection is established.
 2. The data frames are actually transmitted.
 3. The connection is released after completion of data transfer.

4.3 Framing :

Definition :

- While transmitting a bit stream from a sender to a receiver it is necessary to break it into frames. Breaking the bit stream into frames is called as framing.

Concept :

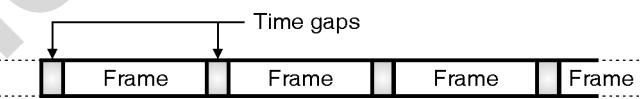
- The bits to be transmitted are first broken into discrete frames at the data link layer.
- In order to guarantee that the bit stream is error free, the checksum of each frame is computed.
- When a frame is received, the data link layer recomputes the checksum.
- If it is different from the checksum present in the frame, then the data link layer knows that an error has occurred.
- It then discards the bad frame and sends back a request for retransmission.

Types :

- Framing can of two types :
 1. Fixed size framing
 2. Variable size framing

4.3.1 Fixed Size Framing :

- Fixed size framing is the type of framing in which all the frames are of same fixed size.
- One way of doing the framing it is by inserting time gaps between frames as shown in Fig. 4.3.1.



(G-178) Fig. 4.3.1 : Framing

- This framing technique is called as the **fixed size** framing because the size of each frame in terms of number of bits is same.
- But practically this framing technique does not work satisfactorily, because networks generally do not make any guarantees about the timing.
- So some other methods are derived.

4.3.2 Variable Size Framing :

- Variable size framing is the type of framing in which all the frames are not of the same fixed size. The sizes of different frames may differ.

Types :

- Some of the variable size framing methods are as follows :
 1. Character count method.



2. Starting and ending characters, with character stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

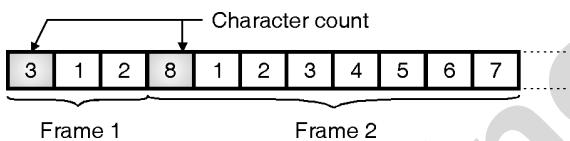
4.3.3 Character Count :

SPPU : May 16

University Questions

- Q. 1** Write a short note on character oriented framing methods. **(May 16, 6 Marks)**

- In this method, a field in the header is used to specify the number of characters in the frame.
- This number helps the receiver to know the exact number of characters present in the frame following this count.
- The character count method is illustrated in Fig. 4.3.2.



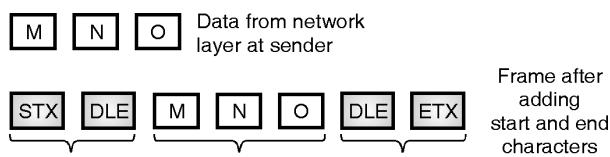
(L-668)Fig. 4.3.2 : Character count method

- The two frames shown in Fig. 4.3.2 contain 3 and 8 characters respectively and numbers 3 and 8 are inserted in the headers of the corresponding frames.
- The disadvantage of this method is that, an error can change the character count itself.
- If the wrong character count number is received due to error then the receiver will get out of synchronization and will not be able to locate the start of next frame.
- The character count method is rarely used in practice.

4.3.4 Starting and Ending Character with Character Stuffing :

- The problem of character count method is solved here by using a starting character before the starting of each frame and an ending character at the end of each frame.
- Each frame is preceded by the transmission of ASCII character sequence DLE STX. (DLE stands for data link escape and STX is start of TeXt).
- After each frame the ASCII character sequence DLE ETX is transmitted. Here DLE stands for Data Link Escape and ETX stands for End of TeXt.

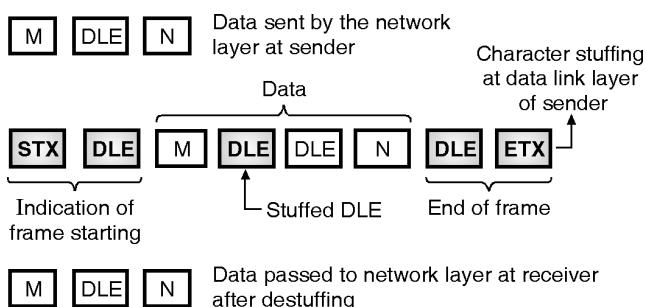
- So if the receiver loses the synchronization, it just has to search for the DLE STX or DLE ETX characters to return back on track. This is shown in Fig. 4.3.3.



(L-669) Fig. 4.3.3

Character stuffing :

- The problem with this system is that the characters DLE STX or DLE ETX can be a part of data as well.
- If so, they will be misinterpreted by the receiver as start or end of frame.
- This problem is solved by using a technique called **character stuffing** which is as follows.
- The data link layer at the sending end inserts an ASCII DLE character just before each accidental DLE character in the data being transmitted.
- The data link layer at the receiving end will remove these DLE characters before transferring the data to the network layer.
- Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once.
- This is called character stuffing and it is shown in Fig. 4.3.4.



(G-181) Fig. 4.3.4 : Character stuffing

Destuffing :

- Destuffing process is exactly opposite to the character stuffing process.
- Note that at the receiving end the destuffing is essential.

Disadvantages :

- The main disadvantage of this framing method is that we have to use the 8 bit characters and ASCII code.
 - This problem can be overcome by using the next framing technique.

4.3.5 Starting and Ending Flags, with Bit Stuffing :

- In this framing technique at the beginning and end of each frame, a specific bit pattern 0111 1110 called **flag byte** is transmitted by the sending station.
 - Since there are six consecutive 1s in the flag byte a technique called **bit stuffing** which is similar to character stuffing is used. It is as explained below :

Bit stuffing :

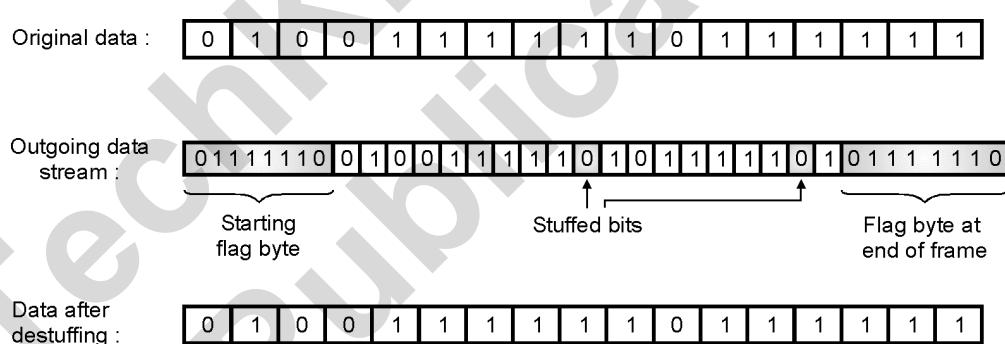
- Whenever the sender data link layer detects the presence of five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing bit stream.

Thus the six consecutive 1s will never appear in the data stream. Hence there is no chance of misinterpretation.

- This is called bit stuffing and it is illustrated in Fig. 4.3.5.
 - When a receiver detects presence of five consecutive ones in the received bit stream, it automatically deletes the 0 bit following the five ones.
 - This is called de-stuffing. It is shown in Fig. 4.3.5.
 - Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

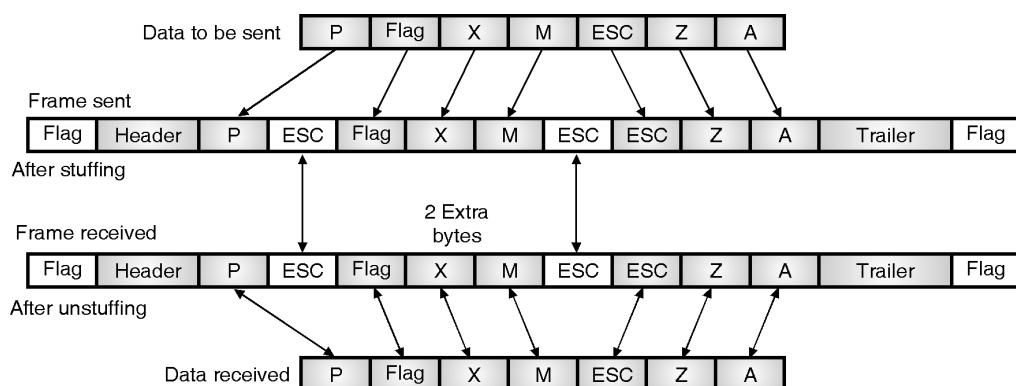
Byte stuffing :

- In 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 called as the escape character (ESC).
 - At the receiver these ESC bytes are removed from the data section and the next character is treated as data.



(G-183)Fig. 4.3.5 : Bit stuffing and destuffing

- Fig. 4.3.6 demonstrates the concept of byte stuffing.

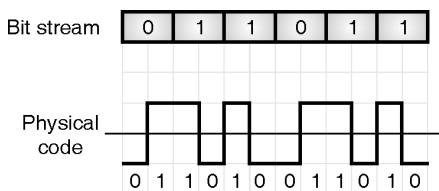


(G-182) Fig. 4.3.6 : Byte-stuffing



4.3.6 Physical Layer Coding Violations :

- This method of framing is applicable only to those networks in which the encoding on the physical medium contains some redundancy.
- Some LANs encode each bit of data using two physical bits for example the use of the Manchester coding refer Fig. 4.3.7.



(G-184) Fig. 4.3.7 : Manchester coding of data

- The physical Manchester code makes a transition at the middle of the bit interval as shown.
- Therefore a 1 bit is encoded into a 10 pair and a 0 bit is encoded into a 01 pair as shown in Fig. 4.3.7.
- This helps in recognizing the boundaries of bits in a precise manner.
- This use of invalid physical code is a part of 802 LAN standards.

Which method of framing is used practically ?

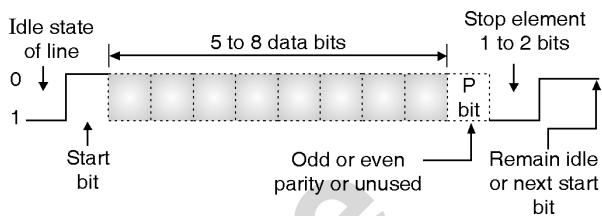
- Many data link protocols use the combination of the character count technique with one of the other techniques so as to have an extra safety.

4.3.7 Frame Synchronization :

- The data transmitted from source to destination machine is in the serial form.
- Due to errors occurring in bit during transmission, due to factors like noise and others, the start of bit and end of bit or start of frame and end of frame may not be recognised by the receiver properly.
- The receiver may lose synchronisation with the transmitter if the transmitter sends a long stream of bits and if no steps are taken to synchronise the transmitter and receiver.
- Serial transmission occurs in one of the following ways :
 1. Asynchronous
 2. Synchronous

Asynchronous frame format :

- The asynchronous frame format is shown in Fig. 4.3.8.

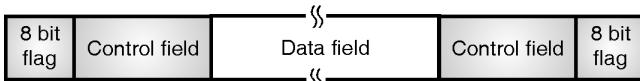


(G-185) Fig. 4.3.8 : Asynchronous frame format

- The strategy with this scheme is to avoid the timing problem by not sending long, uninterrupted streams of bits.
- In this format data is transmitted one character at a time and each character is five to eight bits in length.
- Timing or synchronisation must only be maintained within each character.
- The receiver has the opportunity to resynchronise at the beginning of each new character.
- For synchronisation start and stop bits are added at the beginning and end of the character.
- Using these bits the receiving machine resynchronises at the beginning of each new byte.
- When the receiver detects a start bit; it sets a timer and begins counting bits as they come in. After n bits, the receiver looks for a stop bit.
- As soon as it detects the stop bit, it ignores any received pulses until it detects the next start bit.

Synchronous frame format :

- In synchronous frame format the bit stream is combined into longer frames which may contain multiple bytes without start and stop bits as shown in Fig. 4.3.9.



(G-186) Fig. 4.3.9 : Synchronous frame format

- To prevent any possible timing problems between the transmitter and receiver, their clocks must be synchronised perfectly.
- One of the ways to synchronize is to provide a separate clock line between transmitter and receiver.
- The other way to provide synchronization is to include the clocking information in the data signal itself.



- As shown in the Fig. 4.3.9, the frame with synchronous format starts with a preamble called a flag which is eight bits long.
- The same flag is used as a postamble i.e. at the end of the frame. The receiver looks for the occurrence of the flag pattern to signal the start of the frame.
- This is followed by some number of control fields then a data field, more control fields and finally the flag is repeated.
- The advantage of synchronous transmission is its speed because it uses lesser number of overhead bit than asynchronous frames.

4.4 Error Control :

- The next problem to be dealt with is to make sure that all frames are eventually delivered to the network layer at the destination, in proper order.
- Generally the receiver sends back some feedback (positive or negative) to convey the information about whether it has received a frame or not.
- A positive acknowledgement (feedback) ACK indicates a successful and error free delivery of a frame. Whereas a negative acknowledgement (NAK) means that something has gone wrong and that particular frame needs to be retransmitted.
- Due to the presence of noise burst a frame may vanish completely.
- So the receiver does not receive anything and it does not react at all (no acknowledgement).
- This problem is overcome by introducing a timer in the data link layer. Its function of this timer is as follows.

4.4.1 Function of a Timer :

- As soon as a sender transmits a frame, it also starts the data link timer.
- The timer timing is set by taking into account the factors such as the time required for the frame to reach the destination, processing time at the destination and the time required for the acknowledgement to return back.
- Normally the frame is received correctly and the acknowledgement will return back to the sender before the timer runs out.

- This shows that a frame has been received and the timer is cancelled.
- But if a frame is lost or acknowledgement is lost, then the timer will go off.
- This will alert the sender that there is some problem.
- The solution to this problem is that the sender retransmits the same frame.
- But when a frame is transmitted multiple times, there is a possibility that the receiver will receive the same frame two or more times and pass it to the network layer more than once.
- This is called as **duplication**.
- To avoid this each outgoing frame is assigned a distinct sequence number.
- This will help the receiver to distinguish retransmission.

4.5 Flow Control :

- This is another important design issue related to the data link layer.

Need of flow control :

- In flow control the problem to be handled is what to do with the sender computer wants to send data at a faster rate than the capacity of the receiver to receive them.
- This happens when the sender is using a faster computer than the receiver.
- The data sent at a very fast rate will completely overwhelm the receiver.
- The receiver will keep losing some of the frames simply because they are arriving too quickly.
- The solution to this problem is to introduce the **flow control**.

Principle of flow control :

- The flow control is a mechanism to control the rate of frame transmission to a value which can be handled by the receiver.
- It requires some kind of a feedback mechanism from the receiver to the sender, so as to adjust the sending rate automatically.
- We are going to discuss some flow control techniques based on this principle.



- It is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver; otherwise there will be overflow of data.
- The data flow should not be so fast that the receiver is over-whelmed.
- The speed of processing of any receiving device is a limited and it also has a limited amount of memory storage space, for storing the incoming data.
- There has to be some system, for reverse communication from the receiver to transmitter.
- The receiver can tell the transmitter about adjusting the data flow rate to suit its speed or even stop temporarily.
- As the rate of processing at the receiver is generally slower than the rate of transmission.
- Each receiver has a finite memory called **buffer**.
- The incoming data is first stored in the buffer and then sequentially processed.
- If the buffer begins to fill up, the receiver must be able to tell the sender to stop transmission until the buffer gets empty.
- Similarly the transmitter also has a buffer for storing the bits if the transmission is stopped.

Definition of flow control :

- Flow control can be defined as a set of procedures which are used for limiting the amount of data a transmitter can send before waiting for acknowledgement.

4.6 Elementary Data Link Protocols :

- In this section we are going to discuss some elementary data link layer protocols.

4.6.1 An Unrestricted Simplex Protocol :

- This protocol is the simplest possible protocol.
- The transmission of data takes place in only one direction. So it is a simplex (unidirectional) protocol.
- It is assumed that the network layers of sender and receiver are always ready.

- It is also assumed that we can ignore the processing time and the buffer space available infinite.
- The communication channel is imagined to be noise free so it does not damage or lose any frames.
- All this is highly unrealistic. This protocol is also called as "**utopia**".
- This protocol consists of two distinct procedures, namely a sender and a receiver.
- They run in the data link layers of their respective machines.
- No sequence numbers or acknowledgements are used.

4.6.2 A Simplex Stop and Wait Protocol :

- The most unrealistic restriction in the previous protocol is the assumption that the receiving network layer can process the data with zero processing time.
- In the simplex stop and wait protocol it is assumed that a finite processing time is essential.
- However like the first protocol, the communication channel is assumed to be noise free and the communication is simplex i.e. only in one direction at a given time.
- This protocol deals with an important problem i.e. how to prevent the sender from flooding the receiver due to the data rates faster than processing speed of the receiver.

Principle :

- In this protocol, a small dummy frame is sent back from the receiver to the transmitter to indicate that it can send the next frame.
- The small dummy frame is called as **acknowledgement**.
- The transmitter sends one frame and then waits for the dummy frame called acknowledgement.
- Once the acknowledgement is received, it sends the next frame and waits for the acknowledgement. Hence this protocol is known as **stop and wait** protocol.

Advantage :

- The best thing about this protocol is that the incoming frame is always an acknowledgement. It need not be even checked.



4.6.3 A Simplex Protocol for Noisy Channel :

- This is the third protocol in which we go one step ahead and assume that the communication channel is noisy and can introduce errors in the data travelling over it.
- The channel noise can either damage the frames or they may get lost completely.

Principle :

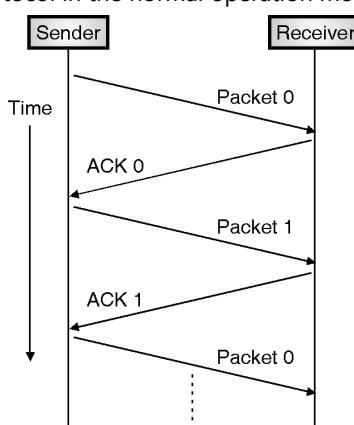
- In this protocol, the sender waits for a positive acknowledgement before advancing to the next data item.
- There is a timer set at the sender when a frame is sent. If the sender times out it will resend the same frame again.
- So it is called as **PAR** (Positive acknowledgement with retransmission) or Automatic Repeat Request (**ARQ**) type protocol.
- If a frame is badly damaged or lost then the sender would retransmit it.
- Note that due to retransmission (time out or any other reason), there is always a possibility of duplication of frames at the receiver.
- To avoid this, the sender puts a **sequence number** in the header of each frame it sends.
- The receiver can check the sequence number of each arriving frame to check for the possible duplicate frame. If a frame is duplicated then receiver will discard it.

Operation of stop and wait protocol :

- The operation can be divided into two modes :
 1. Normal operation and 2. Time out.

1. Normal operation :

- Refer Fig. 4.6.1 to understand the operation of stop and wait protocol in the normal operation mode.

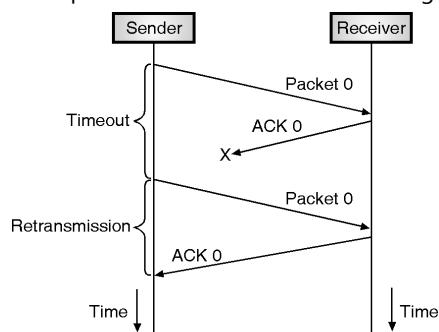


(G-220) Fig. 4.6.1 : Operation of stop and wait in the normal mode

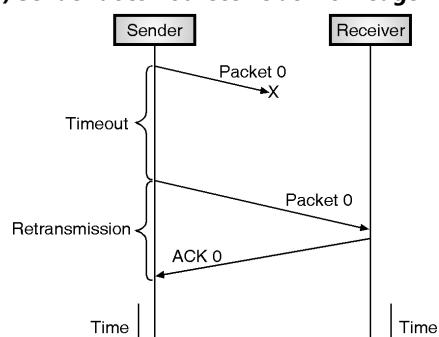
- After transmitting one frame, the sender waits for an **acknowledgement (ACK)** from the receiver before transmitting the next one.
- Thus a sender sends packet 0 and waits for its acknowledgement.
- It sends the next frame only after receiving acknowledgement of the previous frame.
- In this way, the sender can recognize that the previous packet is transmitted successfully and we could say "stop and wait" guarantees reliable transfer between nodes.
- To support this feature, the sender keeps a record of each frame it sends.
- Also, to avoid confusion caused by delayed or duplicated ACKs, "stop-and-wait" sends each packet with unique sequence numbers and receives those numbers in each ACKs.

2. Operation in Time out mode :

- If the sender does not receive **ACK** for previously sent frame after a certain period of time, the sender times out and retransmit that frame again.
- There are two cases when the sender does not receive ACK; one is when the ACK is lost and the other is when the frame itself is not received i.e. it got lost.
- These two possible cases are illustrated in Fig. 4.6.2.



(a) Sender does not receive acknowledgement



(b) Frame is lost

(G-221) Fig. 4.6.2 : Timeout and retransmission



- To support this feature, the sender keeps timer for each frame.
- We have stated earlier that a timer is introduced in the data link layer.

4.6.4 Piggybacking :

SPPU : May 12

University Questions

Q. 1 What is piggybacking in Go-Back-N ARQ ?
(May 12, 4 Marks)

Need :

- In all the practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission.
- One way of achieving full duplex transmission is to have two separate channels one for forward data transmission and the other for reverse data transfer (for acknowledgements).
- But this will waste the bandwidth of the reverse channel almost entirely.
- A better solution would be to use each channel (forward and reverse) to transmit frames both ways, with both channels having the same capacity.

Principle :

- Let A and B be the users. Then the data frames from A to B are intermixed with the acknowledgements from A to B.
- By checking the kind field in the header of the received frame the received frame can be identified as either data frame or acknowledgement.
- One more improvement can be made. When a data frame arrives from A to B, the receiver B does not send the ACK frame back to A immediately.
- Instead B (receiver)waits until its network layer passes in the next data packet to be sent to A.
- The acknowledgement is then attached to this outgoing data frame and sent to A.
- Thus the acknowledgement travels alongwith next data frame from B to A and there is no need to send back the ACK frame separately.

Definition :

- Piggybacking is the technique in which the receiver temporarily delays the outgoing acknowledgement of the previously received frame.

Advantage of piggybacking :

- The major advantage of piggybacking is better use of available channel bandwidth.
- This happens because an acknowledgement frame need not be sent separately.

Disadvantages :

1. The disadvantage of piggybacking is the additional complexity.
2. If the data link layer waits too long before transmitting acknowledgement, then retransmission of frame would take place.

4.7 Sliding Window Protocols :

SPPU : May 07, May 13

University Questions

Q. 1 Why is a sliding window protocol preferred over a stop on wait protocol? Explain with appropriate examples.
(May 07, 4 Marks)

Q. 2 Explain sliding window protocol.

(May 13, 8 Marks)

- The next three protocols are more robust and bi-directional protocols.
- All these protocols are special type of protocol called **Sliding Window Protocols**.
- They show a different performance in terms of their efficiency, complexity and buffer requirements.

Sequence Number :

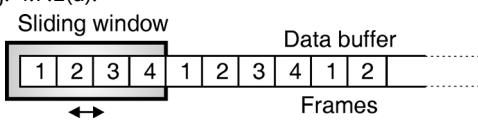
- One of the important features of all the sliding window protocols is that each outbound frame contains a sequence number, ranging from 0 to some maximum value.
- The maximum value is generally equal to $(2^n - 1)$. The value of n can be arbitrary.

Sliding Windows :

- Sliding windows are basically the imaginary boxes at the transmitter and receiver.



- This window holds the frames at the transmitting as well as receiving ends and provides the upper limit on the number of frames that can be transmitted before acknowledgement is obtained.
- So in short we can say that, at any instant of time, the sender maintains a set of sequence numbers corresponding to the frames it is permitted to send.
- These frames which are being permitted to sent are said to be residing inside the **sending window**.
- The receiver also maintains a **receiver window**. It corresponds to the set of frames that the receiver is permitted to accept.
- The sender and receiver windows can be of different sizes.
- The positive or negative acknowledgement (ACK or NAK) should be used after every frame.
- That means the sender sends frame, waits for the acknowledgement and sends the next frame or retransmits the original one, only after receiving either positive or negative acknowledgement from the receiver.
- In order to improve the efficiency, the sender sends multiple frames at time, the receiver checks the CRC of all the frames one by one and sends one acknowledgement for all the frames.
- This is the principle of operation of sliding window technique.
- In this technique, an imaginary window consisting of "n" number of data frames is defined.
- This means that up to n number of frames can be sent before receiving an acknowledgement.
- This is known as sliding window because this window can slide over the data buffer to be sent as shown in Fig. 4.7.1(a).



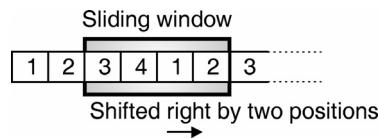
(G-222)Fig. 4.7.1(a) : Sliding window

- In Fig. 4.7.1(a) we have shown a sliding window of size $n = 4$.
- That means the sender can send four frames, at a time and then wait for the acknowledgement for the receiver.

- So there will be one acknowledgement corresponding to four sent frames.
- Note the numbering of frames in Fig. 4.7.1(a).
- As the window size is 4, the frame numbering is 1, 2, 3, 4 then again 1, 2, 3, ... the maximum frame number is restricted to n.

4.7.1 Sender and Receiver Sliding Windows :

- The sender as well as the receiver maintain their own sliding windows.
- The sender sends the number of frames allowed by the size of its own sliding window and then waits for an acknowledgement from the receiver.
- The receiver sends an acknowledgement which includes the number of the next frame that the sender should send.
- For example if the sender has sent frames 1 and 2 to the receiver and if receiver receives them correctly, then the acknowledgement sent by the receiver will include number-3 indicating the sender to send frame number-3.
- Now if the sender transmits the first 4 frames as per the size of its window and receives an acknowledgement for the first two frames, then the sender will slide its window two frames to the right as shown in Fig. 4.7.1(b) and sends 5th and 6th frames (i.e. frames 1 and 2 of the next lot).



(G-223)Fig. 4.7.1(b) : Illustration of sliding window mechanism

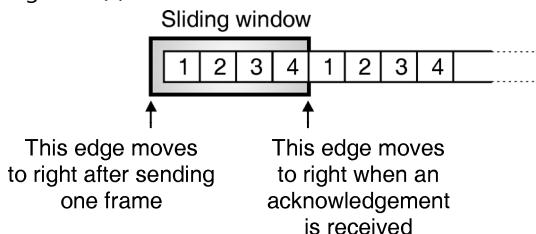
- The receiver now has four frames again, so it checks frames 3, 4, 1, 2 by checking their CRC.
- If it finds frame 3 faulty then it will send an acknowledgement which includes number 3. The sender will send 4-frames starting from frame-3 onwards.
- The sliding window mechanism thus uses two buffers and one window so as to exercise the flow control.
- The application program on the sender side will create the data to be transmitted and loads into the sender's buffer.



- Then the sender's sliding window is imposed on this buffer. These frames are then sent till all the frames have been sent.
- The receiver receives these data frames and carries out checks such as CRC, missing or duplicate frames etc. and stores the correct frames in the receiver buffer.
- The application program at the receiver then takes this data.

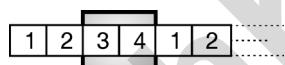
4.7.2 Movement of Sender's Window :

- Fig. 4.7.1(c) shows the sender's window.



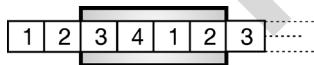
(G-224) Fig. 4.7.1(c) : Sender sliding window

- If the senders window size is 4 and frames 1 and 2 are sent but acknowledgement has not been received so far, then as shown in Fig. 4.7.1(d), the sender's windows will only contain two frames i.e. 3 and 4.



(G-225) Fig. 4.7.1(d) : Sender's window after sending first two frames but no acknowledgement

- Now if the sender receives acknowledgement bearing number 3 then it understands that the receiver has correctly received frames 1 and 2.
- The senders window now expands and includes the next two frames as shown in Fig. 4.7.1(e).

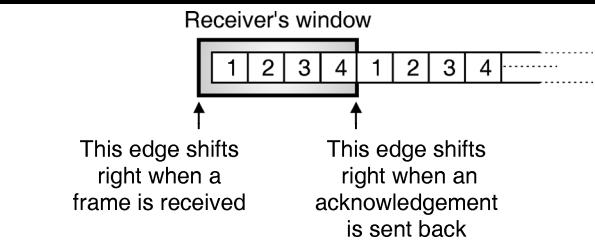


(G-226) Fig. 4.7.1(e) : Sender's window after receiving acknowledgement bearing number-3

- In this way the left edge of senders window will shift right when the data frames are sent and the right edge of the senders window will shift right when the acknowledgement is received.

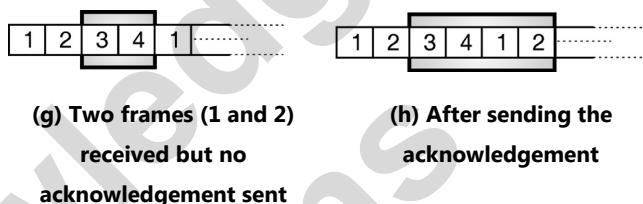
4.7.3 Movement of Receiver's Windows :

- Fig. 4.7.1(f) shows the receiver's window. Its left edge shifts right on receiving each data frame, where as its right edge shifts right when an acknowledgement is sent.



(G-227) Fig. 4.7.1(f) : Receiver's sliding window

- If we take the same example that we discussed for the sender's window then the position of receivers windows are as shown in Fig. 4.7.1(g) and (h).



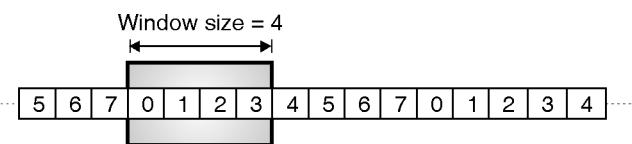
(G-228) Fig. 4.7.1 : Movement of receiver window

Ex. 4.7.1 : Two neighbouring nodes A and B uses sliding window protocol with 3 bit sequence number. As the ARQ mechanism Go back N is used with window size of 4. Assume A is transmitting and B is receiving show window position for the following events :

- Before A send any frame
- After A send frame 0, 1, 2 and receive ACK (acknowledgement) from B for 0 and 1.

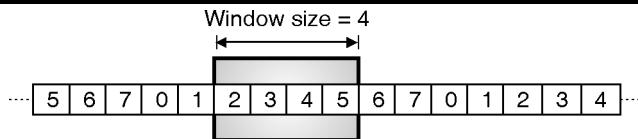
Soln. :

- The number of sequence number bits = m = 3.
∴ The sequence numbers will be 0, 1, 2, 3 ..., 6, 7. We can repeat these numbers. So the sequence will be, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4,
- The size of the window is 4.
- Fig. P. 4.7.1(a) shows the sender window (at A) before sending any frame.



(G-229) Fig. P. 4.7.1(a) : Before A sends any frame

- Fig. P. 4.7.1(b) shows that the window slides 2 positions because acknowledgement for frames 0 and 1 have been received.



(G-230) Fig. P. 4.7.1(b) : After sliding two frames

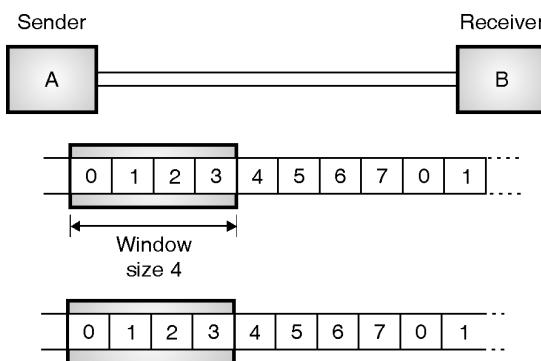
Ex. 4.7.2 : Two neighbouring nodes A and B use Go-Back N ARQ with a 3 bit sequence number. Assuming that A is transmitting and B is receiving. Show the window position and frame flow for the following sequence of events :

1. Initial position. Before A sends any frames window at A and B.
2. After A sends frames 0, 1, 2 and B acknowledge 0, 1 and the ACK are received by A.
3. A sends frames 3,4 and then receives REJ 3 from B.

Soln. :

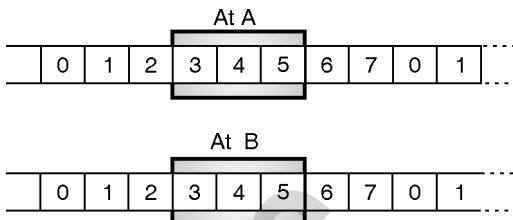
- The number of sequence bits = $m = 3$.
- \therefore The sequence numbers will be 0, 1, 2, 3 ..., 6, 7. Then these numbers will get repeated. So the sequence will be
- 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, ...
- The size of the window is 4.
 - The positions and frame flow at A and B for different situations are as shown in Fig. P. 4.7.2.

Case 1 : Initial position :



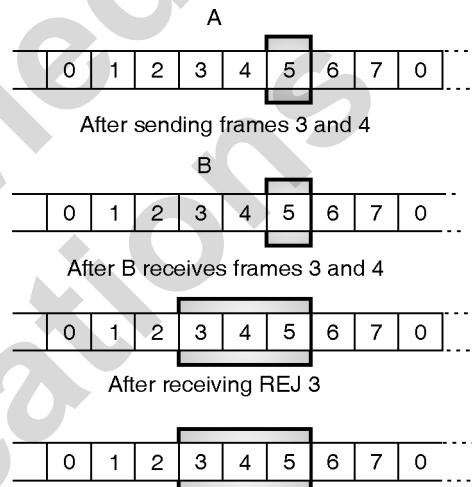
(G-231) Fig. P. 4.7.2(a)

Case 2 : After A sends frames 0, 1, 2 and B acknowledge 0, 1 :



(G-232) Fig. P. 4.7.2(b)

Case 3 : A sends frames 3 and 4 and then receives REJ 3 from B :



(G-233) Fig. P. 4.7.2 (c)

Ex. 4.7.3 : Imagine a sliding window protocol using so many bits for sequence numbers that wraparound never occurs. What relations must hold among the four window edges and the window size ?

Soln. :

Sequence number :

- Frames from the sending end are numbered in a sequential manner. The sequence number of each frame is included in the header.
- If m bits are reserved in the frame header for the sequence number, then the sequence numbers will range from 0 to $2^m - 1$. For example if $m = 4$ then the sequence numbers will range from 0 to 15.

Sliding window :

- Sliding window defines the range of sequence numbers that are of concern to sender and receiver.

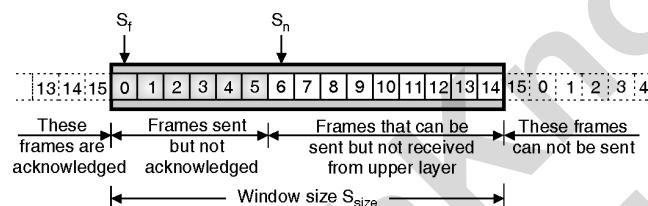


- The range of sequence numbers that are of concern to the sender is known as the **sender sliding window** whereas that concerned to the receiver is known as the **receiver's sliding window**.
- The **sender window** is an imaginary box which covers the sequence numbers of the data frames which can be in transit.
- In each position of this window, some of these sequence numbers represent the frames that have been sent while the other sequence numbers define the frames that can be sent.
- The maximum size of the window is $(2^m - 1)$.

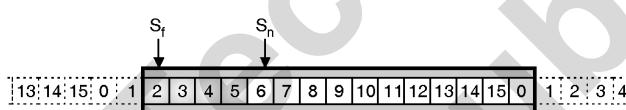
Relation between window edges and window size :

1. Send window :

- Fig. P. 4.7.3 shows the relation between the starting and ending edges of send window and the window size.



(a) Send window before sliding

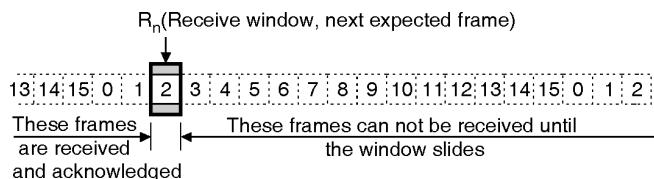


(b) Send window after sliding

(L-796) Fig. P. 4.7.3 : Relation between window edges and window size for send window of Go-back-N protocol

- As shown in Fig. P. 4.7.3, we can define three variables namely S_f (send window, the first outstanding frame), S_n (the send window, next frame to be sent) and S_{size} (send window size).
- S_f defines the sequence number of the first (oldest) outstanding frame. S_n defines the sequence number which is to be assigned to the next frame to be sent and S_{size} defines the size of the window.
- The send window can slide to the right after receiving the acknowledgements as shown in Fig. P. 4.7.3.

2. Receive window :



(c) Receive window



(d) Receive window after sliding

(L-797) Fig. P. 4.7.3 : Relation between window edges and window size for receive window of Go-Back-N protocol

- The size of this window is always 1 for the Go-Back-N ARQ. This window takes care that the correct data frames are received and the acknowledgement for the same is sent.
- Fig. P. 4.7.3 shows the receive window for Go-Back-N ARQ.
- There is only one variable i.e. R_n (receive window, next expected frame) in the receive frame.
- The sequence numbers to the left of the window represent the frames that have already been received and acknowledged.
- The sequence numbers to the right of the window represent the frames that can not be received.
- The receiver window slides by one slot at a time.

4.8 A One Bit Sliding Window Protocol (Stop and Wait ARQ) :

SPPU : May 12, Dec. 12, Dec. 14

University Questions

- Q. 1** Explain stop-and-wait ARQ protocol. **(May 12, 6 Marks)**
- Q. 2** Explain different ARQ techniques. Comment on the performance of each. **(Dec. 12, 8 Marks)**
- Q. 3** Explain in detail stop and wait and selective repeat ARQ system. **(Dec. 14, 6 Marks)**

Principle :

- This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1.
- It uses the stop-and-wait technique which we have discussed earlier. The sender sends one frame and waits to get its acknowledgement.



- The sender transmits its next frame only after receiving the acknowledgement for the earlier frame.
- So one bit sliding window protocol is also called as **stop and wait protocol**.
- The sequence of events taking place when a frame is transmitted and received is as follows :

1. The data link layer of the sending machine fetches the first packet from its network layer.
2. It builds the frame for it and sends it to receiver.
3. The receiver data link layer checks the received frame for duplication.
4. If ok, it passes the frame to its network layer.

(G-234)

The operation of protocol :

- The operation of this protocol is based on the ARQ (automatic repeat request) principle.
- So the sliding window protocols are also called as ARQ protocols.
- In this method the transmitter transmits one frame of data and waits for an acknowledgement from the receiver.
- If it receives a positive acknowledgement (ACK) it transmits the next frame. If it receives a negative acknowledgement (NAK) it retransmits the same frame.

Features added for retransmission :

- For retransmission, four features are added to the basic flow control mechanism :

 1. The transmitter stores the copy of last frame transmitted until an acknowledgement for that frame is received from the destination.
 2. For distinctly identifying different types of frames both data and ACK frames are numbered alternately 0 and 1. The first data frame sent is numbered as 0. This frame is acknowledged by an ACK1 frame. After receiving ACK1 the sender sends next data frame having a number 1.
 3. If an error occurs while transmission, the receiver sends a NAK frame back to the transmitter for retransmission of the corrupted frame. NAK frames which are not numbered tell the transmitter to retransmit the last frame transmitted.

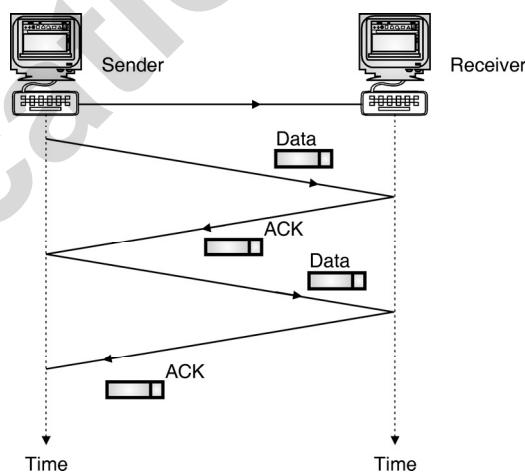
- 4. The transmitter has a timer to take care of the frame ACK which are lost. After a specified time if the transmitter does not receive a ACK or NAK frame it retransmits the last frame.

When is the retransmission necessary ?

- The retransmission of frame is essential under the following events :
 1. If the received frame is damaged.
 2. If the transmitted frame is lost.
 3. If the acknowledgement from the receiver is lost.
- Let us see the operation of the protocol under these circumstances one by one.

Operation under normal condition :

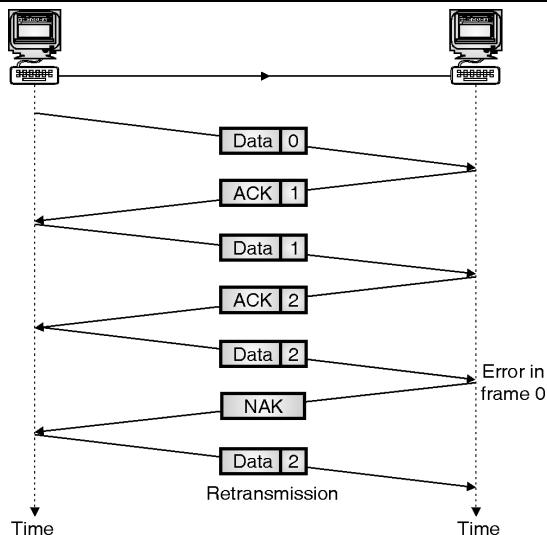
- Fig. 4.8.1 illustrates the protocol operation when everything is normal.
- No frame is lost so retransmission is not necessary.



(G-235) Fig. 4.8.1 : Stop and wait under normal condition

Stop and wait ARQ for damaged frame :

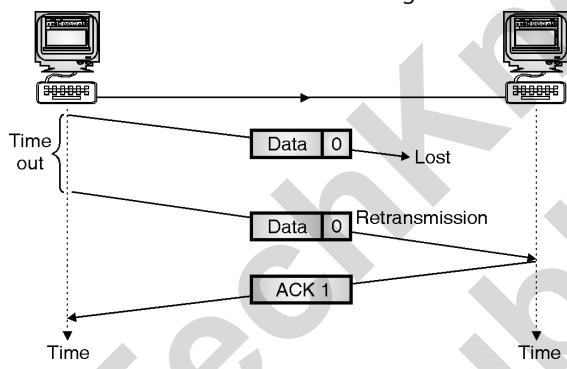
- As seen in Fig. 4.8.2(a) the transmitter transmits data frame numbered 0.
- The receiver returns an ACK1 indicating that the data frame numbered 0 is received without any error.
- The next data frame i.e. data 1 is sent. The corresponding acknowledgement ACK2 is received.
- The process goes on in this way, but if an error occurs the receiver sends a NAK requesting retransmission of the corrupted data frame (data 2). So the transmitter retransmits the data frame 2.



(G-236) Fig. 4.8.2(a) : Stop and wait ARQ damaged frame

Stop and wait ARQ for lost data frame :

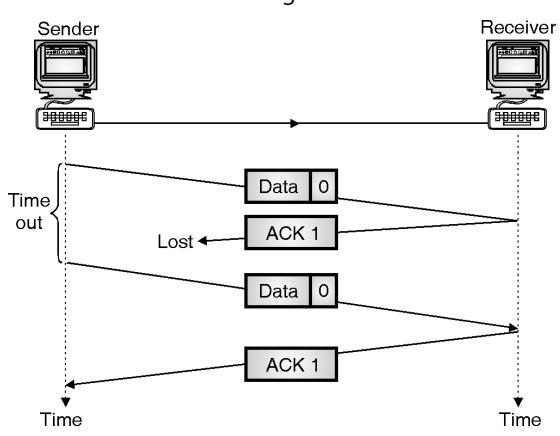
- Fig. 4.8.2(b) shows that if a data frame is lost and if the transmitter does not receive any type of acknowledgement from the receiver with a specified time it retransmits the same frame again.



(G-237) Fig. 4.8.2(b) : Stop and wait ARQ, lost data frame

Stop and wait ARQ for lost acknowledgement :

- Fig. 4.8.2(c) shows that if the acknowledgement sent by the receiver is lost, the transmitter retransmits the same data frame after its timer goes off.



(G-238) Fig. 4.8.2(c) : Stop and wait ARQ, lost ACK frame

- Stop and wait ARQ protocol becomes inefficient when the propagation delay is much greater than the time to transmit a frame.
- e.g. let us assume that we are transmitting frames that are 800 bits long over a channel that has a speed of 1 Mbps and let us also assume that the time taken for transmission of the frame and its acknowledgement is 30 mS.
- The number of bits that can be transmitted over this channel in 30 mS is equal to $30 \times 10^{-3} \times 1 \times 10^6 = 30,000$ bits.
- But in the stop-and-wait ARQ only 800 bits can be transmitted in this time period.
- This inefficiency is due to the fact that in stop and wait ARQ the transmitter waits, for an acknowledgement from the receiver before sending the next frame.
- The product of the bit rate and the delay that elapses before an action can take place is called the Delay-bandwidth product.
- The Delay-bandwidth product helps in measuring the lost opportunity in terms of transmitted bits.

Applications :

- Stop-and-Wait ARQ was used in IBM's Binary Synchronous Communications (Bisync) Protocol. It is also used in Xmodem, a popular file transfer protocol for modem.

Disadvantages of stop and wait protocol :

- Problem with Stop-and-Wait protocol is that it is very inefficient. At any one moment, only one frame is in transition.
- The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

4.9 A Protocol using GO Back n :

**SPPU : Dec. 12, Dec. 14, May 15, Dec. 15, May 17,
Dec. 17, May 18, Dec. 19**

University Questions

- Q. 1 Explain different ARQ techniques. Comment on performance of each. (Dec. 12, 8 Marks)**

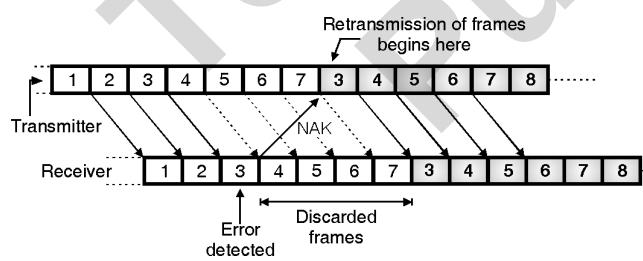


- Q. 2** Explain in detail Go-Back-N and selective repeat ARQ system. **(Dec. 14, Dec. 15, May 17, Dec. 17, May 18, Dec. 19, 6 Marks)**
- Q. 3** Explain Go-back-N automatic repeat request protocol. **(May 15, 5 Marks)**

- In this stop and wait protocol it was assumed that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgement to come back is negligible.
- But in some practical situations, this assumption is not correct.
- In the systems like satellite system the round trip time can be as long as 500 mS (propagation delay). This will reduce the efficiency of the protocol.
- Therefore an improved protocol known as **GO-Back-n ARQ** has been developed.
- It is a method used to overcome the inefficiency of the stop and wait ARQ by allowing the transmitter to continue sending enough frames so that the channel is kept busy while the transmitter waits for acknowledgements.
- In this method if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.

Principle of GO-back-n ARQ :

- Refer Fig. 4.9.1 to understand the principle of GO-Back-n ARQ.



(G-239) Fig. 4.9.1 : Go back n ARQ system

- The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame.
- It transmits the frames continuously as long as it does not receive the "NAK" signal.
- NAK is the negative acknowledgement signal sent by the receiver to the transmitter.

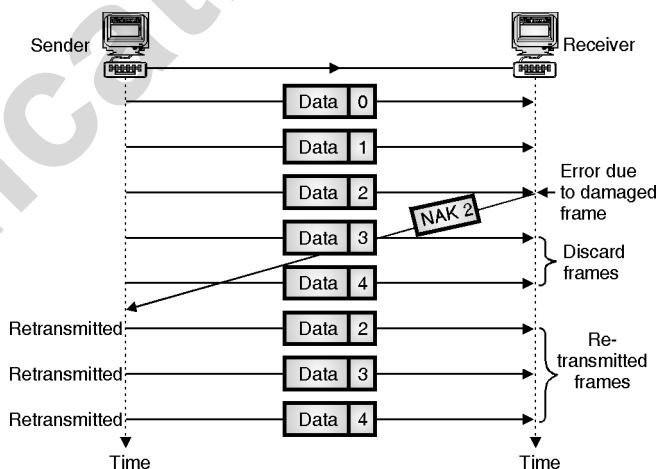
- When the receiver detects an error in the third frame as shown in Fig. 4.9.1, the receiver sends a NAK signal back to sender.
- But this signal takes some time to reach the transmitter. By that time the transmitter has transmitted frames upto frame 7.
- On reception of the NAK signal, the transmitter will retransmit all the frames from 3 onwards.
- The receiver discards all the frames it has received after 3 i.e. 3 to 7. It will then receive all the frames that are retransmitted by the transmitter.

Sources of error :

- The errors can get introduced, if the transmitted frames are damaged or lost or if the acknowledgement is lost.
- Let us consider the operation of this protocol under these conditions.

Operation when the frame is damaged :

- This condition is illustrated in Fig. 4.9.2(a).

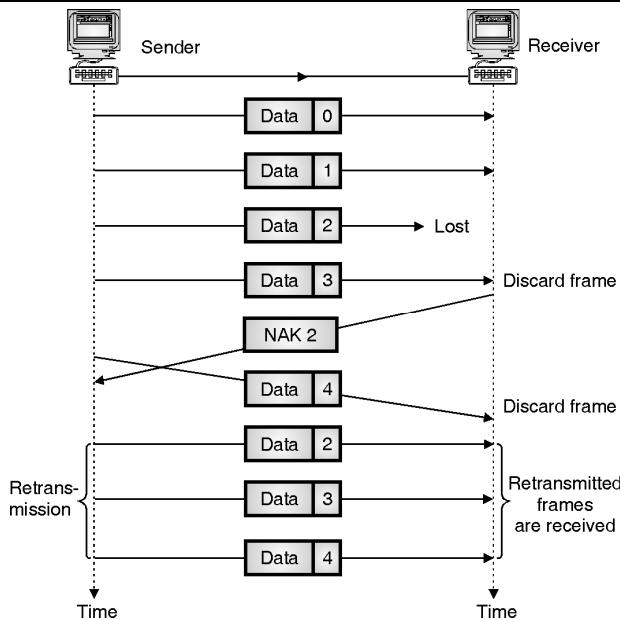


(G-240) Fig. 4.9.2(a) : Go-back-n, damaged data frame

- The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back.
- On receiving this signal, the transmitter starts retransmission from frame 2.
- All the frames received after frame 2 are discarded by the receiver.

Operation when a frame is lost :

- As shown in Fig. 4.9.2(b) the case of lost frame is also treated in the same manner as that of the damaged frame.

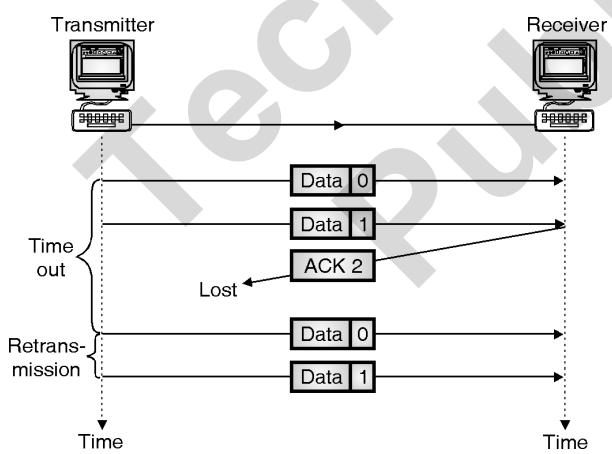


(G-241) Fig. 4.9.2(b) : Go-back-n, lost data frame

- The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

Operation when the acknowledgement is lost :

- Fig. 4.9.2(c) shows the condition for lost acknowledgement.



(G-242) Fig. 4.9.2(c) : Go-back-n, lost ACK frame

- In case of go-back-n method the transmitter does not expect an acknowledgement after every data frame.
- It cannot use the absence of sequential ACK numbers to identify lost ACK or NAK frames, instead it uses a timer.
- The transmitter can send as many frames as the window allows before waiting for an acknowledgement.

- Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the data frames again.
- The disadvantage of Go-back-n ARQ protocol is that in noisy channels it has poor efficiency because of the need to retransmit the frame in error and all the subsequent frames.

Disadvantages of Go back n :

- It transmits all the frames if one frame is damaged or lost.
- It transmits frames continuously as long as it does not receive the NAK signal.
- The NAK signal takes some time to reach the sender. Till that time the sender has already sent some frames. All those will be retransmitted after receiving the NAK.
- The error can get introduced if the NAK is lost.

4.9.1 Pipelining :

- In networking a new task is often started before the previous task has been completed. This is called pipelining.
- The principle of pipelining is not used in stop-and-wait ARQ but it is used in GO-Back-n ARQ and the selective repeat ARQ.
- Pipelining improves the efficiency of transmission.

4.10 Selective Repeat ARQ :

SPPU : Dec. 14, Dec. 15, May 16, May 17, Dec. 17,
May 18, Dec. 19

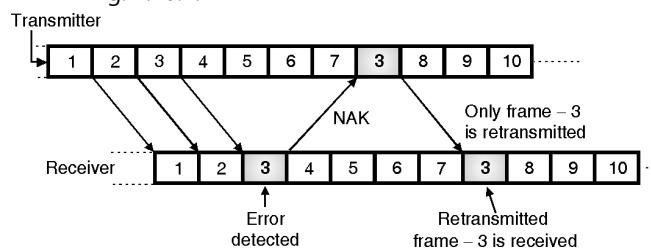
University Questions

- Q. 1** Explain in detail stop and wait and selective repeat ARQ system. (Dec. 14, 6 Marks)
- Q. 2** Explain in detail Go-Back-N and selective repeat ARQ system. (Dec. 15, May 17, Dec. 17, May 18, Dec. 19, 6 Marks)
- Q. 3** Explain selective repeat ARQ for noiseless channels. (May 16, 6 Marks)

- In this method only the specified damaged or lost frame is retransmitted.
- A selective repeat systems differs from the go-back-n method in the following ways :



1. The receiver can do sorting of data frames and is also able to store frames received after it has sent the NAK until the damaged frame has been replaced.
2. The transmitter has a searching mechanism that allows it to choose only those frame which are requested for retransmission.
3. The window size in this method is less than or equal to $(n + 1)/2$, whereas in case of go-back-n it is $n - 1$.
- The principle of operation of this protocol is illustrated in Fig. 4.10.1.



(G-243)Fig. 4.10.1 : Selective repeat ARQ system

- In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next frame.
- It transmits the frames continuously till it receives the "NAK" signal from the receiver.
- The receiver sends the "NAK" signal back to the transmitter as soon as it detects an error in the received frame.
- For example the receiver detects an error in the third frame, as shown in Fig. 4.10.1.
- By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 4.10.1.
- On reception of "NAK" signal, the transmitter will retransmit only the frame-3 and then continues with the sequence 8, 9... as shown in Fig. 4.10.1.
- The frames 4, 5, 6 and 7 received by the receiver which do not contain any error are not discarded by the receiver.
- The receiver receives the retransmitted frames in between the regular frames. Therefore the receiver will have to maintain the frames sequentially.
- Hence the selective repeat ARQ is the most efficient but the most complex protocol, of all the ARQ protocols.
- Thus in selective repeat ARQ only the frame which is damaged or lost is retransmitted by the transmitter.

- The lost ACK or NAK frames are treated in the same manner as the go-back-n method.
- When the transmitter reaches either the capacity of its window $[(n + 1)/2]$ or the end of its transmission it sets a timer.
- If no acknowledgement arrives in the allotted time, all the frames that remain unacknowledged are retransmitted.
- The disadvantage of this method is that because of the complexity of sorting and storage required by the receiver and the extra logic needed by the transmitter to select frames for retransmission, the system becomes more expensive.
- The advantage of this system is that it gives the best throughput efficiency.
- This is due to the use of pipelining in selective repeat ARQ.

4.11 Protocol Performance :

SPPU : May 09, May 11, Dec. 12

University Questions

- Q. 1** Explain stop and wait ARQ, GO Back-n ARQ and selective repeat ARQ. Comment on the performance of each. **(May 09, 10 Marks)**
- Q. 2** Explain stop and wait ARQ, GO Back-n ARQ and selective repeat ARQ. Comment on the performance of each. **(May 11, 8 Marks)**
- Q. 3** Explain different ARQ techniques. Comment on performance of each. **(Dec. 12, 8 Marks)**

- The throughput efficiency is the measure of the performance of an ARQ protocol. For any channel a certain bandwidth and bit error rate are specified.
- For such a channel there will be an optimum operating condition that will support for the maximum "Net Data Throughput" (NDT).
- NDT indicates the number of usable characters detected at the receiver. It indicates the number of correct bits detected in a specified period of time.
- This is done by distinguishing between the total number of bits received (including the check bits) and the number of correct bits.
- Throughput efficiency is defined as :



$$\eta = \frac{t_f}{t_f + 2t_p} \quad \dots(4.11.1)$$

where t_f = Transmission time required to transmit a frame

t_p = Propagation time required to reach destination for a transmitted bit

N = Frame size (bits)

R = Data rate

- Suppose A is a sender and B is a receiver. Then the assumptions are as follows :

Assumptions :

- Receiver sends an immediate acknowledgement on the reception of a data frame.
- Size of acknowledgement frame is very small.
- Flow is unidirectional.
- Sender receives the acknowledgement after $t_f + t_p + t_p$ time. It can send data immediately after receiving acknowledgement.
- If t_f and t_p are constant, t_p/t_f is constant.

$$\text{Let } A = t_p/t_f$$

$$\therefore \eta = 1/(1+2A)$$

- Propagation time is equal to distance (d) of the link divided by velocity of propagation (v).

$$\therefore t_p = d/v$$

Transmission time is equal to the length of the frame (bits), divided by rate R.

$$\therefore t_f = L/R$$

$$\therefore A = \frac{d/v}{L/R} = \frac{Rd}{Lv}$$

Ex. 4.11.1 : Calculate the throughput for stop-and-wait flow control mechanism if the frame size is 4800 bits, bit rate is 9600 bps and distance between device is 2000 km. Speed of propagation over the transmission is 200,000 km/s.

Soln. :

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{4800}{9600} = 0.5 \text{ sec}$$

$$t_p = \frac{2000}{200000} = 0.01 \text{ sec}$$

$$\text{We know, } A = t_p/t_f$$

$$\therefore A = 0.01 / 0.5 = 0.02$$

$$\text{Since, } \eta = 1/(1+2A) = 1/(1+2 \times 0.02)$$

$$= 0.96$$

$$\therefore \% \eta = 96\% \quad \dots\text{Ans.}$$

Ex. 4.11.2 : A channel has a bit rate of 4 kbps and propagation delay of 20 msec. For what range of frame sizes does stop and wait gives an efficiency of at least 50 percent ?

Soln. :

Given : Bit rate = 4 kbps, Propagation delay $t_p = 20 \text{ msec}$, Efficiency $\eta \geq 50\%$ i.e. $0.5 \leq \eta \leq 1$

To find : Range of frame size.

Step 1 : Calculate value of t_f :

$$\eta = \frac{t_f}{t_f + 2t_p}$$

$$\text{For } \eta = 0.5 \text{ we get, } 0.5 = \frac{t_f}{t_f + (2 \times 20 \times 10^{-3})}$$

$$\therefore 0.5 t_f + 20 \times 10^{-3} = t_f$$

$$\therefore t_f = 40 \times 10^{-3} \text{ sec.}$$

Note that t_f = Transmission time for 1 frame

Step 2 : Calculate the frame size :

$$R = \text{Data rate} = 4 \text{ kbps} = 4000 \text{ bps}$$

$$\therefore N = R \times t_f$$

where N = Frame size

$$\therefore N = 40 \times 10^{-3} \times 4 \times 10^3$$

$$= 160 \text{ bits}$$

...Ans.



(G-244)Fig. P. 4.11.2 : 1 frame size

Ex. 4.11.3 : A channel has a bit rate of 4.8 kbytes/sec and a propagation delay of 20 msec. For what range of a frame size does stop and wait protocols given an efficiency of 50%.

Soln. :

Explanation :

- If the channel capacity is B bytes/sec, the frame size L bytes and the round trip propagation time T seconds, the time required to transmit a single frame is L/B sec.
- After the last bit of a data frame has been sent, there is a delay of at least T/2 for the acknowledgement to come back, for a total delay of T.



- In stop-and-wait the line is busy for $T/2$ and idle for T , giving an efficiency of $L/(L + BT)$.

Given :

$$\text{Bit rate (B)} = 4.8 \text{ k bits sec.}$$

$$\text{Propagation delay (T)} = 20 \text{ msec.}$$

$$\text{Efficiency} = 50\%, \text{ Frame size (L)} = ?$$

$$\text{Efficiency} = \frac{L}{(L + BT)}$$

$$0.5 = \frac{L}{(L + 4.8 \times 10^3 \times 20 \times 10^{-3})}$$

$$= \frac{L}{(L + 96)}$$

$$0.5(L + 96) = L$$

$$0.5L + 48 = L$$

$$\therefore L = \frac{48}{0.5} = 96 \text{ bits.}$$

4.11.1 How to Improve the Throughput Efficiency ?

- If the data signalling rate (R) is increased, then the time taken to transmit each block (B/R) will be reduced.
- However as delay remains unchanged, the throughput efficiency will decrease.
- To compensate for this it will be necessary to use longer blocks for higher data rates (R).
- Longer blocks however will have a greater probability of error, therefore an optimum block length is must be obtained for any particular system.
- Throughput efficiency also depends on the type of system used.
- For a half duplex system the transmission efficiency is very poor. An alternative method which gives greater efficiency is to use a continuous mode of transmission instead of block by block transmission.
- In this system the data blocks are transmitted without interruption unless a negative acknowledgement signal (NAK) is received by the transmitting end.
- When NAK is transmitted back to the transmitter it will retransmit the error block. The continuous transmission method avoids the dead time but needs more storage or buffering.

4.12 Solved Examples :

Ex. 4.12.1 : Consider an error free 64 kbps satellite channel used to send 512 byte data frames in one direction with very short acknowledgements coming back the other way. What is the maximum throughput for window sizes of 1, 7, 15 and 127 ?

Soln. :

Given : Data rate $= R = 64 \text{ kbps} = 64 \times 10^3 \text{ bps.}$

Frame size $N = 512 \text{ bytes} = 512 \times 8 \text{ bits}$

Window sizes = 1, 7, 15 and 127.

To find : Maximum throughput.

Step 1 : Calculate t_f :

Transmission time for 1 frame is given by,

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{N}{R} = \frac{512 \times 8}{64 \times 10^3}$$

$$\therefore t_f = 64 \times 10^{-3} \text{ sec}$$

Step 2 : Calculate A :

$$A = \frac{t_p}{t_f}$$

But $t_p = \text{Propagation delay} = 270 \text{ mS}$ for satellite channel

$$\therefore A = \frac{270 \times 10^{-3}}{64 \times 10^{-3}} = 4.2187$$

Step 3 : Maximum throughput :

$$\eta_{\max} = \frac{W}{1 + 2A}$$

Where $W = \text{Window size.}$

1. For $W = 1$, $\eta_{\max} = \frac{1}{1 + (2 \times 4.2187)} = 0.1059$
2. For $W = 7$, $\eta_{\max} = \frac{7}{1 + (2 \times 4.2187)} = 0.7417$
3. For $W = 15$, $\eta_{\max} = 1.589$
4. For $W = 127$, $\eta_{\max} = 13.459.$

Ex. 4.12.2 : A 100 km long cable runs at T_1 data speed.

The propagation speed in cable is $2/3$ of the speed of light. How many bits fit in the cable ?

Soln. :

Given : $L = 100 \text{ km} = 1 \times 10^5 \text{ m},$

Data rate of $T_1 = 1.544 \text{ Mb/s}$

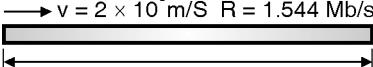
Speed $v = 2/3 \times 3 \times 10^8 \text{ m/S} = 2 \times 10^8 \text{ m/S}$

To find : Number of bits fitting in the cable.



Number of bits in 1 sec. = 1.544×10^6 bits
 Distance covered in 1 sec = 2×10^8 m
 \therefore Number of bits corresponding to 10^5 m cable is given by,

$$x = \frac{1.544 \times 10^6}{2 \times 10^8} \times 10^5$$

 $= 772 \text{ bits}$...Ans.

 $\rightarrow v = 2 \times 10^8 \text{ m/S} R = 1.544 \text{ Mb/s}$

(G-1434) Fig. P. 4.12.2

- Ex. 4.12.3 :** Consider the use of 1000 bit frames on a 1 Mbps satellite channel. What is the maximum Links utilization for :
 1. Stop and wait ARQ.
 2. Continuous ARQ with Window size 7.
 3. Continuous ARQ with Window size 127.

Soln. :

Given : Frame size = 1000 bits, Bit rate = 1 Mbps

To find : Link utilization

1. For stop and wait ARQ :

$$\begin{aligned} t_f &= \frac{\text{Frame size}}{\text{Bit rate}} = \frac{1000}{1 \times 10^6} \\ &= 1 \times 10^{-3} \text{ s i.e. } 1 \text{ mS.} \\ t_p &= 270 \text{ mS propagation delay for a satellite channel} \\ \therefore A &= \frac{t_p}{t_f} = \frac{270}{1} = 270 \\ \therefore \eta &= \frac{1}{1 + 2A} \\ &= \frac{1}{1 + 2(270)} = 1.848 \times 10^{-3} \\ &= 0.1848\% \end{aligned}$$

...Ans.

2. For continuous ARQ with W = 7 :

$$\begin{aligned} \eta &= \frac{W}{1 + 2A} \\ &= \frac{7}{1 + (2 \times 270)} \\ &= 1.2936\% \end{aligned}$$

...Ans.

3. Continuous ARQ with W = 127 :

$$\begin{aligned} \eta &= \frac{127}{1 + (2 \times 270)} \\ &= 23.4696\% \end{aligned}$$

...Ans.

- Ex. 4.12.4 :** Calculate link utilization efficiency for stop-and-wait protocol, if bit rate = 19.2 kbps, Frame size = 960 bits and propagation time = 0.06 sec. for window size = 3 and 7.

Soln. :

Given : Bit rate R = 19.2 kbps = 19.2×10^3 bps

Frame size N = 960 bits

Propagation time t_p = 0.06 sec.

Window size W = 3 and 7.

To find : Link utilization efficiency (η).

Step 1 : Calculate t_f :

Transmission time for 1 frame is t_f is given by,

$$t_f = \frac{\text{Frame size (N)}}{\text{Bit rate (R)}} = \frac{960}{19.2 \times 10^3}$$

$$\therefore t_f = 0.05 \text{ sec}$$

Step 2 : Calculate A :

$$A = \frac{t_p}{t_f} = \frac{0.06}{0.05} = 1.2$$

Step 3 : Calculate efficiency :

When W = 3,

$$\eta = \frac{W}{1 + 2A} \text{ Where } W = \text{Window size}$$

$$\therefore \eta = \frac{3}{1 + (2 \times 1.2)} = 0.8823 \quad \dots \text{Ans.}$$

When W = 7,

$$\eta = \frac{W}{1 + 2A}$$

$$\therefore \eta = \frac{7}{1 + (2 \times 1.2)} = 2.05 \quad \dots \text{Ans.}$$

- Ex. 4.12.5 :** A channel with 10 kbps bit rate and propagation delay of 10 msec, what should be the frame size to obtain efficiency of at least 50% for stop and wait ARQ.

Soln. :

Given : Bit rate : 10 kbps, Propagation delay = 10 msec,
 $0.5 \leq \eta \leq 1$

To find : Frame size

Step 1 : Calculate value of t_f :

$$\eta = \frac{t_f}{t_f + 2t_p} \quad \text{where } t_f = \text{Time for one frame}$$

$$\therefore 0.5 = \frac{t_f}{t_f + (2 \times 10 \times 10^{-3})}$$



$$\therefore t_f = 0.02 \text{ sec}$$

$$\therefore t_f = 20 \text{ msec}$$

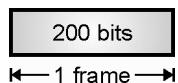
Step 2 : Calculate the frame size (N) :

$$R = 10 \text{ kbps} = 10000 \text{ bps}$$

$$\therefore N = R \times t_f = 10 \times 10^3 \times 20 \times 10^{-3}$$

$$\therefore N = 200 \text{ bits}$$

...Ans.



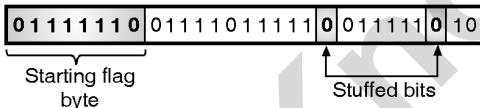
(G-263)Fig. P. 4.12.5

Ex. 4.12.6 : A bit string 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

Soln. :

- The original bit stream and the stream after bit stuffing are shown in Fig. P. 4.12.6.

Original data : 0 111101111101111110

Outgoing data : 

(G-217)Fig. P. 4.12.6

Ex. 4.12.7 : Apply bit stuffing

011011111111111111110010

Soln. : The outgoing data after bit stuffing is shown in Fig. P. 4.12.7.

0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0
↑ ↑ ↑
Stuffed bits

(G-218)Fig. P. 4.12.7

Ex. 4.12.8 : A channel has a bit rate of 4.8 k bits/sec and a propagation delay of 20 m sec. For what range of a frame size does stop and wait protocols given an efficiency of 50%.

Dec. 01, 6 Marks

Soln. :

Explanation :

- If the channel capacity is B bits/sec, the frame size L bits and the round trip propagation time T seconds, the time required to transmit a single frame is L/B sec. After the last bit of a data frame has been sent, there is a delay of at least T/2 for the acknowledgment to come back, for a total delay of T.

- In stop-and-wait the line is busy for and idle for T, giving an efficiency of $L/(L + BT)$.

Given :

$$\text{Bit rate (B)} = 4.8 \text{ k bits sec.}$$

$$\text{Propagation delay (T)} = 20 \text{ m sec.}$$

$$\text{Efficiency} = 50\%, \text{ frame size (L)} = ?$$

$$\text{Efficiency} = \frac{L}{(L + BT)}$$

$$0.5 = \frac{L}{(L + 4.8 \times 10^3 \times 20 \times 10^{-3})}$$

$$= \frac{L}{(L + 96)}$$

$$0.5(L + 96) = L$$

$$0.5L + 48 = L$$

$$\therefore L = \frac{48}{0.5} = 96 \text{ bits}$$

Ex. 4.12.9 : What is effective data rates for the unrestricted and stop wait protocol if capacity 16 Mbps, signal speed 200 Mps, distance between sender and receiver 200 meters, time to create one frame 12 sec, number of bits in a frame 500, number of data bits in a frame 450, and number of bits in an acknowledgement 80 ? **May 04, 8 Marks**

Soln. :

Given :

$$B = \text{Length of block} = 500 \text{ bits}$$

$$R = \text{Input data rate bits/sec} = 16 \times 10^6 \text{ bits/sec.}$$

$$T_d = \text{Total dead time}$$

$$= \text{Turnround time} + \text{Propagation delay time}$$

$$= 2 \text{ sec.}$$

$$\eta = \left(\frac{B/R}{B/R + T_d} \right) \times 100 \%$$

$$= \left(\frac{\frac{500}{16 \times 10^6}}{\frac{500}{16 \times 10^6} + 2} \right) \times 100 \% = 15.62 \times 10^{-3}$$

Review Questions

- State the various design issues for the data link layer.
- State and explain the various services provided to the network layer.



- | | | | |
|-------|---|-------|--|
| Q. 3 | What are the different framing methods ? | Q. 11 | Explain the stop and wait protocol. |
| Q. 4 | Explain character stuffing. | Q. 12 | State drawbacks of stop and wait protocol. |
| Q. 5 | What is bit stuffing ? | Q. 13 | Explain the Go back n protocol. |
| Q. 6 | Explain the function of timer. | Q. 14 | What is pipelining ? |
| Q. 7 | Write a note on error control. | Q. 15 | Write a note on : Selective repeat ARQ. |
| Q. 8 | Explain the simplex protocol for noisy channel. | Q. 16 | Define throughput efficiency and explain how it can be increased ? |
| Q. 9 | What is piggybacking ? | | |
| Q. 10 | Write a note on sliding window protocols. | | |

□□□

TechKnowledge
Publications

Unit III

Chapter

5

Random Access Techniques

Syllabus

Random access techniques : CSMA, CSMA / CD and CSMA / CA, Controlled access techniques : Reservation, Polling, Token passing, Channelization : FDMA, TDMA, CDMA.

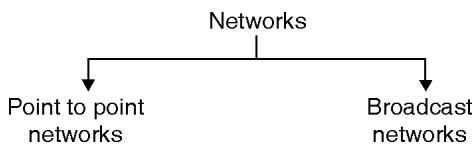
Chapter Contents

- 5.1 Introduction
- 5.2 The Channel Allocation Problem
- 5.3 Multiple Access
- 5.4 Multiple Access (ALOHA System)
- 5.5 Carrier Sense Multiple Access (CSMA)
- 5.6 Collision Free Protocols
- 5.7 Controlled Access
- 5.8 Channelization / Multiple Access Techniques



5.1 Introduction :

- We can classify the networks into two categories as shown in Fig. 5.1.1.

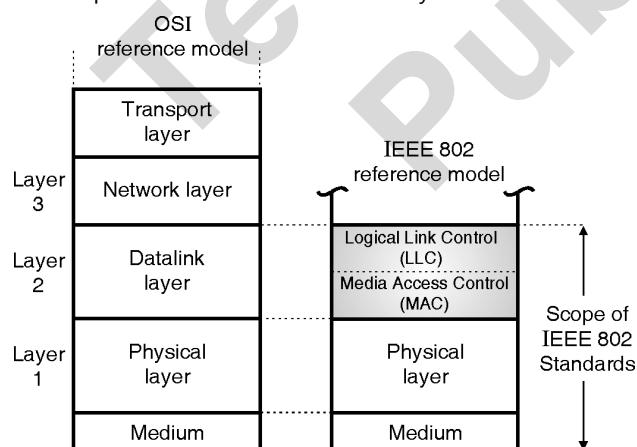


(G-264) Fig. 5.1.1

- In this chapter, we are going to discuss the broadcast networks and their protocols.
- The broadcast channels are also called as **multi-access channels** or **random access channels**.
- In the broadcast networks the most important point is the criteria by which we decide, who is allowed to use the common channel when more than one users want to use it.
- A protocol is used to make this decision.
- Such a protocol, belongs to a sublayer of data link layer called the MAC (Medium Access Control) sublayer.
- The MAC sublayer is very important in LANs because it is a broadcast network.

5.1.1 MAC and LLC Sublayers :

- Fig. 5.1.2 shows the layered OSI model (partial) to show the position of MAC and LLC sublayers.



(G-265) Fig. 5.1.2 : IEEE 802 protocol layers compared to OSI model

- We will discuss the broadcast protocols corresponding to the lower layers (1 and 2) of the OSI model as shown in Fig. 5.1.2.

- Fig. 5.1.2 relates the LAN protocols with the OSI architecture. This architecture was developed by IEEE 802 committee and it has been accepted as LAN standard.
- It is called as IEEE 802 reference model. Let discuss this model layer by layer.

Functions of Media Access Control (MAC) sublayer :

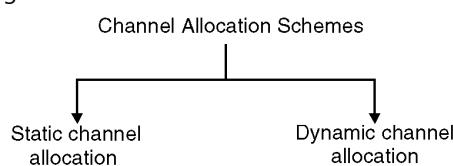
- To perform the control of access to media.
- It performs the unique addressing to stations directly connected to LAN.
- Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

- Error recovery.
- It performs the flow control operation.
- User addressing.

5.2 The Channel Allocation Problem :

- In a broadcast network, the single communication channel is to be allocated to one transmitting user at a time. The other users connected to this medium should wait.
- This is called as channel allocation. There are two different schemes used for channel allocation as shown in Fig. 5.2.1.



(G-266) Fig. 5.2.1

5.2.1 Static Channel Allocation in LANs and MANs :

- The traditional way of allocating a single channel, among many users is by means of frequency division multiplexing (FDM).
- The Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are the examples of static channel allocation.
- In these methods either a fixed frequency band or a fixed time slot is allotted to each user. Thus either the entire available bandwidth or entire time is shared.



- The problem in these methods is that if all the N number of users are not using the channel the channel bandwidth is wasted and if there are more than N users who want to use the channel they cannot do so for the lack of bandwidth.
- For a small number of users and light traffic the static FDM is an efficient method of allocation but its performance is poor for large number of users, bursty and heavy traffic etc.
- The static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used, for computer networks where the traffic is of bursty nature.
- To see the poor performance of static channel, let us consider an example for FDM system where the mean time delay (T) for a channel of capacity C bps, with an arrival rate of λ frames/sec.
- Each frame having a length drawn from an exponential probability density function with mean $1/\mu$ bits/frame is given as,

$$T = \frac{1}{\mu C - \lambda}$$

- If the single channel is divided into N independent subchannels the above equation is modified as follows :

$$T_{FDM} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda}$$

$$T_{FDM} = NT$$

- From the above equation, it is clear that the mean delay using FDM is worse.
- The static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used, for computer networks where the traffic is of bursty nature.

5.2.2 Dynamic Channel Allocation :

- In this method either a fixed frequency or fixed time slot is not allotted to the user.
- The user can use the single channel as per his requirement.

Assumptions :

- Following assumptions are made for the implementation of this method :
 1. Station model – This model consists of N independent stations such as a PC, computer etc. which can generate frames for transmission.

- 2. Single channel – A single channel is available for all communication.
- 3. Collision – If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting signal is garbled. This is called as collision.
- 4. Continuous or slotted time – There is no master clock used to divide time into discrete time intervals. So frames can begin at any random instant. This is continuous time. For a slotted time, the time is divided into discrete time slots.
- 5. Carrier or No carrier sense – Stations sense the channel before transmission or they directly transmit without sensing the channel.

5.3 Multiple Access :

SPPU : Dec. 11

University Questions

- Q. 1** Explain three categories of multiple access protocols. **(Dec. 11, 10 Marks)**

- When a number of stations (users) use a common link of communication system we have to use a multiple access protocol in order to coordinate the access to the common link.
- The three techniques used to deal with the multiple access problem are as follows :
 1. Random Access
 2. Controlled Access
 3. Channelization
- Let us discuss them one by one.

5.3.1 Random Access :

SPPU : May 06, Dec. 06, Dec. 11

University Questions

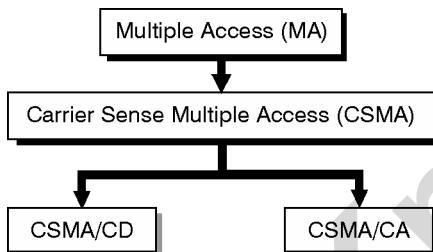
- Q. 1** State various random access techniques. Compare the performance of all the techniques. **(May 06, 6 Marks)**

- Q. 2** Explain any two random access techniques and comment on their performance. **(Dec. 06, 6 Marks)**

- Q. 3** Explain three categories of multiple access protocols. **(Dec. 11, 10 Marks)**



- In the random access technique there is no control station.
- Each station will have the right to use the common medium without any control over it.
- With increase in number of stations, there is an increased probability of **collision** or **access conflict**.
- The collisions will occur when more than one user tries to access the common medium simultaneously.
- As a result of such collisions some frames can be either modified (due to errors) or destroyed.
- In order to avoid collisions, we have to set up a procedure.
- The evolution of the random access methods is shown in Fig. 5.3.1.



(G-267) Fig. 5.3.1 : Evolution of random access methods

5.3.2 Evolution of Random Access Methods :

- The first method in the evolution ladder of Fig. 5.3.1, known as ALOHA used a simple procedure called multiple access (MA).
- It was improved to develop the carrier sense multiple access (CSMA).
- The CSMA further evolved into two methods namely CSMA/CD (CSMA with collision detection) and CSMA/CA (CSMA with collision avoidance) which avoids the collisions.

5.4 Multiple Access (ALOHA System) :

ALOHA System :

- Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as Contention systems.
- The ALOHA system is a contention protocol which was developed at the University of Hawaii in the early 1970's by Norman Abramson and his colleagues.

- The ALOHA system has two versions :
 1. Pure ALOHA – Does not require global time synchronisation.
 2. Slotted ALOHA – Requires time synchronisation.

5.4.1 Pure ALOHA :

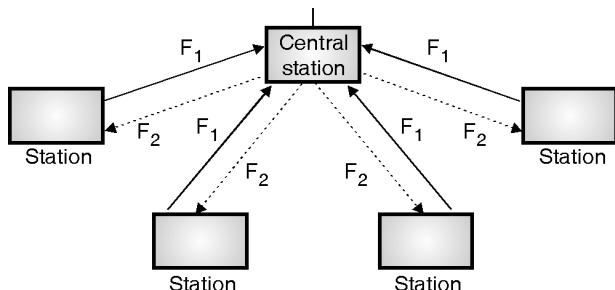
SPPU : Dec. 05, May 09, May 13, Dec. 18

University Questions

- Q. 1** Explain ALOHA, slotted ALOHA and CSMA/CD. Comment on the efficiency of each random access technique. **(Dec. 05, May 09, 10 Marks)**
- Q. 2** Explain pure and slotted ALOHA. **(May 13, 8 Marks)**
- Q. 3** Explain in brief ALOHA, slotted ALOHA mentioning efficiency, advantages in each case. **(Dec. 18, 6 Marks)**

Principle :

- It works on a very simple principle. Essentially it allows for any station to broadcast at any time.
- If two signals collide, each station simply waits a random time and try again.
- Collisions are easily detected. As shown in the Fig. 5.4.1, when the central station receives a frame it sends an acknowledgement on a different frequency.



F_1 = Broadcast frequency from the individual stations.

F_2 = Broadcast frequency from the central station.

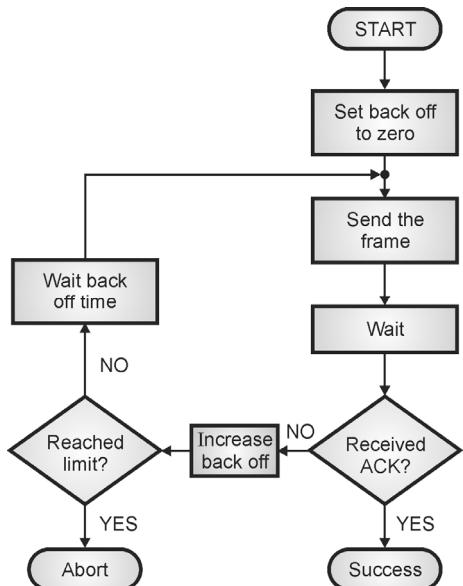
(G-268) Fig. 5.4.1 : Pure ALOHA system

- If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does get an acknowledgement it assumes that collision had occurred and is ready to retransmit.
- The advantage of pure ALOHA is its simplicity in implementation but its performance becomes worse as the data traffic on the channel increases.



5.4.2 Protocol Flow Chart for ALOHA :

- Fig. 5.4.2 shows the protocol flow chart for ALOHA.



(G-269)Fig. 5.4.2 : Protocol flow chart for ALOHA

Explanation :

- A station which has a frame ready for transmission will send it.
- Then it waits for sometime.
- If it receives the acknowledgement then the transmission is successful.
- Otherwise the station uses a backoff strategy, and will send the packet again.
- After sending the packet many times if there is no acknowledgement then the station aborts the idea of transmission.

Contention system :

- Systems in which multiple users share a common channel in such a way that can lead to a conflict or collision are known as the contention systems.
- Whenever two frames try to occupy the channel at the same time, there is bound to be a collision and both will be garbled.
- Retransmission is essential for all the destroyed frames.

5.4.3 Efficiency of an ALOHA Channel :

SPPU : Dec. 05, May 09, Dec. 18

University Questions

- Q. 1** Explain ALOHA, slotted ALOHA and CSMA/CD.
Comment on the efficiency of each random access technique. **(Dec. 05, May 09, 10 Marks)**

- Q. 2** Explain in brief ALOHA, slotted ALOHA mentioning efficiency, advantages in each case.

(Dec. 18, 6 Marks)

- Efficiency of an ALOHA system is that fraction of all transmitted frames which escape collisions i.e. which do not get caught in collisions.
- Consider ∞ number of interactive users at their computers (stations). Each user is either typing or waiting. Initially all of them are in the typing state.
- When a user types a line, the user stops and waits. The station then transmits a frame containing this line and checks the channel to confirm the success. If it is successful then the user will start typing again, otherwise the user waits and its frame is retransmitted many time till it is sent successfully.

Frame time :

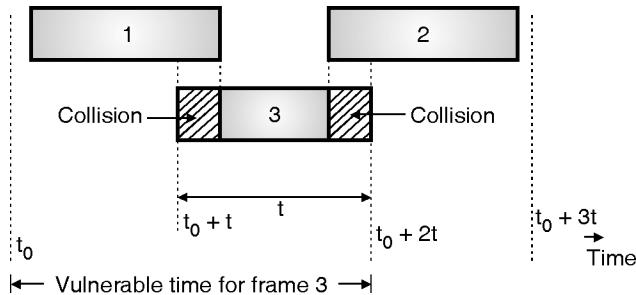
- Let the frame time be defined as the amount of time required to transmit the standard fixed length frame. Note that
- Frame time =
$$\frac{\text{Frame length}}{\text{Bit rate}}$$
- We assume that ∞ number of users generate new frames according to the Poisson's distribution with an average N frames per frame time.
- The value of $N > 1$ indicates that the users are generating frames at a rate higher than that can be handled by the channel.
- So most of the frames will face collision. Hence $0 < N < 1$ in order to reduce number of collisions.
- Let there be k transmission attempts (including retransmissions) per frame time.
- The probability of k transmissions per frame time is also Poisson. Let the mean of number of transmissions be G per frame time. So $G \geq N$.
- At low load $N \approx 0$ there will be less number of collisions so less number of retransmissions and $G \approx N$.
- With increase in load there are many collisions so $G > N$. Combining all these we can say that for all the loads the throughput is given by,

$$S = GP_0$$

- Where P_0 = Probability that a frame does not suffer a collision.



- Consider Fig. 5.4.3.



(G-270) Fig. 5.4.3

- What is the condition for frame 3 in Fig. 5.4.3 to arrive undamaged without collision?
- Let t = Time required to send a frame. If frame 1 is generated at any instant between t_0 to $(t_0 + t)$ then it will collide with frame 3. Similarly any frame (2) generated between $(t_0 + t)$ and $(t_0 + 2t)$ also collides with frame 3.
- As per Poisson's distribution, the probability of generating k frames during a given frame time is given by,

$$P[k] = \frac{G^k e^{-G}}{k!}$$

- So the probability of generating zero frames i.e. $k = 0$ is
- If an interval is two frame time long, the mean number of frames generated during that interval is $2G$.
- The probability that no other frame is transmitted during the Vulnerable period (time when collision can take place) is,

$$P_0 = e^{-2G}$$

- But throughput $S = G P_0$
- $\therefore S = G e^{-2G}$
- Fig. 5.4.5 shows the relation between the offered traffic G and the throughput S . It shows that the maximum throughput occurs at $G = 0.5$ and $S_{max} = 0.184$. So the best possible channel utilization is on 18.4 percent.

5.4.4 Slotted ALOHA :

SPPU : Dec. 05, May 09, May 13, Dec. 18

University Questions

- Q. 1** Explain ALOHA, slotted ALOHA and CSMA/CD. Comment on the efficiency of each random access technique. **(Dec. 05, May 09, 10 Marks)**

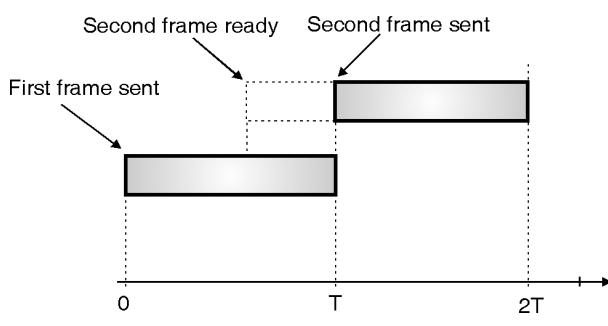
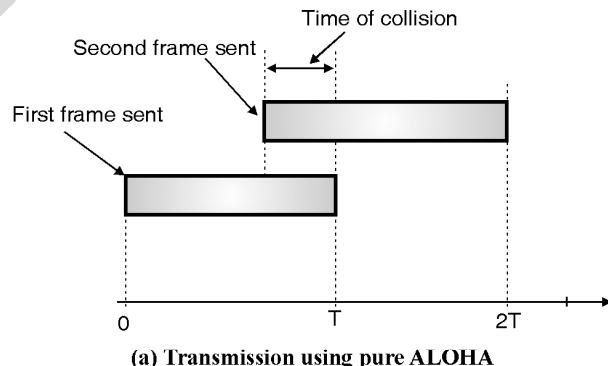
- Q. 2** Explain pure and slotted ALOHA.

(May 13, 8 Marks)

- Q. 3** Explain in brief ALOHA, slotted ALOHA mentioning efficiency, advantages in each case.

(Dec. 18, 6 Marks)

- To overcome the disadvantage of the pure ALOHA system (of low capacity) Robert published a method for doubling the capacity of traffic on the channel.
- In this method it was proposed that the time be divided up into discrete intervals and each interval correspond to one frame.
- This method requires that the users agree on the slot boundaries.
- In this method for achieving synchronisation one special station emits a pip at the start of each interval, like a clock.
- This method is known as the slotted ALOHA system.
- Collisions occur if any part of two transmission overlaps. Suppose that T is time required for one transmission and that two stations must transmit.
- The total time required for both stations to do so successfully is $2T$ as shown in Fig. 5.4.4.
- In case of pure ALOHA allowing a station to transmit at arbitrary times can waste time upto $2T$.



(G-271) Fig. 5.4.4



- As an alternative, in the slotted ALOHA method the time is divided into intervals (slots) of T units each and require each station to begin each transmission at the beginning of a slot.
- In other words, even if station is ready to send in the middle of a slot, it must wait until the beginning of the next one as shown in Fig. 5.4.4(b).
- In this method a collision occurs when both stations become ready in the same slot.
- Slotted ALOHA is thus a discrete time system whereas pure ALOHA is a continuous time system.
- The Vulnerable period has been reduced to half that of pure ALOHA, the throughput for slotted ALOHA is given by,

$$S = Ge^{-G}$$

- The maximum throughput corresponds to $G = 1$ and it is given by $S_{max} = 1/e = 0.368$ as shown in Fig. 5.4.5. So for a slotted ALOHA with $G = 1$ the probability of success is 37%. The probability of empty slots is,

$$P(k) = \frac{G^k e^{-G}}{k!}$$

For $G = 1$ and $k = 0$ we get $P(k=0) = 0.368$.

And the probability of collisions is 26 %.

- The probability of transmission requiring exactly k attempts (i.e. $k - 1$ collisions followed by one success) is given by,

$$P_k = e^{-G} (1 - e^{-G})^{k-1}$$

- And the expected number of transmissions E per carriage return typed is

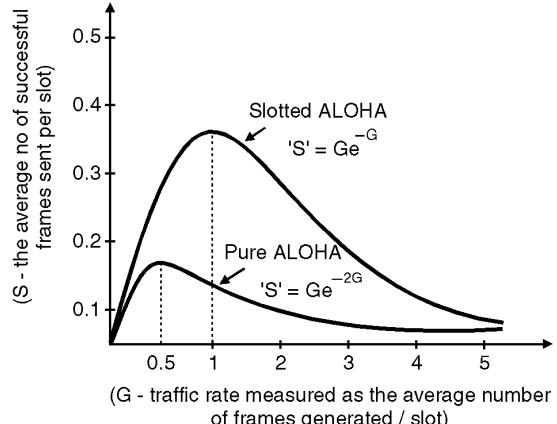
$$E = e^G$$

Conclusion : As E depends exponentially on G , with a small increase in G , there is a large increase in E and drastic fall in performance.

5.4.5 Comparison of Pure and Slotted ALOHA :

- A mathematical model can be created for the relationship between the number of frames transmitted and the number of frames transmitted successfully.
- Let G represent the traffic measured as the average number of frames generated per slot.

- Let S be the success rate measured as the average number of frames sent successfully per slot.
- The relationship between G and S for both pure and slotted ALOHA is given as follows :
 - Pure ALOHA $\rightarrow S = Ge^{-2G}$
 - Slotted ALOHA $\rightarrow S = Ge^{-G}$
 Where e is the mathematical constant = 2.718.
- From the above equation a success rate curve for pure and slotted ALOHA can be plotted as shown in Fig. 5.4.5.
- As seen in the Fig. 5.4.5 both graphs have the same shape. If G is small so is S , which means that if few frames are generated few frames will be transmitted successfully.
- As G increases so does S but upto a certain point. As G continues to increase S approaches to 0 which means that if more frames are generated there will be more collisions and the success rate will fall to 0.
- Similarly for pure ALOHA the maximum occurs at $G = 0.5$ for which $S = 1/2e = 0.184$ which means the rate of successful transmissions is approximately 18.4%.



(G-272)Fig. 5.4.5 : Comparison of pure and slotted ALOHA

- As seen from the graph the maximum for slotted ALOHA occurs at $G = 1$ for which $S = 1/e = 0.368$. In other words the rate of successful transmissions is approximately 0.368 frames per slot time or 37% of the time will be spent on successful transmissions.
- Hence the slotted ALOHA has a double throughput efficiency than the pure ALOHA system.



- The maximum utilization achievable using CSMA can be increased much beyond that obtainable using ALOHA or slotted ALOHA.
- The maximum utilization is dependent on length of the frame and on the propagation time.
- With increase in the length of the frame or reduction in the propagation time the utilization gets improved.

5.5 Carrier Sense Multiple Access (CSMA) :

SPPU : May 14, Dec. 14, Dec. 15, May 17

University Questions

- Q. 1** Explain CSMA and CSMA/CD in detail.
(May 14, 6 Marks)
- Q. 2** Explain CSMA and CSMA/CD. Also comment on the efficiency of each.
(Dec. 14, Dec. 15, May 17, 6 Marks)

- The CSMA protocol operates on the principle of carrier sensing.
- In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-Persistent CSMA :

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.

1-Persistent CSMA :

- In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.
- The disadvantage of this strategy is that if two stations are waiting then they will transmit simultaneously and collision will take place. This will then require retransmission.

P-Persistent CSMA :

- The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.
- A station is assumed to be transmitting with a probability "p".
- For example if $p = 1/6$ and if 6 stations are waiting then on an average only one station will transmit and others will wait.

5.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

SPPU : May 12, Dec. 12, May 14, Dec. 14, May 15, Dec. 15, May 16, May 17, Dec. 17, May 18

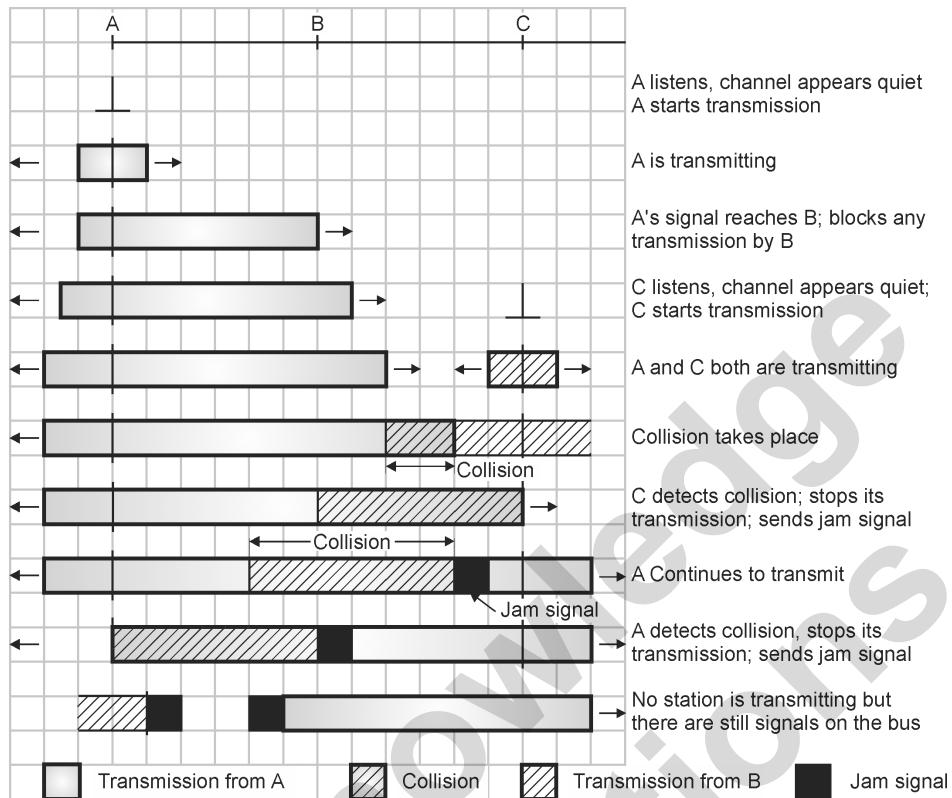
University Questions

- Q. 1** Discuss CSMA/CD random access techniques. How is collision avoidance achieved in the same ?
(May 12, Dec. 12, 8 Marks)
- Q. 2** Explain CSMA and CSMA/CD. Also comment on the efficiency of each.
(May 14, Dec. 14, Dec. 15, May 17, 6 Marks)
- Q. 3** Discuss CSMA/CD random access technique. How is collision avoidance achieved in the same ?
(May 15, Dec. 17, May 18, 7 Marks)
- Q. 4** Write a short note on CSMA/CD.
(May 16, 6 Marks)

- The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

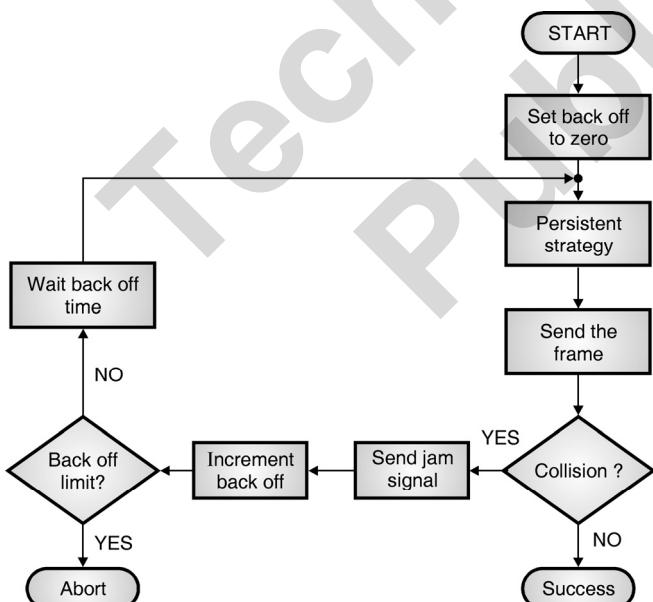
- The problem in CSMA explained earlier is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.
- As soon as a collision is detected, the transmitting stations release a jam signal.
- The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.
- Otherwise there is a possibility that the same frames would collide again.
- After some "back off" delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively.
- A careful design can achieve efficiencies of more than 90% using CSMA/CD. This scheme is as shown in Fig. 5.5.1.



(G-273)Fig. 5.5.1 : CSMA/CD scheme

5.5.2 CSMA/CD Procedure :

- Fig. 5.5.2 shows a flow chart for the CSMA/CD protocol.



(G-276)Fig. 5.5.2 : CSMA/CD procedure

Explanation :

- The station that has a ready frame sets the back off parameter to zero.

- Then it senses the line using one of the persistent strategies.
- It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.
- If the back off has reached its limit then the station aborts the transmission.
- CSMA/CD is used for the traditional Ethernet.
- CSMA/CD is an important protocol. IEEE 802.3 (Ethernet) is an example of CSMA/CD. It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.



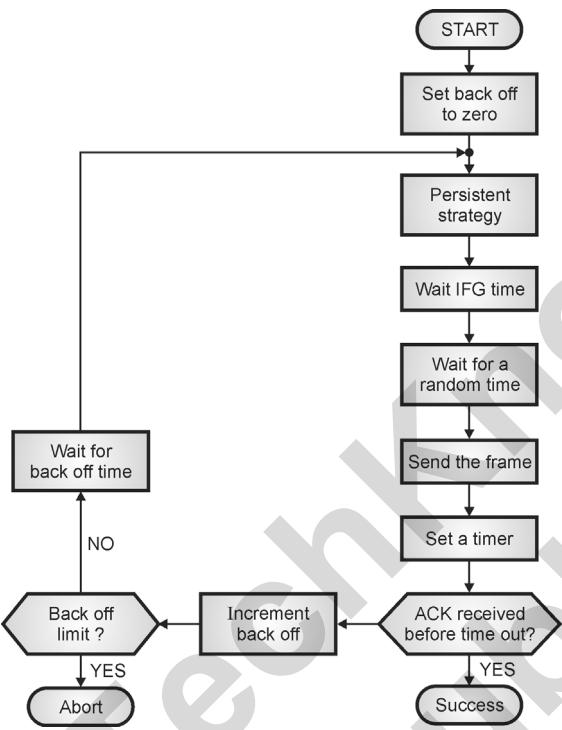
5.5.3 CSMA/CA :

SPPU : Dec. 14, May 17, Dec. 18, May 19

University Questions

- Q. 1** Discuss CSMA/CA random access technique. How is collision avoidance achieved in this technique ?
(Dec. 14, May 17, Dec. 18, May 19, 7 Marks)

- The long form of CSMA/CA is CSMA protocol with collision avoidance.
- Fig. 5.5.3 shows the flow chart explaining the principle of CSMA/CA.



(G-277)Fig. 5.5.3 : CSMA/CA procedure

- The station ready to transmit, senses the line by using one of the persistent strategies.
- As soon as it finds the line to be idle, the station waits for a time equal to an IFG (Interframe gap).
- It then waits for some more random time and sends the frame.
- After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.
- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and senses the line again. CSMA/CA completely avoids the collision.

5.6 Collision Free Protocols :

- As we have seen that almost collisions can be avoided in CSMA/CD, they can still occur during the contention period.
- The collision during contention period affects the system's performance adversely. This happens when the cable is long and length of frames are short. This problem becomes serious as fiber optic networks come into use.
- Here we will discuss some protocols that resolve the collisions during the contention period.

5.6.1 Bit-map Protocol :

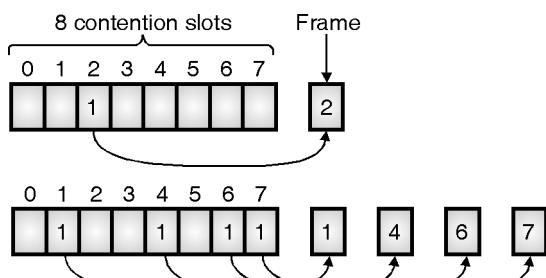
SPPU : May 08

University Questions

- Q. 1** Describe any one collision free protocol.

(May 08, 3 Marks)

- Bit-map protocol is collision-free protocol. In bit-map method, each contention period consists of exactly N slots. If any station has to send frame, then it transmits a 1 bit in the respective slot.
- For example, if station 2 has a frame to send, it transmits a 1 bit during the second slot. In general, station "i" can announce that it has a frame to send by inserting a 1 bit into slot "i".
- In this way each station has complete knowledge of which stations wish to transmit.
- Since everyone agrees on who goes next, there will never be any collisions.
- Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.



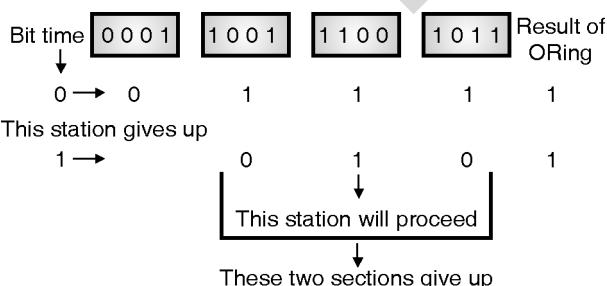
(G-278)Fig. 5.6.1 : A bit-map protocol



- For analyzing the performance of this protocol, we will measure time in units of the contention bit slot, with data frame consisting of d time units.
- For the light load conditions, the bit map will simply be repeated over and over, for lack of data frames because there are very few frames to transmit.
- At high-load, when all the stations have something to send all the time, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame. This indicates that the protocol efficiency is high.
- Generally high numbered stations have to wait half a scan ($N/2$ bit slots) time before starting to transmit, low-numbered stations have to wait on an average $1.5 N$ slots.

5.6.2 Binary Countdown :

- Binary countdown protocol is used to overcome the overhead 1 bit per station. In binary countdown binary station addresses are used.
- A station which has a frame to transmit will broadcasts its address as a binary bit string, starting with the high-order bit. All addresses are assumed to be of same length.
- Here we will see the example to illustrate the working of binary countdown. In this method different station address are ORed together to decide the priority of transmitting.
- If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the stations at first will broadcast their most significant address bit i.e. 0, 1, 1, 1 respectively.



(G-279)**Fig. 5.6.2 : Binary countdown**

- The most significant bits are ORed together. Station 0001 sees the 1 MSB in other station addresses and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

- Other three stations 1001, 1100, 1011 will continue. The next bit is 1 at stations 1100, so station 1011 and 1001 give up. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.

5.6.3 Limited Contention Protocols :

Meaning of contention system :

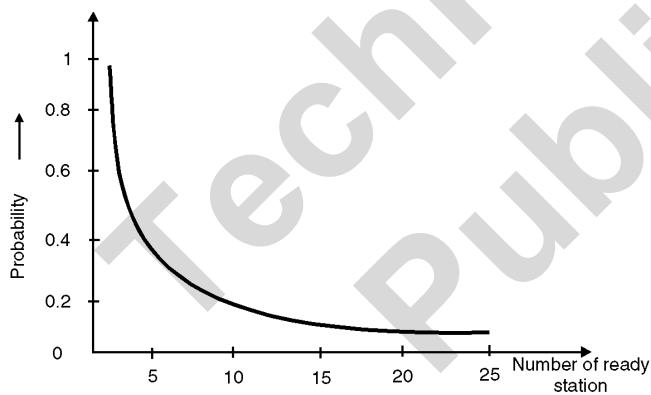
- The systems in which multiple users share a common channel in such a way that results in conflicts (collisions) are known as **contention systems**.

Contention protocols :

- Till now we have considered two different techniques for the channel allocation namely :
 - Contention (such as CSMA) protocols
 - Collision free methods.
- The performance of these techniques can be judged based on two performance parameters namely delay at light loads and efficiency at heavy loads.
- As the load of the channel increases, contention based schemes (protocols) becomes increasingly less attractive, because the overhead associated with channel arbitration will increase, and reduce the efficiency.
- Now consider the collision-free protocols. At low load, they have high delay, (bad performance) but as the load increases, the channel efficiency improves.
- Therefore, it would be an ideal thing to do if we could combine the best properties of the contention and collision-free protocols, to create a new protocol that uses the contention at low loads to provide short delay, but uses a collision-free technique at heavy load to ensure good channel efficiency.
- Such protocols are called as **limited contention protocols**.
- These protocols are a combination of contention and collision-free protocols, because contention protocols provide a low delay at low loads and collision-free protocols provide good channel efficiency at high loads.
- The contention protocols like CSMA/CD are symmetric in nature i.e. each station attempts to acquire the channel with the same probability P.
- But this degrades the performance.



- In case of limited contention protocols the overall performance is improved by assigning different probabilities to different stations.
- In case of symmetric protocols for small number of stations, the chance of success are good but it becomes worse as the number of stations increases.
- In case of limited contention protocols which are asymmetric in nature the probability of some station acquiring the channel can be increased only by decreasing the amount of competition.
- In this method the stations are first divided up into groups. Only the members of group 0 are permitted to compete for slot 0. This reduces the competition.
- If one of them succeeds it acquires the channel and transmits its frame. If the slot lies empty or if there is a collision, the members of group 1 compete for slot 1 and so on.
- Thus by making a correct division of stations into groups, the amount of contention (competition) for each slot (competition) can be reduced.
- Fig. 5.6.3 shows the graph of probability plotted against number of stations ready to transmit their frames.

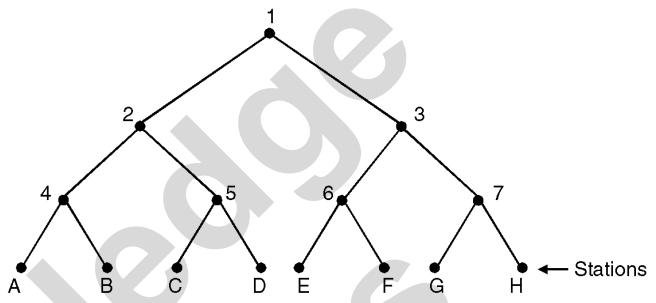


(G-280)Fig. 5.6.3

- The important question is how to assign stations to slots ?
- At one extreme we have one member per group whereas on the other side a single group will contain all the stations (slotted ALOHA).
- What is required is a way to assign stations to slots dynamically depending on load.
- When the load is low, many stations should be assigned per slot whereas when the load is high few (or even one) station per slot should be assigned.

5.6.4 The Adaptive Tree Walk Protocol :

- The assignment of stations to the slots can be done with the help of a simple algorithm called adaptive tree walk protocol.
- It is imagined that the stations are leaves of a binary tree as shown in Fig. 5.6.4.



(G-281)Fig. 5.6.4 : Adaptive tree walk protocol

- The tree for eight stations is shown in Fig. 5.6.4. As shown in the Fig. 5.6.4 in the first contention slot which is slot 0 if a successful frame transmission occurs all stations are allowed to compete for the channel.
- If there is a collision then during slot 1 only those stations corresponding to node 2 in the tree may compete. If one of these stations acquires the channel, the slot following the frame is reserved for stations falling under node 3.
- On the other hand if there is a collision under node 2 during slot 1 then during slot 2 it is the turn of stations falling under node 4 to compete for the channel.
- If a collision occurs during slot 0, the entire tree is searched, depth first to locate all ready stations. Each bit is associated with some particular node in the tree.
- If a collision occurs, the search continues recursively with the node's left and right sides. If a bit slot is idle or if there is only one station that transmits in it then, the searching of its node can stop, because all ready stations have been located.

5.7 Controlled Access :

SPPU : Dec. 11, Dec. 17

University Questions

- Q. 1** Explain different controlled access methods with the help of diagrams. (Dec. 11, 10 Marks)
- Q. 2** Explain the various controlled access methods. (Dec. 17, 6 Marks)



- Earlier we have discussed the random access approach for sharing a transmission medium.
- The random access approach is simpler to implement and are useful in handling the light traffic.
- In this section we will discuss the scheduling approaches to the medium access control.
- There are three important approaches in the scheduling approach as follows :
 1. Reservation system
 2. Polling system
 3. Token passing ring networks.

5.7.1 Reservation Systems :

SPPU : May 12, May 13, Dec. 17

University Questions

Q. 1 Describe different controlled access protocol mentioned below in short : Reservation.

(May 12, 3 Marks)

Q. 2 Describe different controlled access protocol mentioned in short : 1. Reservation 2. Polling 3. Token passing.

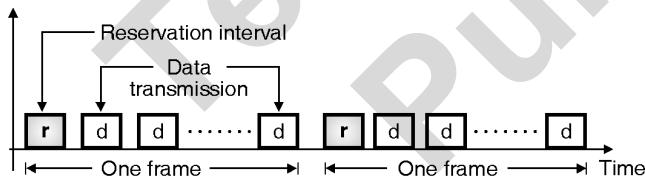
(May 13, 8 Marks)

Q. 3 Explain the various controlled access methods.

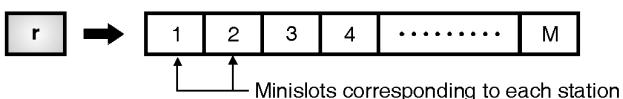
(Dec. 17, 6 Marks)

Principle :

- The principle of reservation system can be understood from Fig. 5.7.1.



(a) Transmission in reservation systems

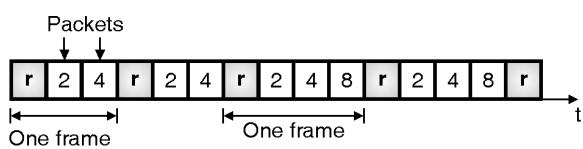


(b) Details of reservation interval

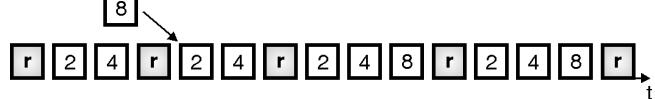
(L-733)Fig. 5.7.1 : Basic reservation system

- In this system each station transmits a single packet at the full rate R bps. The transmissions from the stations can be organized into frames of variable length.
- Before each frame a reserved slot or reservation interval is transmitted as shown in Fig. 5.7.1(a).

- Fig. 5.7.1(b) shows the details of the reservation interval "r". The reservation interval consists of M minislots with one slot allotted to each station.
- These minislots are used by the stations to indicate that they have a packet to transmit in the corresponding frame.
- The station that wants to transmit packet by broadcasting their reservation bit during the appropriate minslot.
- All the stations will listen to the reservation interval, and then determine the order in which packet transmissions in the corresponding frame would take place.
- The frame length would correspond to the number of stations which have a packet to transmit.
- If the length of the packet is variable, then it can be handled if the reservation message includes packet length information.
- This reservation system that we discussed is called as the basic reservation system.
- The basic reservation system can be improved by using the time division multiplexing scheme. In the improved reservation system the idle time slots are allotted to the other stations.
- The operation of the basic reservation system can be explained with the help of Fig. 5.7.2.



(a) Negligible propagation delay



(b) Non negligible propagation delay

(L-734)Fig. 5.7.2 : Operation of reservation system with negligible and non-negligible delays

- Refer Fig. 5.7.2(a) which shows a system with negligible propagation delay. In the first frame, only the stations 2 and 4 transmit their packets. But in the middle portion, station 8 also wants to transmit its packet. So the frame gets expanded from two slots to three slots.
- The maximum throughput from this system can be attained when all the stations transmit their packet in each frame.



- The corresponding maximum throughput is given by,

$$\rho_{\max} = \frac{1}{1 + v} \text{ ...for one packet reservation/minislot}$$
- If $v \ll 1$ then the value of ρ_{\max} can be very high.
- Now refer Fig. 5.7.2(b) which shows a reservation system with some finite non zero propagation delay which can not be neglected. In this system the stations will transmit their reservations in the same way as they used to do before.
- It is possible to modify the basic reservation system so that stations can reserve more than one slot per packet transmission per minislot.
- Let us assume that a minislot can reserve say upto k packets.
- Then the maximum achievable throughput is given by,

$$\rho_{\max} = \frac{1}{1 + (v/k)} \text{ ...for } k \text{ packet reservation/minislot}$$
- Note that this value of ρ_{\max} will be higher than that for the single packet reservation/minislot.

Effect of number of stations (M) :

- The reservation intervals introduce overhead which is proportional to M . That means the reservation interval becomes $M \times v$.
- As the number of stations (M) become very large, this overhead will become significant. This then becomes a serious problem.
- This problem can be sorted out by not allocating a minislot to each station and then instead making the stations to compete for a reservation of minislot by using a random access technique such as ALOHA or slotted ALOHA.

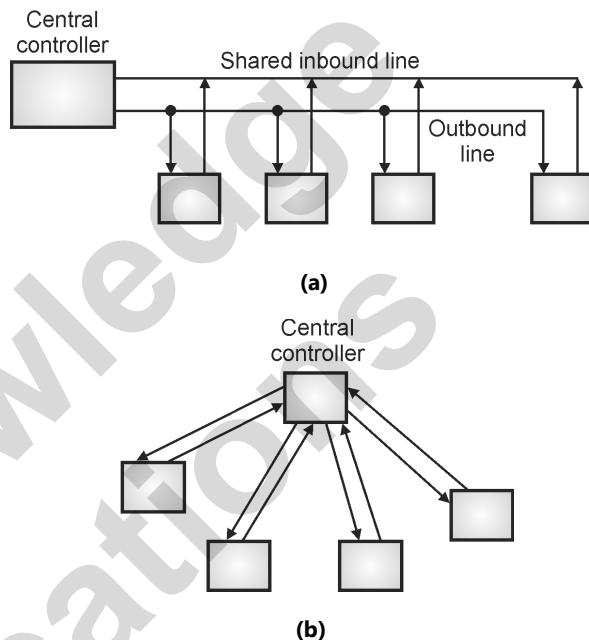
5.7.2 Polling : **SPPU : May 12, May 13, Dec. 17**

University Questions

- Q. 1** Describe different controlled access protocol mentioned below in short : Polling.
(May 12, 3 Marks)
- Q. 2** Describe different controlled access protocol mentioned in short : 1. Reservation 2. Polling 3. Token passing. **(May 13, 8 Marks)**
- Q. 3** Explain the various controlled access methods.
(Dec. 17, 6 Marks)

Principle :

- Now consider polling system shown in Fig. 5.7.3. In this system the stations access the common medium one by one (by taking turns).
- At any given time only one of the stations will transmit into the medium.

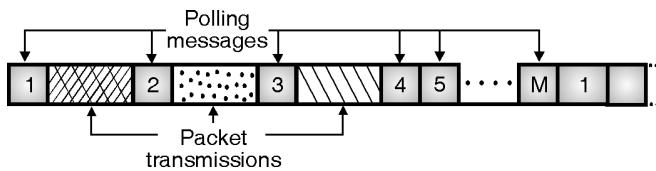


(L-735)Fig. 5.7.3 : Examples of polling systems

- When a station finishes its transmitting, then some mechanism is used to pass the right of transmission to another station which wants to transmit next.
- There are different ways of passing the right of transmission from one station to the other station.
- Fig. 5.7.3(a) shows a scheme in which M stations communicate with a central controller. The outbound line is used for carrying the information from the central controller to the M users whereas the shared inbound line is required to carry the information from users to the central computer.
- Thus the inbound line acts as the shared medium that requires a medium access control (MAC).
- The host computer acts as a central controller. It sends control messages which co-ordinate the transmissions from the stations.
- The central controller sends a polling message to a particular station. That station sends its message on the shared inbound line. Once this process is over, the station gives a go-ahead message.



- It is possible that the central controller may poll the stations in a round robin (serial) fashion or it may do it according to some pre-determined rule.
- Fig. 5.7.3(b) shows another system where it is possible to use polling. The central controller of this system can make use of radio transmission.
- Fig. 5.7.4 shows the sequence of polling messages.



(L-736)Fig. 5.7.4 : Polling messages and transmissions in a polling system

- Station 1 gets the polling message first. The polling message will propagate. It is received by all stations but only station 1 begins transmission. All this process needs a time called **walk time**.
- The next period is occupied by the transmission from station 1.
- This period will then be followed by the walk time corresponding to station-2. This process will continue until all the M stations are polled. Thus in this system the stations are polled in the round robin manner.
- The walk time can be considered to be an overhead in the polling system because it is an unproductive time. The total walk time τ' is the sum of walk time corresponding to each station.

5.7.3 Token Passing :

SPPU : Dec. 11, May 13, Dec. 17

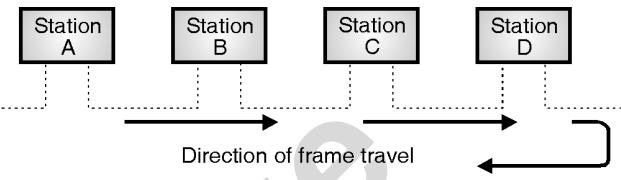
University Questions

- Q. 1** Explain different controlled access methods with the help of diagrams. **(Dec. 11, 10 Marks)**
- Q. 2** Describe different controlled access protocol mentioned in short : 1. Reservation 2. Polling 3. Token passing. **(May 13, 8 Marks)**
- Q. 3** Explain the various controlled access methods. **(Dec. 17, 6 Marks)**

Principle :

- **Token** is a special frame which is used to authorize a particular station for transmission.

- In the token passing method, the token is given to that station, which is authorized to send its data. Thus the station that has the token with it can transmit others listen.



(L-737)Fig. 5.7.5 : Token passing network

- In a token passing network, each station has a predecessor and successor as shown in Fig. 5.7.5.
- The frames travel in one direction. They come from the predecessor and go to the successor as shown in Fig. 5.7.5.
- A token frame is circulated around the ring when no data is being transmitted and the line is idle.
- The stations which are ready to send data, will wait for the token. As the token circulates the first ready station in the ring will grab the circulating token and transmit one or more frames.
- This station will keep sending the frames as long as it has frames to send or the allotted time is not complete.
- It then passes this token on the ring from which the next ready to transmit station will grab it.
- This is the simplest possible token passing technique in which all the stations have equal priority or right to send.
- In the practical system, some other features such as priority and reservation are added.

5.8 Channelization / Multiple Access Techniques :

Definition :

- The multiple access techniques are the techniques in which the total bandwidth of the common link is shared in the frequency domain, time domain or through codes.
- Depending on the method of sharing there are five multiple access techniques as given below :
 1. FDMA : Frequency Division Multiple Access
 2. CDMA : Code Division Multiple Access.
 3. TDMA : Time Division Multiple Access



4. CSMA : Carrier Sense Multiple Access

Need of multiple access :

- A multiple access technique is not necessary if we have only one user. But if there are multiple users who need to share a wireless communication system, then we need to use a multiple access system.
- In **Frequency Division Multiple Access (FDMA)**, a different frequency band is assigned to individual users. All users transmit simultaneously.
- In the **Time Division Multiple Access (TDMA)** system a separate time slot is allotted to each user and only one user is allowed to transmit or receive at any instant of time.
- In **Code Division Multiple Access (CDMA)** systems, the narrowband message signal is multiplied by a large bandwidth carrier called spreading signal.
- In CDMA each user is given a unique code sequence or signature sequence. This sequence allows the user to spread the information signal across the assigned frequency band.
- In CDMA the bandwidth as well as time of the channel is shared by the users.

5.8.1 FDMA :

**SPPU : Dec. 12, May 14, Dec. 14, May 15,
Dec. 15, May 17**

University Questions

Q. 1 Explain FDMA, TDMA and CDMA in detail.

(Dec. 12, May 14, Dec. 14, May 17, 6 Marks)

Q. 2 Explain TDMA and FDMA.

(May 15, Dec. 15, 5 Marks)

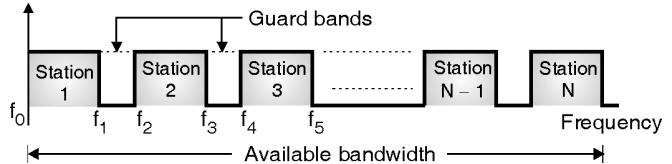
Principle :

- In the frequency division multiple access (FDMA), the available channel (medium) bandwidth is shared by all the stations. That means each station will have its own specific slot reserved in the entire channel bandwidth.
- So each station uses its allocated frequency band to send its data.
- Each band is thus reserved for a specific station. e.g. the frequency band f_0 to f_1 is for station-1, then f_2 to f_3 is for station-2 and so on.

Concept :

- The concept of FDMA is illustrated in Fig. 5.8.1.

- FDMA is a data link layer protocol which uses FDM at the physical layer.



(L-739)Fig. 5.8.1 : Concept of FDMA

- Guard bands are provided in between the adjacent frequency slots. e.g. ($f_1 - f_2$) is a guard band between the bands allotted to stations 1 and 2. Guard bands avoid the adjacent channel interference.
- FDMA is used in cellular phones and satellite networks.

Features of FDMA :

The features of FDMA are as follows :

1. The overall channel bandwidth is being shared by the multiple users. Therefore a number of users can transmit their information simultaneously.
2. If a FDMA channel is not in use, it will be idle and cannot be used by any other user. Therefore FDMA does not utilize the available spectrum efficiently.
3. If a frequency band (channel) is assigned to a user in FDMA, then the mobile unit and the base station start transmitting simultaneously.
4. The adjacent frequency bands in the FDMA spectrum are likely to interfere with each other. Therefore it is necessary to include the guard bands between the adjacent frequency bands.
5. FDMA needs near to ideal RF filtering to reduce the adjacent channel interference.
6. The mobile unit based on FDMA needs to use a duplexer in order to isolate signals from the transmitter and receiver operating simultaneously.
7. No code words and synchronization is not required.
8. Power efficiency is reduced.
9. FDMA is an old and proven system and is used for the analog signals.
10. The complexity of FDMA systems is less.
11. FDMA is a continuous transmission method. So few bits are required for overhead purposes (like synchronization and framing bits).

Merits of FDMA :

1. All the stations can operate continuously all 24 hours without having to wait for their turn to come.



2. The power required for transmission depends on the number of channels being transmitted.
3. The signal to noise ratio is improved due to the use of FM.
4. No synchronization is necessary.
5. FDMA is a less complex system.

Demerits of FDMA :

1. Each channel can use only a part of the total bandwidth.
2. In spite of guard bands being provided, there is some adjacent channel interference present.
3. Due to the nonlinearity of the system the inter modulation products are generated.
4. It can process only one phone circuit at a time.
5. The cell site cost of FDMA systems is high.
6. The bandwidth of FDMA channels is narrow.

5.8.2 TDMA :

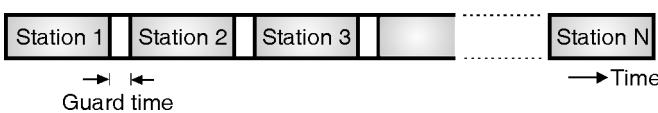
**SPPU : Dec. 12, May 14, Dec. 14, May 15, Dec. 15,
May 17, May 18, Dec. 19**

University Questions

- Q. 1 Explain FDMA, TDMA and CDMA in detail.
(Dec. 12, May 14, Dec. 14, May 17, 6 Marks)**
- Q. 2 Explain TDMA and FDMA.
(May 15, 5 Marks, Dec. 15, 6 Marks)**
- Q. 3 Explain TDMA and CDMA with neat diagram.
(May 18, Dec. 19, 6 Marks)**

Principle :

- TDMA stands for Time Division Multiple Access.
- In TDMA, the entire bandwidth can be used by every user (station) but not simultaneously.
- A station can use the entire bandwidth only for the allocated time slot.
- Thus each channel is allocated a time slot only during which it can send its data. Thus the time is shared, frequency band is not shared.
- Fig. 5.8.2 illustrates the concept of TDMA. Guard times are inserted between the adjacent time slots in order to prevent any cross talk. No data transmission takes place during the guard times.



(L-740)Fig. 5.8.2 : Concept of TDMA

- TDMA is a data link layer protocol which uses TDM at the physical layer.
- TDMA finds its application in cellular phones and satellite networks.

TDMA Features :

- The features of TDMA are as follows :
 1. TDMA is used for the transmission of data and digital voice signals.
 2. It is necessary to include "guard times" between the adjacent channels for reducing the cross talk.
 3. Synchronization is necessary in TDMA.
 4. Power efficiency of TDMA is better than that of the FDMA.
 5. TDMA is a method of time division multiplexing the digitally modulated carriers between various earth stations in a satellite network through a common satellite transponder.
 6. Each earth station transmits a **short burst** of digitally modulated carrier during the time slot assigned to it in the TDMA frame
 7. Since TDMA uses different time slots for transmission and reception, the duplexers are not required to be used.
 8. The number of time slots in a TDMA system is determined by parameters like bandwidth, modulation method etc.
 9. As TDMA transmits data in bursts and not continuously, the battery consumption is reduced considerably.
 10. In TDMA, the handoff process is simple.

Advantages of TDMA :

1. At any instant of time, the carrier from only one station is present at the transponder. This reduces the intermodulation distortion.
2. TDMA is suitable for transmission of digital information.
3. It is possible to store the digital information, change the rate etc. in TDMA.

Advantages of TDMA over FDMA :

- The advantages of TDMA over FDMA are as follows :



- In TDMA since only one station is present at any given time, the intermodulation products will not get generated.
- The entire channel bandwidth can be allotted to a single channel at given instant of time. This is particularly advantageous for the digital channels which demand larger bandwidths.
- The frequency selective fading does not affect the TDMA to the extent it affects the FDMA.
- TDMA is well suited for the digital signals therefore it can be easily used for data transmission.
- As only one channel is being transmitted at a time it is not necessary to separate out various channels at the receiver.

Disadvantages :

- Precise synchronization is required.
- Bit and frame timing must be achieved and maintained.

5.8.3 Code Division Multiple Access (CDMA) :

SPPU : May 12, Dec. 12, May 14, Dec. 14, May 17

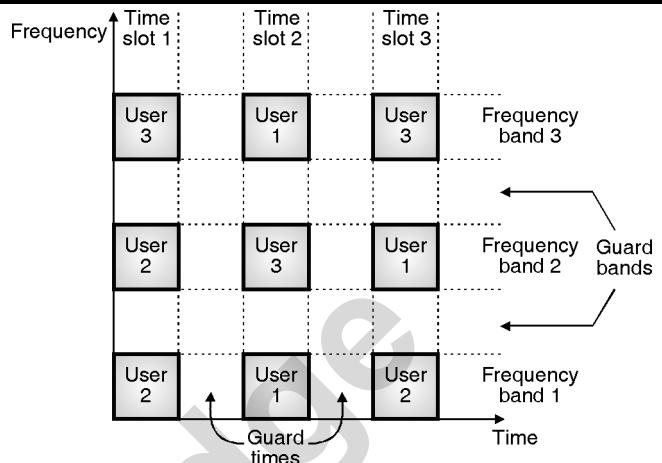
University Questions

Q. 1 Explain FDMA, TDMA and CDMA in detail.

(May 12, Dec. 12, May 14, Dec. 14, May 17, 6 Marks)

Concept :

- An alternative to FDMA and TDMA is another system called code division multiple access (CDMA).
- The most important feature of CDMA is as follows :
- In CDMA more than one user is allowed to share a channel or subchannel with the help of direct-sequence spread spectrum (DS-SS) signals.
- In CDMA each user is given a unique code sequence or signature sequence.
- This sequence allows the user to spread the information signal across the assigned frequency band.
- At the receiver the signal is recovered by using the same code sequence.
- At the receiver, the signals received from various users are separated by checking the cross-correlation of the received signal with each possible user signature sequence.



(L-74) Fig. 5.8.3 : Structure of CDMA showing the guard bands and the guard times

- In CDMA the users access the channel in a random manner. Hence the signals transmitted by multiple users will completely overlap both in time and in frequency.
- The CDMA signals are spread in frequency. Therefore the demodulation and separation of these signals at the receiver can be achieved by using the pseudorandom code sequence. CDMA is sometimes also called as spread spectrum multiple access (SSMA).
- In CDMA as the bandwidth as well as time of the channel is being shared by the users, it is necessary to introduce the guard times and guard bands as shown in Fig. 5.8.3.
- CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

Advantages of CDMA :

- Some of the advantages of CDMA are :
 - It does not need any synchronization.
 - More number of users can share the same bandwidth.
 - Sharing of bandwidth as well as time is possible.
 - Due to codeword allotted to each user, interference (crosstalk) is reduced.

Disadvantages :

- The CDMA system is more complicated.
- Guard band and guard time both are required to be provided.

**CDMA Applications :**

- Following are some of the important CDMA services :
 1. Voice services
 2. Data services
 3. Circuit switched data
 4. Packet switched data
 5. Message services
 6. CDMA radio
 7. Location based services
 8. CDMA radio channel

5.8.4 Comparison of FDMA, TDMA and CDMA :

**SPPU : Dec. 10, May 11, May 13, May 15,
May 16, Dec. 17**

University Questions

Q. 1 Compare and contrast FDMA and CDMA in detail.
(Dec. 10, May 15, 8 Marks)

Q. 2 Compare FDMA, CDMA and TDMA.

(May 11, May 13, May 16, Dec. 17, 6 Marks)

Sr. No.	Parameter	FDMA	TDMA	CDMA
1.	Concept	Overall band width is shared among many stations.	Time sharing takes place.	Sharing of bandwidth and time both takes place.
2.	Interference	Due to nonlinearity of transponder amplifiers, inter modulation products are generated due to interference between adjacent channels.	Due to incorrect synchronization there can be an interference between the adjacent time slots.	Both type of interferences will be present.
3.	Synchronization	Synchronization is not necessary.	Synchronization is essential.	Synchronization is not necessary.
4.	Code word	Code word is not required.	Code word is not required.	Code words are required.
5.	Guard times and bands	Guard bands between adjacent channels are necessary.	Guard times between adjacent time slots are necessary.	Guard bands and Guard times both are necessary.
6.	Hand-over	Hard handover	Soft handover	Soft handover
7.	Key resources	FDMA allocates a separate frequency slot to each user.	TDMA allows only one user to transmit at any given time.	CDMA allows the use of same carrier frequency and can simultaneously transmit.
8.	Sharing of resources.	Each user is allocated a unique channel. No other user can share that channel when a call is in progress.	Each user makes use of non-overlapping time slots. The data transmission occurs in bursts.	Each user has its own pseudorandom codeword that is orthogonal to other keywords.
9.	System complexity	Low	Higher	Higher
10.	System flexibility	Simple and Robust, inflexible	Flexible	Flexible



Ex.5.8.1 : Measurements of a slotted ALOHA channel with an infinite number of user. Show that 10% of the slots are idle.

1. What is channel load ?
2. What is throughput ?
3. Is the channel overloaded or underloaded.

Soln. :

1. Channel load :

$$\text{For a slotted ALOHA, } P_0 = e^{-G}$$

$$\text{But } P_0 = 10\% \text{ i.e. } 0.1$$

$$\therefore 0.1 = e^{-G}$$

$$\therefore -2.3 = -G$$

$$\therefore G = 2.3$$

2. Throughput :

$$S = G e^{-G} = 2.3 e^{-2.3} = 0.23$$

3. Since G is beyond 1 the channel is overloaded.

Ex. 5.8.2 : Consider building a CSMA/CD network running at 1Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 2,00,000 km/sec, what is the minimum frame size ?

Soln. :

Given : Bit rate $R = 1 \times 10^9$ Bits/sec, No repeaters used.

$$\text{Length } L = 1 \text{ km} = 1 \times 10^3 \text{ m}$$

$$\text{Speed } v = 2,00,000 \text{ km/S} = 2 \times 10^8 \text{ m/S}$$

To find : Minimum frame size

1. Let the time for a signal to propagate between two farthest stations be τ . The contention interval is such that width of each slot is 2τ .
2. On a 1 km long cable $\tau \approx 5 \mu\text{sec}$. $\therefore 2\tau = 10 \mu\text{sec}$.
3. To make CSMA/CD work, it must be ensured that the minimum frame size should be equal to $2\tau = 10 \mu\text{sec}$.

$$\text{But } R = 1 \times 10^9 \text{ bits/sec}$$

$$\therefore 1 \text{ sec} = 1 \times 10^9 \text{ bits}$$

$$\therefore 10 \times 10^{-6} \text{ sec} = ? \text{ bits}$$

$$\therefore \frac{1}{10 \times 10^{-6}} = \frac{1 \times 10^9}{x}$$

$$\begin{aligned} \therefore x &= 1 \times 10^9 \times 10 \times 10^{-6} \\ &= 10 \times 10^3 \\ &= 10,000 \text{ bits.} \end{aligned}$$

\therefore Minimum frame size = 10,000 bits or 1250 bytes.

Ex. 5.8.3 : A large population of ALOHA users manages to generate 50 requests/sec, including both originals and retransmissions. Time is slotted in units of 40 msec.

- (a) What is the chance of success on the first attempt ?
- (b) What is the probability of exactly k collisions and then a success ?
- (c) What is the expected number of transmission attempts needed ?

Soln. :

1. There are 50 requests/sec and time is slotted in units of 40 msec.

$$1 \text{ sec} \equiv 50 \text{ requests (transmissions)}$$

$$\therefore 40 \text{ msec} = x \text{ transmissions.}$$

$$\therefore \frac{1}{40 \times 10^{-3}} = \frac{50}{x}$$

$$\therefore x = 50 \times 40 \times 10^{-3}$$

$$\therefore x = 2$$

2. But number of transmissions (x) = e^G

$$\therefore 2 = e^G$$

$$\therefore G = 0.693$$

3. Probability of k collisions and then a success is,

$$P_k = e^{-G} (1 - e^{-G})^{k-1}$$

$$\therefore P_k = e^{-0.693} (1 - e^{-0.693})^{k-1}$$

4. Chance of success in the first attempt is $G e^{-G}$

$$\text{i.e. } 0.693 e^{-0.693} = 0.3465 \text{ or } 34.65\%.$$

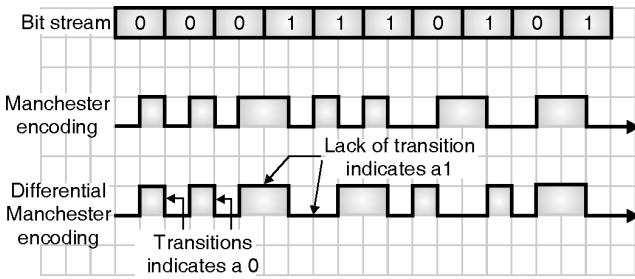
Ex. 5.8.4 : Sketch Manchester encoding and differential Manchester encoding for bit stream.

1. 0 0 0 1 1 1 0 1 0 1

2. 1 1 0 0 1 0 1 1 1 0

Soln. :

The required waveforms are as shown in Fig. P. 5.8.4.



(G-337)Fig. P. 5.8.4

Ex. 5.8.5 : Measurement of slotted ALOHA channel with an infinite number of users show that 20% slots are idle.

1. What is the channel load ?
2. What is the throughput ?
3. Is the channel underload or overload ? Show with graph.

Soln. :

Given : $P_0 = 20\%$ i.e. 0.2, Type : slotted ALOHA

To find : 1. Channel load G 2. Throughput S.
3. Decide the status of the channel

1. Channel load (G) :

$$\text{For the slotted ALOHA, } P_0 = e^{-G}$$

$$\therefore 0.2 = e^{-G}$$

$$\therefore G = \ln(0.2)^{-1} = 1.6094 \quad \dots\text{Ans.}$$

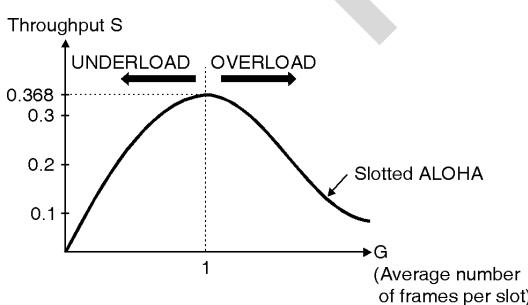
2. Throughput (S) :

$$S = G e^{-G} = P_0 G = 0.2 \times 1.6094$$

$$\therefore S = 0.3218 \quad \dots\text{Ans.}$$

3. Status of the channel :

- From Fig. P. 5.8.5 it is evident that the maximum throughput $S_{max} = 0.368$ corresponds to $G = 1$.
- Since the value of $G = 1.6094$ which is greater than 1, the channel is **overloaded**.



(L-746)Fig. P. 5.8.5 : Graph for slotted ALOHA

Ex. 5.8.6 : An ALOHA network user 19.2 kbps channel for sending message packets of 100 bit long size. Calculate the maximum throughput for pure ALOHA network.

Soln. :

Given : Rate of transmission = 19200 bits.

Frame length = 100 bits

$$\therefore \text{Number of frames per second} = \frac{\text{Rate of transmission}}{\text{Frame length}}$$

$$= \frac{19200}{100} = 192 \text{ frames/sec}$$

- The maximum throughput for a pure ALOHA system is 0.184.

$$\therefore \text{Throughput} = 0.184 \times \text{Number of frames/sec.}$$

$$= 0.184 \times 192$$

$$= 35.328 \text{ frames/sec.} \quad \dots\text{Ans.}$$

Ex. 5.8.7 : Calculate ring latency of 20 stations separated by 100 meters and operate at a speed of 4 Mbps. Assume the delay introduced by each station to be 2.5 bits.

Soln. :

Given : Number of stations N = 20

Length of the ring d = 100 m

Propagation speed V = 2×10^8 m/sec.

Rate of transmission R = 4 Mbps.

Delay introduced by each station = b = 2.5 bits.

Step 1 : Calculate the total delay :

$$\text{Delay introduced by N stations} = \frac{N \times b}{R} = \frac{20 \times 2.5}{4 \times 10^6}$$

$$= 12.5 \mu\text{sec} \quad \dots(1)$$

$$\text{Additional delay introduced by the ring} = \frac{d}{V} = \frac{100 \text{ m}}{2 \times 10^8 \text{ m/S}}$$

$$= 0.5 \mu\text{s} \quad \dots(2)$$

$$\text{So total delay} = 12.5 + 0.5 = 13 \mu\text{sec.}$$

Step 2 : Calculate the ring latency :

Ring latency is defined as the number of bits that can be simultaneously in transit around the ring.

$$\therefore \text{Ring latency} = \text{Total delay} \times \text{Rate of transmission.}$$

$$= 13 \times 10^{-6} \times 4 \times 10^6$$

$$= 52 \text{ bits} \quad \dots\text{Ans.}$$

Ex. 5.8.8 : ALOHA protocol is used to share 56 kbps satellite channel. If each packet is 1000 bits long find maximum throughput in packets/sec.

Soln. :

Given : Rate of transmission = 56 kbps = 56000 bps
Frame length = 1000 bits

1. For pure ALOHA :

$$\therefore \text{Number of frames/sec} = \frac{56000 \text{ bits}}{1000 \text{ bits/frame}} = 56 \text{ frames/sec}$$



The maximum throughput for pure ALOHA = 0.184

$$\begin{aligned}\therefore \text{Throughput} &= 56 \times 0.184 \\ &= 10.304 \text{ frames/sec.} \quad \dots \text{Ans.}\end{aligned}$$

2. For slotted ALOHA :

Maximum throughput = 0.368

$$\begin{aligned}\therefore \text{Throughput} &= 0.368 \times 56 \\ &= 20.608 \text{ frames/sec.} \quad \dots \text{Ans.}\end{aligned}$$

Ex. 5.8.9 : A group of N users share 56 kbps pure ALOHA channel. Each station outputs 1000 bits frame on an average of once 100 sec. Even if the previous has not yet been sent (buffered) what is maximum value of N ?

Soln. :

For pure ALOHA :

The maximum throughput = 0.184

∴ The maximum usable channel bandwidth is given by,

$$R = 0.184 \times 56 \text{ kbps} = 10.3 \text{ kbps}$$

$$\text{Transmission rate of stations} = \frac{1000 \text{ bits}}{100 \text{ sec}} = 10 \text{ bits/sec.}$$

- Let N be the number of stations that can use the channel.

$$\therefore N = \frac{R}{10 \text{ bits/sec}} = \frac{10.3 \text{ kbps}}{10} = 1030 \quad \dots \text{Ans.}$$

Ex. 5.8.10 : Using 5 bit sequence numbers, what is the maximum size of the send and receiver window for :

1. Stop-and-wait ARQ.
2. Go-back-N ARQ.
3. Selective-repeat ARQ.

Soln. :

- The concept of sender sliding window is used in order to hold the outstanding frames until they are acknowledged.

- That means it is imagined that all the frames stored in a buffer and outstanding frames are enclosed in a window.

1. Stop and wait ARQ :

- There are no outstanding frames at the sending end.

∴ The size of sending window is zero. The size of receive window is always 1.

2. Go-back-N ARQ :

- The maximum size of send window with an "m" bit sequence number is 2^{m-1} .

- Hence for a 5 bit sequence number ($m = 5$) the maximum send window size is $2^5 - 1 = 31$.

∴ The maximum receive window size is always 1.

3. Selective repeat ARQ :

- The maximum send and receive window size is $2^m/2$.

∴ For $m = 5$ the window size is $2^5/2 = 16$.

Review Questions

- Q. 1 Explain the layered architecture of LAN explaining the function of the LLC and MAC sublayer.
- Q. 2 What is static and dynamic channel allocation ?
- Q. 3 Compare and explain the pure and slotted ALOHA system.
- Q. 4 Explain the different CSMA protocols.
- Q. 5 What is CSMA with collision detection ?
- Q. 6 Why there is no need of CSMA/CD for a full duplex Ethernet LAN ?
- Q. 7 Explain CSMA/CD.
- Q. 8 What is CSMA/CA ?
- Q. 9 Write a note on : Physical layer implementation in traditional Ethernet.
- Q. 10 Compare the data rates of traditional, fast and Gigabit Ethernets.
- Q. 11 Explain the physical layer implementation in fast Ethernet.
- Q. 12 What are the common fast Ethernet implementations ?
- Q. 13 Explain the frame format of 802.3, 802.4 and 802.5.
- Q. 14 What is Fast Ethernet ?
- Q. 15 Explain the LLC and MAC in IEEE 802 standard and explain the operation of CSMA/CD as used in LAN.
- Q. 16 Explain CDMA.
- Q. 17 Explain FDMA and TDMA.
- Q. 18 What are the problems related to FDMA and TDMA ?
- Q. 19 State the advantages and applications of FDMA.
- Q. 20 State the advantages and applications of TDMA.
- Q. 21 State the advantages and applications of CDMA.
- Q. 22 Compare FDMA, TDMA and CDMA..
- Q. 23 Explain SDMA.
- Q. 24 State the advantages and applications of SDMA.
- Q. 25 Explain PDMA.
- Q. 26 State the advantages and applications of PDMA.



Unit III

Chapter

6

Ethernet

Syllabus

IEEE standards - 802.3, 802.4, 802.5, 802.6, Comparison of Ethernet standards : Standard Ethernet, Fast Ethernet, Gigabit Ethernet with reference to MAC layer and physical layer (Wired Network Only).

Case study : Campus network design case study.

Chapter Contents

6.1	Ethernet	6.7	Fast Ethernet
6.2	IEEE Standards	6.8	Gigabit Ethernet
6.3	Traditional Ethernet (IEEE 802.3)	6.9	Token Bus : IEEE 802.4
6.4	Changes in the Standards	6.10	Token Ring System [IEEE 802.5]
6.5	Bridged Ethernet	6.11	High Level Data Link Control (HDLC) Protocol
6.6	Switched and Full Duplex Ethernet	6.12	IEEE 802.6 Standard



6.1 Ethernet :

- Both Internet and ATM were designed for wide area networking.
- But in many applications, a large number of computers are to be connected to each other.
- For this the local area network (LAN) was introduced. The most popular LAN is called **Ethernet**.
- The IEEE 802.3 standard is popularly called as Ethernet. It is a bus based broadcast network with decentralized control.
- It can operate at 10 Mbps or 100 Mbps or even above 1 Gbps.
- Computers on an Ethernet can transmit whenever they want to do so.
- If two or more machines transmit simultaneously, then their packets collide.
- Then the transmitting computers just wait for an arbitrary time and retransmit their signal.
- There are various technologies available in the LAN market but the most popular one of them is **Ethernet**.
- In this section we are going to discuss three generations of Ethernet :
 1. Traditional Ethernet (10 Mbps)
 2. Fast Ethernet (100 Mbps)
 3. Gigabit Ethernet (1000 Mbps)

Why is it called Ethernet ?

- This system is called as Ethernet after the luminiferous ether through which the electromagnetic radiation was once thought to propagate.

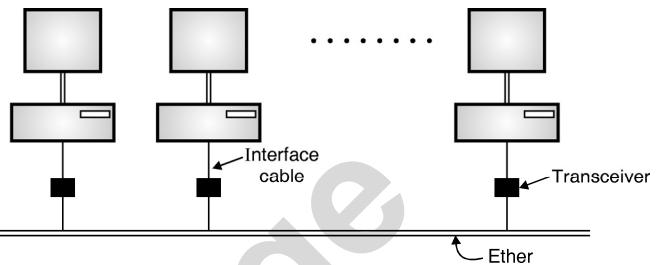
Transmission medium :

- The transmission medium is thick co-axial cable (called ether) upto 2.5 km long. Repeaters are placed after every 500 meters.
- Upto 256 machines can be attached to the multidrop cable.

Architecture of Ethernet:

- The architecture of the original Ethernet is shown in Fig. 6.1.1.
- The original Ethernet was standardized as IEEE 802.3 standard.

- The committee also standardized a token bus (802.4) and token ring (802.5) standards which were not as popular as Ethernet.



(G-293) Fig. 6.1.1 : Architecture of original Ethernet

Computer connected to internet via LAN :

- When a computer is connected to Internet via LAN, it has to use all the five layers of the internet model.
- The three upper layers (network, transport and application) are common to all the LANs.
- The data link layer is divided into two sublayers namely the logical link control (LLC) and the medium access control sublayer (MAC).
- The LLC sublayer is designed to be the same for all the LANs so that all the LANs can be connected to each other and operate without any problem.
- This means that only the MAC sublayer and physical layer of various LANs will be different from each other.
- If we compare different types of Ethernets then it is observed that, the MAC sublayer is slightly different but the physical sublayer is almost the same.

6.1.1 Traditional Ethernet :

- The traditional Ethernet is the oldest version of Ethernet created in 1976 which is designed to operate at the maximum data rate of 10 Mbps.
- The access to the network by a device is through the CDMA/CD i.e. the MAC uses CSMA/CD and the media is shared between all the hosts connected in LAN.

Why Ethernet has been so successful ?

- First, an Ethernet is extremely easy to administer and maintain.
- There are no switches, which can fail, no routing or bath tables that have to be kept up-to-date. We can add new host easily to this network second, it is inexpensive, cable is cheap, only network adapter is little costly.



6.1.2 Bridged Ethernet :

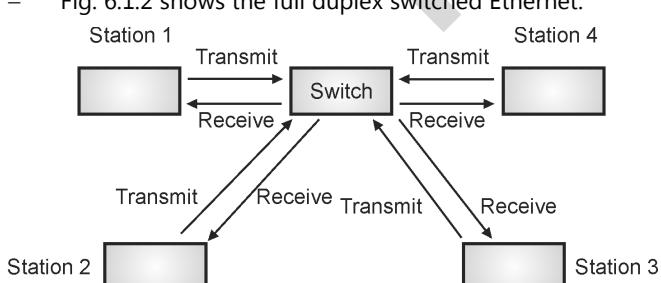
- We can divide a LAN into smaller segments by inserting bridges in between.
- Bridges affect the Ethernet LAN in the following two ways :
 1. The bandwidth requirement increases.
 2. The collision domains get separated.

6.1.3 Switched Ethernet :

- The concept of bridged LAN can be extended to the switched LAN.
- An N port switch is used to connect the N stations that are present in the given LAN.
- The bandwidth is shared only between the stations and the switch.
- The collision domain is divided into N domains. The packet handling becomes faster due to the use of layer-2 switches.

6.1.4 Full Duplex Ethernet :

- The 10 Base 5 and 10 Base 2 Ethernets have a serious limitation. The communication on them is always half duplex.
- That means a station can either transmit or receive at a time. It cannot send and receive simultaneously.
- So the full duplex switched Ethernet evolved from the switched Ethernet in which each station can communicate with the centralized switch in the full duplex mode.
- Fig. 6.1.2 shows the full duplex switched Ethernet.



(G-294) Fig. 6.1.2 : Full duplex switched Ethernet

- Due to the full duplex mode, the capacity of each domain increases from 10 to 20 Mbps.
- We have to use two links between each station and the switch, one to send the data and other to receive it.

- The full duplex switched Ethernet does not need CSMA/CD anymore because the carrier sensing need not be done any more.

6.1.5 Fast Ethernet :

- Fast Ethernet is the protocol designed to work at higher data rates than the traditional one. Typically it can support the data rates upto 100 Mbps.
- The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

Autonegotiation :

- This is the new feature of the fast Ethernet. The autonegotiation will make it possible to negotiate on the mode or data rate of operation between the communicating devices.

6.1.6 Gigabit Ethernet :

- The gigabit Ethernet protocol has been designed in order to operate at data rates upto 1000 Mbps or 1 Gbps. This is the highest bit rate of all the types.
- The MAC layer was supposed to remain unchanged for all the versions of the Ethernet but it does not remain so when such a high data rate is to be supported.
- The Gigabit Ethernet is capable of operating in either half duplex or full duplex modes.

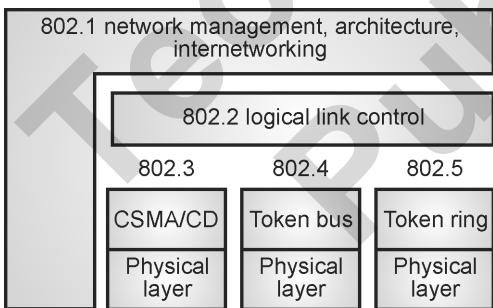
6.2 IEEE Standards :

- The Institution of Electrical and Electronics Engineers (IEEE) has developed the layered architecture and other standards of LAN, under their project 802 set up in 1980. The IEEE 802 standards are as follows :

- 802.1 Architecture, Management and Internetworking
- 802.2 Logical Link Control (LLC)
- 802.3 Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
- 802.4 Token Bus
- 802.5 Token Ring
- 802.6 Distributed Queue Dual Bus (DQDB)Metropolitan Area Networks (MANs)
- 802.7 Bandpass Technical Advisory Group



- 802.8 Fibre Optic Technical Advisory Group
- 802.9 Integrated Data and Voice Network
- 802.10 Security Working Group
- 802.11 Wireless LAN Working Group
- 802.12 Demand Priority Working Group
- 802.13 Not Used
- 802.14 Cable Modem Working Group
- 802.15 Wireless Personal Area Networking Group
- 802.16 Broadband Wireless Access Study Group.
- In LANs, all the stations share the common cable (i.e. media). Therefore IEEE adopted three mechanisms of media access control namely :
 1. Carrier sense multiple access/collision detection (CSMA/CD)
 2. Token bus and 3. Token ring
- Thus there are three protocols for the MAC sublayer. The IEEE standard 802.3 (CSMA/CD), 802.4 (Token bus), 802.5 (Token ring) are associated with these protocols as shown in Fig. 6.2.1.
- The physical layer protocols do the job of signal encoding, data rate control and interfacing to the transmission medium. The Logical Link Control layer (LLC) specifications are given in IEEE 802.2.



(G-295) Fig. 6.2.1 : IEEE LAN and related standards

6.3 Traditional Ethernet (IEEE 802.3) :

- The traditional Ethernet is the oldest version of Ethernet created in 1976 which is designed to support data rates upto 10 Mbps.
- The access to the network by a device is through the CDMA/CD i.e. MAC uses CSMA/CD and the media is shared between all the hosts connected on the Ethernet.

Medium access control sublayer :

- The MAC layer controls the operation of the access method which is CSMA/CD.
- It receives the data from the upper layer, frames it and passes it to the PLS sublayer for encoding.
- The access method used is 1-persistent CSMA/CD.

6.3.1 Traditional Ethernet Frame :

SPPU : May 16, May 17, Dec. 17, May 19, Dec. 19

University Questions

Q. 1 Explain the frame format for IEEE 802.3.

(May 16, May 17, Dec. 17, May 19, Dec. 19, 6 Marks)

- Fig. 6.3.1 shows the frame format of traditional Ethernet.

Preamble	SFD	Destination address	Source address	Length PDU	Data and padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 – 46 bytes	4 bytes

(G-305) Fig. 6.3.1 : Traditional Ethernet frame

Frame format :

- The 64-bit (8 bytes) preamble allows the receiver to synchronize with the signal, it is a sequence of alternating 0's and 1's.

DA and SA :

- Both the source and destination hosts are identified with a 48-bit (6 bytes) address.
- These are indicated by the 6 byte number entered in the destination address (DA) and source address (SA) fields of the frame.
- The packet type field serves as the de-multiplexing key.

Data :

- Each frame contains upto 1500 bytes of data. The minimum size of a frame is 46 bytes of data, the reason for this is that the frame must be long enough to detect a collision.
- Each frame includes 32 bit (4 bytes) checksum. CRC is the last field in the Ethernet frame.
- The Ethernet is a bit-oriented framing protocol. An Ethernet frame has 14-byte header, two 6-bytes addresses and 2-byte type field.
- The sending adapter attaches the preamble, CRC and postamble before transmitting and the receiving adapter removes them.



Start Frame Delimiter (SFD) :

- This is the second field in the Ethernet frame and it is of 1 byte length. The byte stored at this field is 10101011.
- This field signals the beginning of the frame.
- The SDF is used to communicate to the station that this is the last chance for synchronization.
- The last two bits 11 alert the receiver that the next field in the frame contains the destination address.

6.3.2 Frame Length :

- There is a restriction imposed on the minimum and maximum length of the frame of the Ethernet.
- The minimum frame length is 512 bits or 64 bytes and the maximum frame length is 12,144 bits or 1518 bytes.
- The format of the minimum length frame is shown in Fig. 6.3.2(a) and that of the maximum length frame is shown in Fig. 6.3.2(b).

Destination address	Source address	Length PDU	Data and padding	CRC
6 bytes	6 bytes	2 bytes	46 bytes	4 bytes

64 bytes

(a) Minimum length frame

Destination address	Source address	Length PDU	Data and padding	CRC
6 bytes	6 bytes	2 bytes	1500 bytes	4 bytes

1518 bytes

(b) Maximum length frame

(G-306) Fig. 6.3.2 : Minimum and Maximum length frame formats of traditional Ethernet

- The restriction on the minimum length is to ensure correct operation of CSMA/CD, whereas the restriction on the maximum length is just out of some historical reasons.

6.3.3 Addressing :

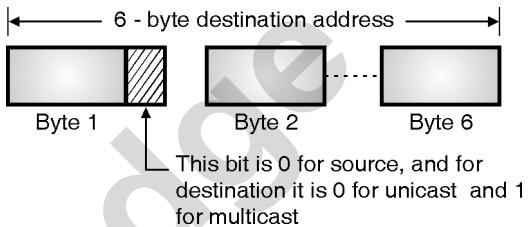
- There can be various types of stations connected on an Ethernet network such as PC on workstation or printer.
- Each station has its own network interface card (NIC) which fits inside the station to contain the 6 byte physical address of the station.
- Fig. 6.3.3 shows a 6-byte Ethernet address in the hexadecimal notation.

04 – 02 – 01 – 06 – 1C – 5B

(G-307) Fig. 6.3.3 : Ethernet address

6.3.4 Types of Addresses :

- A source address is only unicast address. This is because the frame comes from only one source.



(G-308) Fig. 6.3.4 : Difference between unicast and multicast addresses

- The destination address can be one of the following three types :
 1. Unicast
 2. Multicast
 3. Broadcast
- Fig. 6.3.4 shows how to differentiate between the unicast address and multicast address.

1. Unicast destination address :

- Uni means one. So this type of address defines only one destination and the relation between the sender and the receiver is one-to-one.
- The frame sent by the sender is meant only for one particular receiver.

2. Multicast destination address :

- Multi means many. So this type of address defines a group of destination addresses to which the same message is to be delivered. Thus the sender-receiver relation is one to many.

3. Broadcast address :

- 1. Broadcasting process is the process in which the sender transmit and all others receive or listen.
- 2. This type of destination address is a special case of multicast address in which all stations are destinations.

6.3.5 Physical Properties of Ethernet :

- Let us see some physical properties of Ethernet.
- An Ethernet segment is implemented on a coaxial cable of upto 500 m.



- A **transceiver**, which is a small device directly attached to the tap, detects when the line is idle and drives the signal when the host is transmitting. Tap must be at least 2.5 m apart.
- Transceiver also receives incoming signals. It is in turn, connected to an Ethernet adapter, which is plugged into the host. All the power of Ethernet is in adapter.
- Multiple Ethernet segments can be joined together by repeaters. A **repeater** is a device that forwards digital signals.
- Note that, no more than four repeaters may be positioned between any pair of hosts.
- Ethernet has a total reach of only 2500 m and it is limited to supporting a maximum of 1024 hosts with 100 base T, twisted pair.
- The common configuration have several point-to-point segments coming out of a multi-way repeater, called a hub, multiple 100-Mbps Ethernet segments can also be connected by a hub.

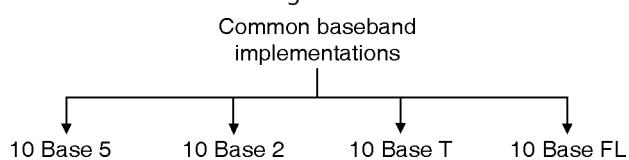
6.3.6 Physical Layer Implementation of Standard Ethernet :

SPPU : May 10, Dec. 12, May 14, Dec. 18

University Questions

- Q. 1** Explain the following physical layer implementations in standard Ethernet :
1. 10Base5
 2. 10Base2
 3. 10BaseT
 4. 10BaseF
- with respect to media, maximum length and line encoding. **(May 10, Dec. 12, Dec. 18, 8 Marks)**
- Q. 2** Differentiate : 10 Base 2, 10 Base 5 and 10 Base T specification. **(May 14, 6 Marks)**

- The standard has defined four different implementations for the baseband (digital) 10 Mbps Ethernet as shown in Fig. 6.3.5.



(G-312) Fig. 6.3.5 : Categories of traditional Ethernet

IEEE 802.3 10 Mbps Specifications (Ethernet) :

- IEEE 802.3 committee defines alternative physical configurations. Various defined options are as follows :
 1. 10 BASE 5
 2. 10 BASE 2
 3. 10 BASE – T (T stands for twisted pair)
 4. 10 BASE – FL (F stands for optical fiber)
- All the four options stated above are for the 10 Mbps Ethernet.

1. 10 Base 5 : Thick Ethernet :

- The first implementation of the traditional Ethernet is called 10 Base 5 or thick Ethernet or thicknet.
- This was the first Ethernet technology.
- The name thicknet is due to the use of thick coaxial cable.
- The thicknet uses the bus topology.
- It is the original 802.3 medium specification and is based directly on Ethernet.
- A 50Ω coaxial cable is used.
- The data is converted into Manchester digital signalling.
- Maximum length of cable segment is 500 m.
- We have to use repeaters if the length is to be increased further.
- At the most four repeaters are allowed to be used. Hence the effective length of the medium is 2.5 km because there will be 5 segments of 500 m each with 4-repeaters.

2. 10 Base 2 : Thin Ethernet :

- This is second implementation of the traditional Ethernet, and it is also known as cheapernet.
- It uses a comparatively thin coaxial cable and bus topology.
- This is a low cost system than 10 BASE 5 and used for the personal computer LANs.
- This specification as well uses 50Ω coaxial cable and the data is converted into Manchester digital signalling before putting it on the cable.
- Thin Ethernet uses a thin cable, supports less number of users and specified for an effective length of 185 metres only.



- The data rate is same as that of 10 BASE 5 specification i.e. 10 Mbps hence it is possible to combine them in a network.
- Note that the 10 BASE 2 should not be used to connect two segments of 10 BASE 5 cable.

3. 10 Base-T : Twisted pair Ethernet :

- This is the third physical layer implementation of traditional Ethernet. It makes use of a physical star topology.
- The twisted pair cable of unshield type is used instead of coaxial cable as the common medium.
- The data is converted into Manchester digital signaling before putting it on the cable.
- The maximum segment length is reduced to only 100 m. It is much less than the 10 BASE 5 specification.
- The advantage of this type is that the twisted pair wire is easily available in any building (due to the existing telephone connection).
- As an alternative an optical fiber link can be used. Then the maximum length becomes 500 m.

4. 10 Base FL : Fiber Link Ethernet :

- This is the fourth physical layer implementation of traditional Ethernet.
- It makes use of the star topology for connecting stations to a hub.
- The transceiver is connected to the hub by using two pairs of fiber optic cables.
- This standard contains three specifications as follows :
 1. 10 BASE FP (P for passive).
 2. 10 BASE FL (L for link).
 3. 10 BASE FB (B for backbone).
- All these specifications use a pair of optical fibers for each transmission link.
- The data is converted into the Manchester code and then the Manchester signal is converted into light signal (off for 0 and on for 1). Hence the frequency of the Manchester bit stream actually needs to be 20 Mbps on the fiber.

6.4 Changes in the Standards :

- The 10 Mbps standard Ethernet has undergone several changes before moving to the higher data rates.

- These changes allowed the Ethernet to evolve and becomes compatible with the other high speed LANs.
- In this section we have discussed some of these changes.

6.5 Bridged Ethernet :

SPPU : Dec. 11

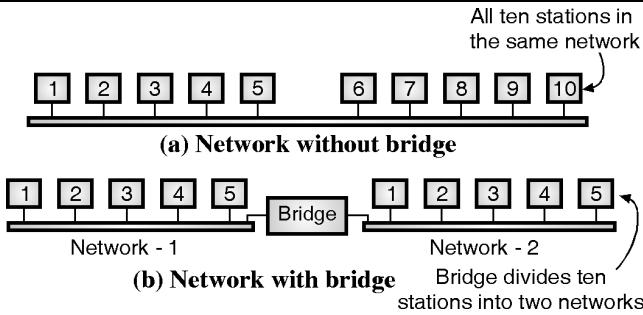
University Questions

Q. 1 What are the advantages of dividing an Ethernet LAN with a bridge ? **(Dec. 11, 6 Marks)**

- The 10 Mbps standard Ethernet has undergone many changes before it was upgraded to the higher data rates.
- Bridged Ethernet is one of those changes. The other two changes are switched Ethernet and full duplex Ethernet.
- There are two effects of using bridges on Ethernet LANs. They are as follows :
 1. They increase the bandwidth.
 2. They separate the collision domains.
- Let us discuss both these effects.

1. Increase in bandwidth :

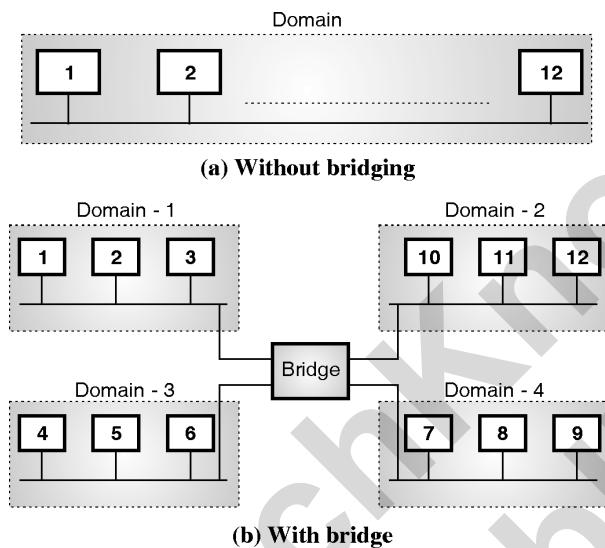
- In the traditional Ethernet the total capacity the network is 10 Mbps and it is shared among all the stations when a frame is to be sent. The stations share the bandwidth of the network.
- If only one station has frames to send, then it can use the entire bandwidth 10 Mbps for itself. But if there are more than one stations simultaneously, then the 10 Mbps capacity will be shared among them.
- The bridge can help increase the bandwidth per station. A bridge divides the network into two or more networks. Each such network is independent from the others and each one will have the full 10 Mbps bandwidth.
- Refer Fig. 6.5.1 in which the original network is divided into two independent networks by inserting a bridge in between.
- Each new network now has 5 stations and each network is independent bandwidth wise can have a capacity of 10 Mbps. Thus the use of bridges increases the bandwidth per station.



(G-313)Fig. 6.5.1 : Increase in Bandwidth due to bridge

2. Separation of collision domain :

- Fig. 6.5.2 explains the concept of separation of collision domains.



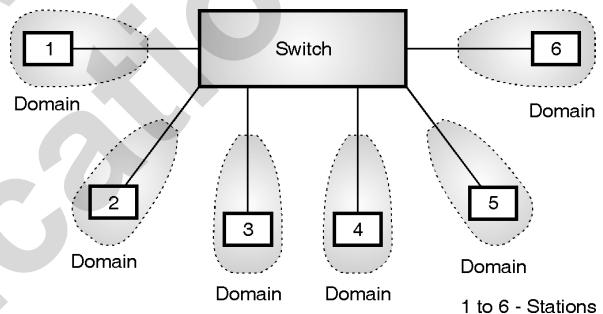
(G-314) Fig. 6.5.2 : Collision domains in the nonbridged and bridged network

- Fig. 6.5.2(a) shows the collision domains for the original network without bridge whereas Fig. 6.5.2(b) shows the collision domains for the same network now with a bridge.
- With the use of bridge, the collision domain becomes much smaller and probability of collision is reduced because smaller number of stations now compete for the access of the medium.
- Without bridging all the 12 stations compete for access to the medium and with bridging only 3 stations would compete for access to medium.
- Thus the use of bridge separates the collision domains and reduces the possibility of collisions.

6.6 Switched and Full Duplex Ethernet :

6.6.1 Switched Ethernet :

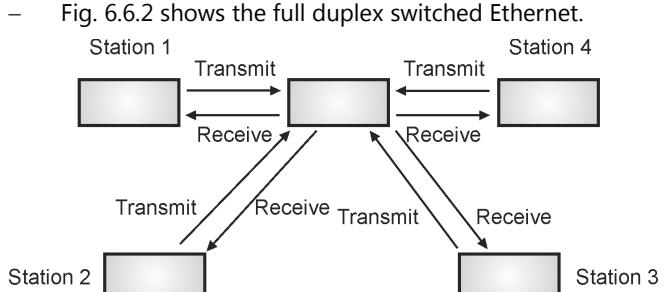
- The concept of bridged LAN can be extended to form the switched LAN.
- An N port switch is used to connect N number of stations on the LAN.
- Each member of the LAN is connected to a port of the switch.
- The entire bandwidth is shared only between the stations and the switch.
- The collision domain is divided into N domains. This reduces the possibility of collisions in the network.
- Due to the use of a layer 2 switch faster handling of packets is also possible.
- The concept of switched Ethernet is illustrated in Fig. 6.6.1.



(G-315)Fig. 6.6.1 : Switched Ethernet

6.6.2 Full Duplex Ethernet :

- The 10 Base 5 and 10 Base 2 Ethernets have a serious drawback. The communication on them is always half duplex.
- That means a station can either transmit or receive at a time. It cannot send and receive simultaneously.
- So the full duplex switched Ethernet was developed from the basic switched Ethernet.
- Fig. 6.6.2 shows the full duplex switched Ethernet.



(G-316)Fig. 6.6.2 : Full duplex switched Ethernet



- Due to the full duplex mode, the capacity of each domain increases from 10 to 20 Mbps.
- We have to use two communication links between each station and the switch.
- One of the link is used to send data and the other one is used to receive it.
- The full duplex switched Ethernet does not need CSMA/CD because there is no more need of carrier sensing.

MAC :

- The traditional Ethernet is a connectionless protocol at the MAC sublayer.
- That means there is no flow control or error control and the sender does not know anything about whether the frame has reached the destination without error or it has been damaged/lost.
- When the receiver receives the frame, it does not send any acknowledgement back to the sender.
- In order to provide the flow and error control, a new sublayer called MAC control is added between the LLC sublayer and MAC sublayer.

6.7 Fast Ethernet : SPPU : Dec. 14, May 17**University Questions**

Q. 1 Discuss Fast Ethernet technology in brief. State its specification. (Dec. 14, May 17, 7 Marks)

- Fast Ethernet is the protocol designed to work upto 100 Mbps and it is compatible with the standard Ethernet.
- The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

MAC sublayer :

- In the evolution of Ethernet, care has been taken to keep the MAC sublayer untouched.
- So MAC sublayer of the fast Ethernet is same as that of the traditional Ethernet.
- For the standard Ethernet the bus and star topologies were used.
- But the fast Ethernet uses only the star topology.

Access method :

- The access method also remains the same. It is CSMA/CD.
- However the fast Ethernet is a full duplex protocol and does not need the CSMA/CD.
- But the CSMA/CD is used for backward compatibility, with the traditional Ethernet.

Frame format :

- Frame format of fast Ethernet is same as that of the traditional Ethernet.

Minimum and maximum frame lengths :

- Minimum and maximum frame lengths of the fast Ethernet frame are same as those of traditional Ethernet.

Addressing :

- Addressing is also same as that for the traditional Ethernet.

6.7.1 Autonegotiation :

- This is the new feature of the fast Ethernet.
- Due to this feature the two stations can make the negotiation on the mode or data rate of operation.

Features of the autonegotiation :

- The important features of autonegotiation are :

 1. The non-compatible devices can be connected to each other.
 2. One device can be allowed to have multiple capabilities.
 3. A station can check hub's capabilities.

6.7.2 Physical Layer Implementation :

SPPU : May 10, Dec. 17, May 19

University Questions

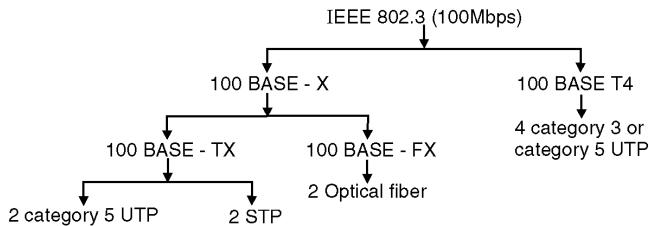
Q. 1 Explain following physical layer implementation in Fast Ethernet :
 1. 100 BaseTX
 2. 100 BaseFX
 3. 100 BaseT4.

With respect to media, maximum length and line encoding. (May 10, May 19, 6 Marks)

Q. 2 Compare 100BASE-TX, 100BASE-FX, 100BASE-T4. (Dec. 17, 7 Marks)



- Fig. 6.7.1 shows the various types of cables used for the fast Ethernet.



(G-318) Fig. 6.7.1 : IEEE 802.3 100 BASE – T options

- As shown, it can be either a two wire or four wire implementation.
- The 100 Base X is a two wire implementation. It can be either a twisted pair cable (100 Base – TX) or fiber optic cable (100 Base – FX).
- The 100 Base T4 is a four wire specification and it is designed only for the twisted pair cable.
- All of the 100 BASE – T options shown in Fig. 6.7.1 use the IEEE 802.3 MAC protocol and frame format.
- 100 BASE – X indicates the options which use the medium specifications defined by FDDI.
- All the 100 BASE – X types use two physical links between any two nodes, one of them is used for transmission and the other one for the reception.
- Refer Fig. 6.7.1. The 100 BASE – TX uses either the shielded twisted pair (STP) or a high quality (category 5) unshielded twisted pair (UTP). Whereas 100 BASE-FX uses optical fiber.
- There is a disadvantage of using any of the 100 BASE-FX option because a new cable needs to be installed.
- So 100 BASE-T4 provides a low cost option because it uses category 3 voice grade UTP or a higher quality (category 5) UTP.
- 100 BASE – T4 uses four twisted pair lines between any two nodes in order to achieve 100 Mbps data rate over a low quality cable.
- For all the 100 BASE – T options, the star topology is used.

Comparison of 100BASE-TX, 100BASE-FX, 100BASE-T4:

Sr. No.	Parameter	100 Base TX	100 Base FX	100 Base T4
1.	Used for	Fast Ethernet	Fast Ethernet	Fast Ethernet
2.	Type of implementation	Two wire twisted pair cable	2 wire fibre optic	4 wire twisted pair
3.	Frame format	802.3 MAC	802.3 MAC	802.3 MAC
4.	Medium used	Either STP or UTP	Optical fiber	Twisted pair cable
5.	Number of wires	2	2	4
6.	Maximum length	100 m	100 m	100 m
7.	Block encoding	4 B / 5B	4B / 5B	–
8.	Line encoding	MLT-3	NRZ-I	8B / 6T

6.8 Gigabit Ethernet :

SPPU : May 12, Dec. 12, May 13

University Questions

Q. 1 Describe gigabit ethernet with reference to the following :

- MAC sublayer
- Frame bursting
- Topology. **(May 12, May 13, 8 Marks)**

Q. 2 Discuss gigabit ethernet with reference to the following :

- MAC sub-layer
- Gigabit Ethernet frames. **(Dec. 12, 8 Marks)**

- The Gigabit Ethernet protocol has been designed in order to support the data rates upto 1000 Mbps or 1 Gbps.
- The MAC layer was supposed to remain unchanged throughout the evolution of the Ethernet but it does not remain so when the rate of 1 Gbps is to be supported.
- The Gigabit Ethernet is capable of operating in either half duplex or full duplex modes.
- If it operates in the half duplex mode, then the access method used is CSMA/CD.



- But if the full duplex mode is used then CSMA/CD is not required.
- Almost all the implementations in Gigabit Ethernet use the full duplex mode.
- The half duplex mode is used only for the backward compatibility with the standard and fast Ethernets.

Topology :

- This Ethernet uses a point-to-point topology if only two stations are to be connected.
- But it uses the star topology if more number of stations are to be connected to each other.
- The Gigabit Ethernet was designed with some specific goals in mind :
 1. To increase the data rate to 1 Gbps.
 2. To make it downward compatible with the older version i.e. standard or fast Ethernet.
 3. To make use of the same 48-bit address.
 4. To utilize the same frame format.
 5. Not to change the minimum and maximum frame lengths.
 6. To use the autonegotiation as defined in fast Ethernet.

6.8.1 MAC Sublayer : SPPU : May 12, May 13

University Questions

- Q. 1** Describe gigabit ethernet with reference to the following :
1. MAC sublayer
 2. Frame bursting
 3. Topology.
- (May 12, May 13, 8 Marks)**

- The MAC sublayer can not remain unchanged or same as standard or fast Ethernet if the data rate of 1 Gbps is to be achieved.
- The Gigabit Ethernet has to use two approaches for the medium access :
 1. Full duplex and 2. Half duplex.
- The full duplex approach is being followed by almost all the implementations of Gigabit Ethernet.
- But if the half duplex approach is followed then the Gigabit Ethernet can be made compatible with standard or fast Ethernet.

Full duplex mode :

- In this approach, a central switch is connected to all computers or other switches.
- Each switch has buffers for each input port. The incoming data are stored on these buffers until it is transmitted.
- There is no collision in this mode. Hence CDMA/CD is not used.
- As there is no collision, the length of cable is dependent on the signal attenuation in the cable and not on the collision detection process.

Half duplex mode :

- The Gigabit Ethernet is used very rarely in the half duplex mode.
- For this mode a hub can be used instead of the switch.
- The CDMA/CD which is not used for the full duplex mode, has to be used for the half duplex mode.
- The maximum length of the cable is entirely decided by the minimum value of the frame size.
- In relation with the minimum frame size the following three methods have been defined :
 1. Traditional method
 2. Carrier extension and
 3. Frame bursting

1. Traditional method :

- In the traditional method, the minimum length of the frame is kept same as that in the traditional Ethernet. (512 bits or 64 bytes).
- But in Gigabit Ethernet the length of each bit is $1/1 \times 10^9 = 1$ nsec. The bit length for a 10 Mbps Ethernet is $1/10 \times 10^6 = 100$ nS. Thus the length of each bit is 1/100 times shorter in the Gigabit Ethernet as compared to that in the 10 Mbps Ethernet.
- Hence the slot time for Gigabit Ethernet is given by

$$\text{Slot time} = 512 \text{ bits} \times 1 \times 10^{-9} \text{ sec.} = 0.512 \mu\text{sec.}$$
- Due to reduced slot time, the collision is detected 100 times earlier and therefore the maximum length of the network is restricted to only 25 m i.e. 100 times less than the maximum length of the traditional Ethernet (2.5 km).
- This length is very short and not suitable for connecting computers even in one single office.



- Due to these demerits the traditional approach is not suitable.

2. Carrier extension method :

- In order to increase the length of the network the minimum frame length is increased to 512 byte i.e. 4096 bits in the carrier extension approach.
- This is 8 times longer than the minimum frame size of 64 bytes in the traditional approach. Therefore the maximum length of the network also is increased 8 times and becomes $25 \times 8 = 200$ m.

3. Frame bursting :

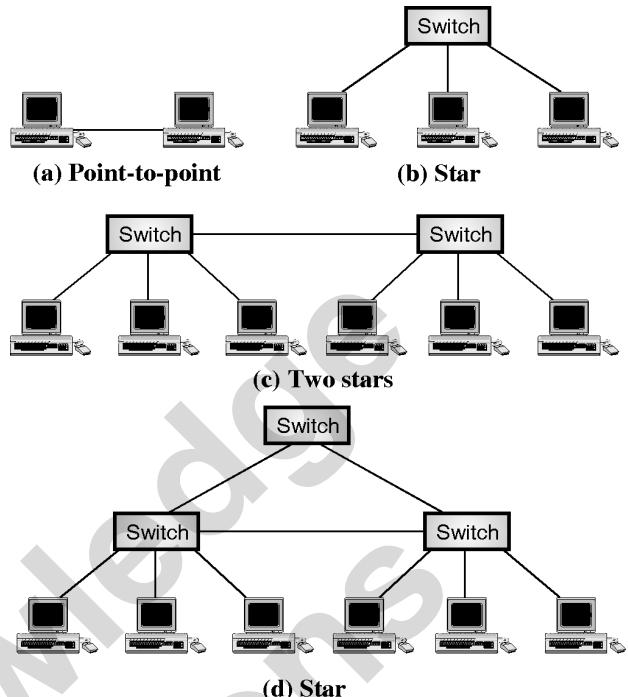
- The carrier extension technique increases the maximum length of the network. But it is very inefficient technique because for sending short frames we need to send a lot of redundant data so make the frame length equal to 4096 bits.
- The efficiency can be increased with the help of the **frame bursting** technique. Here instead of adding an extension to each frame, multiple frames are sent to make the minimum frame length of 4096 bits.
- However in order to make these multiple frames appear like one frame, padding is added between the frames. This is same as that used for the carrier extension approach. Thus we send a large frame without adding any redundant bits.

6.8.2 Physical Layer :

- The physical layer in the Gigabit Ethernet is not as simple as that in the standard or fast Ethernet.
- Some of its features are as follows :

Topology :

- The topology used for connecting the stations in Gigabit Ethernet depends on the number of stations to be connected.
- For example : if two stations are to be connected, a point to point topology may be used. For three or more stations a star topology is used with a hub or switch at the center.
- Another option is to connect several startopologies with a star topology being a part of another one as shown in Figs. 6.8.1(c) and (d).



(L-799)Fig. 6.8.1 : Topologies of Gigabit Ethernet

6.8.3 Physical Layer Implementation :

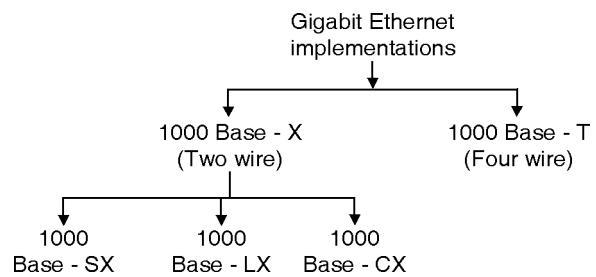
SPPU : May 06, May 11

University Questions

- Q. 1** Discuss Gigabit Ethernet with reference to the following :
1. MAC sub layer
 2. Gigabit Ethernet frames
 3. 1000 BaseX specification.

(May 06, May 11, 9 Marks)

- We can categorize the Gigabit Ethernet as either a two wire or a four wire implementation.
- The two wire implementation is known as 1000 Base X and the four wire implementation is known as 1000 Base-T.
- The four wire implementation uses twisted pair cable.
- Fig. 6.8.2 shows the physical layer implementations for the Gigabit Ethernet.



(G-323) Fig. 6.8.2 : Physical layer implementations of Gigabit Ethernet

**Encoding :**

- The Gigabit Ethernet cannot use the Manchester encoding due to its high bit rate.
- Hence the 8B/10B block encoding followed by NRZ encoding is used for all the two wire implementations.

6.8.4 Ten Gigabit Ethernet :

- The next step of Gigabit Ethernet is ten gigabit Ethernet. The IEEE committee calls this Ethernet as standard 802.3ae.
- The goals of 10GB Ethernet are as follows :
 1. Data rate is to be upgraded to 10 Gbps.
 2. This Ethernet should be downward compatible to the standard, fast and gigabit Ethernet.
 3. Frame format and 48-bit address should be same as the older versions.
 4. Minimum and maximum frame lengths should remain same.
 5. This Ethernet should be connectable to the existing LAN, WAN and MAN.
 6. This Ethernet should be mode compatible with the technologies like Frame Relay and ATM.

MAC sublayer :

- This Ethernet operates only in the full duplex mode. Hence there is no possibility of contention. So CDMA/CD is not used in this Ethernet.

Physical layer :

- The physical layer of this Ethernet is designed to work with the optical fiber cable.
- The three commonly used implementations are :
 1. 10 G Base-S
 2. 10 G Base-I
 3. 10 G Base-E

6.8.5 Comparison of Standard and Gigabit Ethernet :**SPPU : Dec. 05, May 08****University Questions**

- Q. 1** Write a short note on Gigabit Ethernet. Compare Gigabit Ethernet with Traditional Ethernet.

(Dec. 05, May 08, 6 Marks)

Sr. No.	Parameter	Standard Ethernet	Fast Eternet	Gigabit Ethernet
1.	Maximum speed	10 Mbps	100 Mbps	1 Gbps
2.	MAC technology	CSMA/CD	CSMA/CD	CSMA/CD
3.	Maximum segment length	500 m		25 m to 70 m at full speed
4.	Topology	Bus / star		Point to point or star
5.	Bandwidth requirement	Low	High	Very high
6.	Medium	Either copper cables or optical fiber cables	Either copper cables or optical fiber cables	Either copper cables or optical fiber
7.	Minimum frame size	64 bytes	64 bytes	64 bytes
8.	Mode	Half duplex or full duplex	Full duplex	Full duplex and half duplex

6.9 Token Bus : IEEE 802.4 :**SPPU : May 07, Dec. 18****University Questions**

- Q. 1** Explain IEEE 802.4 specification.

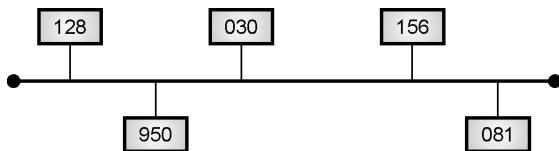
(May 07, 6 Marks)

- Q. 2** Write short notes on :

1. IEEE 802.4 (Token Bus)

2. IEEE 802.5 (Token Ring). **(Dec. 18, 7 Marks)**

- The IEEE 802.4 standard for media access control (MAC) is known as Token bus.
- Token bus is a linear or tree shaped cable through which different stations are interconnected.
- Logically the interconnected stations form a ring as shown in Fig. 6.9.2.

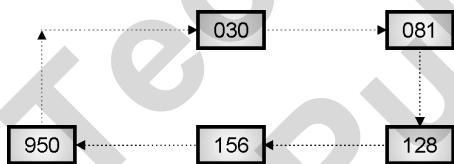


(G-326) Fig. 6.9.1 : Physical topology in token passing

- The physical topology is bus topology as shown in Fig. 6.9.1.
- Each station knows its own identification number and the identity of the stations preceding and following it.
- The sequence number and the physical location of a station on the bus are not related to each other.
- Look at the sequence of stations in the logical sequence of token passing, shown in Fig. 6.9.2.
- It shows that the stations connected on a bus are arranged in a logical sequence.

Token :

- After initialization of the logical ring, the station which has the highest number sends out the first frame.
- After doing so it passes a permission to its neighbouring station that now the neighbouring station can send its frame.
- This permission is passed by sending a special control frame called "Token".



(G-327) Fig. 6.9.2 : Logical sequence of token passing

Media access control (MAC) :

- The operation of token bus taken place as follows :

 1. At any time, the station which holds the token only can transmit its data frames on the bus. Every frame contains source and destination addresses.
 2. All the other stations are ready to receive these data frames.
 3. As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence. That station is allowed to transmit its data now. Likewise the token is circulated over the entire ring to all the stations.

4. In one cycle of operation, each station will get an opportunity to transmit once. The same station can get more number of chances to transmit in one cycle if more than one addresses are assigned to it.

Frame format :

- The frame format as specified by IEEE 802.4 is as shown in Fig. 6.9.3.

Number of bytes →	1(min)	1	1	2-6	2-6	4	1
Preamble	Bit synchronization	SD	FC	DA	SA	DATA	FCS
SA	Source Address						ED
SD	Frame Start Delimiter						
DATA	Data Field						
FC	Frame Control (type)						
FCS	Frame Check Sequence						
DA	Destination Address						
ED	End Delimiter						

(G-2705) Fig. 6.9.3 : Format of IEEE 802.4 frame

- The frame consists of following fields :

 1. **Preamble** : Preamble is at least one octet (8 bits) long and used for bit synchronization.
 2. **Start Delimiter (SD)** : It is a unique one byte pattern which indicates that the frame begins here.
 3. **Frame Control (FC)** : This field indicates the type of frame. It is one octet long and indicates if the frame is a data frame or control frame. Token is one of the control frames.
 4. **Destination Address (DA)** : It contains the destination address and it is 2 to 6 bytes long.
 5. **Frame Check Sequence (FCS)** : This field contains a CRC code. It is 4 byte long and used to check on DA, SA, FC and Data fields.
 6. **End Delimiter (ED)** : This a one byte unique bit pattern which marks the end of the frame.

- The total length of the frame from FC to FCS field including the Data field can be at the most 8191 octets.

Token management :

- The active stations control and manage the token. Each one of them can initiate and respond to the control frames such as claim token frame, solicit successor frame, set successor frame and who follows frame.
- The function of these frames is to initialize the bus and for adding or removing a station.

**Physical specifications :**

- Data rates at which a token passing LAN operates can be 1, 5 or 10 M bits/sec using analog signaling over 75 ohm coaxial cable.
- Two types of transmission systems are used :
 1. Carrierband (single channel)
 2. Broadband (multiple channel)
- Both these systems use some kind of modulation to reduce the effect of noise.
- The carrier band system FSK (frequency shift keying) modulation is used.
- It is a bi-directional transmission system. 1 M bits/sec bus is implemented using a flexible semi-rigid co-axial cable.
- The more expensive versions of the bus can operate at 5 to 10 M bits/sec.
- The broadband system uses a unidirectional transmission. It uses a combination of phase and amplitude modulation.
- Separate carriers are used for the transmit and receive directions.
- As this is a multiple channel system, there will be several transmit and receive carriers.
- Each carrier provides a data rate of 5 or 10 M bits/sec. Broadband LANs can cover a span of several kilometres.

6.10 Token Ring System [IEEE 802.5] :**SPPU : May 08, May 11, Dec. 18****University Questions**

Q. 1 Describe IEEE 802.3 and IEEE 802.5 frame formats in detail. **(May 08, 3 Marks)**

Q. 2 Discuss the medium access control technique used in Token Ring network with suitable example. **(May 11, 8 Marks)**

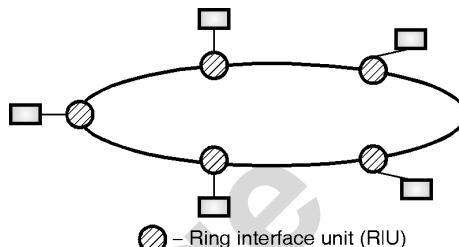
Q. 3 Write short notes on :

1. IEEE 802.4 (Token Bus)

2. IEEE 802.5 (Token Ring). **(Dec. 18, 7 Marks)**

Block diagram :

- A token ring system is as shown in Fig. 6.10.1.

**(G-329) Fig. 6.10.1 : Token ring system**

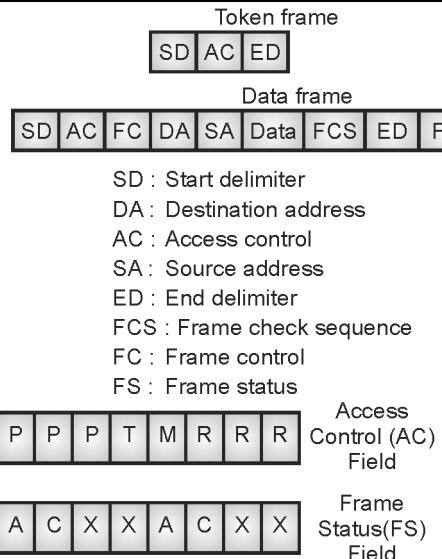
- It consists of a number of stations connected to the ring through a Ring Interface Unit (RIU).
- The RIU is basically a repeater, therefore it regenerates the received data frames and sends them to the next station after some delay.

Media access control (MAC) :

- As discussed in token bus system, here also the access to the medium (i.e. who will transmit) is controlled by the special control frame called token.
- The token is passed from one station to the other round the ring.
- The sequence of token passing is dependent on the physical location of the stations connected to the ring.
- It is not dependent on logical number as in case of token bus system.
- A station which is in possession of the token only can transmit his frames.
- It may transmit one or more data frames but before the expiry of Token Holding Time (THT). Thus every station gets a fixed time to transmit its data.
- Typically this time is of 10 m sec. After the THT, the token frame must be handed over to some other station.

Frame format :

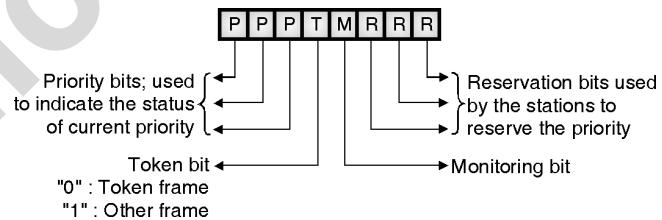
- The IEEE 802.5 has standardized the formats for the token frame and data frame.
- They are as shown in Fig. 6.10.2.



(G-2703) Fig. 6.10.2 : Formats of IEEE 802.5 frames

- The token frame and data frame contain the following fields :
- Start Delimiter (SD) :** This is a one byte long field containing a unique pattern which is used to mark the start of the token or data frames.
 - Access Control (AC) :** This is also a one octet long field. It consists of the priority bits (P), token bits (T), monitoring bits (M) and reservation bits (R) as shown in Fig. 6.10.2.
 - Frame Control (FC) :** This one byte long field is used to indicate the type of frame, Data frame or control frame. It is also used to distinguish between different types of control frames.
 - Destination Address (DA) :** It is 2 to 6 octets long and indicates the destination address.
 - Source Address (SA) :** This is also a 2 to 6 octet long field which indicates the source address.
 - Data Field :** There is no limitation on the size of this field. So it can have 0 or more number of octets. The token holding time will decide the maximum size of the data field.
 - Frame Check Sequence (FCS) :** This field is 4 byte long. It consists of a CRC code for error detection.

- End Delimiter (ED) :** This is one octet long field. It contains a unique bit pattern to mark the end of token or data frame.
- Frame Status (FS) :** The details of this one byte long field are as shown in Fig. 6.10.2.
 - It consists of two address recognized bits (A), two frame copied bits (C) and reserved bits (X).
 - The fourth bit of the AC (access control) field is called as token bit. It enables the stations to distinguish between data and control frames.
 - If it is "0" it indicates a token frame and a "1" indicates other frames.
 - A station which is waiting to transmit its frame, waits for the token bit. As soon as the token bit is found to be "0" (indicating a token frame) it seizes the token by disconnecting the ring at RIU.
 - The station will then insert a "1" in place of "0" and continues with the rest of the data frame.
 - So this station has grabbed the token and hence can transmit its data frames on the ring.



(G-331) Fig. 6.10.3 : Format of the access control (AC) field

Priority management :

- As shown in Fig. 6.10.3 the first three bits in the AC field are priority bits.
- These bits represent eight different priority levels. They indicate the current level of priority.
- The last three bits (R bits) are called as reservation bits. They are used to reserve the priority level.

Ring management :

- One of the stations on the ring acts as an active monitoring station.
- It identifies and rectifies various error conditions. Persistently circulating frames are detected by the monitoring bit (M).



- If the current active monitor fails, any other station can take over its job as monitoring station.

Physical specifications :

- A differential Manchester encoding is used to transmit the data.
- The IEEE 802.5 does not specify the physical transmission medium.
- In practice a shielded twisted pair cable is used. The data rates vary between 1 and 4 M bits/sec.

6.10.1 Comparison of Access Control Methods :

- Out of many existing access methods the CDMA/CD, token passing on bus and token passing on ring are most important. Their comparison is as follows :

CDMA/CD :

- It provides a totally decentralized control.
- The maximum waiting time for a station to access the medium is not guaranteed.
- The bandwidth for any station is not guaranteed.
- Short delay for light traffic.

Token passing on bus :

- Higher reliability.
- Maximum waiting time for access is guaranteed, because every station gets a fixed time for transmission.
- System can be easily expanded.
- Medium utilization is high.

Token ring :

- High reliability.
- Easily expandable.
- Maximum waiting time for access is guaranteed.
- Maximum utilization of media bandwidth.

6.11 High Level Data Link Control (HDLC) Protocol :**SPPU : Dec. 10, May 11, May 13, May 14****University Questions**

- Q. 1** What is HDLC ? Explain with the help of its frame format. Describe all fields in detail.

(Dec. 10, 4 Marks)

Q. 2 Explain various station types and configurations used in HDLC. **(May 11, 8 Marks)**

Q. 3 What is HDLC ? Explain with the help of its frame format. **(May 13, 8 Marks)**

Q. 4 What is HDLC ? Explain with the help of its frame format. Describe all fields in detail. **(May 14, 6 Marks)**

- The high level data link control (HDLC) protocol was developed by ISO.

- It is the most widely accepted data link layer protocol. It has the advantages of flexibility, adaptability, reliability and efficiency of operation.

- HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.

- For the HDLC protocol the following three types of stations have been defined :

1. Primary station
2. Secondary station
3. Combined station

1. Primary station :

- A primary station takes care of the data link management. When communication between the primary and secondary stations takes place, the primary station would connect and disconnect the data link.
- The frames sent by a primary station are called commands.

2. Secondary station :

- A secondary station operates under the control of a primary station.
- When communication between primary and secondary stations takes place, the frames sent by the secondary station takes place are called responses.

3. Combined station :

- A combined station can act as primary as well as secondary stations.
- Therefore it can send both commands and responses.

Operating modes for data transfer :

- In HDLC both synchronous and asynchronous modes of communication are permitted.



- The meaning of the words synchronous and asynchronous is different from that of a physical layer.
- Following modes of operation are possible for data transfer :
 1. Normal response mode (NRM)
 2. Asynchronous response mode (ARM)
 3. Asynchronous balanced mode (ABM)
- The first two modes of operation are suitable for an unbalanced type of data transfer between one primary and the other secondary stations whereas the third one is suitable for a balanced type of data transfer.

Normal Response Mode (NRM) :

- This mode is suitable for point-to-point as well as point-to-multipoint configurations.
- Here the primary station will control the overall data link management. It is a synchronous mode of communication.

Asynchronous Response Mode (ARM) :

- This mode is used for communication between primary and secondary stations.
- As the name indicates it is an asynchronous mode of communication.
- In ARM the secondary station can transmit response (frame) without taking permission from the primary station.
- This is not allowed in NRM. Therefore NRM is a more disciplined mode than ARM.
- The responsibility of link management function still lies with the primary station.

Asynchronous Balanced Mode (ABM) :

- This mode is applicable to the point to point communication between two combined station.
- As both these stations are combined stations, they are capable of link management functions.
- As the communication is asynchronous, one station can transmit a frame without permission from the other station.
- In this mode information frames can be transmitted in full duplex manner.

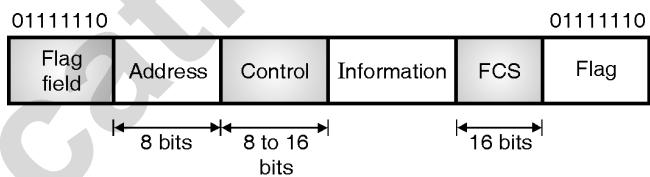
6.11.1 Frame Structure in HDLC :

SPPU : Dec. 10, May 13, May 14, Dec. 15

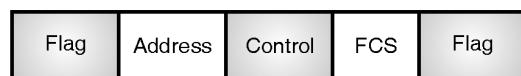
University Questions

- Q. 1** What is HDLC ? Explain with the help of its frame format. Describe all fields in detail. **(Dec. 10, 4 Marks)**
- Q. 2** What is HDLC ? Explain with the help of its frame format. **(May 13, May 14, 8 Marks)**
- Q. 3** Explain the HDLC frame formats i.e. I-frame, S-frame, U-frame. **(Dec. 15, 6 Marks)**

- In the discussion of ARQ, we saw that the functionality of a protocol depends on the control fields that are used in the header.
- The format of the HDLC frame is defined in such a way that it can accommodate various data transfer modes.
- The HDLC uses two different frame formats as shown in Fig. 6.11.1(a) and Fig. 6.11.1(b).



(a) Information transfer frame



(b) Supervisory and unnumbered frames

(G-250)Fig. 6.11.1

- If you compare them, then it will be clear that except for the information field both the frames are identical to each other.
- The frame is transmitted from left to right with the lowest order bit transmitted first.

Flag field :

- The flag is a unique 8-bit word pattern (0111110).
- It is used to identify the start and end of each frame as shown in Fig. 6.11.1(a).
- It is also used to fill the idle time between consecutive frames.

**Address field :**

- The address field consists of the address of secondary station irrespective of whether a frame is being transmitted by primary or secondary station.
- Address field consists of 8 bits hence it is capable of addressing 256 addresses.

Control field :

- The control field usually consists of 8 bits but the number of bits can be extended to 16.
- It carries the sequence number of the frame, acknowledgements, request for transmission and other control commands and responses.

Information field :

- The field size of the information field is variable and it can consist of any number of bits.
- It consists of the user's data bits and it is completely transparent.

Frame check sequence (FCS) field :

- This is a 16 bit field which is used for detection of errors in the address, control and information field.
- It is nothing else but a 16 bit CRC code for error detection.

6.11.2 Frame Types in HDLC :**SPPU : Dec. 10, Dec. 15, May 19****University Questions**

Q. 1 What is HDLC ? Explain with the help of its frame format. Describe all fields in detail.

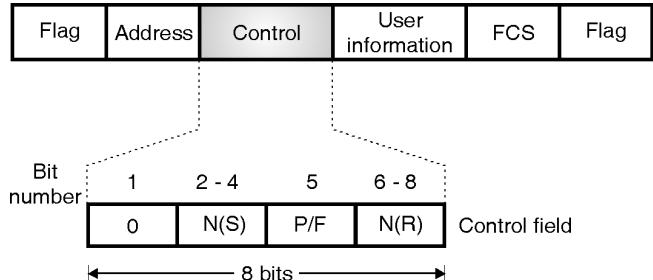
(Dec. 10, 4 Marks)

Q. 2 Explain the HDLC frame formats i.e. I-frame, S-frame, U-frame. **(Dec. 15, May 19, 6 Marks)**

- There are three types of frames defined in HDLC as follows :
 1. The I-frame or information frame.
 2. The S-frame or supervisory frame.
 3. The U-frame or the unnumbered frame.

The I-frame :

- Fig. 6.11.2 shows the format of the information frame or I-frame.

**(G-251)Fig. 6.11.2 : I-frame format**

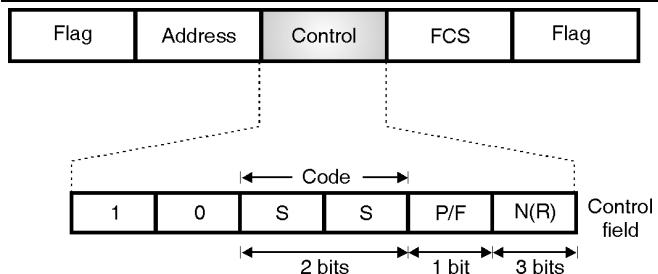
- It is supposed to carry the user data from the network layer.
- It is also possible to include the flow and error control information which is also called piggybacking.

Explanation :

- Concentrate on the control field of the I-frame.
- As shown in the Fig. 6.11.2 if the first bit in the control field is 0 it is identified as an information frame (I-frame).
- The next three bits (2 to 4) are called N (S) and their job is to define the sequence number of the frame.
- Since there are only 3 bits, we can define only eight combinations ($2^3 = 8$).
- Therefore a sequence number is between 0 and 7 only.
- The value of N(S) field corresponds to the value of control variable S as discussed for the three ARQ mechanisms.
- The next bit (5th) is the poll/final (P/F) bit.
- It can have two possible values 0 or 1 out of which only the logical 1 is meaningful. Logic 0 in this position has no meaning.
- When P/F = 1, it means poll when a frame is sent by a primary station to secondary.
- When P/F = 1, it means final when a frame is sent by a secondary station to primary.
- The last three bits (6 to 8) define the N(R) field. It is used for piggybacking.
- The 3 bits in the N(R) field will represent the value of ACK when piggybacking is used.

The S-Frames :

- Fig. 6.11.3 shows the format of S-frames or supervisory frames.

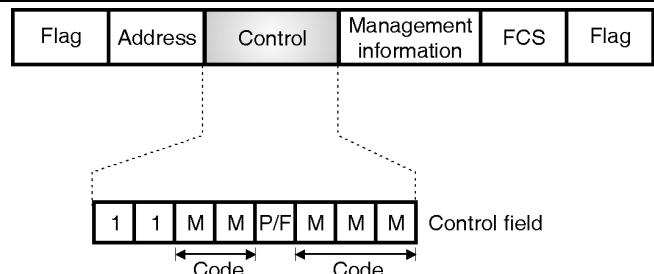


(G-252)Fig. 6.11.3 : S-frame format

- An S-frame does not contain any information field.
- These frames are used for flow and error control when piggybacking is not possible to implement or when piggybacking is not appropriate to implement.
- Refer to the control field of the S-frame.
- A 10 in the first two bits of the control field identifies it as a Supervisory frame or S-frame as shown in Fig. 6.11.3.
- The next two bits define the code field marked SS. There are four possible combinations of these bits.
- They indicate different types of S-frames.
- There are 4 types of supervisory frames corresponding to the four possible value of the S bits in the control field.
 1. SS = 00 → corresponds to receive ready (RR) frames which are used to acknowledge frames when no I frames are available to piggyback the acknowledgement.
 2. SS = 01 → corresponds to Reject (REJ) frames which are used by the receiver to send a NAK when error has occurred.
 3. SS = 10 → corresponds to a Receive Not Ready (RNR) frame and it is used for flow control.
 4. SS = 11 → corresponds to a Selective Repeat Frame which indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.
- The fifth bit in the control field is P/F bit the function of which is as discussed earlier, and the next 3 bits called N(R) correspond to the ACK or NAK value.

U-frames :

- The format of U-frame i.e. the unnumbered frame is shown in Fig. 6.11.4.



(G-253)Fig. 6.11.4 : Format of U-frame

- These frames are used for exchanging the session management and control information between the communicating devices.
- A 11 in the first two bits of the control field identifies an unnumbered (U) frame as shown in Fig. 6.11.4.
- The information field in U-frame is used for carrying the system management information. It does not carry the user data.
- The U-frame code bits (M bits in Fig. 6.11.4) are divided into two sections. Two bits before P/F bit and three bits after the P/F bits.
- These five code bits can create upto $2^5 = 32$ different types of U-frames.
- The unnumbered frame types are used for functions such as initialization, status reporting and resetting.
- The Information frame and supervisory frames implement the error and flow control functions of the data link layer.
- The combination of the I-frames and supervisory frames allows HDLC to implement stop-and-wait, Go-back-n and selective repeat ARQ.

6.11.3 Transparency in HDLC :

- The data field of HDLC frame is capable of carrying text and non-text information.
- The examples of non-text information is audio, video, graphics etc.
- But a problem is introduced for some message types during the transmission.
- If the data field of an HDLC frame contains the pattern 01111110 which is reserved for the flag field, then the receiver will treat that sequence as the end flag.
- Naturally the remaining bits are interpreted as the bits from next frame.
- This is called as lack of data transparency.



6.11.4 Bit Stuffing :

- Bit stuffing is used to overcome the lack of data transparency.
- In HDLC, transparency is achieved by ensuring that the unique flag sequence (0111110) does not appear in the address, control, information and FCS fields.
- At the transmitter an extra '0' bit is inserted after five consecutive 1's occurring anywhere after the opening flag and before the closing flag.
- At the receiver the extra '0' bit following five consecutive "1" is deleted. This technique is called "zero stuffing" or bit stuffing.
- The bit stuffing is not done for three operating conditions.
- First is when the bit sequence is really a flag, second is when the transmission is being aborted, and third is when the channel is idle.

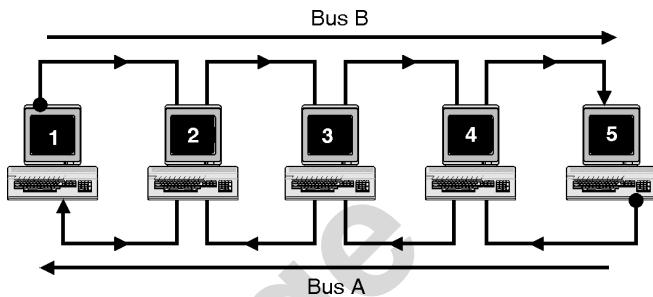
6.11.5 Why is CRC in Data Link Protocols in Trailer and not in Header ?

- Note that for all the data link protocols discussed so far, the CRC field that contains the checksum for error detection and correction, always appears in the trailer i.e. at the end of the frame and not in the header.
- The CRC is obtained by adding all the bits being transmitted, and appended to the outgoing stream as soon as the last bit is transmitted.
- If we want CRC to be in the header i.e. at the beginning of the frame, then the CRC has to be calculated by scanning the frame before transmission.
- This would require each byte to be handled twice, once for computing CRC and then for transmission.
- But if CRC is put in the trailer, then each byte will have to be handled only once.

6.12 IEEE 802.6 Standard :

- The DQDB protocol is a dual bus configuration as suggested by the name itself. Each host in this network gets connected to two backbone network lines.
- The approach used here for a host getting access to the transmission medium is completely different than that in LAN.
- The mechanism for access to the transmission medium in DQDB is known as **distributed queue** mechanism.

- The architecture of DQDB with two unidirectional buses is as shown in Fig. 6.12.1.



(G-1432) Fig. 6.12.1 : Architecture of DQDB

- In Fig. 6.12.1 the two buses A and B are unidirectional buses.
- All the five hosts shown are connected to these buses. Each bus is connected to each host at its input and output ports as shown.

DQDB traffic :

- As shown in Fig. 6.12.1, each bus in DQDB allows the traffic to take place only in one direction.
- However note that buses A and B allow the traffic in opposite directions to each other as shown.

Upstream and downstream :

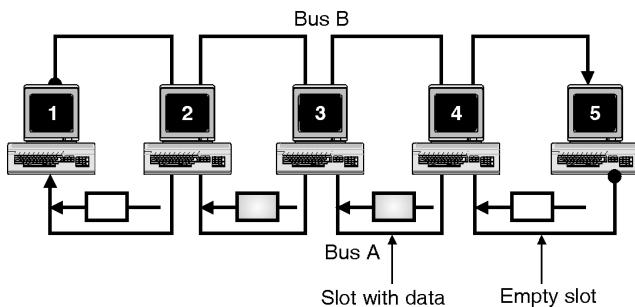
- In Fig. 6.12.1, consider host number 3. From the point of view of this host, the hosts 1 and 2 are **downstream** on bus A whereas hosts 5 and 4 are **upstream** on bus B.
- Similarly the host 5, does not have any **upstream** hosts on bus B but has **four downstream** hosts on bus A.
- Host-5 is considered as the head of Bus A and host-1 is its end.
- Similarly for Bus-B, host-1 is the head and host-5 is the end.

Data flow :

- On each bus, the data flows in the form of 53-byte transmission slots.
- These slots are like boxes or containers which can carry packets.
- The head would generate the slots. Thus host-5 generates empty slots for bus-A whereas host-1 generates them for bus-B.
- An empty slot starts travelling along the bus. A host drops its data into the slot and the destination host will pick it up.



- The sending host should choose a bus for which the destination is downstream. The destination should not be an upstream destination.
- Consider Fig. 6.12.2 to understand the data transmission in DQDB MAN. It shows the transmission from host-4 to host-2.



(G-1433) Fig. 6.12.2 : Data transmission in DQDB

1. Host-2 is downstream to host-4 on bus A. Hence the head of bus-A i.e. host 5 will create an empty slot.
2. As soon as this empty slot reaches host-4, it drops its data into the slot. Host-4 also assigns the destination to this data as host-2.
3. When the slot moves on bus A across host-3, it will see the destination address and will allow it to pass as it is not meant for host-3.
4. As this slot reaches host-2, it realizes that this slot is meant for it (by comparing the destination address with its own address). So host-2 copies the contents of the slot, marks the slot as read and allows it to move along bus A.
5. The slot reaches host-1 i.e. end of bus A where it gets absorbed.

Medium access :

- In DQDB a host reserves the slot before transmitting its data. Note that this slot reservation is done on the bus which is **upstream** to the host.
- However the data transmission takes place on the bus which is **downstream** to the host as discussed earlier.
- For example host-4 (sending host) will set a **reservation bit** in a slot on bus B (upstream bus for host-4).

- This slot on bus B visits all the hosts. Thus all the hosts know that host-4 wants to reserve a slot on bus A.
- Likewise all the hosts who wish to send their data can reserve a slot.
- These reservations made by different hosts are stored in a First In First Out (FIFO) queue structure. So the reservations are to be processed in the order in which they were made.
- Each host maintains two copies (one per bus) of such queues.

Review Questions

- Q. 1 Write a note on : Physical layer implementation in traditional Ethernet.
- Q. 2 Compare the data rates of traditional, fast and Gigabit Ethernets.
- Q. 3 Explain the physical layer implementation in fast Ethernet.
- Q. 4 What are the common fast Ethernet implementations ?
- Q. 5 Compare the reconciliation sublayer in Fast Ethernet with the PLS sublayer in traditional Ethernet.
- Q. 6 What is GMII in Gigabit Ethernet ?
- Q. 7 Write comparison of 802.3, 802.4 and 802.5 standards related to type of cable used, frame structure, cable length, frequency range.
- Q. 8 How does the Token Ring LAN operate ?
- Q. 9 Explain the frame format of 802.3, 802.4 and 802.5.
- Q. 10 What is Fast Ethernet ?
- Q. 11 Explain the LLC and MAC in IEEE 802 standard and explain the operation of CSMA/CD as used in LAN.
- Q. 12 Write a note on : HDLC protocol.
- Q. 13 Draw and explain the frame structure of HDLC.
- Q. 14 State and explain various frame types in HDLC.
- Q. 15 Explain transparency and bit stuffing in HDLC.



Unit IV

Chapter

7

IP Addressing

Syllabus

Network layer services, IPv4 addresses : Static and dynamic configuration, Classful and classless addressing, Special addresses, NAT, Subnetting, Supernetting, Delivery and forwarding of IP packets, Structure of router, IPv4 : Datagrams, Fragmentation, Options, Checksum, IPv6 Addressing : Notations, Address space, Packet format, Transition from IPv4 to IPv6.

Case study : Visit server room of campus and understand how IP addressing is done for your respective campus → Institute → Department.

Chapter Contents

7.1 Network Layer	7.14 Options
7.2 Network Layer Services	7.15 Option Types
7.3 Routing and Forwarding	7.16 Checksum
7.4 Other Services	7.17 Network Layer Security
7.5 IPv4 Addresses	7.18 IPv6 (Next Generation IP)
7.6 Classful Addressing	7.19 IPv6 Addressing
7.7 Classless Addressing in IPv4	7.20 IPv6 Packet Format
7.8 Special Addresses	7.21 Address Space
7.9 NAT – Network Address Translation	7.22 Address Space Allocation
7.10 Delivery and Forwarding of IP Packets	7.23 Migrating to IPv6 (Compatibility to IPv4)
7.11 Structure of a Router	7.24 Transition from IPv4 to IPv6
7.12 Internet Protocol Version 4 (IPv4)	7.25 University Questions and Answers
7.13 Fragmentation	



7.1 Network Layer :

- The network layer is responsible for carrying the packet from the source all the way to destination.
- In short it is responsible for host-to-host delivery.
- The network layer has a higher responsibility than the data link layer, because the data link layer is only supposed to move the frames from one end of the wire to the other end.
- Thus network layer is the lowest layer that deals with the end-to-end transmission.

Position of network layer :

- Fig. 7.1.1 shows the position of network layer in the 5 layer internet model. It is the third layer.

Layer



(G-433) Fig. 7.1.1 : Position of network layer

- It receives services from the data link layer and provides services to the transport layer.
- The network layer was designed to solve the problem of delivery through several links.
- The network layer is also called as the **Internetwork** layer.
- In addition to the host-to-host delivery the network layer is also responsible for **routing** the packets through the router.
- As a pure concept we can imagine that the Internet is a black box which connects a very large number of computers in the entire world together.
- But the Internet also is not a single network. It is infact the network of many networks or links.
- That means the Internet is an **internetwork** which is actually a combination of LANs and WANs.
- All these LANs and WANs are connected to each other via a connecting device such as a **router** which acts as a switch.

Routers :

- Routers have many ports or interfaces. When it receives a packet at one of its ports, it forwards the packet

through another port to the next switch or the final destination.

7.2 Network Layer Services :

SPPU : May 19

University Questions

- Q. 1** Explain network layer services with example.
(May 19, 4 Marks)

- The duty of the network layer in TCP/IP is to provide the host-to-host delivery of datagrams.
- In this section we are going to discuss the services that are expected from the network layer.
- At the sending end, the network layer will accept a packet from its transport layer, encapsulate the packet into datagram and will deliver the packet to the data link layer.
- At the destination, exactly opposite process takes place. That means, at the destination the received datagram is decapsulated to extract the packet from it and the packet is delivered to the transport layer.

7.2.1 Logical Addressing :

SPPU : May 19

University Questions

- Q. 1** Explain network layer services with example.
(May 19, 4 Marks)

- The two computers in communication with each other should have some universal identification system which is called as the **network layer address or logical address**.
- Thus the sending and receiving computers must have two network-layer addresses for them to communicate.

7.2.2 Services Provided at the Source Computer :

SPPU : May 19

University Questions

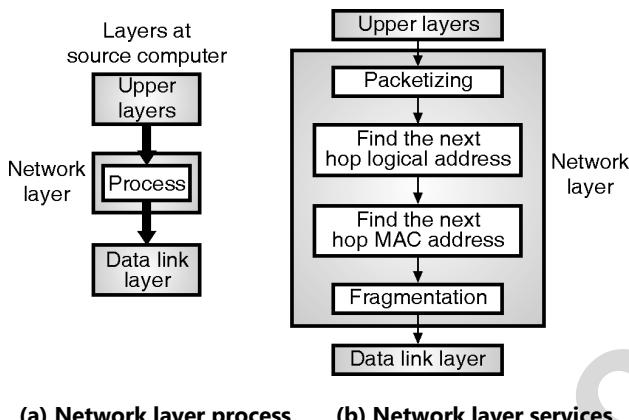
- Q. 1** Explain network layer services with example.
(May 19, 4 Marks)

- The following four services are provided by the network layer at the source computer :

 1. Packetizing.
 2. To find the logical address of the next hop.
 3. To find the physical or MAC address for the next hop.
 4. Fragmentation of the datagram if necessary.



- These services are as shown in Fig. 7.2.1(b).
- The upper layers (transport and application) take services of the network layer.
- For this the upper layers send several pieces of information.
- The network layer processes these pieces of information and creates fragmented datagrams alongwith the next hop MAC address to finally deliver it to the data link layer as shown in Fig. 7.2.1(a).



(G-1999) Fig. 7.2.1

1. Packetizing :

- **Packetizing** is the first duty of the network layer in which it encapsulates the payload (data received from the transport layer) in a packet at network layer at the source.
- Then at the destination the decapsulation process takes place.
- In this way the network layer is doing the job of a postal service in delivering the packages from source to destination.

At the source :

- At the sending end the events take place in the following sequence :

 1. The payload (data) from the upper layer is received.
 2. A header containing the source and destination address and some other information is added to the payload.
 3. This packet is then delivered to the data layer.
 4. If the payload is too large, then the host carries out **fragmentation** on it. Otherwise the host is not allowed to modify the contents of the payload.

2. Finding the logical address of the next hop :

- The datagram prepared with packetizing contains the source and destination addresses of the packet.
- The datagram is to be delivered to the next router. But the source and destination addresses in the datagram do not give any information about the logical address of the next hop.
- The network layer at the source computer finds the logical address of the next hop by consulting a routing table.

3. Finding MAC address of next hop :

- Note that it is the duty of data link layer (and not of network layer) to actually deliver the datagram to the next hop.
- And to do this the data link layer needs the physical or MAC address of the next hop.
- The network layer uses another table to map the logical address of next hop into the corresponding MAC address of next hop.
- However generally an auxiliary protocol called as ARP (Address Resolution Protocol) is used for this purpose.

4. Fragmentation :

- The datagram at this stage may not always be ready to be given to the data link layer.
- The LANs and WANs can carry the data of a limited size in a frame.
- If the data is longer than the maximum specified size for LANs and WANs then it is not possible to fit it in one frame.
- In such circumstances, the datagram should be **fragmented** into smaller data units before passing it to the data link layer.
- The datagram header is copied into all these fragments so that all the necessary information in the datagram is present in every fragment.
- In addition to this some more information regarding the position of that fragment in the whole datagram should be added to the header of the fragment.



7.2.3 Services Provided at Each Router :

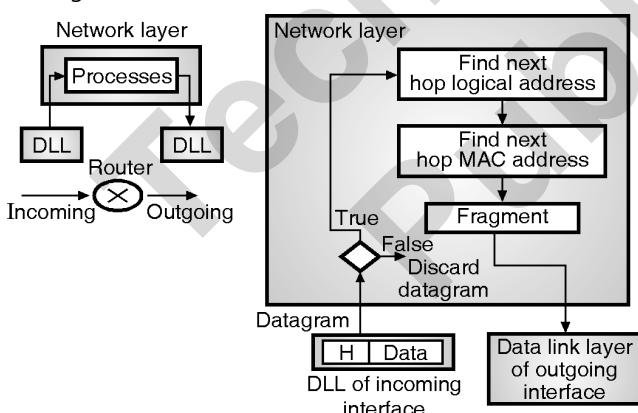
SPPU : May 19

University Questions

Q. 1 Explain network layer services with example.

(May 19, 4 Marks)

- The routers present in between the source and destination are supposed to check the source and destination addresses in the packet in order to forward it to the next network on the path.
- The router is not allowed to decapsulate the received packet unless it is too big and fragmentation needs to be carried out on it.
- The routers are not supposed to change the source and destination addresses.
- In the event of fragmentation, a router has to copy the header in all the fragments.
- At the router the services provided by the network layer are as follows :
 1. To find the next hop logical address.
 2. To find the next hop MAC address.
 3. To carry out fragmentation if required.
- Fig. 7.2.2 shows all these services.



(G-2000) Fig. 7.2.2

- Before providing the services mentioned above the router checks the validity of the incoming datagram with the help of checksum.
- In checking the validation, the following two things are checked :

1. Whether the datagram header is corrupted.
2. Whether the datagram is delivered to the correct router.
- If the incoming datagram fails the validation test then it is simply discarded as shown in Fig. 7.2.2(b).

7.2.4 Services Provided at the Destination Computer :

SPPU : May 19

University Questions

Q. 1 Explain network layer services with example.

(May 19, 4 Marks)

- The sequence of events taking place at the destination is as follows :
 1. The network layer packet is received from the data link layer.
 2. The received packet is decapsulated and the payload is delivered to the upper layer protocol.
 3. If a large packet is fragmented by either the source host or a router, then the responsibility of the network layer at the destination is to wait until all fragments are received, reassemble them and deliver them to the upper layer protocol.
- The network layer at the destination computer is much simpler than that at the source computer or router.
- Before providing any service, the received datagram should be subjected to validation.
- If it passes the validation test then all the services mentioned above should be provided. Otherwise the datagram is discarded.
- The network layer also sets a reassembly timer when it receives fragments of a datagram that are to be reassembled.
- If the reassembly timer expires before arrival of all the fragments, then all data fragments are destroyed and an error message is sent that the entire fragmented datagram be sent again.

7.3 Routing and Forwarding :

- The other two important duties of the network layer, which are related to each other are routing and forwarding.

7.3.1 Routing :

- The responsibility of the network layer is to route the packets from its source to destination.



- The physical network through which the packets travel consists of LANs, WANs and routers.
- Due to this the source and destination are connected to each other via more than one routes.
- It is the responsibility of the network layer to find the best route out of all the possible routes.
- In order to achieve this goal, the network layer must have some concrete strategy for defining the best route.
- In the modern days, this is done by running an appropriate routing protocol, which helps the routers to coordinate their knowledge about the neighbouring routers and prepare routing tables which can be used on the arrival of a packet.
- These routing protocols should be run before commencement of any communication.

7.3.2 Forwarding :

- We can define the process of forwarding as the action taken by a router when it receives a packet at one of its interfaces.
- A router takes such an action with the help of the decision making tables called as **forwarding table** or **routing table**.
- When a packet arrives at one of the interfaces of a router from one of the attached network, the router has to forward it to another attached network.
- The router has to make this decision with the help of a piece of information present in the packet header.
- This piece of information can be the **destination address** or a **label**.
- The router can use this information to find the corresponding output interface number in the **forwarding table**.

7.4 Other Services :

- The other services expected from the network layer are as follows :
 1. Error control.
 2. Flow control.
 3. Congestion control.
 4. Quality of service (QoS).
 5. Security.

- Let us discuss them one by one.

7.4.1 Error Control :

- Eventhough it is possible to implement the error control at the network layer level, the design engineers have neglected this issue.
- One possible reason for this is that the packets may get fragmented at every router due to which the error checking becomes inefficient.
- However a **checksum** field has been added to the datagram in order to control any corruption in the header only.
- The error control is not applicable to the whole datagram.
- Thus there is no direct error control provided by the network layer in the Internet.
- But an auxiliary protocol ICMP is used by the Internet for providing some error control to the datagram.

7.4.2 Flow Control :

- The purpose of providing the flow control is to regulate the data rate of the source so as to avoid the receiver getting overwhelmed.
- The receiver will be overwhelmed if the upper layers at the sending end are producing data at a rate which is higher than the rate at which the upper layers at the destination can consume it (data).
- So as to control the sender's data rate, some kind of a feedback mechanism should be setup so that the receiver can tell the source that it (receiver) has overwhelmed with excess data.
- It is important to remember that the network layer does not directly provide any flow control.
- The flow control is not provided at the network layer level because it is provided for most of the upper layer protocols and there is no need to provide flow control again which makes the design of network layer complex.

7.4.3 Congestion Control :

- This is another important issue to be handled at the network layer. **Congestion** will take place if the source computer sends more datagrams than the capacity of the network or routers.



- In this situation, the routers will drop some of the received packets.
- But this will make the congestion worse because the error control mechanism present at the upper layers will retransmit the packets dropped by the routers.
- Sometimes the congestion becomes so bad that the system collapses and no datagrams are delivered at the destination.
- The congestion control at the network layer is never implemented in the Internet.

7.4.4 Quality of Service (QoS) :

- The quality of service in the Internet has become more important since new applications like multimedia communication have been introduced.
- The Internet has grown as it successfully provides the quality of service to support all the modern day applications.
- However the QoS provisions are not implemented in the network layer. They are mostly implemented in the upper layers.

7.4.5 Security :

- During the early days of the Internet, security was not a major design concern due to limited (small) number of users.
- Hence the network layer was designed without any security provisions.
- But security has become a big concern now. But network layer is connectionless.
- Hence to provide security at the network layer we need to have another virtual level in order to change the connectionless service to connection oriented one.
- The virtual layer is known as IPsec.

7.5 IPv4 Addresses :

- Each computer connected to the Internet should be identified uniquely.
- The identifier used for this purpose is called as the **Internet address** or IP address.
- The hosts and routers on the Internet have unique IP addresses.

- The current version of IP (Internet Protocol) is IPv4 whereas the advanced version is IPv6.
- The IPv4 address is a 32-bit address and it is used for defining the connection of a host or router to the Internet.
- **Thus an IP address is an address of the interface.**

7.5.1 Uniqueness of IP Addresses :

- The IP address is **unique** and **universal**. That means each IP address defines only **one connection** to the Internet.
- At any given time, no two devices connected to the Internet can have the same IP address.
- But if a device is connected to the Internet via two connections through two different networks, then it can have two different IP addresses.
- All the IPv4 addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- The IP addresses for hosts are assigned by the network administrator.
- For Internet it has to be obtained from the network information center.

7.5.2 Address Space :

- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.
- If N numbers of bits are used for defining an address then the address space will be 2^N addresses.
- For IPv4, N is 32 bits. Hence its address space is 2^{32} or 4, 294, 967, 296 (more than 4 billion).
- So theoretically more than 4 billion devices could be connected to the Internet.
- Thus **the address space** of IPv4 is 2^{32} .

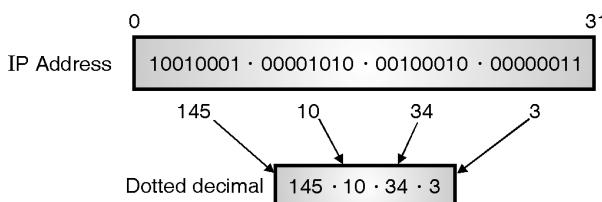
7.5.3 Notation :

- The IPv4 addresses can be shown use three different notations as follows :
 1. Binary notations (base 2).
 2. Dotted decimal notation (base 256).
 3. Hexadecimal notation (base 16).
- Out of these the **dotted decimal** notation is most commonly used.



Dotted decimal notation :

- This notation has become popular because of the two advantages it offers.
- This notation makes the IPv4 address more compact and easy to read.
- The 32 bit IPv4 address is grouped into groups of 8-bits each separated by decimal points (dots).
- Each 8-bit group is then converted into an equivalent decimal number as shown in Fig. 7.5.1.

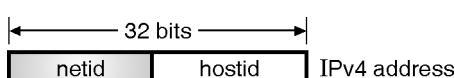


(G-530) Fig. 7.5.1 : Dotted decimal notation

- Each octet (byte) can take a value between 0 and 255.
- Therefore the IPv4 address in the dotted decimal notation has a range from 0.0.0.0 to 255.255.255.255.
- For example the IPv4 address of 1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.

7.5.4 IPv4 Address Format :

- A 32 bit IPv4 address consists of two parts. The first part is called as **net id** i.e. network identification, which identifies a network on the Internet, and the second part is called as the **host id** that identifies a host on that network.
- Fig. 7.5.2 shows the IPv4 address format. Note that the **net id** and **host id** are of variable lengths depending on the class of address.
- Note that class D and E addresses are not divided into net id and host id for the reasons discussed later on.



(G-2002) Fig. 7.5.2 : IPv4 address format

7.6 Classful Addressing :

- The concept of IP addresses is few decades old. It uses the concept of **classes**. This architecture is called as the **classful addressing**.

- Later on in mid 1990s a new architecture of addressing was introduced which was known as **classless addressing**. This new architecture has superseded the original architecture.
- In this section we are going to discuss the classful addressing.

7.6.1 IPv4 Address Classes :

SPPU : May 05, Dec. 10, May 16

University Questions

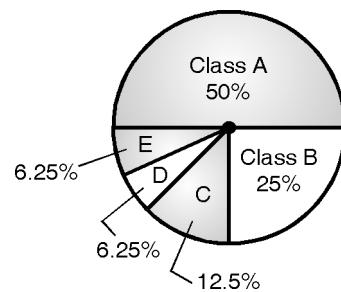
Q. 1 Explain different classes of IP addresses and show by calculations how many networks and hosts are possible in each class ?

(May 05, Dec. 10, 8 Marks)

Q. 2 State classes in IP addressing with range of addresses and number of devices that can be connected.

(May 16, 4 Marks)

- In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E.
- Fig. 7.6.1 shows the percentage of occupation of the address space by each class.
- The number of class A addresses is the highest i.e. 50% and those of classes D and E is the lowest i.e. 6.25%.



Class	No. of addresses
A	2^{31}
B	2^{30}
C	2^{29}
D	2^{28}
E	2^{28}

(G-2003) Fig. 7.6.1 : Classful addressing occupation of address space



7.6.2 Formats of Various Classes :

SPPU : May 05, Dec. 10, May 16

University Questions

Q. 1 Explain different classes of IP addresses and show by calculations how many networks and hosts are possible in each class ?

(May 05, Dec. 10, 8 Marks)

Q. 2 State classes in IP addressing with range of addresses and number of devices that can be connected.

(May 16, 4 Marks)

Class A format :

- The formats used for IPv4 address are as shown in Fig. 7.6.2.
- The IPv4 address for class A networks is shown in Fig. 7.6.2(a).

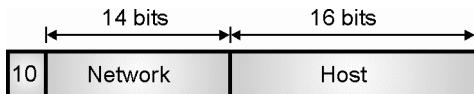


(G-531) Fig. 7.6.2(a) : Class A IPv4 address formats

- The network field is 7 bit long as shown in Fig. 7.6.2(a) and the host field is of 24 bit length.
- So the network field can have numbers between 1 to 126.
- But the host numbers will range from 0.0.0.0 to 127.255.255.255.
- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The "0" in the first field identifies that it is a class A network address.

Class B format :

- The class B address format is shown in Fig. 7.6.2(b).



(G-532) Fig. 7.6.2(b) : Class B format

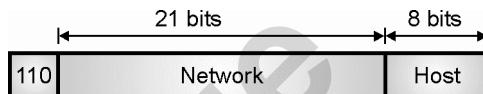
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.
- Class B networks are large. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65,534 (2¹⁶-2) hosts in a class B network.
- Most of the 16,382 class B addresses have been allocated.

- The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

Example : 128.89.0.26, for host 0.26 on net 128.89.

Class C format :

- The class C address format is shown in Fig. 7.6.2(c).



(G-533) Fig. 7.6.2(c) : Class C format

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 7.6.2(d).



Fig. 7.6.2(d) : Class D format

- The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 7.6.2(e) shows the address format for a class E address.
- This address begins with 11110 which shows that it is reserved for the future use.

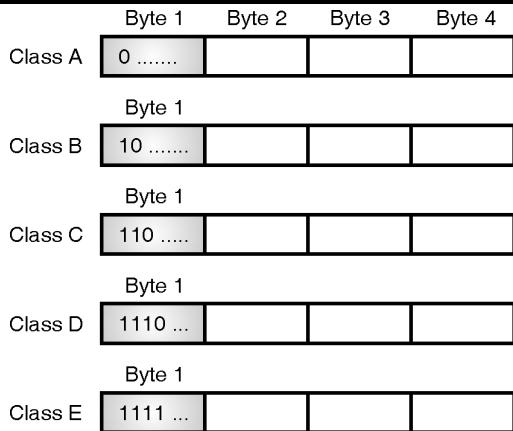


Fig. 7.6.2(e) : IPv4 address for class E network

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation.
- In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

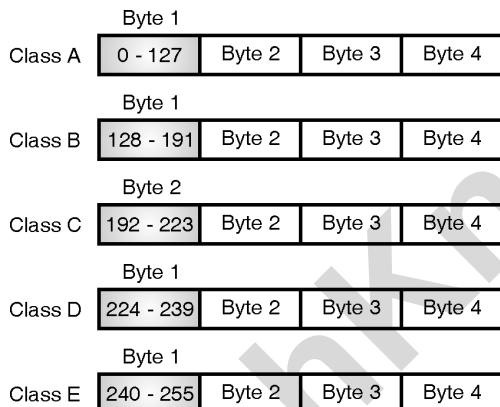
7.6.3 How to Recognize Classes ?

- When an IPv4 address is given to us either in the binary or dotted decimal notation, we can find the class of the address.
- If the given address is in the binary notation then we can identify its class by inspecting the first few bits of the address. This is as shown in Fig. 7.6.3(a).



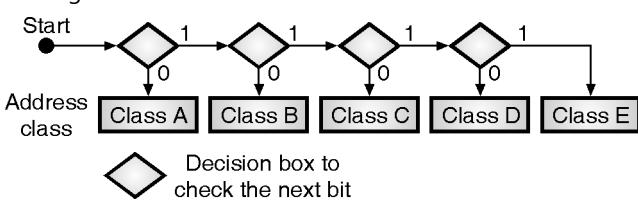
(G-2004) Fig. 7.6.3(a) : Finding the address class

- If the given address is in the dotted decimal notation then we can identify the address class by inspecting the first byte of the address. This is as shown in Fig. 7.6.3(b).



(G-2005) Fig. 7.6.3(b) : Finding the address class

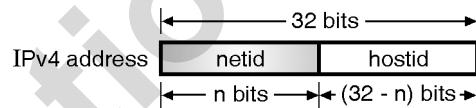
- It is important to note here that there are some special addresses which fall in class A or E.
- These special addresses are to be treated as the exceptions to the classful addressing. We have discussed them later in the chapter.
- In computers, the IPv4 addresses are generally stored in the binary notation format.
- Therefore it is possible to write an algorithm which can identify the address class by using the continuous checking process.
- The principle of such an algorithm has been shown in Fig. 7.6.4.



(G-2006) Fig. 7.6.4 : Algorithm to identify address class

7.6.4 Two Level Addressing :

- The IPv4 addressing is used for defining a destination for an Internet packet at the network layer.
- At the time when classful addresses were designed, the Internet was considered as the network of networks.
- In other words, the whole Internet was divided into a number of smaller networks with many hosts connected to each network.
- Normally an organization, which wants to connect to the Internet, creates a network and the Internet authorities allocate a block of address to the organization. These addresses can be in class A, B or C.
- All the addresses allotted to an organization belong to a single block.
- Therefore each IPv4 address in classful addressing system is made up of two parts namely **net id** and **host id** as shown in Fig. 7.6.5.



(G-2007) Fig. 7.6.5 : Two level addressing in classful addressing

- The job of the **net id** is to define a network and that of the **host id** is to define a particular host in that network.
- As shown in Fig. 7.6.5 if n bits define **net id** then the remaining (32-n) bits define **host id**.
- The value of "n" is not same for all the classes. Infact it is depend on the class as shown in Table 7.6.1.

Table 7.6.1

Class	Value of n
A	$n = 8$
B	$n = 16$
C	$n = 24$

7.6.5 Extracting Information in a Block :

- A block is nothing but a range of addresses.
- For any given block we would be interested to extract the following three pieces of information :
 - The total number of addresses in the block.
 - The first address of the block.



- 3. The last address in the block.
- Before extracting all this information, we have to identify the class of the address as discussed earlier.
- Once we find the class of the block, we will have the values of "n" (the length of **net id** in bits) and $(32 - n)$ i.e. the length of the **host id** in bits.
- It is now possible to obtain the three pieces of information mentioned above as shown in Fig. 7.6.6.

1. Total number of addresses in the block :

- The total number of IPv4 addresses in the given block will be equal to,

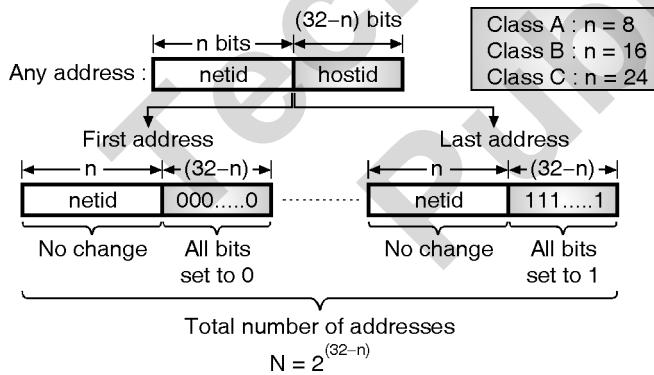
$$N = 2^{(32-n)} \quad \dots(7.6.1)$$

2. First address in the block :

- The first address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and setting all the $(32 - n)$ rightmost bits to 0 as shown in Fig. 7.6.6.

3. Last address in the block :

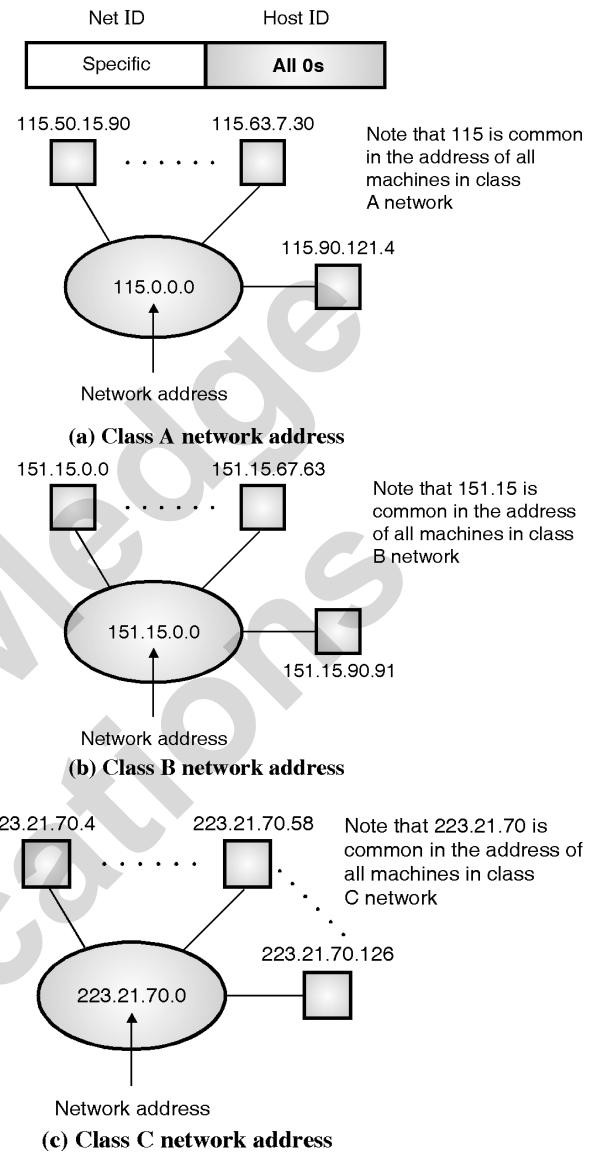
- The last address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and then setting all the $(32 - n)$ rightmost bits to 1 as shown in Fig. 7.6.6.



(G-2008) Fig. 7.6.6 : Information extraction in classful addressing

7.6.6 Network Address :

- The network address is an address that defines the network itself.
- It cannot be assigned to a host. Fig. 7.6.7 shows the examples of network addresses for different classes.



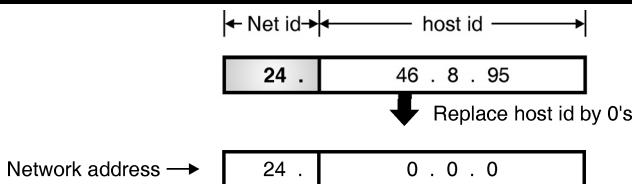
(G-536) Fig. 7.6.7

- The following examples will enable you to find the network address.

Ex. 7.6.1 : For the address 24.46.8.95 identify the type of network and find the network address.

Soln. :

- Examine the first byte. Its value is 24 i.e. it is between 0 and 127. So it is a class A network.
- So only the first byte defines the Net id. So we can find the network address by replacing the host id with 0s.
- The process of obtaining the network address is shown in Fig. P. 7.6.1.



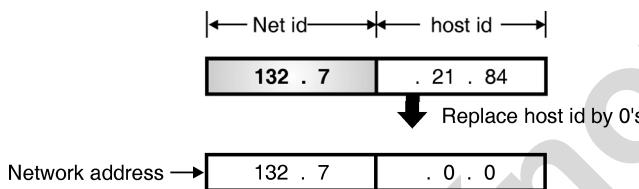
(G-537) Fig. P. 7.6.1

- So the network address is 24.0.0.0.

Ex. 7.6.2 : For the address 132.7.21.84 find the type of network and the network address.

Soln. :

- Examine the first byte. It is 132 i.e. between 128 and 192. So it is a class B network.
- So the first two bytes define the net id. Replace the host id with 0's to get the network address as shown in Fig. P. 7.6.2.



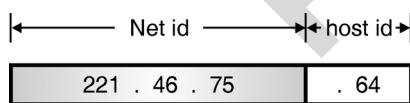
(G-538) Fig. P. 7.6.2

- So the network address is 132.7.0.0.

Ex. 7.6.3 : Find the class of the network if the address is 221.46.75.64.

Soln. :

- The first byte is 221 i.e. between 192 and 255. So this is a class C network.
- The net id and host id are as shown in Fig. P. 7.6.3.



(G-539) Fig. P. 7.6.3

What is the difference between net id and network address ?

- The network address is different from a net id. A network address has both net id and host id, with 0s for the host id.

Where to use the network address ?

- The network address is used to route the packets to the desired location.

7.6.7 Network Mask or Default Mask :

- Earlier we have discussed the methods for extracting different pieces of information.
- But all these methods are theoretical methods which are useful in explaining the concept.
- But practically these methods are not used. When a packet arrives at the input of the router in the Internet, it uses an algorithm to extract the **network address** from the destination address in the received packet.
- This can be achieved by using a **network mask**.

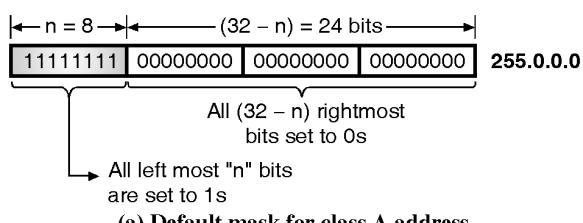
Definition of default mask :

- A **network mask** or **default mask** in classful addressing is defined as a 32-bit number obtained by setting all the "n" leftmost bits to 1s and all the $(32 - n)$ rightmost bits to 0.

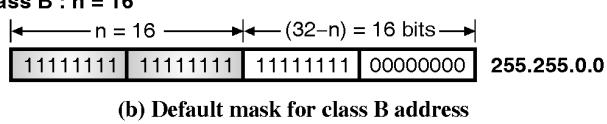
7.6.8 Default Masks for Different Classes :

- We know that the value of n is different for different classes. Therefore their default masks also will be different.
- The default masks for class A, B and C addresses are as shown in Fig. 7.6.8.

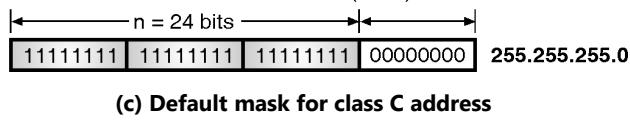
Class A : n = 8



Class B : n = 16



Class C : n = 24



(G-2009) Fig. 7.6.8

- Table 7.6.2 enlists the default masks of the three classes of IPv4 addresses.

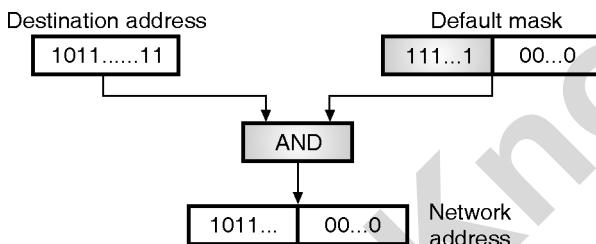


Table 7.6.2 : Default masks

Address class	Default mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

7.6.9 Finding Network Address using Default Mask :

- The router uses the AND operation for extracting the network address from the destination address of the received packet.
- The router ANDs the destination address with the default mask to extract the network address as shown in Fig. 7.6.9.



(G-2010) Fig. 7.6.9 : Finding a network address using the default mask

- It is possible to use the default mask to find the number of addresses and the last address in the block.

7.6.10 Three Level Addressing : Subnetting :

SPPU : Dec. 10, Dec. 16

University Questions

- Q. 1** Define subnetting. **(Dec. 10, 2 Marks)**
Q. 2 Define subnetting, supernetting and classless addressing. **(Dec. 16, 4 Marks)**

- As discussed earlier, the originally designed IP addresses were with two level addressing with **net id** and **host id**.
- The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host.
- But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :

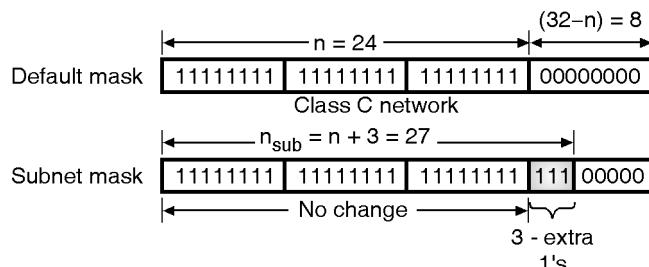
1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

Definition of subnetting :

- We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses.
- In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets**.
- Each such subnet has its own **subnet address**.

Subnet mask :

- The **network mask** or **default mask** that we discussed earlier is used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting** is **not** to be done.
- But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet.
- Fig. 7.6.10 shows the format of a subnet mask. Each subnet has its own **net id** and **host id**.



(G-2011) Fig. 7.6.10 : Default and subnet masks

- If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 7.6.10.
- In Fig. 7.6.10, we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.



7.6.11 Special IP Addresses : SPPU : Dec. 14

University Questions

Q. 1 State special IP addresses and the private IP addresses. (Dec. 14, 4 Marks)

- Fig. 7.6.11 shows some special IP addresses.
 - (a)

0 0 0 0	0 0 0 0
---------	-------	---------

 All zeros means this host
 - (b)

0 0	0 0	Host
-----	-------	-----	------

 A host on this network
 - (c)

1 1 1 1	1 1 1 1
---------	-------	---------

 All 1s means broadcast on the local network
 - (d)

Network	1 1 1 1	1 1 1
---------	---------	-------	-------

 Broadcast on a distant network
 - (e)

127	Anything
-----	-------	----------

 Loop back

(G-540) Fig. 7.6.11 : Special IP addresses

- All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 7.6.11(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 7.6.11(c).
- Refer Fig. 7.6.11(d). This is an address with proper network number and all 1s in the host field.
- This address allow machines to send broadcast packets to distant LANs anywhere in the Internet.
- If the address is "127. Anything" as shown in Fig. 7.6.11(e) then it is a reserved address **loopback testing**. This feature is also used for debugging network software.

7.6.12 Limitations of IPv4 :

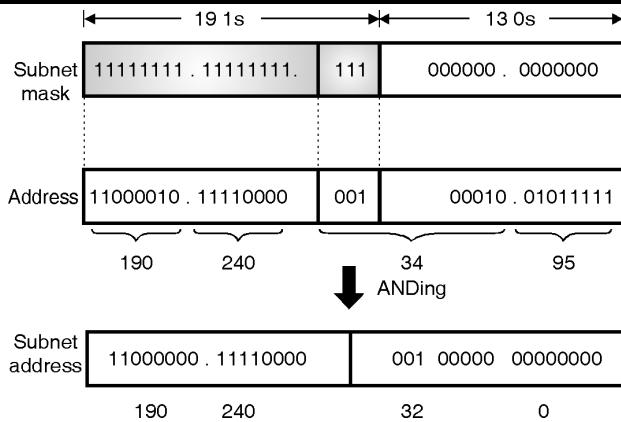
- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify endpoints on networks, and each networked device has a unique IP address.
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses.

- With the proliferation of networked devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming scarce, and the world could theoretically run out of IP addresses.
- If a network has slightly more number of hosts than a particular class, then it needs either two IP addresses of that class or the next class of IP address.
- For example, let us say a network has 300 hosts, this network needs either a single class B IP address or two class C IP addresses.
- If class B address is allocated to this network, as the number of hosts that can be defined in a class B network is $(2^{16} - 2)$, a large number of host IP addresses are wasted.
- If two class C IP addresses are allocated, as the number of networks that can be defined using a class C address is only (2^{21}) , the number of available class C networks will quickly exhaust.
- Because of the above two reasons, a lot of IP addresses are wasted and also the available IP address space is rapidly reduced.
- Other identified limitations of the IPv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng) was proposed.
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.

Ex. 7.6.4 : A router inside an organization receives the same packet with a destination address 190.240.34.95. If the subnet mask is /19 (first 19-bits are 1s and following bits are 0s). Find the subnet address.

Soln. :

- To find the subnet address, AND the destination address with the subnet mask as shown in Fig. P. 7.6.4.



(G-544) Fig. P. 7.6.4

- Thus the subnet address is 190.240.32.0

7.6.13 Classless Addressing :

SPPU : Dec. 15, Dec. 16

University Questions

- Q. 1** What is classless addressing ? Explain.
(Dec. 15, 4 Marks)
- Q. 2** Define subnetting, supernetting and classless addressing.
(Dec. 16, 4 Marks)

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the classless addressing is now being tried out.
- In the classless addressing, there are no classes but the address generation take place in blocks.

Address blocks :

- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.

Restrictions :

- Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.
- 1. The addresses in a block should be continuous, i.e. serial in manner.
- 2. The total number of addresses in a block has to be equal to some power of 2 i.e. $2^1, 2^2, 2^3 \dots$ etc.
- 3. The first address should be evenly divisible by the number of addresses.

7.6.14 Supernetting : **SPPU : May 13, Dec. 16**

University Questions

- Q. 1** What is supernet ? Explain it with suitable example.
(May 13, 8 Marks)
- Q. 2** Define subnetting, supernetting and classless addressing.
(Dec. 16, 4 Marks)

- The class A and class B addresses are almost depleted. But class C addresses are still available.
- But the size of class C address with a maximum number of 256 addresses does not satisfy the needs of an organization. More addresses will be required.
- The solution to this problem is **supernetting**.
- In supernetting an organization combines several class C blocks to create a large range of addresses i.e. several networks are combined to create a supernet.
- By doing this the organization can apply for a set of class C blocks instead of just one.

Example of supernetting :

- If an organization needs 1000 addresses, they can be obtained by using four C blocks (one C block corresponds to 256 addresses).
- The organization can then use these addresses as one supernet as a whole.

Note : The classful addressing is almost obsolete now and it is being replaced with classless addressing.

7.6.15 Who Decides the IP Addresses ?

- No two IP addresses should be same.
- This is ensured by a central authority that issues the prefix or the network number portion of the IP address.



- Locally an ISP is to be contacted in order to get a unique IP address prefix.
- At the global level the Internet Assigned Number Authority (IANA) allots an IP address prefix to the ISP.
- Thus it is ensured that the IP addresses are not duplicated.
- Conceptually IANA is a wholesaler and ISP is a retailer of the IP addresses because ISP purchases IP addresses from IANA and sells them to the customers.

7.6.16 Registered and Unregistered Addresses :

SPPU : Dec. 14

University Questions

Q. 1 State special IP addresses and the private IP addresses. **(Dec. 14, 4 Marks)**

- Registered IP addresses are required for computers which are accessible from the Internet but not every computer that is connected to the Internet.
- For security reasons, networks use firewalls or some other technologies for protecting the computers.
- The firewalls will enable the workstations to access the Internet but do not allow the other systems on the Internet to access them.
- These workstations are given the unregistered private IP addresses.
- These addresses are assigned by the network administrator without obtaining them from an ISP (Internet Service Provider) or IANA.
- These are special network addresses in each class as shown in Table 7.6.3.
- These addresses are to be used for private networks and are called **unregistered addresses**.
- We can choose any of these unregistered address while building our own private network.

Table 7.6.3 : IP addresses for private networks

Class	Network address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

7.6.17 Solved Examples :

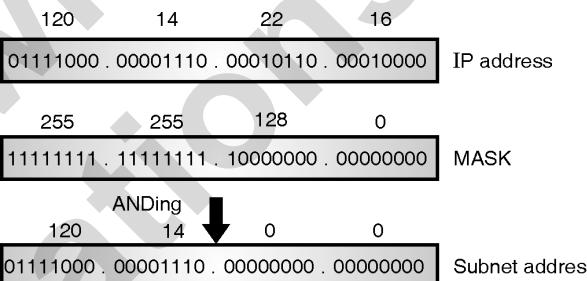
Ex. 7.6.5 : Find the sub-network address and the host id for the following : **May 02, 8 Marks**

Sr. No.	IP address	MASK
(a)	120.14.22.16	255.255.128.0
(b)	140.11.36.22	255.255.255.0
(c)	141.181.14.16	255.255.224.0
(d)	200.34.22.156	255.255.255.240

Soln. :

Step 1 : To find the subnet address :

In order to find the subnet address we have to AND the IP address and the mask as follows :



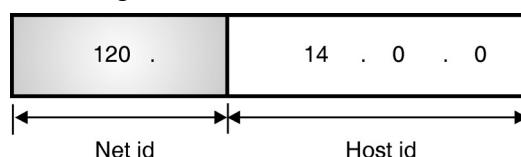
(G-553) Fig. P. 7.6.5(a)

So the subnet address is 120.14.0.0.

Similarly we can find the other subnet addresses.

Step 2 : Host id :

- Examine the first byte of the subnet address. It is 120 which is between 0 and 127. Hence this is a class A network.
- So only the first byte corresponds to the net id and the remaining three bytes correspond to the host id as shown in Fig. P. 7.6.5(b).



(G-554) Fig. P. 7.6.5(b)

So the host id is 14.0.0.

- Similarly we can find the other host id.

Ex. 7.6.6 : The IP address of a host on class C network is 198.123.46.237. Four networks are allowed for this network. What is subnet mask ?

May 02, 8 Marks

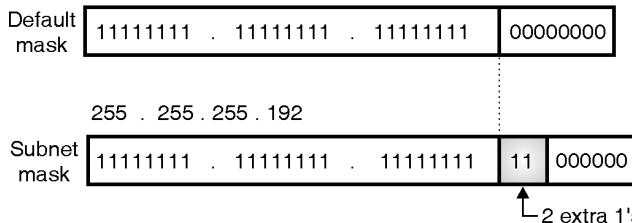


Soln. : The default mask for a class C network is,

255.255.255.0

- In order to have four networks, we must have two extra 1s.
- Hence the default mask and subnet mask are shown in Fig. P. 7.6.6.

255 . 255 . 255 . 0



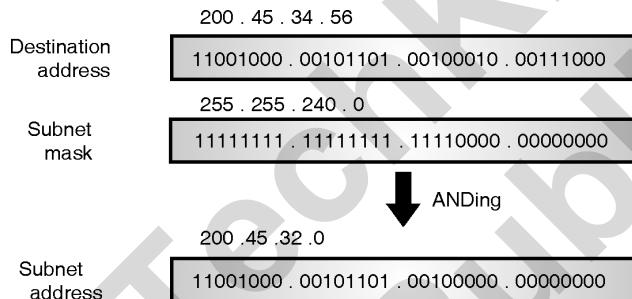
(G-555) Fig. P. 7.6.6

Thus the required subnet mask is 255.255.255.192.

Ex. 7.6.7 : What is the subnet address if the destination address is 200.45.34.56 and subnet mask is 255.255.240.0 ? **May 04, 4 Marks**

Soln. :

To find the subnet address we have to AND the IP address and the subnet mask as shown in Fig. P. 7.6.7.



(G-556) Fig. P. 7.6.7

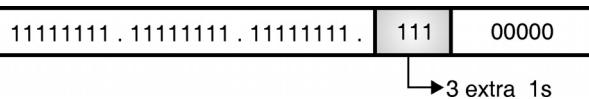
Thus the required subnet address is 200.45.32.0.

Ex. 7.6.8 : A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets.

May 04, 8 Marks

Soln. :

- This is a class C network. So the default mask is,
- 255.255.255.0
- As we need 6 subnets, we need three extra 1s. So the subnet mask is,
- 255.255.255.200
- In the binary form the subnet mask is as shown in Fig. P. 7.6.8.



(G-557) Fig. P. 7.6.8

- In order to have six subnets, we can have 6 different combinations of the 3-extra 1s as shown in Table P. 7.6.8(a).

Table P. 7.6.8(a)

Combination	Subnet number
0 0 0	Subnet 1
0 0 1	Subnet 2
0 1 0	Subnet 3
0 1 1	Subnet 4
1 0 0	Subnet 5
1 0 1	Subnet 6

- So the various addresses of 6 subnets are as shown in Table P. 7.6.8(b).

Table P. 7.6.8(b)

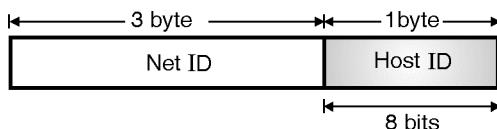
Subnet number	Addresses
1	201.70.64.0 to 201.70.64.31
2	201.70.64.32 to 201.70.64.63
3	201.70.64.64 to 201.70.64.95
4	201.70.64.96 to 201.70.64.127
5	201.70.64.128 to 201.70.64.159
6	201.70.64.160 to 201.70.64.191

Ex. 7.6.9 : For a given class C network 195.188.65.0 design equal subnets in such a way that each subnet has atleast 60 nodes.

May 06, 8 Marks

Soln. :

- Fig. P. 7.6.9(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.

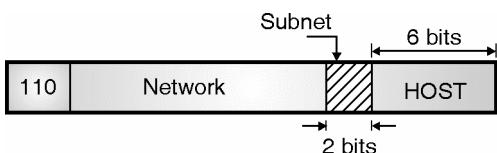


(G-558) Fig. P. 7.6.9(a)

- We are expected to design equal subnets such that each subnet has atleast 60 nodes (i.e. 60 users).



- In order to identify at least 60 users we need 6-bits in the host ID.
- The remaining 2-bits are assigned for subnetting as shown in Fig. P. 7.6.9(b).



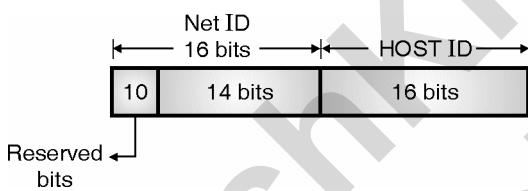
(G-559) Fig. P. 7.6.9(b)

- This shows that there will be four equal subnets each one having at least 60 nodes.

Ex. 7.6.10 : Suppose that instead of using 16-bits for the part of class B address originally, 20-bits had been used. How many class B network addresses would there have been? Give the range of IP addresses in decimal dotted form.

May 07, 6 Marks**Soln. :**

- Fig. P. 7.6.10(a) shows the original class B address format:



(G-567) Fig. P. 7.6.10(a) : Original class B address format

- The first two MSB bits of Net ID part are reserved. Hence, the number of bits actually available for network ID is 14.
- Hence the number of class B networks = $2^{14} = 16382$.

Modification :

- Now with 20 bits instead of 16 being available for the Net ID part the actually available number of bits for Network part becomes 18. This is shown in Fig. P. 7.6.10(b).

$$\therefore \text{Number of class B networks} = 2^{18} = 2,61,888$$



(G-568) Fig. P. 7.6.10(b) : Modified class B address format

- The range of IP addresses in the decimal dotted form would be 128.0.0.0 to 191.255.255.255.

Ex. 7.6.11 : A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of host it can handle ? Give the range of IP addresses in decimal dotted form.

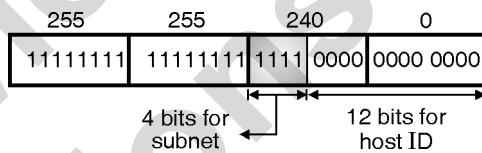
May 07, 6 Marks**Soln. :**

- The structure of class B address is as shown in Fig. P. 7.6.11(a).



(G-564) Fig. P. 7.6.11(a) : Class B address

- The given subnet mask is 255.255.240.0. So it is as shown in Fig. P. 7.6.11(b).



(G-565) Fig. P. 7.6.11(b) : Subnet mask

- Thus there are 4 extra 1s as shown in Fig. P. 7.6.11(b). So there will be 16 subnets and each subnet can have $2^{12} = 4096$ hosts.

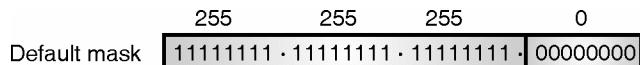
Ex. 7.6.12 : For a given class-C network, design 4 equal subnets having minimum 50 nodes in each subnetwork. **May 08, May 11, 8 Marks**

Soln. :

- The default mask for a class C network is

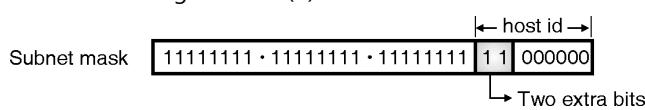
255.255.255.0

- This is as shown in Fig. P. 7.6.12(a).



(G-571) Fig. P. 7.6.12(a)

- In order to design 4 equal subnets having a minimum 50 nodes in each subnetwork, we have to use two extra bits from the host id field. So the subnet mask is as shown in Fig. P. 7.6.12(b).



(G-572) Fig. P. 7.6.12(b)

- In order to have four subnets, we can have four different combinations of the two extra bits as shown in Table P. 7.6.12(a).

**Table P. 7.6.12(a)**

Combination	Subnet
00	subnet 1
01	subnet 2
10	subnet 3
11	subnet 4

- Let the class C address be 201.70.64.0. Then the addresses of the four subnets are as shown in Table P. 7.6.12(b).

Table P. 7.6.12(b)

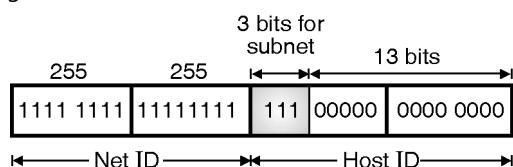
Subnet number	Addresses
1	201.70.64.0 to 201.70.64.63
2	201.70.64.64 to 201.70.64.127
3	201.70.64.128 to 201.70.64.191
4	201.70.64.192 to 201.70.64.255

Ex. 7.6.13 : For a given class B network 144.155.0.0 with default subnet mask, how can you divide it into 8 equal subnets ? How many hosts can be accommodated in each sub-network ?

May 09, 8 Marks, Dec. 11, 10 Marks, May 12, 8 Marks

Soln. :

- Given class B network : 144.155.0.0. The default subnet mask is 255.255.0.0.
- In order to have 8 subnets we need to use 3 extra bits from the host id field as shown in Fig. P. 7.6.13.

**(G-566) Fig. P. 7.6.13**

- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 which can be used for 8 subnets.
- The subnet masks for the 8 possible subnets will have the following subnet masks :

Subnet	Mask
1	255.255.0.0
2	255.255.32.0
3	255.255.64.0
4	255.255.96.0
5	255.255.128.0
6	255.255.160.0
7	255.255.192.0
8	255.255.224.0

Number of hosts in each subnet :

- Due to use of extra 3-bits for subnetting, now we have only 13-bits left in the host id field.
 \therefore No. of hosts in each subnet = $2^{13} = 8192 \text{ ...Ans.}$

Ex. 7.6.14 : Consider any class – C network with default subnet mask. How many actual hosts can be connected in that network ? Divide that network into 4 equal subnets. What is the new subnet mask ? How many hosts can be connected in each subnet ?

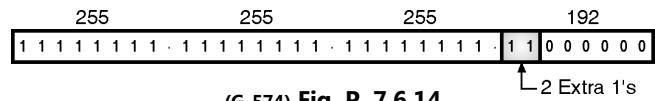
Dec. 09, Dec. 10, 8 Marks

Soln. :

- For a class C network, the default mask is 255.255.255.0
- For a class C network we can connect $2^8 = 256$ total hosts.
- As we need 4 subnets, we need two extra 1s. So the subnet mask is

$$255.255.255.192$$

- In the binary form the subnet mask is as shown in Fig. P. 7.6.14.

**(G-574) Fig. P. 7.6.14**

- In order to have four subnets we can have the 4 combinations of the two extra 1s as shown in Table P. 7.6.14.

Table P. 7.6.14

Combination	Subnet number
0 0	Subnet 1
0 1	Subnet 2



Combination	Subnet number
1 0	Subnet 3
1 1	Subnet 4

- As we have used the 2 MSB bits of host ID field for subnet mask, we have only 6 bits remaining in the host id field.

$$\therefore \text{No. of hosts/subnet} = 2^6 = 64.$$

Ex. 7.6.15 : Consider any class - C network with default subnet mask. Design the subnet in such a way that each has 62 nodes. Write the range of IP addresses for all subnets.

Dec. 12, 10 Marks

Soln. : Refer Ex. 7.6.14.

- But we want only 62 nodes on each subnet. So 2 nodes on each subnet will be inactive.
- Let the class C address be 201.70.64.0. Then the addresses of the four subnets are as shown in Table P. 7.6.15.

Table P. 7.6.15

Subnet number	Addresses
1	201.70.64.0 to 201.70.64.61
2	201.70.64.64 to 201.70.64.125
3	201.70.64.128 to 201.70.64.189
4	201.70.64.192 to 201.70.64.253

Ex. 7.6.16 : For a given C class network 210.50.60.0, how will you divide it into 4 equal subnets ? What will be the new subnet mask ? Give the network and broadcast address of each subnetwork.

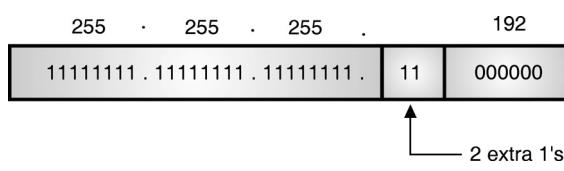
Dec. 13, 8 Marks

Soln. :

Given : IP address : 210.50.60.0 (class C)

Step 1 : Subnet mask :

- This is class C network. So default mask is given by 255.255.255.0



(G-1483) Fig. P. 7.6.16(a) : Subnet mask

- The new subnet mask is 255.255.255.192 ...Ans.

Step 2 : Find network address :

IP address : 210 . 50 . 60 . 0
11010010 · 00110010 · 00111100 · 00000000

Subnet mask : 255 . 255 . 255 . 192
11111111 · 11111111 · 11111111 · 11000000

↓ ANDing

Network address : 210 . 50 . 60 . 0
11010010 · 00110010 · 00111100 · 00000000

(G-1484) Fig. P. 7.6.16(b)

- Network address is 210.50.60.0 ...Ans.

Step 3 : Find broadcast address :

- To find broadcast address, take inverted subnet mask and perform XOR with network address.

Network address : 11010010 · 00110010 · 00111100 · 00000000

Inverted subnet mask : 00000000 · 00000000 · 00000000 · 00111111

↓ XORing

Broadcast address : 11010010 · 00110010 · 00111100 · 00111111

210 . 50 . 60 . 63

(G-1485) Fig P. 7.6.16(c)

- The broadcast address is 210.50.60.63 ...Ans.

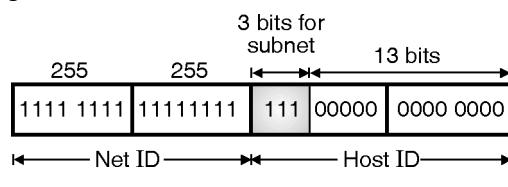
Ex. 7.6.17 : For a given class B network 144.155.0.0 with default subnet mask, how can divide it into 8 subnets ? Write the :

- Range of each subnet.
- Network IP for 7th subnet.
- Broadcast IP for the 7th subnet.
- Subnet mask in subnets.

May 15, 6 Marks

Soln. :

- Given class B network : 144.155.0.0. The default subnet mask is 255.255.0.0. In order to have 8 subnets we need to use 3 extra bits from the host id field as shown in Fig. P. 7.6.17.



(G-566) Fig. P. 7.6.17



- The new subnet mask is 255.255.224.0.
- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 which can be used for 8 subnets.
- The subnet masks for the 8 possible subnets will have the following subnet masks :

Subnet	Mask
1	255.255.0.0
2	255.255.32.0
3	255.255.64.0
4	255.255.96.0
5	255.255.128.0
6	255.255.160.0
7	255.255.192.0
8	255.255.224.0

- The following is the range of subnets :

Subnet	Subnet range
1	144.155.0.0 to 144.155.31.255
2	144.155.32.0 to 144.155.63.255
3	144.155.64.0 to 144.155.95.255
4	144.155.96.0 to 144.155.127.255
5	144.155.128.0 to 144.155.159.255
6	144.155.160.0 to 144.155.191.255
7	144.155.192.0 to 144.155.223.255
8	144.155.224.0 to 144.155.255.255

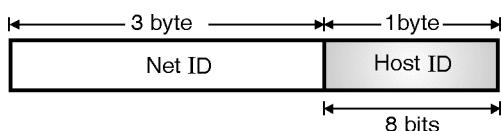
- Network IP for 7th subnet is 144.155.192.0.
- Broadcast IP for 7th subnet is 144.155.223.255.
- Subnet mask is 255.255.224.0.

Ex. 7.6.18 : For a given class C network 195.188.65.0. Design the equal subnets in such a way that each subnet has at least 50 nodes.

May 19, 6 Marks

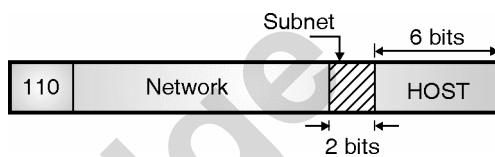
Soln. :

- Fig. 7.6.18(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.



(G-558) Fig. 7.6.18(a)

- We are expected to design equal subnets such that each subnet has atleast 50 nodes (i.e. 50 users).
- In order to identify at least 50 users we need 6-bits in the host ID.
- The remaining 2-bits are assigned for subnetting as shown in Fig. 7.6.18(b).



(G-559) Fig. 7.6.18(b)

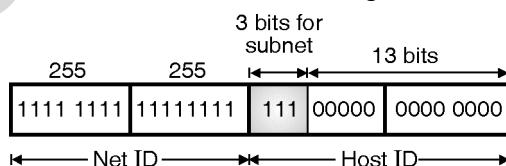
- This shows that there will be four equal subnets each one having at least 50 nodes.

Ex. 7.6.19 : Class B network 150.160.0.0 with default subnet mask, how can you divide it into 8 equal subnets ? How many hosts can be accommodated in each subnetwork ?

Dec. 19, 4 Marks

Soln. :

- Given class B network : 150.160.0.0. The default subnet mask is 255.255.0.0.
- In order to have 8 subnets we need to use 3 extra bits from the host id field as shown in Fig. 7.6.19(a).



(G-566) Fig. 7.6.19(a)

- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 which can be used for 8 subnets.
- The subnet masks for the 8 possible subnets will have the following subnet masks :

Subnet	Mask
1	255.255.0.0
2	255.255.32.0
3	255.255.64.0
4	255.255.96.0
5	255.255.128.0
6	255.255.160.0
7	255.255.192.0
8	255.255.224.0

**Number of hosts in each subnet :**

- Due to use of extra 3-bits for subnetting, now we have only 13-bits left in the host id field.
- No. of hosts in each subnet = $2^{13} = 8192$...Ans.

7.7 Classless Addressing in IPv4 :

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses.
- To overcome these problems, the super netting and subnetting has been tried as discussed earlier.
- But subnetting and supernetting also could not solve the problem of address depletion in IPv4.
- Due to increased number of Internet users, it was evident that a larger address space would be required as a long term solution to this problem.
- For this the length of the IP address should be increased which means the IP packet itself must be changed.
- A long term solution is to switch to IPv6.
- But a short term solution which uses the same address space has been devised for IPv4. It is known as **classless addressing**.
- In the classless addressing, there are no classes but the address generation take place in blocks.
- The classless addressing was announced by the Internet authorities in 1996 in which blocks of variable length which do not belong to any class are used.

7.7.1 Variable Length Blocks :

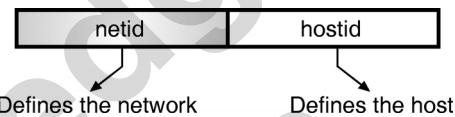
- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.
- Fig. 7.7.1 shows how the address space is divided into non overlapping address blocks.



(G-1804) Fig. 7.7.1 : Variable length blocks in classless addressing

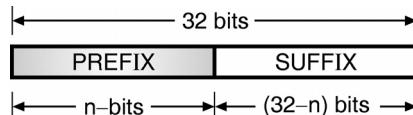
Two level addressing :

- We have discussed the two level addressing for classfull addressing which divided an address into two parts namely : net id and host id.



(G-1805) Fig. 7.7.2 : Two layer addressing in classfull addressing

- The **net id** and **host id** define the network and host respectively.
- It is possible to use the same idea in the classless addressing as well.
- A block of addresses granted to an organization is divided into two parts called as the **prefix** and the **suffix**.
- The role of prefix is same as that of the net id whereas as the role of suffix is same as that of the host id.
- Thus in a block granted to an organization, all the addresses will have the **same prefix** but each address will have a different **suffix**.
- Thus the prefix defines the network (organization to which the address block has been granted) while the suffix defines individual hosts on the network.
- The concept of two level addressing in classless addressing using the prefix and suffix is as shown in Fig. 7.7.1.



(G-1806) Fig. 7.7.3 : Two level addressing using prefix and suffix for classless addressing

- The IPv4 address is 32 bit long out of which the prefix will be of length "n" which can take any value from 0 to 32 and the length of the suffix will be $(32 - n)$ bits.



- Note that the value of "n" i.e. length of the prefix depends on the length of the address block allotted (granted) to an organization.

Ex. 7.7.1 : Find out the values of prefix and suffix lengths in classless addressing if all the available addresses in IPv4 is to be considered as one single block.

Soln. :

- The total addresses in IPv4 is $2^{32} = 4,294,967,296$.
- We have to consider this as one block hence the prefix length $n = 0$. Whereas all the hosts will have their individual addresses. So all the 32 bits will be allotted to the suffix length.

Ex. 7.7.2 : For the same data of the previous example find out the values of prefix and suffix lengths if all the available IPv4 addresses are divided into 4,294,967,296 blocks with each block having only one host.

Soln. :

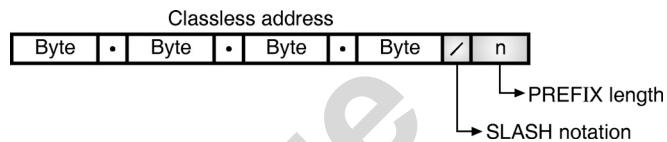
- Here the prefix length for each block is $n = 32$, and the suffix length would be $(32-n) = 0$. The address of the single host in each block will be same as its block address itself.

Note : The two previous examples show that the prefix number n and the number of addresses in a block are inversely proportional to each other. With increase in the value of n, the number of addresses in a block will decrease.

7.7.2 The Slash Notation (CIDR Notation) :

- If an address (classful or classless) is given to us and we want to extract information from it, then the net id in classful addressing or the prefix in classless addressing are extremely important and useful to us.
- However it is not easy to identify the prefix bits in a given classless address.
- It is easy to identify the net id from the given classful address.
- For a given classless address it is not possible to find the prefix length because the given address can belong to a block with any prefix length.
- Therefore, in classless addressing it is essential to include the prefix length to each address if the block of the given address is to be found.

- Hence the prefix length "n" is added to the classless address separated by a **slash** and the notation is known as the **slash notation**.
- Fig. 7.7.4 demonstrates a classless address with slash notation.



(G-1807) Fig. 7.7.4 : Slash notation

- The slash notation is also called as **Classless Interdomain Routing or CIDR notation**.

7.7.3 Network Mask :

- We have discussed the concept of network mask in the classful addressing.
- The same concept is also applicable in the classless addressing as well.
- A **network mask** in classless addressing is a 32 bit number. With its "n" left most bits (corresponding to the prefix) all set to 1s and the remaining $(32-n)$ bits corresponding to the suffix all set to 0s.

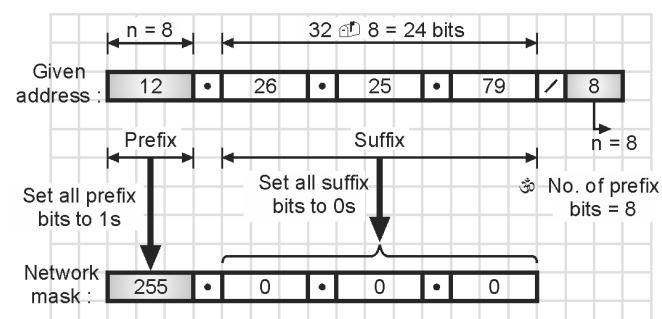
Ex. 7.7.3 : For the following addresses identify the number of prefix bits and write down the network mask :

1. 12.26.25.79 / 8
2. 130.12.230.156 / 16

Soln. :

1. Classless CIDR address : 12.26.25.79 / 8

- As per the slash notation we have $n = 8$ i.e. number of prefix bits is 8.
- Therefore the number of suffix bits $= 32 - 8 = 24$.
- In order to obtain the network mask the prefix bits all set to 1s and the suffix bits all set to zero as shown in Fig. P. 7.7.3(a).



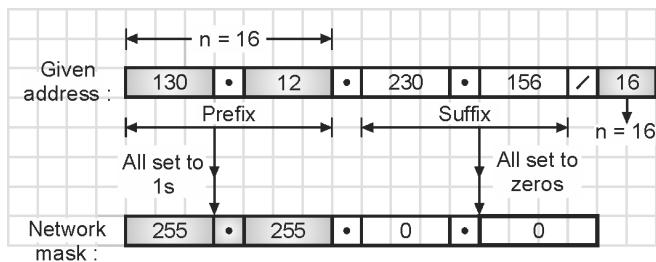
(G-1808) Fig. P. 7.7.3(a)



- Thus the network mask = 255.0.0.0

2. Classless CIDR Address : 130.12.230.156 / 16

- As per the slash notation, n = 16 i.e. number of prefix bits is 16.
- Number of suffix bits = $32 - 16 = 16$
- In order to obtain the network mask, set all the prefix bits to 1s and set all the suffix bits to 0s as shown in Fig. P. 7.7.3(b).



(G-1809) Fig. P. 7.7.3(b)

- Thus the network mask = 255.255.0.0

7.7.4 Extracting the Block Information :

- We can extract all the required information from the given classless address in the CIDR notation. The information that we can obtain is as follows :
 1. The first address (network address)
 2. The number of addresses.
 3. The last address.
- We can obtain the number of addresses in a block as follows :

$$\text{Number of addresses in a block } N = 2^{(32-n)} \quad \dots(7.7.1)$$

Where n = Number of prefix bits.

- The first address or network address in block can be obtained by ANDing the address with the network mask.

$$\text{First address} = (\text{Any address}) \text{ AND } (\text{Network mask}) \quad \dots(7.7.2)$$

- OR what we can do is keep the "n" leftmost bits of any address as it is and set the remaining (32-n) bits to 0s.
- This is equivalent to the ANDing operation mentioned above.
- In order to obtain the last address in the block we have to add the first address with the number of addresses in the block directly.

$$\therefore \text{Last address} = \text{First address} + \text{Number of addresses in the block} \quad \dots(7.7.3)$$

- It is also possible to obtain the last address by ORing the address with complement of the network mask.

$$\therefore \text{Last address} = (\text{Any address}) \text{ OR } [\text{NOT}(\text{Network Mask})] \quad \dots(7.7.4)$$

- One more way of obtaining the last address of the block is to keep all the "n" left most bits (prefix bits) as it is and set all the (32-n) bits (suffix bits) to 1s.

Ex. 7.7.4 : If an address in a block is given in CIDR classless notation as 64.32.16.8 / 27 then find the following :

1. Number of addresses in the block (N)
2. The first address and
3. The last address.

Soln. :

Step 1 : Find n :

$$\text{Given address} = 64.32.16.8 / 27$$

Hence $n = 27$ from the slash notation.

$$\therefore n = 27 \text{ bits.}$$

$$\therefore \text{Prefix bits} = 27, \text{suffix bits} = 32 - 27 = 5$$

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^5 = 32$$

Step 3 : Find the first address :

- Refer Fig. P. 7.7.4(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

$$\text{(G-2708) Network mask} = \begin{array}{|c|c|} \hline n & (32-n) \\ \hline 27 \text{ ones} & 5 \text{ zeros} \\ \hline \end{array}$$

$$\therefore \text{Network mask} = 255.255.255.224$$

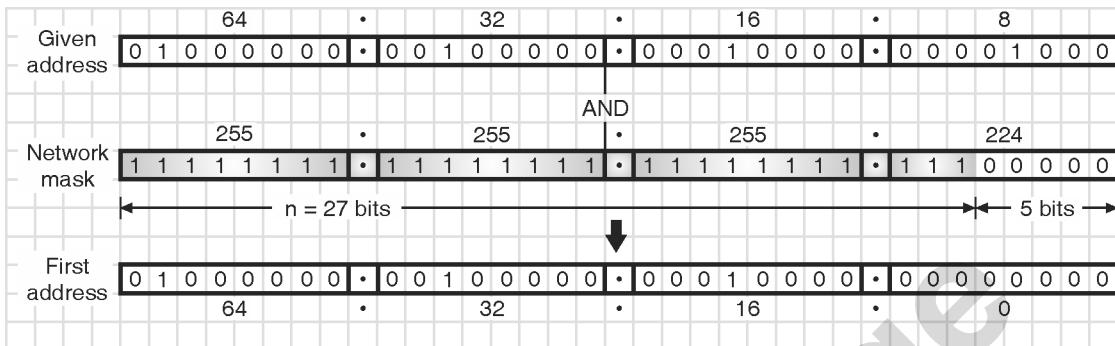
- For ANDing write the given address and network mask in their binary notations as shown in Fig. P. 7.7.4(a).
- \therefore From Fig. P. 7.7.4(a) we get the first address in the block as :

$$\text{(G-2709) First address} = \boxed{64.32.16.0} \quad \dots\text{Ans.}$$

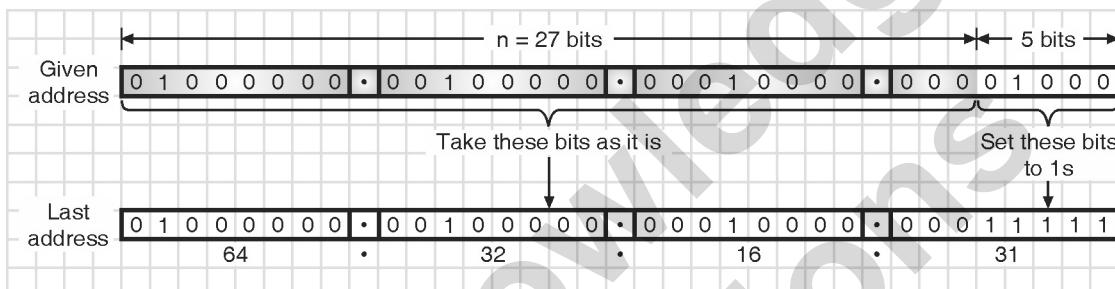
Step 4 : Find the last address :

- To obtain the last address in the block, we have to keep the left most 27 bits in the given address as it is and set the remaining 5 bits to 1s as shown in Fig. P. 7.7.4(b).
- From Fig. P. 7.7.4(b) we get the last address in the block as follows :

$$\text{Last address} = \boxed{64.32.16.31}$$



(G-1810) Fig. P. 7.7.4(a) : First address in the block



(G-1811) Fig. P. 7.7.4(b) : Last address

- Ex. 7.7.5 :** For the classless address 129.65.33.01 / 24 find the following :
- Number of addresses in the block (N)
 - The first address.
 - The last address.

Soln. :

Step 1 : Find n :

- Given address = 129.65.33.01 / 24 hence $n = 24$ from the slash notation.
 $\therefore n = 24$ bits
- \therefore Prefix bits = 24, suffix bits = $32 - 24 = 8$

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^8 = 256 \quad \dots\text{Ans.}$$

Step 3 : Find the first address :

- Refer Fig. P. 7.7.5(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

(G-2710) Network mask = $\begin{matrix} n & (32-n) \\ 24 \text{ ones} & 8 \text{ zeros} \end{matrix}$

$$\therefore \text{Network mask} = 255.255.255.0$$

- For ANDing write the given address and network mask in their dotted decimal notations as shown.

Address :	1 2 9 • 6 5 • 3 3 • 0 1
Network mask :	2 5 5 • 2 5 5 • 2 5 5 • 0
First address (AND) :	1 2 9 • 6 5 • 3 3 • 0

(G-1812) Fig. P. 7.7.5(a) : First address in the block

- From Fig. P. 7.7.5(a) we get the first address in the block as :

(G-2715) First address = 129.65.33.0 ...Ans.

Step 4 : Find the last address :

- To obtain the last address in the block, we have to keep the left most 24 bits in the given address as it is and set the remaining 8 bits to 1s as shown in Fig. P. 7.7.5(b).

Address :	1 2 9 • 6 5 • 3 3 • 0 1
Last address :	1 2 9 • 6 5 • 3 3 • 255

(G-1813) Fig. P. 7.7.5(b) : Last address in the block

- From Fig. P. 7.7.5(b) we get, the last address in the block is as follows :

(G-2711) Last address = 129.65.33.255 ...Ans.

7.7.5 Block Allocation :

- Now let us understand how to allocate the blocks in the classless addressing.



- The global authority for the block allocation is ICANA means Internet Corporation for Assigned Names and Addresses.
- But the individual addresses of the Internet users is not allotted by the ICANA.
- Instead ICANA will assign large blocks of addresses to various ISPs or large organizations.
- These ISPs or organization will assign addresses to the individual Internet users from their allotted blocks.

Restrictions :

Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.

1. The addresses in a block should be continuous, i.e. serial in manner.
2. The total number of addresses in a block has to be equal to some power of 2 i.e. $2^1, 2^2, 2^3 \dots$ etc.
3. The first address should be evenly divisible by the number of addresses.

7.7.6 Relation to Classful Addressing :

- The classful addressing may be imagined as the special case of classless addressing such that the blocks of addresses in class A, B and C type addresses will have the prefix lengths $n_A = 8$, $n_B = 16$ and $n_C = 24$.
- Table 7.7.1 lists the prefix lengths for class A to F classful addresses and using this information we can change a block in classful addressing to a block in classless addressing.

Table 7.7.1 : Prefix lengths for classful addressing

Class	Prefix length	Class	Prefix length
A	/ 8	D	/ 4
B	/ 16	E	/ 4
C	/ 24		

7.7.7 Subnetting :

- The concept of subnetting in classless addressing domain is similar to that discussed for the classful addressing.
- The subnetting is used for creating a three level hierarchy in the classless addressing domain.

- An organization or an ISP have a block of addresses granted to them.
- It can divide these addresses into several subgroups and each subgroup of addresses is assigned to a **subnetwork or subnet**.
- The subnetworks may be subdivided further if the organization want it that way.

7.7.8 Designing Subnets :

Let N = Total number of addresses granted to an organization.

n = Prefix length

N_{sub} = Assigned number of addresses to each subnetwork

N_{sub} = Prefix length for each subnetwork

S = Total number of subnetworks.

- Now follow the steps given below to ensure that the subnetworks operate properly.

Steps to follow :

- The number of addresses in each subnetwork should always be equal to a power of 2. i.e. $2^0, 2^1, 2^2 \dots$ etc.
- We can use the following expression to find the prefix length of each subnetwork.

$$n_{sub} = n + \log_2 \left[\frac{N}{N_{sub}} \right] \quad \dots(7.7.5)$$

- The starting address in each subnet should be divisible by the number of addresses in that subnetwork.
- To achieve this we need to first assign address to larger networks.

Note : These restrictions are similar to those applied when addresses to network were allocated.

7.7.9 Finding Information about Each Network :

- After designing the subnetworks, we can find the information about the subnets such as starting and last addresses, we can use the same procedure that was used to find the information about each network in the Internet.

Ex. 7.7.6 : A block of addresses granted to an ISP is given by $130.34.13.64 / 26$. These addresses are to be divided into four subnetworks with equal number of hosts. Design the subnetworks and obtain all the information about each subnet.



Soln. :

Step 1 : Find total number of addresses (N) :

- From the given address we get $n = 26$ (prefix length).
- Hence the number of addresses in the whole network will be :

$$N = 2^{(32-n)} = 2^{(32-26)} = 2^6 = 64$$

- The first address in this block will be 130.34.13.64 / 26 whereas the last address will be 130.34.13.127 / 26.
- These values have been obtained using the procedure that we have discussed earlier.

Subnet design :

Step 2 : Find number of hosts per subnetwork :

- There are four subnetworks with equal number of guests.
- . Number of hosts per subnetwork is given by,

$$N_1 = N_2 = N_3 = N_4 = \frac{N}{4} = \frac{64}{4} = 16 \quad \dots \text{Ans.}$$

- Note that the first requirement that $64 / 16$ should be a power of 2 has been satisfied here.

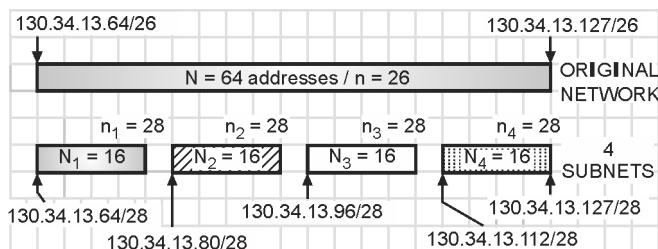
Step 3 : Find the prefix lengths of the subnets :

- The prefix lengths of the four subnets are given by,

$$\begin{aligned} n_1 &= n_2 = n_3 = n_4 = n + \log_2 \left[\frac{N}{N_{\text{sub}}} \right] \\ &= 26 + \log_2 \left[\frac{64}{16} \right] = 26 + \log_2 4 \\ \therefore n_1 &= n_2 = n_3 = n_4 = 28 \quad \dots \text{Ans.} \end{aligned}$$

Step 4 : Starting and ending addresses of all the subnets :

- Refer Fig. P. 7.7.6 which shows all the starting and ending addresses of the 4-subnets.
- It should be noted from Fig. P. 7.7.6 that all the starting addresses should be divisible by the number of addresses in the subnet i.e. by 16.



(G-1814) Fig. P. 7.7.6

7.7.10 Address Aggregation :

- Address aggregation is considered to be one of the advantages of CIDR architecture.
- As we know, ICANN assigns a large block of addresses to an ISP which is divided into smaller subnets and assigned to the customers by the ISPs.
- Thus many blocks of addresses are aggregated in one block and assigned to one ISP.

Ex. 7.7.7 : A router has following CIDR entries in its routing table :

Address/Mask	Next Hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives ?

1. 135.46.63.10
2. 192.53.56.7

MU : Dec. 10, 10 Marks

SPPU : Dec. 11, 8 Marks, May 16, 5 Marks

Soln. :

CIDR – Classless Inter Domain Routing :

- IP is being heavily used for decades. However, due to the exponential growth of internet, IP is running out of addresses.
- This is a potential disaster and the internet community has begun discussion over it. In this section we are going to discuss one of the solutions to this problem.
- One of the solutions is CIDR (Classless Inter Domain Routing). The CIDR is based on the principle of allocating the remaining IP addresses in variable-sized blocks regardless of the class.
- If a site needs say 2000 addresses, then a block of 2048 addresses on the 2048 byte boundary is given to it.
- However the classless routing makes forwarding of packets more complicated.

Forwarding algorithm in the old classful system :

- The steps followed in the old classful system for forwarding packets is as follows :
1. As soon as a packet arrives at a router, a copy of the IP address was shifted right by 28 bits to obtain a 4 bit class number.



2. A 16-way branch then sorts packets into class A, B, C and D (if supported) with eight of the cases for class A, four of the cases for class B, two of the cases for class C and one each for D and E.
3. The code for each class then masked off the 8-, 16-, or 24-bit network number and right aligned it in a 32 bit word.
4. The network number was then searched in the A, B or C table.
5. As soon as the entry was found, the outgoing line was decided and the packet was forwarded upon it.

Forwarding with CIDR :

- The simple forwarding algorithm explain earlier does not work with CIDR.
- Instead now each router table entry is extended by giving if a 32 bit mask.
- So now there is a single routing table for all networks (no different tables for class A, B, C, etc.) which consists of an array of triples. Each triple consists of an **IP address, subnet mask** and **outgoing line**.
- When a packet arrives at the input, the router first extracts its destination IP address.
- Then the routing table is scanned entry by entry to look for a match.
- It is possible that different entries with different subnet mask lengths match.
- In such a case the longest mask is used. For example if there is a match for a/20 mask and a/24 mask then /24 entry is used.

Solution of problem :

- Convert the IP address to bits and then AND it with the subnet mask of the interface whose address is closest to that of the IP addresses.
- The result of the ANDing will give you the network address and the interface to send the packet to.

1. IP = 135.46.63.10 :

- The interface whose address is closest to this IP is interface 1. This interface uses a 22 bit mask. So AND the given IP address with a 22 bit mask as follows :

$$\begin{array}{l} \text{IP} = 135.46.63.10 = 10000111.00101110.00111111.00000101 \\ 22 \text{ bit mask} = 255.255.252.0 = 11111111.11111111.11111100.00000000 \end{array}$$

$$\begin{array}{l} \text{IP AND Mask} = 10000111.00101110.00111100.00000000 \\ \therefore \text{IP AND Mask} = 135.46.60.0 \end{array}$$

(G-1973)

- This result of ANDing matches with the network address of interface 1. Hence the router will forward this packet to interface 1.

2. IP = 192.53.56.7 :

- The interface whose address is closest to this IP is interface 2.
- This interface uses a 23 bit mask. So AND the packet IP address with a 23 bit mask as follows :

$$\begin{array}{l} \text{IP} = 192.53.56.7 = 11000000.00110101.00111000.00000111 \\ 23 \text{ bit mask} = 255.255.254.0 = 11111111.11111111.11111110.00000000 \end{array}$$

$$\begin{array}{l} \text{IP AND Mask} = 11000000.00110101.00111000.00000000 \\ = 192.53.56.0 \end{array}$$

(G-1974)

- This result of ANDing does not match with the network addresses of interface 0 or 1.
- Hence the packet will forwarded to the default i.e. Router 2.

7.8 Special Addresses :

- In the classful addressing, some addresses were reserved for special purpose.
- Similarly in the classless addressing as well some addresses are reserved.

7.8.1 Special Blocks :

- Some address blocks have been reserved for special purpose.

7.8.2 All Zeros Address :

- The block 0.0.0.0 / 32 contains only one address. It is called as the all zero address and has a prefix length of n = 32.
- This address has been reserved for communication when a host has to send an IPv4 packet but it does not know its own address.
- In such situations, the host sends an IPv4 packet to a DHCP server using this all zero address as the source



address and a limited broadcast address (all one address) as the destination address, so as to find its own address.

7.8.3 All one Address-Limited Broadcast Address :

- The block 255.255.255.255 / 32 contains only one address. It is called as an all one address and has a prefix length of n = 32.
- This all one address has been reserved for limited broadcast address i.e. if a host wants to send message to all the hosts simultaneously then the sending host can use all one address as a destination address inside the IPv4 packet.
- Such a broadcasting is confined to the network only because routers do not allow the all one packet to pass through them.
- The datagram sent with the all zero address as destination will be received and processed by all the hosts on the network.

7.8.4 Loopback Address :

- A loopback address is the address which is used to test the software on a machine.
- The block 127.0.0.0 / 8 with a prefix length of 8 is used for the loopback address.
- On using this address, a packet does not leave the machine at all but it returns to the protocol software.
- It can be used for testing the IPv4 software.

7.8.5 Private Addresses :

- The address blocks that are not recognized globally still assigned for private use are known as private addresses.
- These addresses are neither connected to nor isolated from the Network Address Translation (NAT) techniques.
- Table 7.8.1 depict such address blocks.

Table 7.8.1 : Private addresses

Block	Number of addresses	Block	Number of addresses
10.0.0.0 / 8	16,777,216	192.168.0.0 / 16	65,536
172.16.0.0 / 12	1,047,584	169.254.0.0 / 16	65,536

7.8.6 Multicast Addresses :

- The block 224.0.0.0 / 4 with a prefix length of n = 4 has been reserved for the multicast IP communication.

7.8.7 Special Addresses in Each Block :

- The usage of some address in each block for special addresses has been recommended.
- But it has not been made mandatory. These addresses are not assigned to any host.
- One important point to be remembered is that a very small block of addresses should not be used as special addresses.

7.8.8 Network Address :

- The network address is defined as the first address (with the suffix set all to 0s) in a block.
- It is used for defining the network itself. It does not define any host in the network.
- With the same principle, the first address in a subnetwork is called as the subnetwork address.

7.8.9 Direct Broadcast Address :

- We can use the last address in a block or subblock (with the suffix part set to all 1s), as a **direct broadcast address** for that block or subblock.
- A router generally uses this address for sending a packet to all the hosts connected to a specific network.
- This address is used as the destination address in the IPv4 packet and all the hosts will accept and process the datagram which has this destination address.

7.9 NAT – Network Address Translation :

SPPU : Dec. 09, May 11, May 12, May 18, Dec. 19

University Questions

Q. 1 What is NAT ? Explain the operation of NAT with suitable example.

(Dec. 09, 6 Marks, May 12, 8 Marks)

Q. 2 Write short notes on : NAT. **(May 11, 8 Marks)**

Q. 3 Explain the operation of NAT with suitable example. **(May 18, Dec. 19, 4 Marks)**

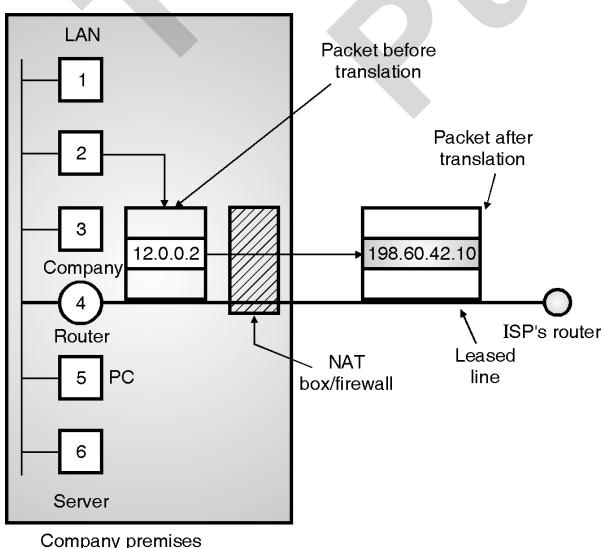
- The problem that existing number of IP addresses is less than the actually required ones is practically important.



- A long term solution to this problem is that the whole Internet should be migrated from IPv4 to IPv6.
- This has begun, but will take year to get complete. (That means all the computers should have IPv6 addresses instead of IPv4 addresses).
- A quick solution to this problem is NAT i.e. Network Address Translation. It is described in RFC 3022.
- The basic idea in NAT is that each company is assigned a single IP address or at the most a small number of IP addresses so as to access the Internet.
- Within the company, every computer gets a unique IP address which is used for routing the internal traffic of the office.
- But when a packet goes out of the company, and goes to ISP, the translation of IP address takes place there.
- In order to make this scheme work, three ranges of IP addresses have been declared as private.
- Companies can use these addresses internally as per their requirement. However no packet containing these addresses is allowed to appear on the Internet. The three reserved ranges are as follows :

Range 1	10.0.0.0 to 10.255.255.255/8	16777216 Hosts
Range 2	172.16.0.0 to 173.31.255.255/12	1048 576 Hosts
Range 3	192.168.0.0 to 192.168.255.255/16	65 536 Hosts

- Generally most companies choose the addresses from the first range.
- Refer Fig. 7.9.1 which explains the operation of NAT.



(G-551) Fig. 7.9.1 : NAT

- It shows that within the company premises, every machine has a unique address of the form 12.a.b.c.
- But when a packet leaves the company premises, it passes through the NAT box.
- This box converts the internal IP address 12.0.0.2 in Fig. 7.9.1 to the company's true IP address 198.60.42.10.
- The NAT box is generally combined with a firewall. It is also possible to integrate the NAT box into company's router.

7.10 Delivery and Forwarding of IP Packets :

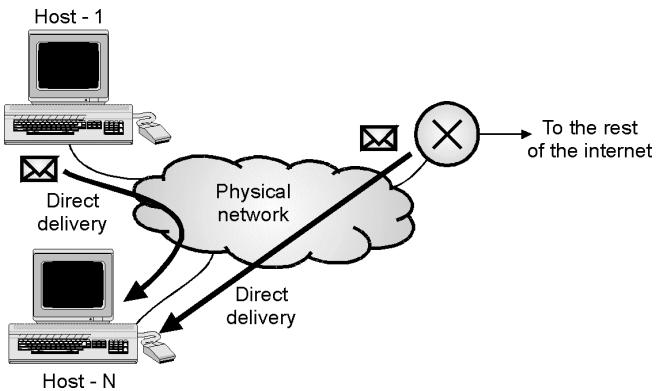
- In this section and some of the following sections we are going to discuss the delivery and forwarding of IP packets.
- **Delivery** of IP packets can be defined as the way in which a packet is handled by the underlying networks under the supervision and control by the network layer.
- Delivery of IP packets is of two types :
 1. Direct delivery.
 2. Indirect delivery.
- **Forwarding** is defined as the manner in which an IP packet is delivered to the next station.
- Two important forwarding techniques are : first is forwarding based on the destination address of the packet and the second one is on the basis of the label attached to the packet.

7.10.1 Delivery :

- The network layer supervises how the packets are being handled by the underlying physical networks.
- This handling is known as the delivery of packets.
- The two different methods of delivery are :
 1. Direct delivery
 2. Indirect delivery.

1. Direct delivery :

- In the direct delivery the destination host and the one who delivers the packet are in the same physical network as shown in Fig. 7.10.1(a).

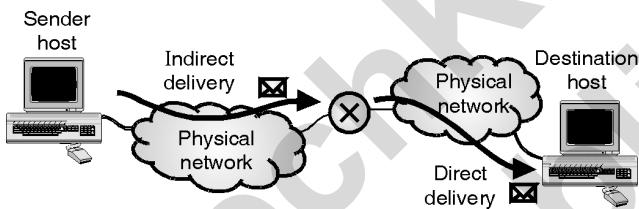


(G-440) Fig. 7.10.1(a) : Direct delivery

- The sender can extract the network address of the destination using the mask.
- It then compares this address with the addresses of the networks to which it is connected.
- If these two addresses are identical then the delivery is direct.

2. Indirect delivery :

- In the indirect delivery of packets, the sender host and the destination host are not the part of the same physical network as shown in Fig. 7.10.1(b).



(G-441) Fig. 7.10.1(b) : Indirect delivery

- In such a situation, the packets travel from one router to the other and are finally delivered to the destination host.
- The indirect delivery involves one direct and zero or more indirect deliveries. The last delivery is always a direct one.

7.10.2 Forwarding :

- Forwarding is defined as the process of placing the packet in its route towards its destination.
- Forwarding is possible only if the host or a router have a routing table of their own.
- A sender host or a router will refer to this routing table when it receives a packet and from the table they will find the root to the final destination.

– But this simple solution has practically become impossible today in the internetwork environment due to a large number of entries required to be made in a routing table.

1. Forwarding techniques :

- Many techniques have been invented and tested in order to make the size of the routing tables manageable. Some of them are as follows :

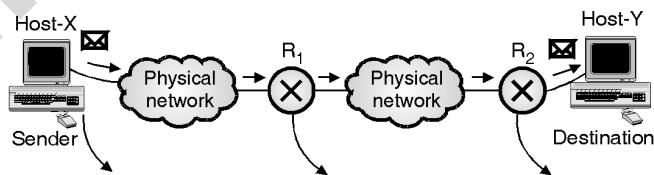
1. Next hop method versus Route method.

2. Network specific method versus Host specific method.

3. Default method.

2. Next hop method versus route method :

- The Route method is the most basic method in which the information about the complete route is stored in the routing tables of hosts and routers as shown in Fig. 7.10.2(a).
- This makes the routing tables extremely large and difficult to manage.
- In order to reduce the size of routing tables, the next hop method is used in which the routing table contains only the address of the next hop (upto the next router) instead of information about the complete route. This is as shown in Fig. 7.10.2(a).



Based on route		Based on next hop		Based on route	
Destination	Route	Destination	Route	Destination	Route
Host Y	R ₁ , R ₂ Host Y	Host Y	R ₂ , Host Y	Host Y	Host Y
Based on next hop		Based on next hop		Based on next hop	
Destination	Next hop	Destination	Next hop	Destination	Route
Host Y	R ₁	Host Y	R ₂	Host Y	-

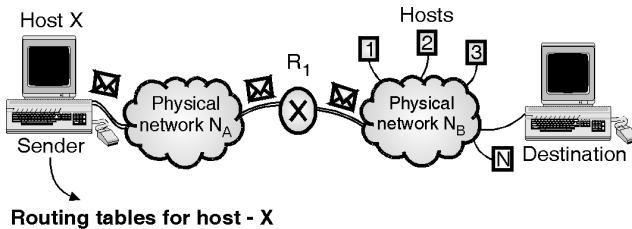
(G-442) Fig. 7.10.2(a) : Route method versus Next Hop method

3. Network specific method versus host specific method :

- In the host specific method, the routing table of a host or router will specify each destination host connected to the same physical network.



- This increases the number of entries in a routing table and makes it large.
- But in the network specific method, we have only one entry corresponding to the destination network N_B only as shown in Fig. 7.10.2(b).



Host specific method

Destination	Next hop
Host - 1	R ₁
Host - 2	R ₂
⋮	⋮
Host - N	R ₁

Network specific method

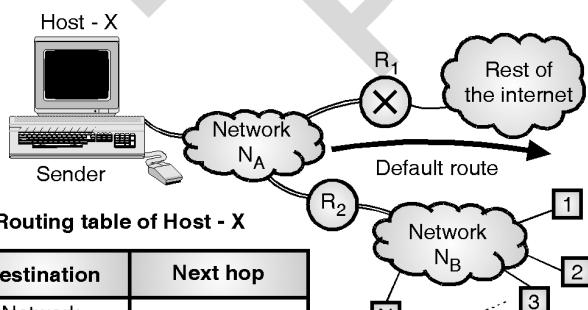
Destination	Next hop
Network N_B	R ₁

(G-443) Fig. 7.10.2(b) : Host specific method versus network specific method

- That means we consider all hosts connected to the same network N_B as one single entry.
- This will reduce the routing table and simplify the searching process considerably.

4. Default method :

- This is one more method of simplifying the routing tables.
- Refer Fig. 7.10.2(c) in which the sending host X is connected to a network with two routers R_1 and R_2 .



Destination	Next hop
Network N_B	R ₂
Any other network	R ₁

(G-444) Fig. 7.10.2(c) : Default method

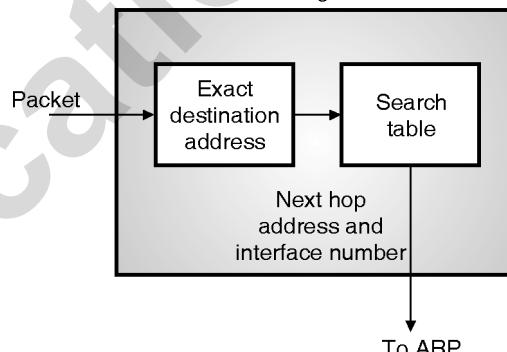
- Router R_2 routes the packets to the hosts connected to network N_B .

- However router R_1 is used for the rest of the Internet.
- Hence in the routing table instead of listing all networks in the entire Internet, host X will have only one entry called as the default entry (normally defined as network address 0.0.0.0).

5. Forwarding process :

- In order to explain the forwarding process let us assume that hosts as well as routers use classless addressing.
- For classless addressing, in the routing table we should have one row of information for each block.
- This table should be searched on the basis of the network address (first address in the block).
- But the problem here is that the destination address does not tell anything about the network address.
- Therefore we have to include the mask (/n) in the table. Therefore we need to have an extra column to include the mask for the corresponding block.

Forwarding module



To ARP

Mask	Network address	Next hop address	Interface
.....
.....
.....

(G-445) Fig. 7.10.3 : Forwarding module in classless address

- The forwarding module for the classless addressing is as shown in Fig. 7.10.3.

6. Forwarding based on label :

- In 1980s people started making efforts to somehow change IP to behave like a connection oriented protocol, in which the routing would be replaced by switching.



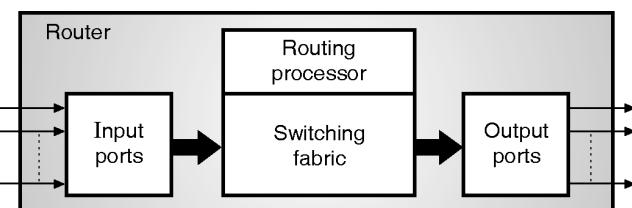
- As discussed earlier, the difference between connectionless network and a connection oriented network is as follows :
- In the connectionless networks, the datagram approach is followed in which a packet is forwarded by the routers on the basis of destination address in the header of the packet.
- However in the connection oriented networks the virtual circuit approach is followed in which a switch forwards a packet on the basis of the **label** attached to the packet.
- The other difference between the two types of networks is that routing involves **searching** of the routing table whereas switching involves **accessing** of the table.

7.11 Structure of a Router :

- We know that the principle of operation of a router is as follows :
- A router receives a packet at one of its input ports (also called as an interface), then takes help of the routing table to decide upon the output port from which the packet is to be forwarded and finally sends the packet from the appropriate output port.
- In this section, we are going to discuss about what is inside the router.

7.11.1 Components of a Router :

- Fig. 7.11.1 shows the internal block diagram of a router which shows that a router contains four components as follows :
 1. Input ports.
 2. Output ports.
 3. The routing processor.
 4. The switching fabric.



(G-2078) Fig. 7.11.1 : Router components

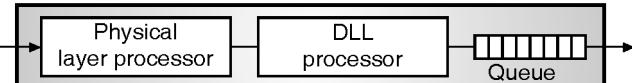
- Let us discuss about these components now.

7.11.2 Input Ports :

- The schematic diagram of an input port is as shown in Fig. 7.11.2.

- The functions of the router related to the physical and datalink layer are performed by its input port.

Input port



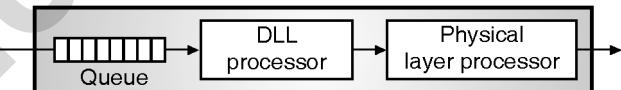
(G-2079) Fig. 7.11.2 : Schematic diagram of an input port

- The functions performed by the input port are as follows :
 1. It constructs bits from the received signal.
 2. It decapsulates packet from the frame.
 3. It detects and corrects the errors.
 4. The packet is ready to be forwarded.
 5. The buffers will hold the ready to forward packets before directing them to switching fabric.

7.11.3 Output Ports :

- The functions performed by the output port are same as those performed by the input port but in the reverse order.
- The schematic diagram of an output port has been shown in Fig. 7.11.3.

Output port



(G-2080) Fig. 7.11.3 : Schematic diagram of output port

- The functions of the output port are as follows :
 1. The outgoing packets are buffered or queued.
 2. The packets are encapsulated to create the frames.
 3. The physical layer functions are applied to the frame. This will create signals that can be sent on the line.

7.11.4 Routing Processor :

- The routing processor in a router performs the functions of the network layer.
- This processor makes use of the destination address to find the following two simultaneously :
 1. Output port number from where the packet is to be sent out.
 2. The address of the next hop.



- The routing processor carries out the above mentioned activities by accessing the routing table.
- Due to this reason, the activity of the routing processor is called as **table lookup**.
- In the modern day routers, the function of the routing processor is assigned to the input port.

7.11.5 Switching Fabric :

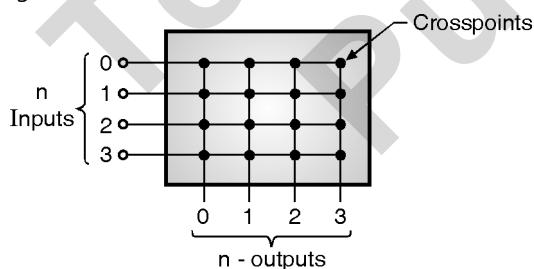
- Moving a packet from the input queue to the output queue is the most difficult task in a router.
- The size of the input / output queue and the overall delay in delivering a packet are dependent on the speed at which a packet is moved from the input queue to the output queue.
- The modern day routers use different types of switching fabrics. We will discuss some of them in brief.

7.11.6 Types of Switching Fabrics :

- Some of switching fabric types used by the routers are as follows :
 - Crossbar switch.
 - Banyan switch.
 - A batcher-banyan switch.

7.11.7 Crossbar Switch :

- The simplest type of switching fabric is the cross bar switch, the construction of which is as shown in Fig. 7.11.4.



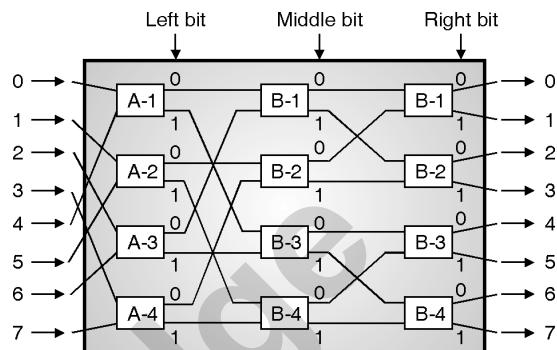
(G-2081) Fig. 7.11.4 : A crossbar switch

- The crossbar switch uses electronic microswitches at each crosspoint and connects n inputs to n outputs in a grid, using the switches.

7.11.8 Banyan Switch :

- This switch is named after the banyan tree. It is a multistage switch with microswitches used at every stage as shown in Fig. 7.11.5.

- If there are m inputs and m outputs, then there will be $\log_2 m$ stages and $m/2$ microswitches in every stage.

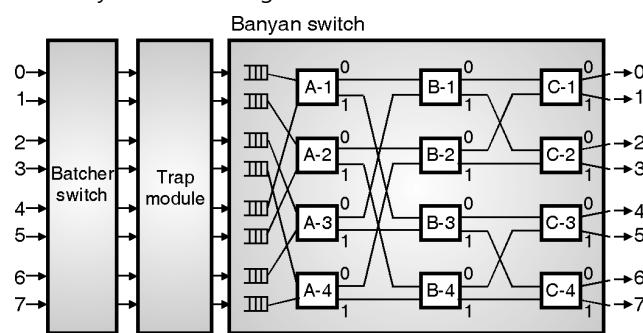


(G-145) Fig. 7.11.5 : A three layer switch

- A three layer banyan switch is used at the network layer and it is a kind of router.
- A three layer banyan switch is shown in Fig. 7.11.5.
- It has $n = 8$ inputs and same number of outputs. A three bit number is used to decide the internal path over which the input is passed to output.
- The number of microswitches at each stage is $n/2$ i.e. 4 switches.
- The first stage routes the cell based on the high order bit in the binary bit string.
- The second stage routes the cell based on the middle bit and last stage routes it based on the low order bit.
- Note that number of stages = $\log_2 (n) = \log_2 8 = 3$.

7.11.9 Batcher Banyan Switch :

- The banyan switches have a problem that there is a possibility of collision even when two packets are not headed for the same output port.
- This problem can be overcome by using the batcher banyan switch of Fig. 7.11.6.



(G-146) Fig. 7.11.6 : Batcher banyan switch



- This switch sorts the incoming packets according to their final destination.

7.12 Internet Protocol Version 4 (IPv4) :

- We have already discussed the addressing mechanism, delivery and forwarding for the IP packets.
- Now we will discuss the format of IP packet in the next few sections.
- In the discussion we will see that an IP packet consists of a base header and options which are sometimes useful in controlling the packet delivery.

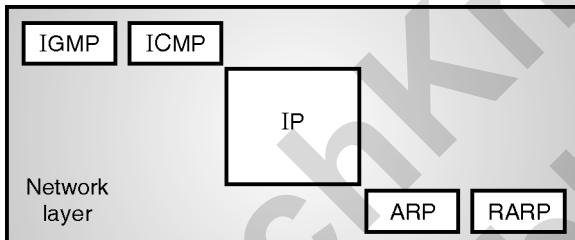
7.12.1 Position of IP :

SPPU : Dec. 02

University Questions

**Q. 1 Explain Internal Organization of the Network Layer.
(Dec. 02, 8 Marks)**

- The main protocols corresponding to the network layer in the TCP/IP suite as well as Internet layer are : ARP, RARP, IP, ICMP and IGMP. This is as shown in Fig. 7.12.1.



(G-524)Fig. 7.12.1 : Protocols at network layer

- Out of these protocols IP is the most important protocol.
- It is responsible for host to host delivery of datagrams from a source to destination.
- But IP needs to take services of other protocols.
- IP takes help from ARP in order to find the MAC (physical) address of the next hop.
- IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error.
- IP is basically designed for unicast delivery.
- But some new Internet applications as well as multimedia need multicast delivery.
- So for multicasting, IP has to use the services of another protocol called IGMP.

- IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

7.12.2 Internet Protocol (IP) :

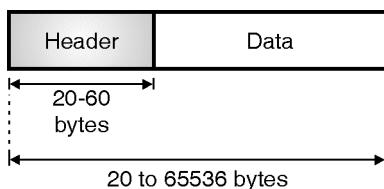
- The Internet Protocol is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.
- IP is used as the transmission mechanism by the TCP / IP protocols. That means the TCP or UDP packets are encapsulated in the IP packet and the IP carries it from source to destination.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is an unreliable protocol because it does not provide any error control or flow control.
- IP can only detect the error and discards the packet if it is corrupted.
- If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.
- The version of IP that we are going to discuss is called as IPv4 i.e. IP version 4.
- IP is also called as a **best effort delivery protocol**.
- The meaning of the term best effort delivery is that the IP packet can get lost or corrupted or delayed.
- They may arrive out of order at the destination or may create congestion in the network.

7.12.3 Datagrams :

- Packets in IP layer are called datagrams. Fig. 7.12.2 shows the typical format of an IP packet.
- A datagram has two parts namely the header and data as shown.
- The length of datagram is not fixed. It varies from 20 bytes to 65536 bytes.



- The length of the header is 20 to 60 bytes. The information necessary for the routing and delivery of the datagram has been stored in the header.
- The other part of the datagram is the data field which is of variable length.



(G-525) Fig. 7.12.2 : IPv4 datagram format

- It is a custom in TCP/IP to show the header in 4-byte (32 bit) sections.

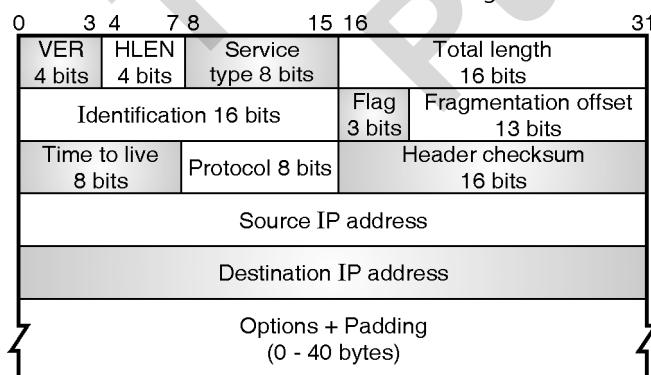
7.12.4 IPv4 Header Format :

SPPU : Dec. 09, Dec. 11, Dec. 12, May 16

University Questions

- Q. 1** What is fragmentation ? Explain how it is supported in IPv4 and IPv6. **(Dec. 09, 8 Marks)**
- Q. 2** Compare between IPv4 and IPv6. Draw header diagram. **(Dec. 11, 8 Marks)**
- Q. 3** Is fragmentation supported by IPv4 and IPv6 ? Explain. **(Dec. 12, 6 Marks)**
- Q. 4** Draw and explain IPv4 header format. **(May 16, 6 Marks)**

- The IP frame header contains routing information and control information associated with datagram delivery.
- The IP header structure is as shown in Fig. 7.12.3.



(G-2082) Fig. 7.12.3 : IPv4 header format

- Various fields in the header format are as follows :

1. VER (Version) :

- This is a 4 bit field which is used to define the version of IP protocol.

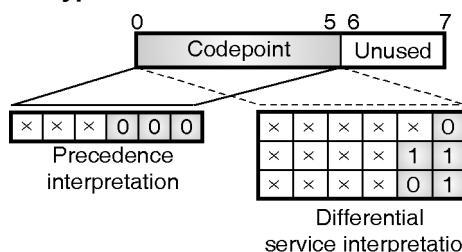
- The current version of IP is 4 i.e. IPv4 but in future it may be completely replaced by the latest version of IP i.e. IPv6.
- This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version.
- If the processing machine is using some other version of IP, then the datagram will be discarded.

2. HLEN (Header length) :

- This 4-bit long field is used for defining the length of the datagram header in 4-byte words.
- The value of this field is multiplied by 4 to get the length of the IPv4 header which varies between 20 and 60 bytes.
- When there are no options, the value of this field is 5 and the **header length** is $5 \times 4 = 20$ bytes.
- When the value of option field is maximum the value of HLEN field is 15 and the corresponding header length is maximum i.e. $15 \times 4 = 60$ bytes.

3. Service type :

- In the earlier designs of IP header, this field was called as **Type of Service (TOS)** field and its job was to define how the datagram should be handled.
- At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc.
- But now the interpretation of this field has been changed by IETF.
- This field is now supposed to define a set of **differential services**.
- Fig. 7.12.4 illustrates the new interpretation of the **service type** field.



(G-2083) Fig. 7.12.4 : New interpretation of service type field

- As seen in Fig. 7.12.4, in the new interpretation, the service type field is divided into two subfields namely,



- the 6 bit **codepoint** subfield and a 2 bit **unused** subfield.
- We can use the 6-bit **codepoint** subfield in two different ways, as follows :
 1. For the purpose of precedence interpretation.
 2. For the differential service interpretation.

Precedence interpretation :

- If the three right most bits are zeros, then the three leftmost bits are interpreted the same as the precedence bits in the service field (old interpretation).
- That means it is compatible with the old interpretation of this field.
- The precedence interpretation is used for defining the priority level of this datagram (from 0 to 7) in the situations like congestion.
- In the event of congestion, the datagrams with lowest precedence (0) will be discarded first.

Differential service interpretation :

- When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation.
- In that case these 6 bits can be used for defining a total of 56 ($64 - 8$) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 7.12.1.

Table 7.12.1 : Values of codepoints

Category	Codepoint	Assigning authority
1.	$\times \times \times \times 0$	Internet
2.	$\times \times \times \times 1 1$	Local
3.	$\times \times \times \times 0 1$	Temporary or Experimental

- The first, second and third categories contain 24, 16 and 16 service types respectively.
- The Internet authorities assign the first category.
- The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

- This 16 bit field is used to define the total length of the IP datagram.

- The total length includes the length of header as well as the data field.
- The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1) = 65535$ bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers.
- This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.
- All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments.
- The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram.
- We can find the length of data by subtracting the header length from the total length.
- As stated earlier the header length can be obtained by multiplying the contents of HLEN field by four.

$$\therefore \text{Length of data} = \text{Total length} - \text{header length}$$
- The total length (maximum value) of 65,535 bytes might seem to be large but in future the size of IP datagram is likely to increase further because the improvement in technology will allow more bandwidth.

Why do we need the total length field ?

- We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame. Then why to include this field ?
- The answer to this question is that in many situations we do not need this field at all.
- But in some special situations, only the datagram is not encapsulated in the frame but there are some padding bits as well that are included.
- In such situations, the machine (host or router) that decapsulates the datagram, needs to check the **total length** field so as to understand how much is the data and how much is the padding ?

5. Identification :

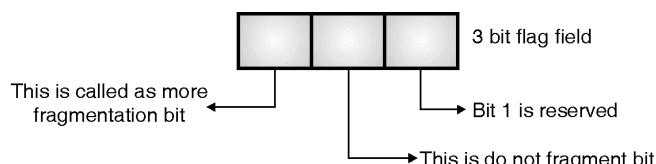
- This field is used to identify the datagram originating from the source host.



- When a datagram is fragmented, the contents of the identification field get copied into all fragments.
- This identification number is used by the destination to reassemble the fragments of the datagram.

6. Flags :

- **Flags :** This is a three bit field. The 3 bits are as shown in Fig. 7.12.5.



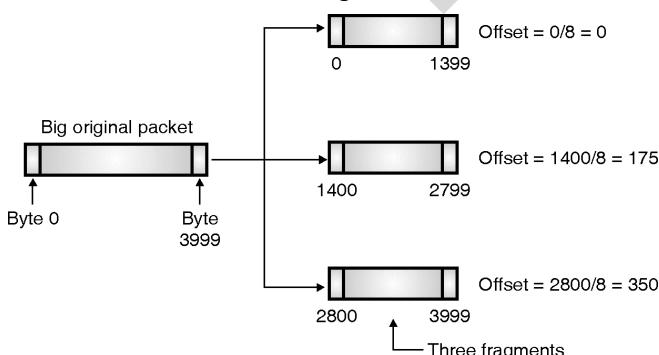
(G-527)Fig. 7.12.5 : Flag bits

First bit is reserved, and it should be 0.

- The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented.
- But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.
- The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. Fragmentation offset :

- This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- To understand this refer Fig. 7.12.6.



(G-528)Fig. 7.12.6 : Example of fragmentation

- The original IP packet (datagram) contains 4000 bytes numbered from 0 to 3999.

- It is fragmented into three fragments.
- The first fragment contains 1400 bytes numbered from 0 to 1399. The offset for this fragment is $0/8 = 0$. Similarly the offsets for the other two fragments are $1400/8 = 175$ and $2800/8 = 350$ respectively as shown in Fig. 7.12.6.
- The offset is measured in units of 8 bytes. Because the length of the offset field is 13 bits, so the fragments should be of size such that first byte number is divisible by 8.

8. Time to Live (TTL) :

- This is an 8-bit field which controls the maximum number of routers visited by the datagram during its lifetime.
- A datagram has a limited lifetime for travelling through an Internet.
- Originally the TTL field was designed to hold the **timestamp**.
- This timestamp value was decremented by one, everytime the datagram visits a router.
- As soon as the timestamp value reduces to zero the datagram is discarded.
- But for this scheme to become successful, all the machines must have synchronized clocks and they must know the time taken by a datagram to travel from one router to the other.
- Today the TTL field is used to **control** the maximum number of hops i.e. router by a datagram.
- At the time of sending a datagram, the source host will store a number in the TTL field.
- This number is approximately twice the maximum number of routers present between any two hosts.
- Everytime this datagram visits a router, this value is decremented by one.
- If after decrementing, the value of TTL field reduces to zero then that router discards the datagram.

Need of TTL field :

- Sometimes the routing tables in the Internet get corrupted, due to which a datagram may travel between two or more routers for a very long time but never ever gets delivered to the destination host.



- The TTL field is needed in such situations for **limiting the lifetime of a datagram**.
- The TTL field is also used to **limit the journey of a packet intentionally**.
- For example if a packet is to be confined to a local network only then a 1 is stored in the TTL field of this packet.
- As soon as it reaches the first router, then TTL field value is decremented from 1 to 0 and the packet will be discarded.

9. Protocol :

- This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer.
- The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.
- The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered.
- At the destination, the value of this field helps in the process of demultiplexing.
- Table 7.12.2 shows some of the values of this field corresponding to different high level protocols.

Table 7.12.2

Value	Protocol	Value	Protocol
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

10. Header checksum :

- A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

11. Source address :

- This field is used for defining the IP address of the source. It is a 32 bit field.

12. Destination address :

- This field is used for defining the IP address of the destination. It is also a 32 bit field.

13. Options :

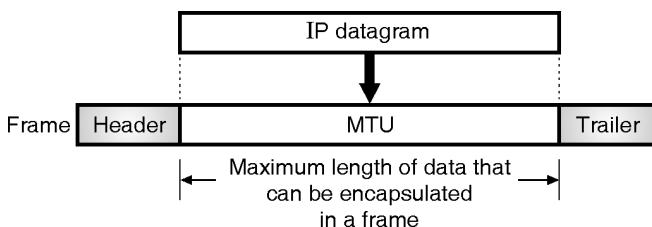
- Options are not required for every datagram.
- They are used for network testing and debugging. We have discussed all the options in detail, later in this chapter.

7.13 Fragmentation :

- In the Internet, a datagram sent by a host has to travel through different networks before it is delivered to the destination host.
- At every router, the received frame is decapsulated, the IP datagram is extracted and processed and encapsulated in another frame.
- The size and format of the frame received by a router depends on the protocol used by the previous physical network to the router.
- As an example, imagine that a router connects a LAN to a WAN. Then the frame received by the router is in the LAN format and the one forwarded by it is in the WAN format.

7.13.1 Maximum Transfer Unit (MTU) :

- The frame format of each data link layer protocol is different in its own way.
- One of the important field in the frame format is the **maximum size of data field**.
- Therefore when we encapsulate an IP datagram in a frame, the datagram size should be less than the maximum data size specified by the maximum size field.
- The concept of MTU has been illustrated in Fig. 7.13.1.



(G-2084) Fig. 7.13.1 : Concept of MTU

- Now the problem is that the value of MTU changes from one protocol to the other used for the physical network.
- We have to make the IP protocol independent of the physical network. In order to do so the maximum length of IP datagram was decided to be equal to 65,535 bytes.



- If we use a physical network protocol which has MTU = 65,535 bytes, then the transmission will become more efficient.
- For the other protocols having MTU smaller than 65,535 bytes, the IP datagram is divided into small parts called **fragments** so that they can pass through the physical networks successfully.
- This process of dividing the IP datagram in smaller parts is called as **fragmentation**.
- The fragmentation generally does not take place at the source because the transport layer there will adjust the segment size in such a way that they will fit in the IP datagrams and data link layer frames.
- After **fragmentation**, each fragment will have its own header. Most of the fields of the original header are copied into the fragment header but some fields are changed.
- Such a fragmented datagram can be fragmented further if it comes across a network with even smaller MTU.
- The fragmentation of a datagram can be carried by the source host or any router on the route of the datagram.
- But the process of reassembly of all the fragments will be carried out only by the **destination host**.
- All the fragments of a datagram are free to take any route and we do not have any control over them.
- In short each fragment acts as an independent datagram.
- The reassembly of fragments is not done during the transmission because of the loss of efficiency associated with it.
- At the time of fragmentation, all the required parts of the header are copied into the fragments.
- But the **options** field may or may not be copied as discussed later on.
- The following three fields are altered when the host or router fragments a datagram :
 1. Flags.
 2. Fragmentation offset.
 3. Total length.
- The remaining fields in the IP header are copied as it is.

- The value of checksum should be calculated again regardless of fragmentation.
- And the final point about fragmentation is that only data in a datagram is fragmented.

7.13.2 Fields Related to Fragmentation :

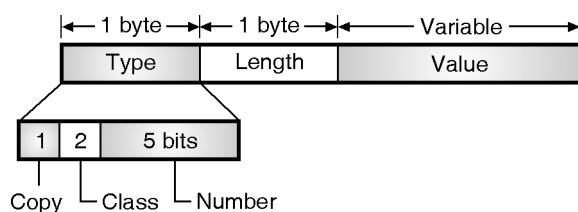
- The following three fields in an IP datagram header are related to the fragmentation and reassembly of an IP datagram :
 1. Identification.
 2. Flags and
 3. Fragmentation offset field.

7.14 Options :

- In the IP header there are two parts : A fixed part and a variable part. We have already discussed the fixed part of 20 byte length.
- At the most 40 byte long variable part consists of options which we are going to discuss in this section.
- Options as the name suggests are not required for a datagram.
- Their main application is for network testing and debugging.
- Options are not a required part of a datagram but **option processing** is very much a required part of the IP software.
- This implies that if the options are present in the header, then all the implementations should be able to handle them.

7.14.1 Format :

- The format of an option has been shown in Fig. 7.14.1.



(G-2085) Fig. 7.14.1 : Option format

- As shown, it consists of three fields namely, a type field (1-byte), length field (1-byte) and a variable length value field.



- Let us discuss these fields one by one.

1. Type :

- As shown in Fig. 7.14.1, the type field is an 8-bit field and it contains three subfields as follows :
 - Copy (1 bit).
 - Class (2 bits).
 - Number (5 bits).

(a) Copy :

- This is a 1 bit subfield. So it can have only two possible values, 0 or 1. If copy = 0, then the option must be copied only into the first fragment.
- Whereas if copy = 1, then the option field must be copied into all the fragments.

Copy	Meaning
0	Copy option field only in first fragment.
1	Copy option field in all fragments.

(b) Class :

- This 2-bit subfield is used to define the purpose of option.
- It has four possible values, out of which only two (00 and 10) are defined right now.
- The other two possible values (01 and 11) are not yet defined.
- If class = 00, it indicates that the option is being used for datagram control.
- Whereas if copy = 10 then the option is used for debugging and management.

Copy	Meaning
00	Datagram control.
01	Not defined or reserved.
10	Debugging and management.
11	Not defined or reserved.

(c) Number :

- This 5-bit subfield is used for defining the type of option.
- This subfield has 32-possible values (types), but currently only 6-types are defined as shown in Table 7.14.1.

Table 7.14.1

Number	Type of option
00000	End of option.
00001	No option.
00011	Loose source route
00100	Timestamp
00111	Record root
01001	Strict source route

- We will discuss these later in this chapter.

2. Length :

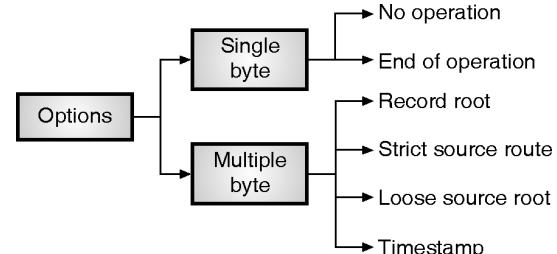
- This 8-bit field is used for defining the total length of the option with the type field and the length field included.
- The length field will not be present in all the option types.

3. Value :

- This is variable length field which contains the specific data which is required by that option.
- Similar to the length field, the value field also will not be present in all the option types.

7.15 Option Types :

- As we started earlier, only six options are being used currently.
- Fig. 7.15.1 shows the classification of these options.



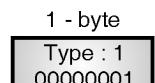
(G-2086) Fig. 7.15.1 : Categories of options

- Options are classified into two option types i.e. single byte options and multiple byte options.
- There are two single byte options, which do not require the data or length fields.
- The remaining four options are multibyte options which require the data and length fields.
- Let us now discuss these options one by one.

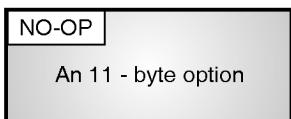


7.15.1 No Operation Option :

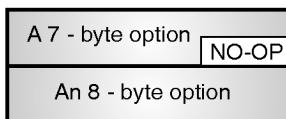
- This is a **single byte** option which is being used as a **filler** between options.
- As shown in Fig. 7.15.2, we can use the no operation option to align the next option on a 16 bit or 32 bit boundary.



(a) No operation option



(b) NO-OP is being used to align beginning of an option

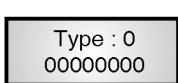


(c) NO-OP is being used to align the next option

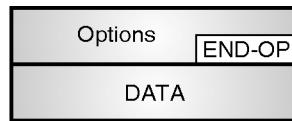
(G-2087) Fig. 7.15.2 : No operation option

7.15.2 End of Option Option :

- The second one byte option is the **end of option** option.
- It finds its application in **padding** at the end of the option field.
- Two important points about this option are as follows :
 1. We can use it only as the last option.
 2. We can use only one end of option. That means after this option, the receiver should expect the **payload data** to arrive.
- There if we need more than 1 byte to align the option field, then we must use more than one **no-operation** options and after that only one end-of-operation option as shown in Fig. 7.15.3.



(a) End-of-option



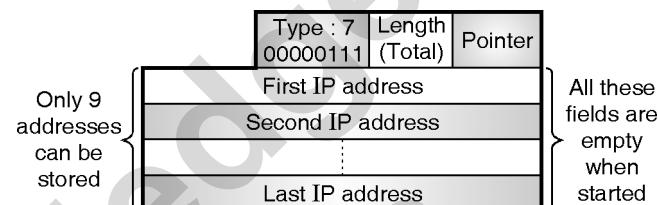
(b) Used for padding

(G-2088) Fig. 7.15.3

7.15.3 Record-Route Option :

- The record route option is a multiple byte option and it is used for recording the Internet routers which handle the datagram.

- Since the maximum size of the header is 60 bytes, including 20 bytes of base header, this option can list upto 9-IP addresses of the routers.
- So actually only 40 bytes are left for the option part. The format of the record-root option is as shown in Fig. 7.15.4.
- The source creates fields that are to be filled by each router visited by the datagram.



(G-2089) Fig. 7.15.4 : Round trip option

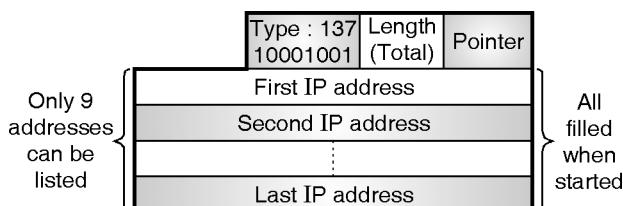
- The pointer field is an offset integer field which contains the byte number of the first empty entry.
- That means it points towards the first available entry.
- All the empty fields for the IP address are empty when the datagram leaves the source.
- The value of pointer field is 4 which points to the first empty field.
- When the datagram starts travelling, each router visited by this datagram, will insert its outgoing IP address in the next empty field and increments the value of pointer by 4.

7.15.4 Strict-Source-Route Option :

- This is also a multi byte option which is used by the source to determine the route in advance for the datagram travelling over the Internet.
- Due to this it becomes possible for the sender to choose root to get a specific type of service (i.e. minimum delay, maximum throughput etc.).
- It is also possible for a sender to choose a safer and more reliable root.
- If a datagram specifies a strict source route, then the datagram must visit all the routers which are defined in the option.
- It should not visit any router whose IP address is not listed in the datagram.
- If it does so then that datagram will be discarded and an error message will be issued.



- However the strict source routing is not generally preferred even by the regular users of the Internet, as they are not much aware of the physical topology of the Internet.
- Fig. 7.15.5 shows the format of the strict source route option.

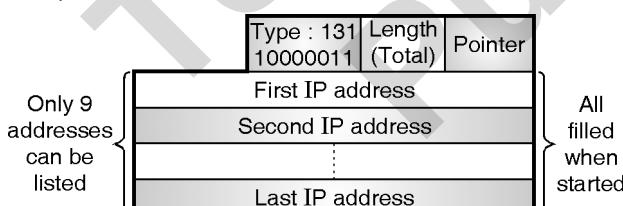


(G-2090) Fig. 7.15.5 : Format of strict source root option

- You will see that it is very similar to the format of the **record-root option** that we have discussed earlier with one exception that all the nine IP addresses of routers are entered by the sender itself.

7.15.5 Loose-Source-Root Option :

- This option is similar to the strict source root option discussed earlier.
- However this option is not as strict as the strict source root option, it is more relaxed.
- Here each router whose IP address is mentioned in the list must be visited by the datagram as before but the datagram is allowed to visit the other routers also.
- Fig. 7.15.6 shows the format of the loose-source-root option.

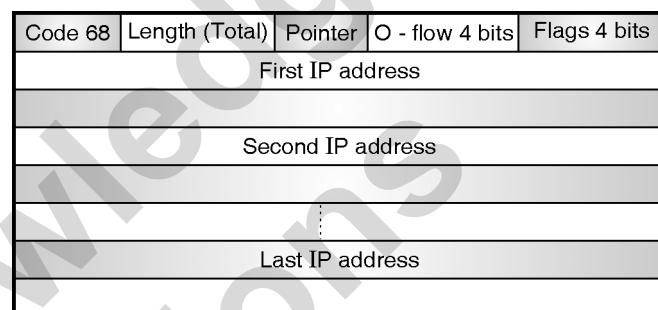


(G-2091) Fig. 7.15.6 : Format of loose-source root option

7.15.6 Time Stamp Option :

- The time stamp option is a multiple byte option and it is used for recording the time of datagram processing by a router, i.e. the time instant at which the datagram is processed by a router.
- This time is measured from midnight universal time and expressed in milliseconds.

- The users and managers can use the time of processing a datagram to track the behavior of the router in the Internet.
- With the help of the time stamp option, we can estimate the time taken by a datagram to travel from one router to the other.
- However this option is not used by most of the Internet as they are not aware of the physical topology of the Internet. Fig. 7.15.7 shows the format of the time stamp option.



(G-2092) Fig. 7.15.7 : Format of timestamp option

7.16 Checksum :

- Most TCP/IP protocol use the error detection method which is called as **checksum**.
- The purpose of using the checksum is to protect the packet from the corruption that may happen when the packet travels from source to destination.
- Checksum does not carry any information. Therefore it is the **redundant** bits added to the packet.
- The sending machine calculates the checksum and send its value with the packet.
- At the receiver the same calculation is performed on the whole packet including the checksum.
- The receiver will accept the packet if the result of the calculation is **satisfactory**. Otherwise the packet will be rejected.

7.16.1 Checksum Calculation at the Sender :

- At the sending end, the packet header is divided into n-bit sections (the value of n is generally 16).
- All these sections are added together using the one's complement arithmetic.



- The addition (sum) will also be 16 bit long.
- The **checksum** is obtained by inverting (complementing) all the bits in the sum.

Steps to calculate the checksum :

1. Divide the packet into K sections with each section containing n-bits.
2. Add all the K-sections together using one's complement arithmetic.
3. Complement the final result of addition to obtain the checksum.

7.16.2 Checksum Calculation at the Receiver :

- The receiver receives the packet and divides it into K sections and then adds all the sections.
- The result of addition is then complemented. The packet is accepted if the final result is zero, otherwise it is rejected.

Checksum in the IP packet :

- If we want to implement the checksum in an IP packet then we should follow the same principle discussed earlier in this section.
- The stepwise procedure for calculating the checksum is as follows :
 1. Set the value of the checksum field to 0.
 2. Divide the entire header into 16 bit sections and add all of them together.
 3. Complement the result (sum).
 4. Insert the complemented result into the checksum field.
- In the IP packet, the checksum covers only the header and not the data due to the following three reasons :
 1. All the high level protocols, which encapsulate their data in the IP datagram have a checksum field which takes into account the whole packet. Therefore the IP datagram need not consider the encapsulated data again while calculating its own checksum.
 2. The second reason is that when an IP packet visits a router, only its header changes but there is no change in data. Therefore, the checksum should take into account only that part which changes i.e. the header.
 3. If the data were included in the checksum calculation, then each router would have to recalculate the

checksum for the whole packet which would increase the **processing time**.

7.17 Network Layer Security :

- Security at the network layer is applied between a host and a router, two hosts or two routers.
- The applications such as routing protocols, which use the network layer services directly protected by using network layer security.
- As UDP is a connectionless protocol, it is not possible to apply the transport layer security protocols to UDP.
- In this case, the applications which use the service of UDP can have benefit from network layer security service.
- IPsec (IP security) is the only application layer security which we will discuss in the following subsection.

7.17.1 IPsec (IP security) :

- Internet or network security was a big challenge faced by the security experts.
- Though adding security by encryption and integrity checks could be used in application layer, the problem was whether the end-user would understand and use the application properly.
- Another disadvantage was that the existing program was needed to be modified or change.
- To overcome these drawbacks, it was decided that the encryptions would be applied in the IP layer so that the users are not involved in that process.
- This is known as IPsec (IP security) and it was designed to remove these drawbacks.
- IPsec is a protocol suite officially recognised by Internet Engineering Task Force (IETF) which uses symmetric-key cryptography which provides packet security at the network layer.

Features of IPsec :

1. The most important feature of IPsec is that it is based on NULL encryption algorithm. So, if any algorithm is hacked, the designed framework can still survive.
2. Another important feature of IPsec is that it is used to encrypt and authenticate data flow in only one direction known as security association (SA).

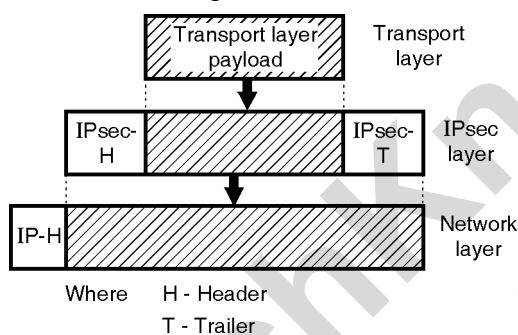
- Therefore, in any bi-directional flow, it is secured by two security associations (SA) which increases the level of security further.

7.17.2 Modes of Operation of IPsec :

- IPsec can be used in two modes :

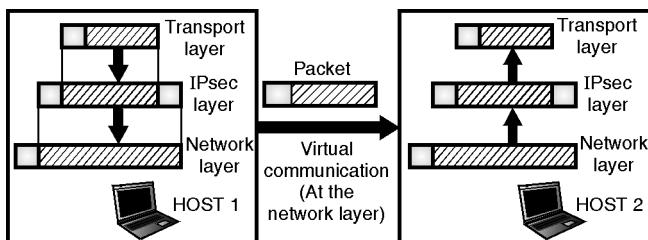
1. Transport mode :

- In this mode, the IP header is not modified or encrypted.
- It remains untouched. The IPsec header follows the IP header.
- In the network layer, the payload to be encapsulated is protected in transport mode of IPsec.
- Only the packet from transport layer is protected by transport mode, it does not protect whole IP packet. This is as shown in Fig. 7.17.1(a).



(G-2328) Fig. 7.17.1(a) : IP security in transport mode

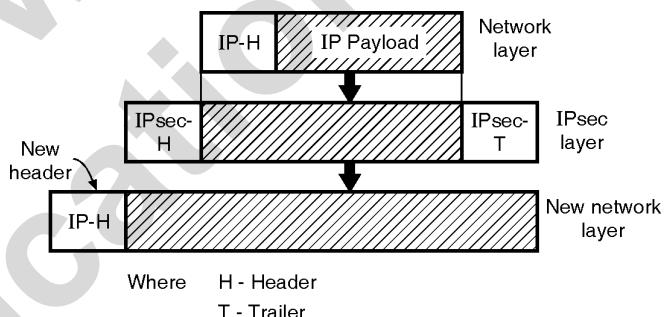
- When we need end-to-end (i.e. host-to-host) protection of data at that time transport mode is used.
- IPsec is used by the sending host for authentication and / or encryption of the payload which is delivered from the transport layer.
- Whereas IPsec is used by the receiving host which checks the authentication and / or decryption of IP packet and it is delivered to the transport layer. This is illustrated in Fig. 7.17.1(b).



(G-2329) Fig. 7.17.1(b) : Action in transport mode

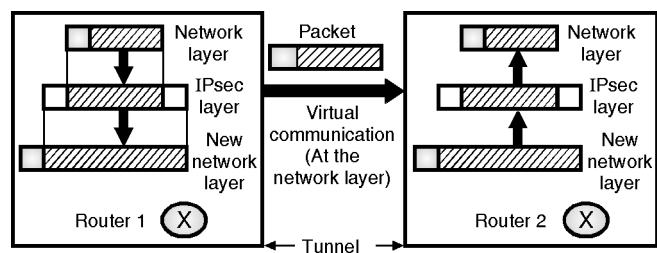
2. Tunnel mode :

- In this mode, the entire IP packet that is the data portion (payload) as well as the header is encrypted or authenticated.
- Thus, the tunnel mode is more secure than the transport mode of operation.
- At the receiving end, the machine which has IPsec installed on it decrypts each packet.
- The main drawback of tunnel mode is that an extra IP header is required which in turn increases the packet size to a great extent.
- In tunnel mode, entire IP packet is protected by IPsec. IPsec security methods are applied to the entire IP packet which consists of IP header, then it adds new IP header. Fig. 7.17.1(c) shows IP security in tunnel mode.



(G-2330) Fig. 7.17.1(c) : IP security in tunnel mode

- The new IP header contains different information than the original IP header.
- Tunnel mode is used between a host and a router, a router and a host or between two routers. This is illustrated in Fig. 7.17.1(d).



(G-2331) Fig. 7.17.1(d) : Action in tunnel mode

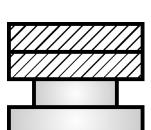
- As if the whole packet goes through the tunnel which is imaginary, the entire packet (original) is protected from disturbance between the sender and the receiver.



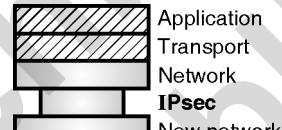
7.17.3 Comparison between Transport and Tunnel Mode :

Table 7.17.1 : Comparison of transport and tunnel mode

Sr. No.	Parameter	Transport mode	Tunnel mode
1.	Position of IPsec layer	Between transport layer and network layer refer Fig. A.	Between network layer and new network layer refer Fig. B.
2.	Flow	From network layer to IPsec layer	From network layer to IPsec layer and then back to network layer.
3.	IP header	In transport mode IPsec does not protect the IP header.	In tunnel mode IPsec protects the original IP header.
4.	New IP header	Not required	Required



(G-2332) Fig. A



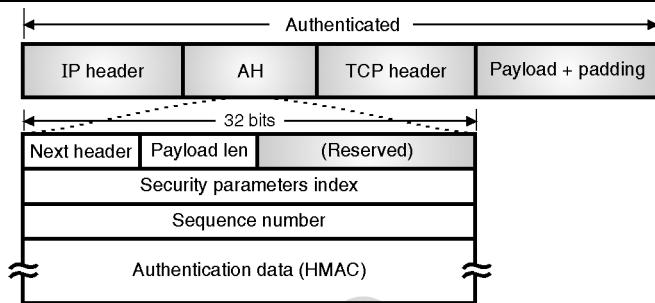
(G-2333) Fig. B

7.17.4 Security Protocols of IPsec :

- At the IP level to provide authentication and / or encryption IPsec defines two protocols namely AH (authentication header) and ESP (encapsulating security payload).

7.17.4.1 Authentication Header (AH) :

- The Authentication Header (AH) is a protocol used by IPsec for integrity checking and gives antireplay security.
- AH does not promise secrecy i.e. data is not encrypted.
- In IPv4, the AH is between the IP header and TCP header. In IPv6, AH is added to the IP header and is treated as just an extension header.
- The AH format is shown in Fig. 7.17.2.



(G-685) Fig. 7.17.2 : The IPsec authentication header

- The AH format is described as follows :
 - The **Next Header** field stores the previous value of the IP protocol field and indicates the presence of AH header.
 - The **security parameter index** is an arbitrary value which identifies the connection or the security association of the source and destination.
 - Sequence number** field is nothing but a counter to count every packet which is actually sent. It is used to detect and prevent replay attacks.
 - If a replay is detected, the sequence numbers are never reused and a new SA is established to continue communication.
- Authentication data** is variable-length field. It uses symmetric-key cryptography as IPsec is based on this cryptography. Before an SA is established, the sender and the receiver decide a shared key. This shared key is not transmitted but it is used as a digital signature for authentication.
- This is that type of coding where hash is computed over the packet and the shared key is known as HMAC (Hashed Message Authentication Code).

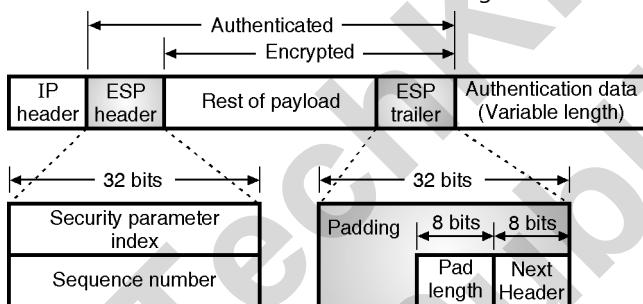
Advantages and disadvantages of AH :

- AH is advantageous where integrity or antireplay security is needed.
- AH is not much efficient as it does not provide secrecy of data.
- Another disadvantage is that number of sent packets are reduced as the packet has to be buffered and signature has to be authenticated before the packet is transmitted.



7.17.4.2 Encapsulating Security Payload (ESP) :

- Another type of IPsec header is Encapsulating Security Payload (ESP).
- It is a protocol suite which can be used for transport as well as tunnel mode of operation.
- Just like AH, it contains 32-bit words which are security parameters index and sequence number field.
- Another field, which is added after this, is the Initialization Vector, which is used for encryption of data.
- Integrity checks through HMAC are provided by the ESP and are included after payload instead of header.
- The ESP format is shown in Fig. 7.17.3.
- ESP (Encapsulating security payload) provides the services such as source authentication, integrity and confidentiality.
- Header as well ad trailer is added in ESP.
- At the end of packet ESP's authentication data are added because of which calculation become easier.
- The ESP header format is as shown in Fig. 7.17.4.



(G-2334) Fig. 7.17.4 : Encapsulating security payload (ESP)

- In the IP header, the value of the protocol field is 50 if an IP datagram carries ESP header and trailer.

- The next header field i.e. a field inside the ESP trailer holds the protocol field with original value.

- The process of ESP is as follows :

1. To the payload ESP trailer is added.
2. Both the payload and the trailer are encrypted.
3. Add ESP header.
4. For creation of the authentication data the ESP header, payload and ESP trailer are used.
5. To the end of the ESP trailer add the authentication data.
6. When the protocol value changes to 50 then the IP header is added.
- The ESP format is described as follows :

1. Security parameter index :

This 32-bit field is same as that defined for the AH protocol.

2. Sequence number :

This 32-bit field is same as that defined for the AH protocol.

3. Padding :

Padding is variable length field of 0's (0 to 255 bytes).

4. Padlength :

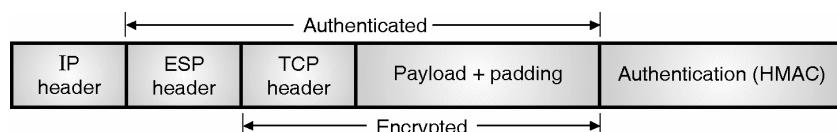
This is 8 bit field which defines the number of padding bytes. The range of value is between 0 and 255. This is very rare to have the maximum value.

5. Next header :

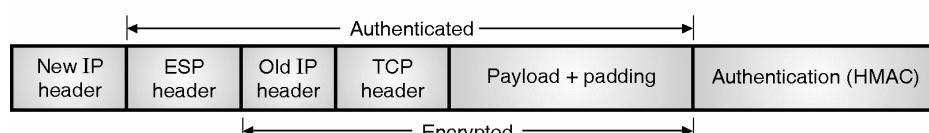
This 8 bit field is same as that next header field of AH protocol.

6. Authentication data :

There is difference between authentication data field of AH and ESP protocol. In AH protocol for the calculation of the authentication data, part of the IP header is included. In ESP, it is not included.



(a) ESP in transport mode



(b) ESP in tunnel mode

(G-686) Fig. 7.17.3 : ESP format



7.17.5 Services Provided by IPsec :

- At the network layer, AH and ESP provides some security services for packets.
- Table 7.17.2 shows list of available services for two protocols.

Table 7.17.2 : IPsec services

Sr. No.	Services	AH	ESP
1.	Replay attack protection	✓	✓
2.	Access control	✓	✓
3.	Confidentiality	.	✓
4.	Message integrity	✓	✓
5.	Entity authentication	✓	✓

1. Replay attack protection :

Using sequence numbers and a sliding receiver window, the replay attack is prevented in both protocols.

2. Access protocol :

With the help of Security Association Database (SAD), indirectly IPsec provides access control.

3. Confidentiality :

ESP provides confidentiality whereas AH does not provide confidentiality.

4. Message integrity / Message authentication :

Both protocols provides message integrity.

5. Entity authentication / data source authentication :

- AH and ESP provides entity authentication.

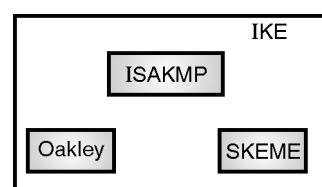
7.17.6 Security Association :

- A very important aspect of IPsec is **Security Association (SA)**.
- **Security Association** is logical relationship between two hosts needed in IPsec.
- The task of Security Association (SA) is to change the **connectionless** service, which is provided by IP into a connection-oriented service onto which we can apply security.
- **Security Association Database (SAD)** is a database, which contains collection of a set of Security Associations (SAS). Inbound and outbound are two SADs.

- **Security Policy (SP)** is another important aspect of IPsec. The function of **security policy** is to define the type of security, which is applied to a packet when it is transmitted or when it arrives at destination.
- Each host, which uses the IPsec protocol, is required to keep a SPD (Security Policy Database).
- **The outbound SPD** is consulted when a packet is to be transmitted out whereas the inbound SPD is consulted when a packet arrives.

7.17.7 Internet Key Exchange (IKE) :

- For the generation of inbound and outbound security association, a protocol is designed known as the **Internet Key Exchange (IKE)**.
- For IPsecs, IKE creates SAS.
- This protocol is complex which is based on the following protocols :
 1. Oakley
 2. SKEME
 3. ISAKMP
- The **Oakley** is a key creation protocol which was developed by Hilarie Orman.
- For key exchange another protocol named as SKEME was designed by Hugo Krawcyzk.
- In a key exchange protocol, for entity authentication SKEME uses public key encryption.
- ISAKMP (Internet Security Association and Key Management Protocol) which implements exchanges defined in IKE which is designed by the National Security Agency (NSA).
- This protocol defines a number of protocols, packets and parameters which allows the IKE exchanges to takes place in standard manner and formatted message for the generation of security associations. (SAS).
- Fig. 7.17.5 shows Internet Key Exchange (IKE) components.

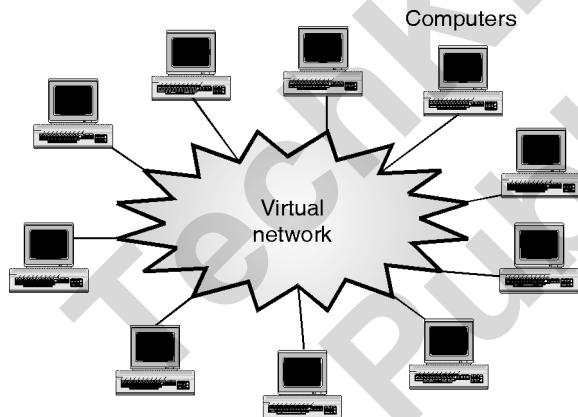


(G-2335) Fig. 7.17.5 : Components of IKE



7.17.8 Virtual Private Networking (VPN) :

- Due to Internet software, it appears that the Internet is a single, seamless system of communication to which lots of networks containing a large number of computers are connected.
- The internal details of these real or actual networks get hidden when they become a part of the Internet.
- Every computer connected to the Internet has its own unique address assigned to it.
- The users of the Internet do not have to bother about the internal structure of the physical networks and the details related to them.
- Thus the user is a part of a **virtual network**. Internet is thus the best example of virtual networks.
- The concept of virtual networks states that in such types of networks, different computer networks are not only connected together but you feel that they are a part of a big single network.
- The concept of virtual networks is illustrated in Fig. 7.17.6.



(G-1447) Fig. 7.17.6 : Concept of virtual network

7.18 IPv6 (Next Generation IP) :

- IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4.
- IPv6 was designed to enable high-performance and larger address space.
- This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.

7.18.1 Advantages of IPv6 :

- 1. Improved header format :**
 - IPv6 uses an improved header format. In its header format the options are separated from the base header.
 - These options are inserted when needed, between the base header and upper layer data.
 - The routing process is simplified due to this modification. The speed of the routing process increases and the routing time is reduced.
- 2. Larger address space :**
 - IPv6 has 128-bit address, which is 4 times wider in bits compared to IPv4's 32-bit address space. So there is a large increase in the address space.
Address space of IPv6 = (2^{128})
- 3. New options :**
 - IPv6 has increased functionality due to the addition of entirely new options that are absent in IPv4.
- 4. More security :**
 - IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH : Authentication Header) for enhancing the security.
- 5. Possibility of extension :**
 - The design of IPv6 is done in such a way that there is a possibility of extension of protocol if required.
- 6. Support to resource allocation :**
 - To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification. With flow label mechanism, routers can recognize to which end-to-end flow the given packet belongs to.
- 7. Plug and play :**
 - IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.
- 8. Clearer specification and optimization :**
 - IPv6 follows good practices of IPv4, and omits flaws/obsolete items of IPv4.

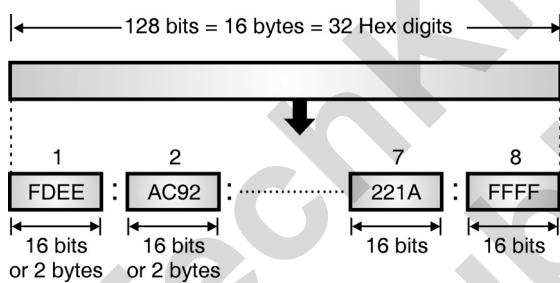


7.19 IPv6 Addressing :

- IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4.
- IPv6 was designed to enable high-performance and larger address space.
- This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.
- The IPv6 was developed due to the address depletion of IPv4.
- The structure of IPv6 address is fundamentally different than that of IPv4.
- Therefore there is absolutely no possibility of address depletion taking place in future.

7.19.1 IPv6 Address :

- An IPv6 address is 128 bit long. It consists of 16 bytes as shown in Fig. 7.19.1.
- Thus the IPv6 address is 4 times longer than that of IPv4.



(G-545) Fig. 7.19.1 : IPv6 address

7.19.2 Notations :

- An address is stored in the computers in the binary form.
- But it is impossible for humans to handle a 128 bit binary address.
- Therefore many notations have been proposed to represent the IPv6 addresses, so that they become easier to handle for human beings.
- Some of the proposed notations are :
 1. Dotted decimal notation.
 2. Colon hexadecimal notation.
 3. Mixed representation.
 4. CIDR notation.

1. Dotted decimal notation :

- In order to maintain the compatibility with IPv4 addresses. We may feel tempted to use the dotted decimal notation.
- But practical observation is that this notation is convenient only for the 4 byte address of IPv4. It is not at all convenient for the 16 byte IPv6 addresses as it seems too long.
- Therefore this notation is very rarely used.

2. Colon hexadecimal notation :

- The 128 bit address can be made more readable and easy to handle. IPv6 has specified the **colon hexadecimal notation**.
- IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128 bits are divided into 8 sections, each one is 16 bits or 2 bytes long.
- The 16 bits or 2 bytes in binary correspond to four hexadecimal digits of 4-bits each.
- Hence the 128 bits in hexadecimal form will have $8 \times 4 = 32$ hexadecimal digits.
- These are in groups of 4 digits as shown and every group is separated by a colon as shown in Fig. 7.19.2.

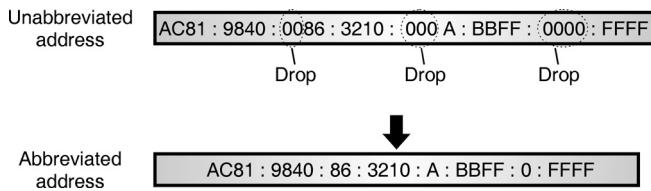
AC 81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

Fig. 7.19.2 : Colon hexadecimal notation

- IPv6 uses 128-bit addresses. Only about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.
- These unused addresses may be used in the future for expanding the address spaces of existing address types or for totally new uses.

7.19.3 Abbreviation :

- The IPv6 address, in hexadecimal format contains 32 digits and it is very long.
- But in this address many hex digits are zero.
- We can take advantage of this to shorten the address by abbreviating it.
- A section corresponds to four digits between any two colons. The leading zeros in a section can be omitted to reduce the length of the address as shown in Fig. 7.19.3.

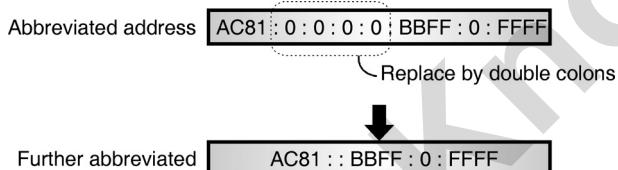


(G-546) Fig. 7.19.3 : Abbreviated address

- Note that only the leading zeros can be dropped but the trailing zeros can not be dropped. This is illustrated in Fig. 7.19.3.
- Thus due to abbreviation the length of the address has reduced to 24 hex digits from 32.

Further abbreviation :

- We can make further abbreviation if there are consecutive sections consisting of only zeros.
- This is known as **zero compression**.
- We can remove the zeros completely and replace them with double colon as shown in Fig. 7.19.4.



(G-547) Fig. 7.19.4 : Further abbreviation (Zero compression)

- This further abbreviation has reduced the address length to just 13 hex digits.
- It is important to note that abbreviation can be done only once per address.
- Also note that if there are two sets of zero sections, then only one of them can be abbreviated.

3. Mixed representation :

- Sometimes, the IPv6 address is represented using a mixed representation which combines the **colon hex** and **dotted decimal** notations.
- This notation is appropriate during the transition time during which an IPv4 address is being embedded in IPv6 address.
- In the mixed representation the rightmost 32 bits correspond to the IPv4 address. Hence they are represented by the dotted decimal notation.
- Whereas the leftmost 96 bits (6 sections) are represented in colon hex notation.

4. CIDR notation :

- The type of addressing used in IPv6 is **hierarchical addressing**.
- Therefore IPv6 allows classless addressing and CIDR notation.
- Fig. 7.19.5 illustrates the CIDR address with a 60 bit prefix.
- It has been discussed later on in this chapter, how we can divide an IPv6 address into a prefix and a suffix.



(G-2132) Fig. 7.19.5 : CIDR address

Ex. 7.19.1 : IPv6 uses 16-byte addresses. If a block of 1 million addresses is allocated every picosecond, how long will the addresses last ?

Dec. 07, 6 Marks

Soln. :

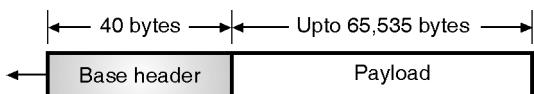
$$\begin{aligned}
 1. \text{ Total number of address bits} &= 16 \times 8 = 128 \\
 2. \text{ Number of addresses} &= 2^{128} = 3.4 \times 10^{38} \\
 3. \text{ One picosecond} &= 1 \times 10^{-12} \text{ seconds} \\
 4. \text{ 1 million addresses} &= 1 \times 10^6 \text{ address} \\
 \therefore 1 \text{ picosecond} &= 1 \times 10^6 \text{ addresses} \\
 \therefore x &= 3.4 \times 10^{38} \\
 \therefore x &= \frac{3.4 \times 10^{38}}{1 \times 10^6} \times 1 \text{ picoseconds} \\
 &= 3.4 \times 10^{32} \text{ picoseconds} \\
 &= 3.4 \times 10^{20} \text{ seconds} \\
 &= 9.44 \times 10^{16} \text{ hours} \\
 &= 3.9352 \times 10^{15} \text{ days} = 1.0781 \times 10^{13} \text{ years}
 \end{aligned}$$

7.20 IPv6 Packet Format :

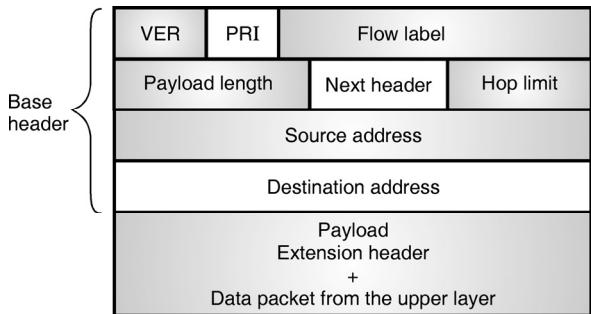
- Fig. 7.20.1(a) shows IPv6 packet. Fig. 7.20.1(b) shows the packet format (Base header) of IPv6.
- Each packet can be divided into two parts viz : base header and payload.
- Base header is the mandatory part and payload is an optional one.
- The payload follows the base header.
- The payload is made up of two parts :



1. An optional extension headers and
2. The upper layer data.
- The base header is 40 byte long whereas the payload consisting of the extension header and upper layer data can have information worth upto 65, 535 bytes.



(G-2245) Fig. 7.20.1(a) : IPv6 packet



(G-550) Fig. 7.20.1(b) : Format of an IPv6 datagram (Base header)

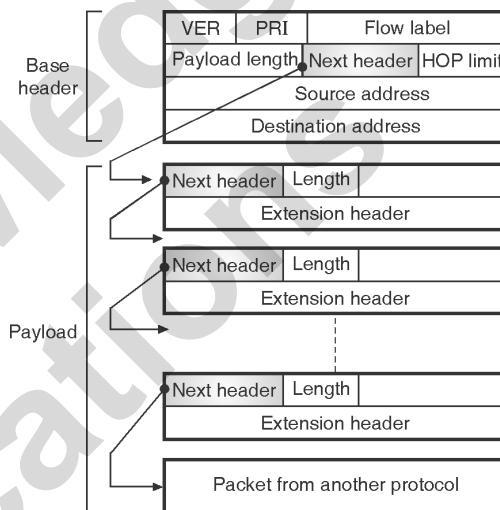
Base header :

- Fig. 7.20.1(b) shows the base header. It has eight fields. These fields are as follows :
- 1. **Version (VER)** : The contents of this 4 bit field defines the version of IP such as IPv4 or IPv6. If VER = 6, then the version is IPv6.
- 2. **Priority** : This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion.
- 3. **Flow label** : It is a 24 bit (3 byte) field which is supposed to provide a special handling for a particular flow of data.
- 4. **Payload length** : The contents of the 16 bit or 2 byte length field are used to indicate the total length of the IP datagram excluding the base header. That means it gives the length of only the payload part of the datagram.
- 5. **Next header** : It is an 8 bit field which defines the header which follows the base header in the datagram.
- 6. **Hop limit** : Contents of this 8 bit (1 byte) field have the same function as TTL (time to live) in IPv4.
- 7. **Source address** : It is a 16 byte (128 bit) Internet address which corresponds to the originator or source which has produced the datagram.

8. **Destination address** : This is a 16 byte (128 bit) internet address which corresponds to the address of the final destination of datagram. But this field will contain the address of the next router and not the final destination if source routing is being used.

7.20.1 Payload :

- The meaning and format of payload field in IPv6 is different as compared to payload field in IPv4.
- Fig. 7.20.2 shows payload field in IPv6.



(G-2246) Fig. 7.20.2 : IPv6 payload

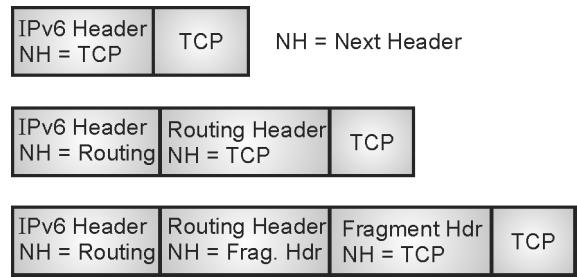
- In IPv6, the payload is combination of zero or more extension headers (options) which is followed by data from other protocols such as UDP, TCP etc.
- In IPv4, option is a part of the header, whereas in IPv6 it is designed as extension headers.
- Depends on the situation the payload can have as many extension headers as required.
- Extension header is made up of two mandatory fields : next header and the length which is followed by information which is related to the particular option.
- Value of next header field i.e. code defines which type of the next header is (e.g. source routing options, fragmentation option etc.)
- The last next header describes the protocol which carries the datagram.
- Some next header codes are listed in Table 7.20.1.

**Table 7.20.1 : Next header codes**

Sr. No.	Code	Next header code
1.	00	HOP by hop option
2.	02	ICMPv6
3.	06	TCP
4.	17	UDP
5.	43	Source routing option
6.	44	Fragmentation option
7.	50	Encrypted security payload
8.	51	Authentication header
9.	59	Null (no next header)
10.	60	Destination option

7.20.2 Extension Headers :

- As stated earlier the length of the base header is 40 bytes and it always remains constant.
- But in IPv6, the fixed base header can be followed by upto six extension headers.
- In IPv4 these are optional headers.
- This gives more functionality to the IP datagram.
- The IPv4 header has space for some optional fields requiring a particular processing of packets.
- These optional fields are not used often, and they can deteriorate router performance because their presence must be checked for each packet. IPv6 replaces these optional fields by **extension headers**.
- In IPv6, optional Internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet (see Fig. 7.20.3).
- There are a small number of such extension headers, each identified by a distinct Next Header value. An IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header.
- There are seven kinds of extension header :

**(G-2712) Fig. 7.20.3 : Examples of headers chain**

- Extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header, except for the Hop-by-Hop Options header and the Routing header.
- Therefore, extension headers must be processed strictly in the order of their appearance in the packet; a receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header before processing all the preceding ones.
- Each extension header has a length equal to a multiple of 64 bits (8 bytes).
- A full implementation of IPv6 must include support for the following extension headers :
- When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order :
 1. IPv6 header
 2. Hop-by-Hop Options header
 3. Destination Options header
 4. Routing header
 5. Fragment header
 6. Authentication header
 7. Encapsulating Security Payload header
 8. Destination Options header
 9. Upper-layer header

1. Fragmentation :

- The fragmentation in IPv6 is conceptually same as that discussed for IPv4, but the fragmentation in IPv6 takes place at a different place than that in IPv4.
- In IPv4 the fragmentation is done by the source or router, but in IPv6 the fragmentation may be carried out only by the original source.



2. Authentication and Privacy :

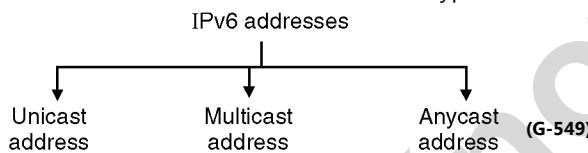
- IPv6 provides authentication and privacy using options in the extension header.

7.21 Address Space :

- The address space of IPv6 contains 2^{128} addresses which is a very big number.
- If we compare it with the address space of IPv4, then it can be seen that, the address space of IPv6 is 2^{96} times bigger than that of IPv4.
- Therefore there is no possibility of address depletion in IPv6.

7.21.1 Address Types :

- IPv6 defines three different types of addresses. The destination address can be one of these types :



1. Unicast address :

- A unicast address is meant for a single computer as a destination.
- A packet sent to a unicast address is meant to be delivered to the computer specified by the address.
- In IPv6 a large block of addresses has been designated from which it is possible to assign unicast addresses to the interfaces.

2. Anycast address :

- This is a type of address which is used to define a group of computers with addresses which have the same prefix.
- A packet sent to an anycast address must be delivered to only one of the member of the group which is the closest or the most easily accessible.
- No special or separate address block is assigned for anycasting in IPv6.
- Instead the anycast addresses are assigned from the block of unicast addresses.

3. Multicast addresses :

- A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network.

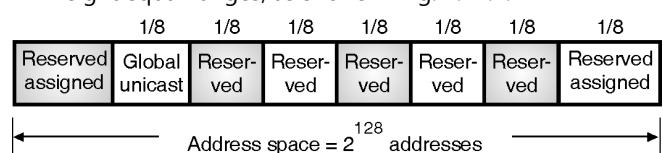
- A packet sent to a multicast address is meant to be delivered to each member of the group.
- There are no broadcast addresses in IPv6, because multicast addresses can perform the same function.
- The type of address is determined by the leading bits.
- All the multicast addresses start with FF (1111 1111) and all other addresses are unicast addresses.
- Anycast addresses are assigned from the unicast address space and they do not differ syntactically from unicast addresses.
- Anycast addressing is a rather new concept and there is not much experience about the widespread use of anycast addresses.
- Therefore, some restrictions apply to anycast addressing in IPv6 until more experience is gained.
- An anycast address may not be used as the Source Address of an IPv6 packet and anycast addresses may not be assigned to hosts but to routers only.
- As will be discussed later, a block is designated for multicasting in IPv6, from which the same address is assigned to the members of the group.

7.21.2 Broadcasting and Multicasting :

- In IPv6 the broadcasting is not defined at all, as in case of IPv4.
- In IPv6 broadcasting is considered as a special case of multicasting.

7.22 Address Space Allocation :

- Address space allocation in IPv6 is a process which divides the address space of IPv6 in several blocks.
- Each block is allocated for some special purpose and has a different size.
- Most of the blocks in IPv6 are not assigned yet and will be used in future.
- The entire address space in IPv6 has been divided into eight equal ranges, as shows in Fig. 7.22.1.



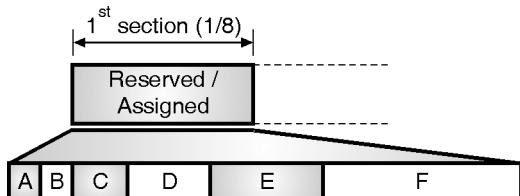
(G-2133) Fig. 7.22.1 : Address space allocation in IPv6



- As shown in Fig. 7.22.1, the number of addresses in each section is one eighth of the total address space.
- So number of addresses in each section is equal to 2^{125} addresses.

7.22.1 The First Section :

- The first section is marked as Reserved/Assigned in Fig. 7.22.2.
- That means some address blocks in this section are reserved and the remaining are assigned as shown in Fig. 7.22.2(a).



A : 1/256 IPv4 compatible. D : 1/64 Reserved.
 B : 1/256 Reserved. E : 1/32 Reserved.
 C : 1/128 Reserved. F : 1/16 Reserved.

(G-2134) Fig. 7.22.2(a) : The first section

- As shown in Fig. 7.22.2(a), the first section is divided in six blocks of variable sizes (blocks A to F).
- Out of these six blocks, three blocks have been reserved and remaining three are not assigned.

7.22.2 Second Section :

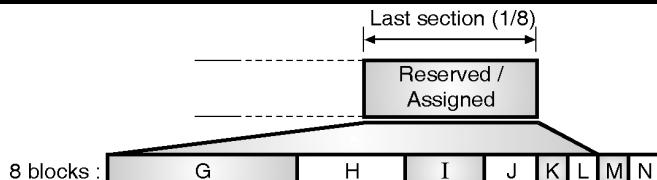
- The second section is not divided into blocks. So it is considered as one single block and is used for the **global unicast** addresses.

Sections three to seven :

- These five sections from third to seventh are unassigned.

Last section :

- The last section in Fig. 7.22.2 which is marked as Reserved /Assigned is further divided into eight blocks of different sizes as shown in Fig. 7.22.2(b).
- Some of these blocks are not assigned while the other blocks are reserved for some special purpose as shown in Fig. 7.22.2(b).



G : 1/16 Reserved. K : 1/512 Reserved.

H : 1/32 Reserved. L : 1/1024 Link local

I : 1/64 Reserved. M : 1/256 Reserved.

J : 1/128 Unique local unicast N : 1/256 Multicast.

(G-2135) Fig. 7.22.2(b) : The last section

- From all this discussion it is very clear that out of the total address space of IPv6 more than 5/8th of the space is still not assigned, and only 1/8th of the address space has been assigned for the global unicast addresses for unicast communication between the users.
- The prefix for each type of address has been shown in Table 7.22.1.

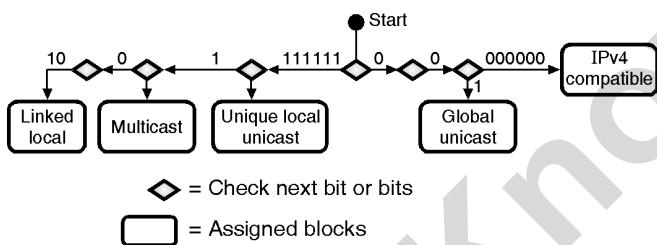
Table 7.22.1 : Prefixes for IP addresses

Block Prefix	CIDR	Block Assignment	Fraction
1 0000 0000	0000::/8	Reserved (IPv4 compatible)	1/256
0000 0001	0100::/8	Reserved	1/256
0000 001	0200::/7	Reserved	1/128
0000 01	0400::/6	Reserved	1/64
0000 1	0800::/5	Reserved	1/32
0001	1000::/4	Reserved	1/16
2 001	2000::/3	Global unicast	1/8
3 010	4000::/3	Reserved	1/8
4 011	6000::/3	Reserved	1/8
5 100	8000::/3	Reserved	1/8
6 101	A000::/3	Reserved	1/8
7 110	C000::/3	Reserved	1/8
8 1110	E000::/4	Reserved	1/16
1111 0	F000::/5	Reserved	1/32
1111 10	F800::/6	Reserved	1/64

Block Prefix	CIDR	Block Assignment	Fraction
1111 1110	FC00::/7	Unique local unicast	1/128
1111 1110 0	FE00::/9	Reserved	1/512
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1110 11	FEC0::/10	Reserved	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

7.22.3 Algorithm :

- The diagram shown in Fig. 7.22.3 has been created to illustrate that the prefixes given in Table 7.22.1 really find the block to which the IPv6 address belongs to.
 - Note that, in order to make this diagram simpler we have not shown the reserved blocks.



(G-2136) Fig. 7.22.3 : An algorithm to find the allocated blocks

7.22.4 Assigned or Reserved Blocks :

- In this section, we are going to discuss the purposes and characteristics of the reserved as well as assigned blocks starting from the first row of Table 7.22.1.

1. IPv4 compatible addresses :

- The addresses which use the prefix (00000000) are reserved, however a part of it is used for defining some IPv4 compatible addresses.
 - There are 2^{120} addresses in this block because it occupies 1/256 the fraction of the total address space.
 - This block can be defined using CIDR notation as follows :

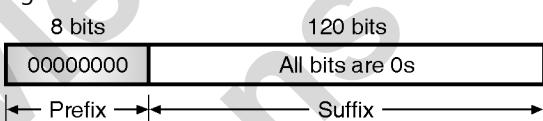
0000::/8

- This address block is further divided into many smaller subblocks. We will discuss them later in this chapter.

7.22.5 Unspecified Address :

- The unspecified address is a subblock which contains only one address.

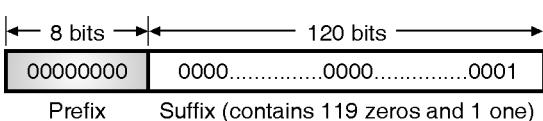
- By letting all suffix bits to zero, this address can be defined. That means this address is an all zeros address.
 - During the bootstrapping process, when a host does not know its own address, the unspecified address is used to send an enquiry to find the unknown address of the host.
 - This address is used by the host as a **source address**. However it is important to note that the unspecified address cannot be used as the **destination address**.
 - This one-address subblock can be represented as ::/128 in the CIDR notation, and its format has been shown in Fig. 7.22.4.



(G-2137) Fig. 7.22.4 : Format of the unspecified address

7.22.6 Loopback Address :

- Like the previous one, this subblock also contains only one address which a host uses for testing itself without going into the network.
 - Here the application layer creates an address, sends it to the transport layer and then passes it to the network layer.
 - However it does not go to the physical layer. Instead, it returns to the transport layer and finally passed on to the application layer.
 - This feature is very useful because using it we can test the functions of software package in these layers even before the computer is connected to the network.
 - Fig. 7.22.5 shows the format of the loopback address which has the prefix of 00000000 and a suffix containing 119 zeros and one 1.
 - We can represent this address in the CIDR notation as ::1/128.



(G-2138) Fig. 7.22.5 : Format of the loopback address



7.22.7 Difference between Loopback Address of IPv4 and IPv6 :

- In IPv4 classful addressing, the loop back addresses get a whole block allotted to them but in IPv6 loopback address is only one single address.
- In IPv4 the loop back addresses are accommodated as a part of class A address but in IPv6 it is only one single address in the reserved block.

7.22.8 Embedded IPv4 Addresses :

- As discussed in the migration from IPv4 to IPv6 in this transition period, the hosts can continue to use their IPv4 address which are embedded in IPv6 addresses.
- In order to achieve this, IPv6 has designed two formats namely **compatible format** and **mapped** format.

7.22.9 Compatible Address :

- The compatible address is an IPv6 address with 96 bits of zeros followed by 32 bits of IPv4 address.
- Fig. 7.22.6 shows the format of IPv6 compatible address.

Prefix	All 0 bits	IPv4 address
00000000	All 0 bits	IPv4 address

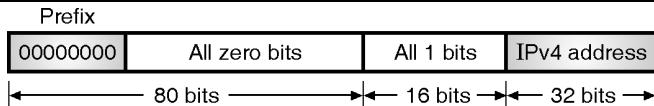
↔ 96 bits ↔ 32 bits ↔

(G-2139) Fig. 7.22.6 : Format of compatible address

- The situation in which the compatible address is required to be used is as follows :
- If an IPv6 host wants to communicate with another IPv6 host but the packet is going to pass through a region in which still the IPv4 is being used by the networks.
- In order to ensure a successful passage of this packet the sender will have to use the **compatible address**.
- This is a reserved subblock which contains 2^{32} addresses and has a CIDR notation of ::/96.

7.22.10 A Mapped Address :

- The format of a mapped address is shown in Fig. 7.22.7. It shows that this address consists of 80 bits of zeros, followed by 16 bits of 1s, followed by 32 bits of IPv4 address.
- It is used when an IPv6 computer wants to communicate with an IPv4 computer.



(G-2140) Fig. 7.22.7 : Mapped address

- This packet can travel for an IPv6 guest, through a mostly IPv6 network and finally delivered to an IPv4 destination host.

7.22.11 Calculation of Checksum :

- The compatible and mapped addresses have been designed in such a way that the checksum can be calculated by either using the embedded address or the complete address because the extra zeros and ones are in multiples of 16.
- Hence they do not affect the checksum calculation in any way.
- So the value of checksum remains same even if the packet address is changed from IPv6 to IPv4.

7.23 Migrating to IPv6 (Compatibility to IPv4) :

1. It was IPv4's success that made an upgrade necessary, which means that there is a large number of IPv4 users that to be upgraded to IPv6. Keeping the transition orderly was a major objective of the entire IPng program. The cutover date when IPv6 would be turned on and IPv4 turned off has not been decided.
2. The simple strategy for upgrading involves deployment of IPv6 protocol stack in parallel with IPv4. In other words, hosts that upgrade to IPv6 will continue to simultaneously exist as IPv4 hosts.
3. An experimental IPv6 backbone, or 6 bone, has been set up to handle IPv6 Internet traffic in parallel with the regular Internet. Such hosts will continue to have 32-bit IPv4 addresses but will add 128-bit IPv6 addresses. By 1999, hundreds of networks were linked to the 6 bone.
4. The transition can be achieved through two approaches: protocol tunneling or IPv4/IPv6 dual stack.

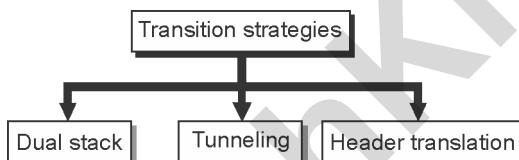


7.24 Transition from IPv4 to IPv6 :

- It is required to use a new version of the IP protocol.
- For that transition from IPv4 to IPv6 we have to define a transition day on that day each and every router or host stop using old version and should start using the new version.
- As there are huge number of systems in the Internet, transition from IPv4 to IPv6 is not practical suddenly.
- It will take some amount of time to move each and every system in the internet from IPv4 to IPv6.
- The transition from IPv4 to IPv6 should be smooth to prevent any problems in the system.

7.24.1 Transition Strategies :

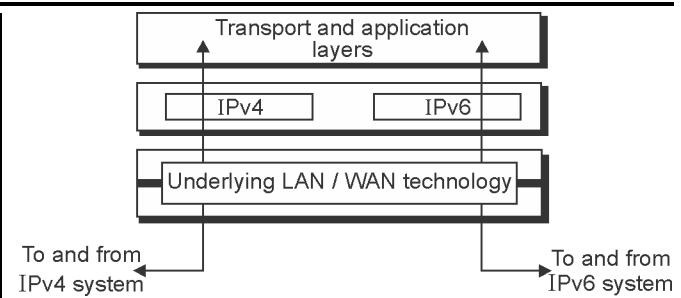
- Fig. 7.24.1(a) shows the strategies for transition from IPv4 to IPv6.



(G-2531) Fig. 7.24.1(a) : Transition strategies

1. Dual Stack :

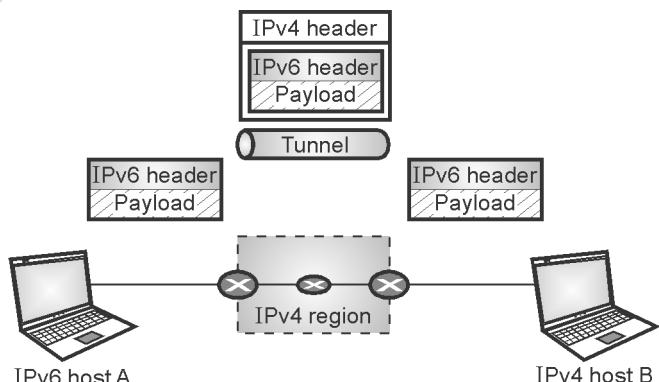
- Before completely migrating to version 6 it is recommended that all hosts should have a dual stack of protocols at the time of transition.
- Simultaneously station should run IPv4 and IPv6, until the Internet uses IPv6.
- The layout of dual stack configuration is as shown in Fig. 7.24.1(b).
- A source host send query to the DNS for deciding which version to use while sending a packet to a destination.
- A source host sends IPv4 packet if an IPv4 address is returned by the DNS, and sends IPv6 packet if DNS returns IPv6 address.



(G-2532) Fig. 7.24.1(b) : Dual stack strategy

2. Tunneling :

- When two computers are using IPv6 want to communicate with each other and a region through which the packet must pass uses IPv4, in such case **tunneling** strategy is used.
- The packet should have IPv4 address while passing through this region.
- When it enters in this region the IPv4 packet is encapsulated in IPv4 packet and when it exists the region it leaves its capsule.
- It looks like as if the IPv6 packet enters in a tunnel from one end and comes out from the other end.
- The protocol value is set to 41 for making it clear that IPv4 packet is holding an IPv6 packet as a data.
- The tunneling strategy is as shown in Fig. 7.24.1(c).



(G-2533) Fig. 7.24.1(c) : Tunneling strategy

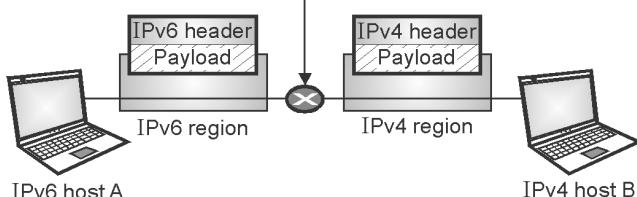
3. Header translation :

- If some systems use IPv4 and the majority of the Internet has moved from IPv4 to IPv6, in that case header translation strategy is used where the receiver does not understand IPv6 but the sender wants to use IPv6 only.



- In this situation tunneling will not work because the packet should be in the IPv4 format which has to be understood by the receiver.
- In this strategy through header translation the format of header must be totally changed.
- The IPv6 packet header is converted into an IPv4 header. Fig. 7.24.1(d) shows header translation strategy.

Header translation process



(G-2534) Fig. 7.24.1(d) : Header translation strategy

7.24.2 Use of IP Addresses :

- A host may need to use both IPv4 and IPv6 addresses during the transition. IPv4 addresses must disappear after completion of transition.
- During the transition it is necessary that the DNS server is to be ready to map a host name to address type.
- After migrating all hosts in the world the IPv4 dictionary will disappear.

7.24.3 Comparison between IPv4 and IPv6 :

SPPU : Dec. 11, May 12, Dec. 13, Dec. 15

University Questions

- Q. 1** Compare between IPv4 and IPv6. Draw header diagram. **(Dec. 11, May 12, 8 Marks)**
- Q. 2** Differentiate IPv6 over IPv4. **(Dec. 13, 8 Marks)**
- Q. 3** Differentiate between IPv4 and IPv6. **(Dec. 15, 4 Marks)**

IPv4	IPv6
In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)
The IPv4 address is written by dotted-decimal notation, e.g. 121.2.8.12	IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98: 5432:4567.
The basic length of the IPv4 header comprises a minimum of 20 bytes (without option fields). The maximum total length of the IPv4 header is 60 bytes (with option fields), and it uses 13 fields to identify various control settings.	The IPv6 header is a fixed header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
IPv4 header has a checksum, which must be computed by each router	IPv6 has no header checksum because checksums are, for example, above the TCP/IP protocol suite, and above the Token Ring, Ethernet, etc.
IPv4 contains an 8-bit field called Service Type. The Service Type field is composed of a TOS (Type of Service) field and a procedure field.	The IPv6 header contains an 8-bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets
The IPv4 node has only Stateful auto-configuration.	The IPv6 node has both a stateful and a stateless address autoconfiguration mechanism.



IPv4	IPv6
Security in IPv4 networks is limited to tunneling between two networks	IPv6 has been designed to satisfy the growing and expanded need for network security.
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Header includes options	All optional data is moved to IPv6 extension headers.

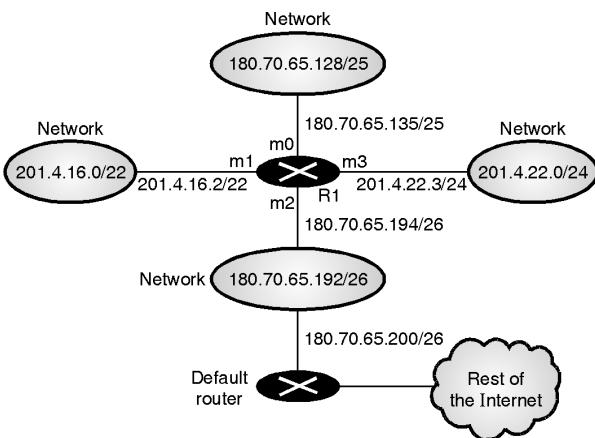
Ex. 7.24.1 : A router is networking four different networks with network addresses 180.70.65.192/26, 180.70.65.128/25, 201.4.22.0/24, 1.4.16.0/22 and default router on 180.70.65.200 make a routing table for this router and explain the forwarding process for packet with destination IP 18.24.32.78.

May 12, 10 Marks

Soln. :

Step 1 : Draw the configuration :

The configuration is as shown in Fig. P. 7.24.1.



(G-1510) **Fig. P. 7.24.1 : The given configuration**

Step 2 : Make the routing table :

The routing table is as shown in Table P. 7.24.1.

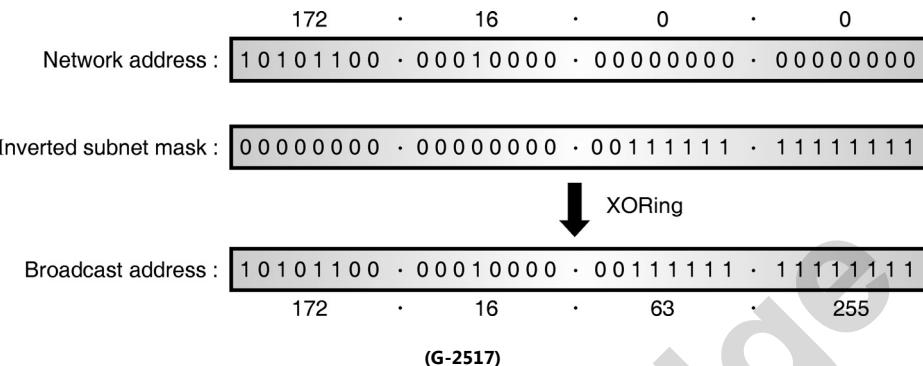
Table P. 7.24.1 : Routing table

Mask	Network address	Next Hop	Interface
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	...	m1
Any	Any	180.70.65.200	m2

Step 3 : Forwarding process for packets to IP 18.24.32.78 :

IP 18.24.32.78 :

- The destination address is 18.24.32.78. The router performs the following steps :
- 1. The first mask (/26) is applied to the destination address. The result is 18.24.32.0 which does not match the corresponding network address.
- 2. Similarly the remaining masks are applied one by one. The results do not match with the corresponding network addresses. Hence the packet is forwarded to the default router.



∴ Broadcast address for last subnet = 172.16.63.255... **Ans.**

Step 5 : To find the range of valid hosts in last subnet :

Subnet number	Address
1	172.16.0.0 to 172.16.0.63
2	172.16.0.64 to 172.16.0.127
3	172.16.0.128 to 172.16.0.191
4	172.16.0.192 to 172.16.0.255

∴ Range of valid hosts in last subnet is 172.16.0.192 to 172.16.0.255 ... **Ans.**

Review Questions

- Q. 1 Write a note on IP.
- Q. 2 Explain fragmentation in IP.
- Q. 3 What is the name of a packet in IP ?
- Q. 4 Explain the IP header.
- Q. 5 What is MTU and how is fragmentation related to it ?
- Q. 6 Compare IPv4 and IPv6.
- Q. 7 Name and describe three types of IPv6 addresses.
- Q. 8 Write a note on mobile IP.
- Q. 9 What is fragmentation ? Explain how is it supported in IPv4 and IPv6.
- Q. 10 Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed ? Explain.

Q. 11 What is fragmentation ? Explain how it is supported in IPv4 and IPv6.

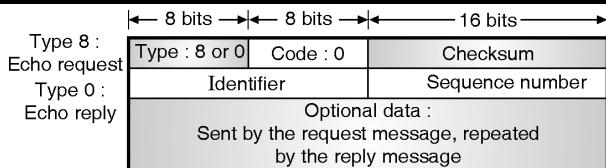
Q. 12 Given an IP address, how will you extract its net id and host id.

7.25 University Questions and Answers :

Q. 1 What is PING ? Explain with suitable example how PING works. **(Dec. 18, 6 Marks)**

Ans. :

- **Ping** is a basic internet program that allows its user to verify whether a particular IP address exists or not.
- Ping is used to ensure that the computer to which the user wants to reach is actually operating.
- Ping can also be used for trouble shooting, to test connectivity and determine the response time.
- Ping works by sending an ICMP **echo request** message to the host the user wants to communicate to and then waiting for the reply.
- Now a days a version of ping command is provided by most systems which can create a string of echo-request and echo-reply messages for providing statistical information.
- It is also possible to check whether a node is functioning properly or not with the help of the echo-request echo reply pair of messages. The format of the echo request echo reply pair of messages is as shown in Fig. 1.



- In Fig. 1, the protocol does not formally define the identifier and sequence number fields. Therefore the sender can use them in an arbitrary manner.

(G-2113) Fig. 1 : Echo request and echo reply messages

□□□

TechKnowledge
Publications

Unit V

Chapter

8

Routing Algorithms

Syllabus

Routing : Metric, Static vs dynamic routing tables, Routing protocol, Unicast routing protocols - Optimality principle, Intra and inter domain routing, Shortest path routing, Flooding, Distant vector routing, Link state routing, Path vector routing, Interior gateway routing protocol - OSPF, EIGRP, RIP, Exterior gateway routing protocol – BGP.

Case study : Case study on network simulation tools such as packet tracer.

Chapter Contents

8.1 Routing	8.11 Routing Protocols
8.2 Routing Algorithms	8.12 RIP (Routing Information Protocol)
8.3 Static Algorithms	8.13 Request and Response Messages (RIP)
8.4 Dynamic Routing Algorithms	8.14 RIP Version 2
8.5 Distance Vector Routing Algorithm	8.15 OSPF
8.6 Link State Routing	8.16 Border Gateway Protocol (BGP)
8.7 Hierarchical Routing	8.17 BGP Sessions
8.8 Least Cost Algorithms	8.18 Interior Gateway Routing Protocol (IGRP)
8.9 Path Vector Routing	8.19 Enhanced IGRP (EIGRP)
8.10 Unicast Routing Protocols	



8.1 Routing :

SPPU : March 19

University Questions

Q. 1 Understand and apply what is routing ? Explain different types of routing algorithm.

(March 19, 6 Marks)

- Routing is a very important issue in the network layer. A router creates its routing table so as to help forwarding a datagram in the connectionless services.
- It also helps in creating a virtual circuit in the connection oriented service.
- In the following sections we are going to discuss about the types of routing and different routing algorithms such as distance vector routing, link state routing and hierarchical routing.

8.1.1 Types of Routing :

- Routing can be broadly classified into three types :
 1. Unicast routing.
 2. Broadcast routing
 3. Multicast routing.
- We can also classify the routing into two types as follows :
 1. Intradomain routing.
 2. Interdomain routing.

8.1.2 Intra and Interdomain Routing :

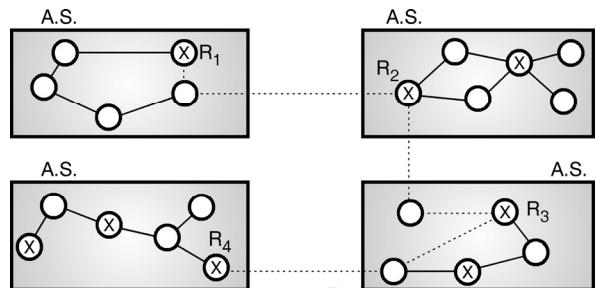
SPPU : May 12

University Questions

Q. 1 Explain the difference between interdomain and intradomain routing protocols with example.

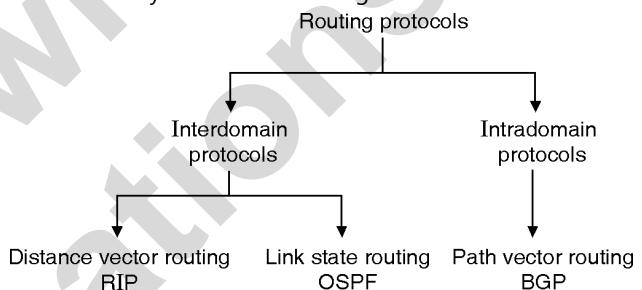
(May 12, 8 Marks)

- Today the size of the Internet is so big that one routing protocol cannot handle the task of updating the routing tables of all the routers.
- Hence an internet is divided into **Autonomous Systems (AS)**.
- An Autonomous System (AS) is a group of networks and routers which is controlled by a single administrator. An AS is shown in Fig. 8.1.1.



(G-1292) Fig. 8.1.1 : Autonomous systems

- The **intradomain routing** is defined as the routing inside an autonomous system whereas the routing between autonomous system is known as the **interdomain routing**.
- Several intradomain and interdomain protocols are used. They are as shown in Fig. 8.1.2.



(G-1291) Fig. 8.1.2 : Classification of routing protocols

- The examples of interdomain routing protocols are :
 1. Distance vector routing
 2. Link state routing.
- An example of intradomain routing protocol is path vector routing.
- Each A.S. is allowed to choose one or more intradomain routing protocols in order to handle the routing inside the A.S.
- But only one interdomain routing protocol will handle routing between autonomous systems.
- The Routing Information Protocol (RIP) is an implementation of distance vector routing.
- Whereas the OSPF is an implementation of link state protocol. The BGP is an implementation of the path vector protocol.

Difference between intra and interdomain routing :

SPPU : May 08

University Questions

Q. 1 Explain the difference between Interdomain and Intradomain routing protocols. Justify your answer by taking an example of each type of protocol.

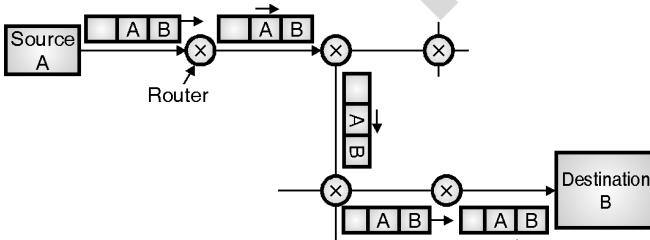
(May 08, 8 Marks)



- In routing, the problems of scale and administrative autonomy can be solved by organizing routers into Automatic Systems (AS).
- Each AS consists of a group of routers that are under the same administrative control.
- Routers within the same AS run the same routing algorithm such as Link state or Distance Vector algorithms.
- The routing algorithm running within an AS is called as intra-autonomous system protocol or intra-domain routing protocol.
- There can be a large number of ASs connected to each other. The task of inter-connecting them is handled by the inter-autonomous system protocol or inter domain routing protocol.
- The example of intradomain routing protocol is RIP. Refer section 8.12 for RIP.
- The example of interdomain routing protocol is OSPF. Refer section 8.15 for OSPF.

8.1.3 Unicast Routing :

- In unicast routing there is a one to one relation between the source and the destination.
- That means only one source sends packets to only one destination.
- The type of source and destination addresses included in the IP datagram are unicast addresses assigned to the hosts.
- The concept of unicast routing is illustrated in Fig. 8.1.3.



(G-448) Fig. 8.1.3 : Unicast routing

- In unicast routing when a router receives a packet, it forwards that packet through only one of its ports which corresponds to the optimum path.
- The router can discard the packet if it cannot find the destination address.

Metric :

- A metric is defined as the cost assigned for passing through a network.
- The metric assigned to each network depends on the type of protocol.

Interior and exterior routing :

- An Internet is so large that for one routing protocol it is impossible to handle the task of updating the routing tables of all the routers.
- So an Internet is divided into a number of Autonomous Systems (AS). An AS is group of networks and routers.

Interior routing :

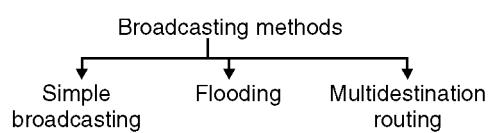
- The routing that takes place inside an AS is called as interior routing.

Exterior routing :

- The routing that takes place among various autonomous systems is called as exterior routing.

8.1.4 Broadcast Routing :

- In certain applications, the host has to send packets to many or all other hosts.
- If the sender sends a packet to all destinations simultaneously then it is called as **broadcasting**.
- Various methods of broadcasting are as follows :



(G-449) Fig. 8.1.4 : Various methods of broadcasting

1. Simple broadcasting :

- In this method the source will simply send a distinct (a separate) packet to each destination.
- This method has two drawbacks :
 1. A lot of bandwidth is wasted.
 2. The source has to have a complete list of all destinations.

2. Flooding :

- Flooding is another method used for broadcasting. The problem with flooding is that it has a point to point routing algorithm.
- So it consumes a lot of bandwidth and generates too many packets.



3. Multidestination routing :

- This is the third algorithm used for broadcasting.
- In this algorithm each packet will contain a list of destinations or a bit map which indicates the desired destination.
- When such a packet arrives at a router, the router first checks all the destinations.
- Then it decides the set of output lines that will be required based on the destination addresses.
- The router then generates a new copy of the received packet for each output line to be used.
- It includes a list of only those destinations that are to use the line in each packet going out on that line.
- This will save bandwidth to a great extent. Also generation of too many packets right from the sending end will also be avoided.

8.1.5 Multicast Routing :

- In multicasting a message from a sender is to be sent to a group of destinations but not all the destinations in a network.
- A process has to send a message to all other processes in the group. For a small group it is possible to send a point-to-point message.
- But this is expensive if the group is large. So we have to send messages to a well defined groups which are small compared to the network size.
- Sending message to such a group is called **multicasting** and the routing algorithm used for multicasting is **multicast routing**.
- Multicast routing is a special class of broadcast routing.

8.2 Routing Algorithms :

SPPU : Dec. 12, Dec. 13

University Questions

Q. 1 What is routing ? State different types of routing. Write properties of routing algorithm.
(Dec. 12, 8 Marks)

Q. 2 What is routing ? State different types of routing. Explain two interior gateway routing protocols.
(Dec. 13, 8 Marks)

- One of the important functions of the network layer is to route the packets from the source machine to the destination machine.
- The major area of network layer design includes the algorithms which choose the routes and the data structures which are used.
- **Routing algorithm** is a part of network layer software. It is responsible for deciding the output line over which a packet is to be sent.
- Such a decision is dependent on whether the subnet is a virtual circuit or it is datagram switching.

8.2.1 Desired Properties of a Routing Algorithm :

SPPU : Dec. 12

University Questions

Q. 1 What is routing ? State different types of routing. Write properties of routing algorithm.
(Dec. 12, 8 Marks)

- There are certain desirable properties of a routing algorithm as follows :
- | | |
|----------------|-----------------|
| 1. Correctness | 2. Robustness |
| 3. Stability | 4. Fairness and |
| 5. Optimality. | |

8.2.2 Types of Routing Algorithms :

SPPU : Dec. 12, Dec. 13

University Questions

Q. 1 What is routing ? State different types of routing. Write properties of routing algorithm.
(Dec. 12, 8 Marks)

Q. 2 What is routing ? State different types of routing. Explain two interior gateway routing protocols.
(Dec. 13, 8 Marks)

- Routing algorithms can be divided into two groups :
 1. Non-adaptive algorithms.
 2. Adaptive algorithms.
- 1. Non-adaptive algorithms :**
 - For this type of algorithms, the routing decision is not based on the measurement or estimation of current traffic and topology.
 - However the choice of the route is done in advance, off-line and it is downloaded to the routers.
 - This is called as static routing.



2. Adaptive algorithms :

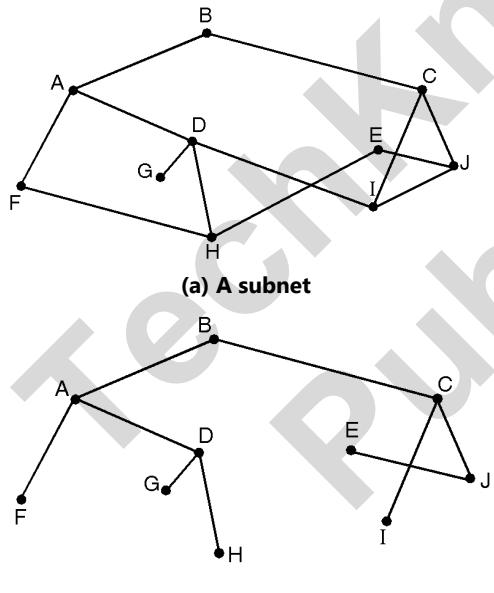
- For these algorithms the routing decision can be changed if there are any changes in topology or traffic etc.
- This is called as dynamic routing.
- In the following sections we are going to discuss various static and dynamic algorithms.

8.2.3 Optimality Principle :

- A general statement about optimality is called as optimality principle.
- It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K will also be along the same route.

Sink tree :

- A set of optimal routes from all the sources to a given destination form a tree called sink tree and it is shown in Fig. 8.2.1.



(G-450) Fig. 8.2.1

- The root of the sink tree is at the destination.
- Note that a sink tree need not be unique. Other trees with the same path lengths may also exist.
- All the routing algorithms are supposed to discover and use the sink trees for all routers.
- In the sink tree of Fig. 8.2.1, the distance metric is the number of hops. In Fig. 8.2.1(b) a sink tree for router B has been shown.

- The paths from B to every router with minimum number of hops.

8.3 Static Algorithms :

SPPU : March 19

University Questions

- Q. 1** Understand and apply what is routing ? Explain different types of routing algorithm.

(March 19, 6 Marks)

- The examples of static algorithms are :
 1. Shortest path routing.
 2. Flooding.
 3. Flow based routing.

8.3.1 Shortest Path Routing :

- This algorithm is based on the simplest and most widely used principle. Here a graph of subnet is prepared in which each node represents either a host or a router and each arc represents a communication link.
- So as to choose a path between any two routers, this algorithm simply finds the shortest path between them.

How to decide the shortest path ?

- One way of measuring the path length is the number of hops.
- Another way (metric) is the geographical distance in kilometres.
- Some other metrics are also possible.
- For example we can label each arc (link) with the mean queuing and transmission delay and obtain the shortest path as the fastest path.

Labels on the arcs :

- The labels on the arcs can be computed as a function of distance bandwidth, average traffic, mean queue length, cost of communication, measured delay etc.
- The algorithm compares various parameters and calculates the shortest path, on the basis of any one or combination of criterions stated above.

Various shortest path algorithms :

- There are many algorithms for computing the shortest path between two nodes.
- One of them is Dijkstra algorithm. The other one is Bellman-Ford algorithm.



8.3.2 Flooding :

- This is another static algorithm.
- In this algorithm every incoming packet is sent out on every outgoing line except the line on which it has arrived.
- That is why the name flooding. Each line except the incoming lines are flooded with the copies of the same packet.
- One disadvantage of flooding is that it generates a large number of duplicate packets.
- In fact it produces infinite number of duplicate packets unless we somehow stop the process.
- There are various damping techniques such as :
 1. Using a hop counter.
 2. To keep a track of which packets have been flooded.
 3. Selective flooding.
- To prevent endless copies of packets circulating for very long time through the network a hop count may be used to suppress onwards transmission of packets after a number of hops which exceed the network "diameter".
- The other problem is that destination must be prepared to receive multiple copies of an incoming packet.
- Flooding has two interesting characteristics that arise from the fact that all possible routes are tried :
 1. As long as there is a route from source to destination the packet will be definitely delivered to the destination.
 2. One copy of the packet will reach the destination via the quickest possible route.

Selective flooding :

- This is slightly more practical type of flooding principle.
- In this algorithm every incoming packet is not sent out on every output line.
- Instead packet is sent only on those lines which are likely to go in the desired direction.

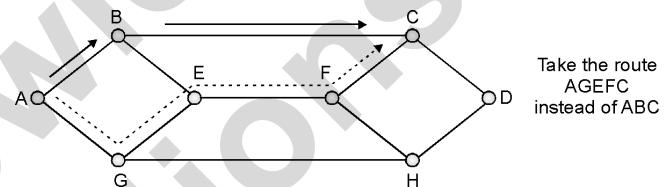
Applications of flooding :

- Flooding does not have many practical applications.
- But it is useful in military applications where a large number of routers are blown into pieces (damaged) at any instant.

- So placing a packet on every outgoing line really makes sense.
- In such applications robustness of flooding is very much desirable.
- Second application is in the distributed database applications.
- Flooding always chooses the shortest path so it produces the shortest possible delay.

8.3.3 Flow Based Routing :

- This is a static algorithm which uses topology and load condition (traffic) for deciding a route.
- For example in Fig. 8.3.1, there is always a huge traffic from A to B.



(G-462) Fig. 8.3.1 : Flow based routing

- Then the traffic from A to C should not be routed through B.
- Instead route it through AGEFC even though it is a longer path than ABC. This is called as a **flow based routing**.
- It is possible to optimise the routing by analysing the data flow mathematically.
- This is possible if the average traffic from one node to the other is known in advance and it is constant in time.
- The mathematical analysis is based on idea that for a given line if the capacity and average data flow are known, then it is possible to calculate the mean packet delay using the Queueing theory.
- From the mean delays on all the lines it is possible to calculate the mean packet delay for the whole subnet.
- To use the technique of flow based routing, the following information should be known in advance :
 1. Subnet topology
 2. Traffic matrix.
 3. Line capacity matrix which specifies capacity of each line.



8.4 Dynamic Routing Algorithms :

SPPU : March 19

University Questions

Q. 1 Understand and apply what is routing ? Explain different types of routing algorithm.

(March 19, 6 Marks)

- The modern computer networks normally use the dynamic routing algorithms.
- Two dynamic routing algorithms namely distance vector routing and link state routing are used popularly.
- Both these algorithms are suitable for the packet switched networks.
- Both these algorithms assume that a router knows the address of each neighbouring router and the cost of reaching each neighbour.
- In the distance vector routing, each node tells its neighbours about its distance to every other node in the network.
- In the link state routing, a node tells every other node in the network the distance to its neighbours.
- So both these routing algorithms are distributed type and so they are suitable for large internetworks.

8.5 Distance Vector Routing Algorithm :

SPPU : May 06, Dec. 16, March 19

University Questions

Q. 1 Discuss one distance vector routing protocol and one link state routing protocol. (May 06, 8 Marks)

Q. 2 Explain distance vector routing with count to infinity problem. (Dec. 16, March 19, 6 Marks)

- In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there.
- This algorithm is sometimes called by other names such as :
 1. Distributed Bellman-Ford routing algorithm.
 2. Ford-Fulkerson algorithm
- In distance vector routing, each router maintains a routing table.
- It contains one entry for each router in the subnet.
- This entry has two parts :

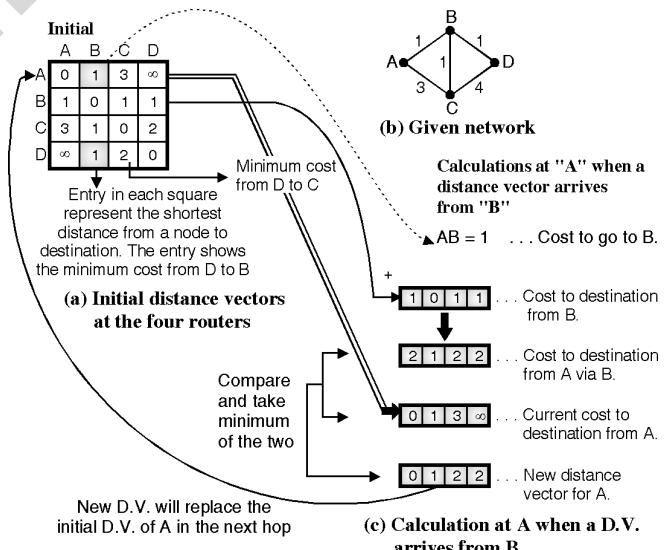
1. The first part shows the preferred outgoing line to be used to reach the specific destination.
2. Second part gives an estimate of the time or distance to that destination.

Distance vector :

- In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest path to each router is not known.
- A **distance vector** is defined as the list of <destination, cost> tuples, one tuple per destination.
- Each router maintains a distance vector.
- The cost in each tuple is equal the sum of costs on the shortest path to the destination.

Updation of router tables :

- A router periodically sends a copy of its distance vector to all its neighbours.
- When a router receives a distance vector from its neighbour, it tries to find out whether its cost to reach any destination would decrease if it routed packets to that destination through that particular neighbouring router. This is illustrated in Fig. 8.5.1.
- Fig. 8.5.1 shows how the D.V. at A is automatically modified when a D.V. is received from B.



(G-463) Fig. 8.5.1 : Distance vector algorithm at router A

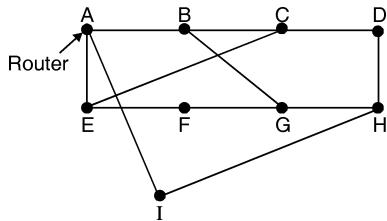
- A similar calculation takes place at the other routers as well.
- So the entries at every router can change. In Fig. 8.5.1(a) the initial distance vector is shown.



- The entries indicate to the costs corresponding to the shortest distance between the routers indicate to that square.
- For example, AC = 3 indicates the cost corresponding to the shortest path in terms of number of hops from A to C.
- Even if nodes asynchronously update their distance vectors the routing tables eventually converge.
- The well known example of distance vector routing is the Bellman-Ford algorithm.

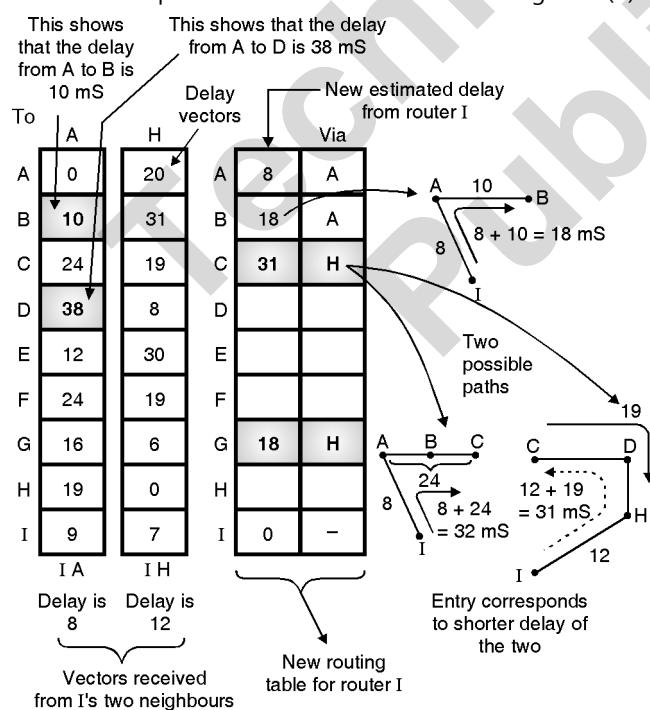
Routing procedure in distance vector routing :

- The example of a subnet is shown in Fig. 8.5.2(a) and the routing tables are shown in Fig. 8.5.2(b).



(G-464) Fig. 8.5.2(a) : A subnet

- The entries in router tables of Fig. 8.5.2(b) are the delay vectors.
- For example consider the shaded boxes of Fig. 8.5.2(b).

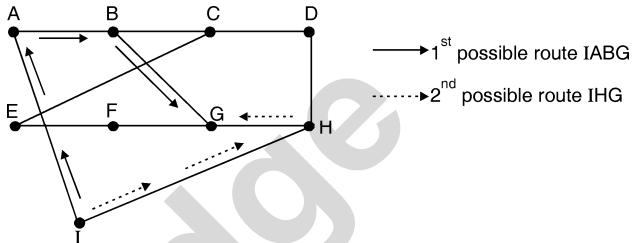


(G-465) Fig. 8.5.2(b) : Routing tables

- The entry in the first shaded box shows that the delay from A to B is 10 msec, whereas the entry in the other

shaded box indicates that the delay from A to D is 38 msec.

- Consider how router I computes its new route to router G. Fig. 8.5.2(c) shows the two possible routes between I and G.



(G-466) Fig. 8.5.2(c)

- I knows that the reach G via A, the delay required is :

(L-891)

$$\begin{aligned} \text{I to A} & \quad \text{Delay} = 8 \text{mS} \\ \text{A to G} & \quad \text{Delay} = 16 \text{mS} \end{aligned} \quad \therefore \text{I to G} \quad \text{Delay} = 8 + 16 = 24 \text{ msec}$$

Whereas the delay between I and G via H (route IHG) is :

(L-892)

$$\begin{aligned} \text{I to H} & \quad \text{Delay} = 12 \text{mS} \\ \text{H to G} & \quad \text{Delay} = 6 \text{mS} \end{aligned} \quad \therefore \text{I to G} \quad \text{Delay} = 12 + 6 = 18 \text{ msec}$$

- The best of these values is 18 msec corresponding to the path IHG.
- Hence it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H.
- The new routing table for router I is shown in Fig. 8.5.2(b).
- Similarly we can calculate the delays, from I to different destinations from A to I and enter the minimum possible delay into the I's router table.

8.5.1 Disadvantages :

- The distance vector routing takes a long time in converging to the correct answer.
- This is due to a problem called count-to-infinity problem. This problem can be solved by using the split horizon algorithm.
- Another problem is that this algorithm does not take the line bandwidth into consideration when choosing a root.
- This is a serious problem due to which this algorithm was replaced by the Link State Routing algorithm.

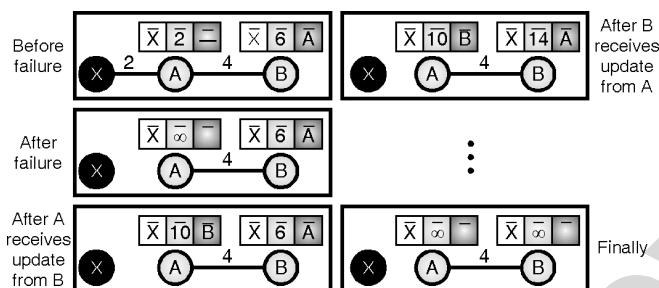


8.5.2 Looping in Distance Vector Routing Protocol :

- A problem in distance vector routing is its instability.
- A network using this protocol can become unstable.

Two node loop instability :

- A network with three nodes has been shown in Fig. 8.5.3.
- Note that the routing tables are shown partially for discussion.



(G-1499) Fig. 8.5.3 : Two node loop instability

- At the beginning both nodes A and B know how to reach node X.
- But the link joining A and X fails suddenly. So node A changes its table.
- If A could send its changed routing table to B immediately, everything is okay. No problem will occur.
- But the system becomes unstable if B sends its routing table to A before receiving A's routing table.
- This is because node A receives the updated B's routing table and assumes that B has found a new path to reach node X.
- So A immediately updates its routing table (which is incorrect).
- Based on this update now A sends its new update to B. Now B thinks that something has changed around A and so it updates its routing table.
- Due to this process, the cost of reaching X increases gradually and finally becomes infinite.
- At this moment both A and B understand that now it is impossible to reach X.
- Note that during this entire time the system is unstable.
- A thinks that the route to X goes via B whereas B thinks that the route is via node A.

- So if A receives a packet for X, it goes to B and then again returns back to A.
- Similarly if B receives a packet destined for X, it goes to A and returns back to B.
- This bouncing of packets between nodes A and B is known as the **two-node loop problem**.
- This problem can be solved by using one of the following strategies :
 1. Defining infinity
 2. Split horizon
 3. Split horizon and poison reverse.
- There is a similar problem called three node loop problem present in the system using distance vector routing.

8.5.3 Count to Infinity Problem :

SPPU : Dec. 16, March 19

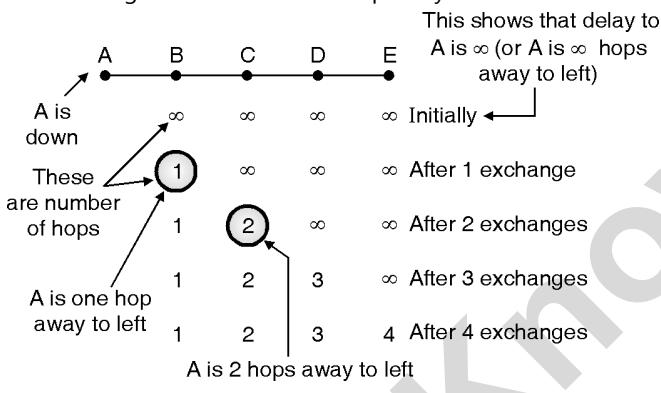
University Questions

Q. 1 Explain distance vector routing with count to infinity problem. (Dec. 16, March 19, 6 Marks)

- Theoretically the distance vector routing works properly but practically it has a serious problem.
- The problem is that we get a correct answer but we get it slowly.
- In other words it reacts quickly to good news but it reacts too slowly to bad news.
- Consider a router whose best route to destination X is large.
- If on the next exchange neighbour A suddenly reports a short delay to X, the router will switch over and start using the line to A for sending the traffic to destination X.
- Thus in one vector exchange, the good news is processed.
- Let us see how fast does a good news propagate.
- Consider a linear subnet of Fig. 8.5.4 which has five nodes. The delay metric used is the number of hops.
- Assume that A is initially down and that all the other routers know this.



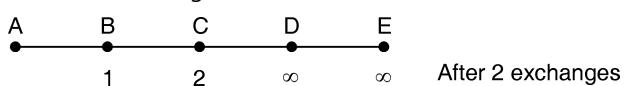
- So all the routers have recorded that the delay to A is infinity.
- When A becomes OK, the other routers come to know about it via the vector exchanges.
- Then suddenly a vector exchange at all the routers will take place simultaneously.
- At the time of first vector exchange, B comes to know that its left neighbour has a zero delay to A.
- So as shown in Fig. 8.5.4(a). B makes an entry in its routing table that A is one hop away to the left.



(G-467) Fig. 8.5.4(a)

- All the other routers still think that A is down. So in the second row of Fig. 8.5.4(a), the entries below C D E are ∞ .
- On the second vector exchange, C comes to know that B has a path of 1 hop length to A, so C updates its routing table and indicates a path of 2 hop length.
- But D and E do not change their table entries.
- So after the second vector exchange the entries in the third row of Fig. 8.5.4(a) are :

(G-468(a))



- Similarly D and E will update their routing tables after 3 and 4 exchanges respectively.
- So we conclude that the good news of A has recovered has spread at a rate of one hop per exchange.

Explanation of Fig. 8.5.4(b) :

- Now refer Fig. 8.5.4(b). Here initially all routers are OK.

A	B	C	D	E	
1	2	3	4		Initially \leftarrow All routers are initially ok
3	2	3	4		After 1 exchange
3	4	3	4		After 2 exchanges
5	4	5	4		After 3 exchanges
5	6	5	6		After 4 exchanges
7	6	7	6		After 5 exchanges
7	8	7	8		After 6 exchanges
∞	∞	∞	∞		

(G-468) Fig. 8.5.4(b)

- The routers B, C, D and E have distances of 1, 2, 3 and 4 respectively to A.
- So the first row of Fig. 8.5.4(b) is as follows :

A	B	C	D	E	
1	2	3	4		Initially \leftarrow First row of above figure

These are distances of B,C,D,E to A

- Now imagine that suddenly A goes down or line between A and B is cut.
- At the first packet exchange B does not hear anything from A (because A is down). But C says " I have a path of length 2 to A".
- But poor B does not understand that this path is through B itself.
- So B thinks that it can reach A via C with a path length 3. (B to C 1 hop and C to A 2 hops) so it accordingly updates its routing table. But D and E do not update their entries.
- So the second row of Fig. 8.5.4(b) looks as follows :

A	B	C	D	E	
1	2	3	4		Initially
3	2	3	4		After 1 exchange

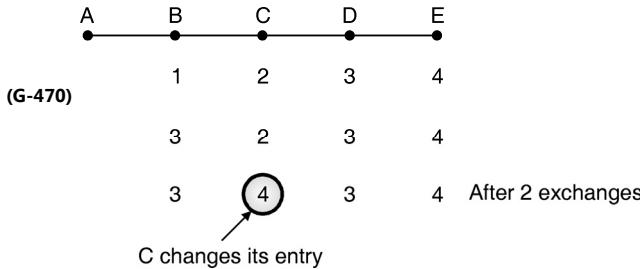
Updated entry No change

(G-469)

- On the second exchange C realizes that both its neighbours (B and D) claim to have a path of length 3 to A.



- So it picks one of them at random and makes its new distance to A as 4. This is shown in row 3 of Fig. 8.5.4(b). It is repeated below.



- Similarly the other routers keep updating their tables after every exchange.
- It is expected that finally we should get ∞ in the router tables of B, C, D and E indicating that A is down.
- We do reach this state at the end in Fig. 8.5.4(b) but after a very long time.
- The conclusion is bad news propagates slowly. This problem is called as **count-to-infinity** problem.
- The solution to this problem is to use the split horizon algorithm.

8.5.4 Split Horizon Algorithm :

- To avoid the count to infinity problem, several changes in the algorithm have been suggested.
- But none of them work satisfactorily in all situations.
- One particular method which is widely implemented, is called as the **split horizon algorithm**.
- In this algorithm, the minimum cost to a given destination is not sent to a neighbour if the neighbour is the next node along the shortest path.
- For example if node A thinks that the best route to node B is via node C, then node A should not send the corresponding minimum cost to node C.

8.6 Link State Routing :

SPPU : Dec. 11, May 12, Dec. 12

University Questions

Q. 1 Explain in detail link state routing algorithms with example.

(Dec. 11, 8 Marks, May 12, 10 Marks, Dec. 12, 8 Marks)

- Distance vector routing was used in ARPANET upto 1979. After that it was replaced by the link state routing.

- Variants of this algorithm are now widely used.
- The link state routing is simple and each router has to perform the following five operations.

Router operations :

1. Each router should discover its neighbours and obtain their network addresses.
 2. Then it should measure the delay or cost to each of these neighbours.
 3. It should construct a packet containing the network addresses and the delays of all the neighbours.
 4. Send this packet to all other routers.
 5. Compute the shortest path to every other router.
- The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
 - Then a shortest path algorithm such as Dijkshtra's algorithm can be used to find the shortest path to every other router.

Protocols :

- Link state routing is popularly used in practice.
- The OSPF protocol which is used in the Internet uses the link state algorithm.
- IS-IS i.e. Intermediate system – Intermediate system is the other protocol which uses the link state algorithm.
- IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

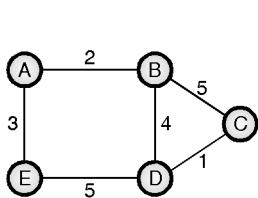
Building a routing table in link state routing :

Link state routing :

- Now we will discuss the development of routing table in link state routing.
- Here the term **link state** is used for defining the characteristic of a link or edge, which represents a network in the Internet. The **cost** associated with each link is important.
- The links having lower costs are preferred to the links having higher costs.
- A nonexisting or broken link is indicated by an ∞ cost. In this method, each node must have a complete map of the network.
- That means each node should have complete information about the state of each link.



- The collection of states of all the links in an Internet is called as **Link-State Database (LSDB)**.
- For the entire Internet, there is only one LSDB and its copy is available with each node.
- Each node uses it to create the least cost tree. The example of LSDB is as shown in Fig. 8.6.1(b) for the Internet shown in Fig. 8.6.1(a).
- The next step is creation of LSDB (which contains all the information about the Internet) at each node.



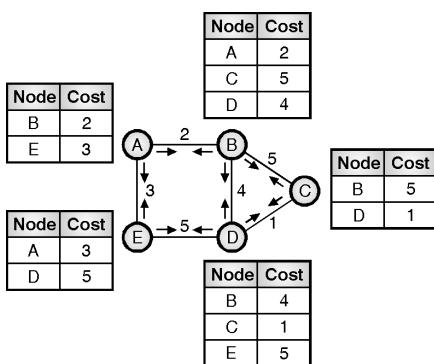
(a) Internetwork

	A	B	C	D	E
A	0	2	∞	∞	3
B	2	0	5	4	∞
C	∞	5	0	1	∞
D	∞	4	1	0	5
E	3	∞	∞	5	0

(b) Link state database (LSDB)

(G-2201) Fig. 8.6.1

- This can be achieved by a process called **flooding**.
- Each node sends a greeting message to all its immediate neighbours,
- so as to collect two important pieces of information as follows :
 - The identity of the neighbouring node.
 - Cost of the link.
- The packet containing this information is called as **LS Packet (LSP)**, which is sent out of each interface.
- After receiving all the new LSPs each node will create the comprehensive LSDB as shown in Fig. 8.6.1(c).
- This LSDB is same for each node which shows the whole map of the internet.
- That means a node can use the LSDB to make the whole map of the Internet.



(G-2202) Fig. 8.6.1(c)

8.6.1 Comparison of Link State Routing and Distance Vector Routing :

SPPU : May 09, Dec. 09, May 13, May 16, Dec. 18

University Questions

- Q. 1** Differentiate between distance vector routing and link state routing.
(May 09, Dec. 09, May 13, 8 Marks)
- Q. 2** Compare link state routing and distance vector routing.
(May 16, 4 Marks)
- Q. 3** Compare and contrast distance vector routing with link state routing.
(Dec. 18, 4 Marks)

Sr. No.	Distance vector routing	Link state routing
1.	Each router maintains routing table indexed by and containing one entry for each router in the subnet.	It is the advanced version of distance vector routing
2.	Algorithm took too long to converge.	Algorithm is faster.
3.	Bandwidth is less.	Wide bandwidth is available.
4.	Router measure delay directly with special ECHO packets.	All delays measured and distributed to every router.
5.	It doesn't take line bandwidth into account when choosing the routes.	It considers the line bandwidth into account when choosing the routes.

8.7 Hierarchical Routing :

SPPU : Dec. 07, May 12

University Questions

- Q. 1** Explain the hierarchical routing with suitable example.
(Dec. 07, 6 Marks, May 12, 10 Marks)

- As the size of the network increases, the size of the routing tables of the routers also increases.
- As a result of large routing tables, the router memory is consumed to a great extent, more CPU time is needed to scan the tables and more bandwidth is required to send status report about the tables.



- Sometimes the network becomes so large that the size of the router table becomes excessively large and practically it becomes impossible for every router to have an entry for all the other routers except itself.
- Then the hierarchical routing such as the one used in telephone networks should be used.
- In this type of routing the total number of routers are divided into different **regions**.
- A router will know everything about the all other belonging to its own region only.
- It does not know anything about the internal structure of other regions.
- This reduces the size of the router table.
- When various networks are connected together, each network is treated as a separate region.
- For very large networks the hierarchy is prepared as follows :

Level 1 : Regions

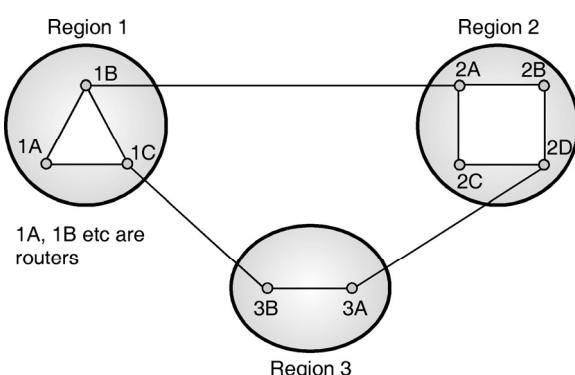
Level 2 : Clusters : It is a group of regions.

Level 3 : Zones : Zone is a group of clusters.

Level 4 : Groups : Group contains many zones.

8.7.1 Two Level Hierarchical Routing :

- For networks of smaller size, a two level hierarchical routing is sufficient.
- Fig. 8.7.1(a) shows network containing 3 regions.
- Fig. 8.7.1(b) shows the full routing table of router 1A which has 9 entries because in all there are 9 routers.



(G-471) Fig. 8.7.1(a) : A network

Full routing table for 1A

Destination	Line	Hops
1 A	-	-
1 B	1 B	1
1 C	1 C	1
2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

(G-2304) Fig. 8.7.1(b) : Full routing table for router 1A

- Now with a two level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in Fig. 8.7.1(c). This table has only 5 entries.

Hierarchical routing table for 1A

Destination	Line	Hops
1 A	-	-
Region 1	1 B	1
	1 C	1
	2 A	2
Region 3 → 3	1 B	2
	1 C	2

(c) Hierarchical routing table for router 1A

(G-2305) Fig. 8.7.1

- In the hierarchical table of Fig. 8.7.1(c), there are entries for all local routers (1 A, 1 B and 1 C) belonging to the region of 1 A as before. But there are no detailed entries for the other regions.
- Instead all other regions have been compressed into a single router per region.
- For example traffic from 1A to any router in region-2 is via 1 B-2 A line as shown by the shaded entry in Fig. 8.7.1(c).
- Similarly all the traffic from 1A to region 3 is routed through the line 1C-3B.
- Comparison of Figs. 8.7.1(b) and (c) shows how hierarchical routing reduces the size of routing tables.

**Disadvantage :**

- The reduced table size has a price tag attached to it. It comes at the expense of increased path length.
- But it is practically acceptable.

How many levels a hierarchy should have ?

- Kamoun and Kleinrock have discovered that for an N router subnet, the optimum number of hierarchy levels is $\log_e N$ and it requires a total of $\log_e N$ entries per router table.

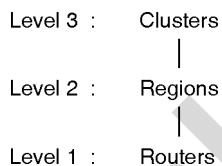
Ex. 8.7.1 : For hierarchical routing with 4800 routers, what region and cluster sizes should be chosen to minimize the size of the routing table for a three-layer hierarchy ?

May 11, 8 Marks

Soln. :

- The three level hierarchy has got the three levels as shown in the following diagram.

(L-910)



- If the number of clusters is x, number of regions per cluster is y, and the number of routers in each region is z then the each router needs z entries for the local routers, $(y - 1)$ entries for routing to other regions within its own cluster and $(x - 1)$ entries for distant clusters.

∴ Total number of entries in the router table

$$= (x - 1) + (y - 1) + z = x + y + z - 2$$

8.8 Least Cost Algorithms :

- We have already defined the term **cost** associated with a link and the factors affecting / deciding its value.
- These link costs or hop costs are used as inputs to a least cost routing algorithm.

Principle :

- The principle of least cost routing algorithms is as follows :
- If there is a network of nodes connected by bidirectional links, where each link as a cost associated with it in each direction, the cost of a path between two nodes is defined as the sum of cost of links traversed. For each pair of nodes find the path with least cost.

Examples :

- The well known examples of least cost routing algorithms are :
 1. Dijkstra's algorithm and 2. Bellman-Ford algorithm.

8.8.1 Bellman-Ford Algorithm :

- Let us suppose that node 1 is the "destination" node and consider the problem of finding a shortest path from every node to node 1.
- We assume that there exists at least one path from every node to the destination.
- 1. To simplify the presentation, let us denote $d_{ij} = \infty$ if (i, j) is not an arc of the graph. Using the convention we can assume without loss of generality that there is an arc between every pair of nodes, since walks and paths consisting of true network arcs are the only ones with less than ∞ .
- 2. A shortest walk from a given node i to node 1, subject to constraint that the walk contains at most 'h' arcs and goes through node 1 only once, is referred to as shortest ($\leq h$) walk and its length is denoted by D_i^h .

Note that such a walk may not be a path, that is, it may contain repeated nodes. We will later give conditions under which this is not possible.

- 3. By convention, we take

$$D_1^h = 0, \text{ for all } h$$

- We will prove that D_1^h can be generated by the iteration.

$$D_i^{h+1} = \min_j [d_{ij} + D_j^h], \text{ for all } i \neq 1 \quad \dots(8.8.1)$$

- Starting from the initial conditions,

$$D_i^0 = \infty \text{ for all } i \neq 1 \quad \dots(8.8.2)$$

- This is the Bellman Ford algorithm illustrated in Fig. 8.8.1.

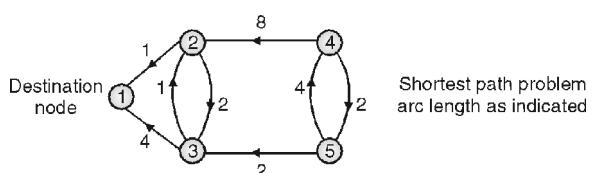
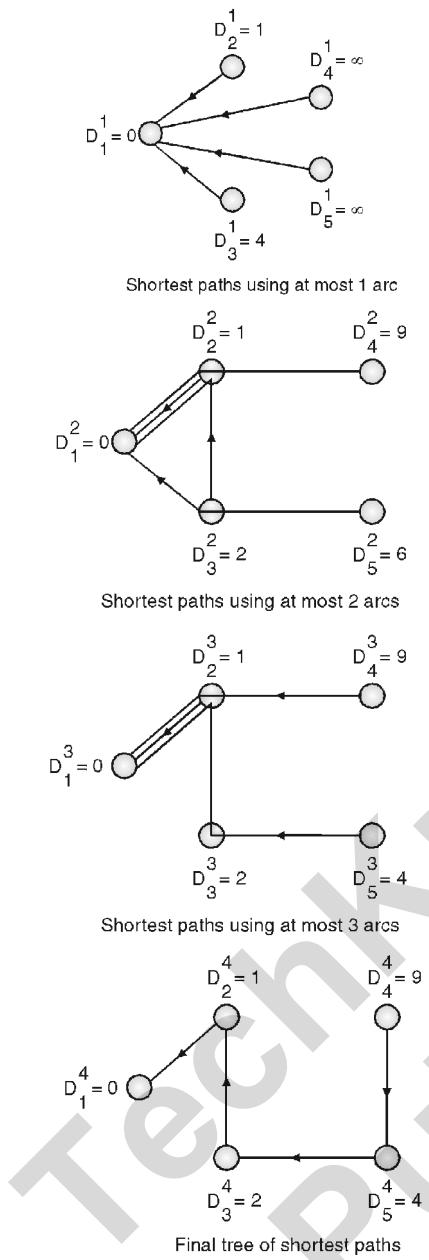


Fig. 8.8.1 (Contd...)



(G-1376) Fig. 8.8.1 : Successive iterations of the Bellman-Ford method

- Thus Bellman Ford algorithm first finds the one-arc shortest walk lengths, then find the two-arc shortest path lengths and so forth.
- In this example, the shortest ($\leq h$) walks are paths because all arc lengths are positive and therefore all cycles have positive length.
- The shortest paths are found after $N - 1$ iterations, which is equal to 4 in this example.

- Once we show this, we will argue that the shortest walk lengths are equal to shortest path lengths, under the additional assumption that all cycles not containing node 1 have non-negative length.
- We say that the algorithm terminates after ' h ' iterations if,

$$D_i^h = D_i^{h-1}, \text{ for all } i$$

The following proposition provides the main result.

6. Proposition :

- Consider the Bellman-Ford algorithm Equation (8.8.1) with initial conditions $D_i^0 = \infty$ for all $i \neq 1$. Then
 - The scalars D_i^h generated by the algorithm are equal to the shortest ($\leq h$) walk lengths from node i to node 1.
 - The algorithm terminates after a finite number of iterations if and only if all cycles not containing node 1 have non-negative length. Furthermore, if the algorithm terminates, it does so after at most $h \leq N$ iterations and at termination, D_i^h is the shortest path length from i to 1.

Proof :

- We argue by induction. From Equation (8.8.1) and (8.8.2) we have,

$$D_i^1 = d_{i1}, \text{ for all } i \neq 1$$

- So D_i^1 is indeed equal to shortest (≤ 1) walk length from i to 1. Suppose that D_i^k is equal to shortest ($\leq k$) walk length from i to 1 for all $k \leq h$. We will show that D_i^{h+1} is the shortest ($\leq h + 1$) walk length from i to 1. Indeed, a shortest ($\leq h + 1$) walk from i to 1 either consists of less than $h + 1$ arcs, in which case its length is equal to D_i^h , or else it consists of $h + 1$ arcs with the first arc being (i, j) for some $j \neq 1$, followed by an $h - 1$ arc walk from j to 1 in which node 1 is not repeated.
- The latter walk must be a shortest ($\leq h$) walk from j to 1 [otherwise by concatenating arc (i, j) and a shorter ($\leq h$) walk from j to 1, we would obtain a shorter ($\leq h + 1$) walk from i to 1] we thus conclude that,
- Shortest ($\leq h + 1$) walk length = $\min \{D_i^h, \min_{j \neq 1} [d_{ij} + D_j^h]\}$

...(8.8.3)



- Using the induction hypothesis, we have $D_j^k \leq D_j^{k-1}$ for all $k \leq h$ [since the set of ($\leq k$) walks from node j to 1 contains the corresponding set of ($\leq k-1$) walks]

Therefore,

$$D_i^{h+1} = \min_j [d_{ij} + D_j^h] \leq \min_j [d_{ij} + D_j^{h-1}] = D_i^h \quad \dots(8.8.4)$$

- Furthermore, we have $D_i^h \leq D_i^1 = d_{i1} = d_{i1} + D_1^h$ so from Equation (8.8.3) we obtain,

- Shortest ($\leq h+1$) walk length = $\min\{D_i^h, \min_j [d_{ij} + D_j^h]\}$
 $= \min\{D_i^h, D_i^{h+1}\}$

In view of $D_i^{h+1} < D_i^h$ [Cf. Equation (38.4)] this yields

Shortest ($\leq h+1$) walk length = D_i^{h+1}

Completing the induction proof.

- (b) If the Bellman-Ford algorithm terminates after 'h' iterations, we must have

$$D_i^k = D_i^h, \text{ for all } i \text{ and } k \geq h \quad \dots(8.8.5)$$

- So we cannot reduce the lengths of the shortest walks by allowing more arcs in these walks. It follows that there cannot exist a negative-length cycle not containing node 1, since such a cycle could be repeated an arbitrarily large number of times in walks from some nodes to node 1, thereby making their length arbitrarily small and contradicting Equation (8.8.5).
- Conversely, suppose that all cycles not containing node 1 have non-negative length. Then by deleting all such cycles from shortest ($\leq h$) walks, we obtain paths of less or equal length.
- Therefore for every i and h, there exists a path that is a shortest ($\leq h$) walk from i to 1 and the corresponding shortest path length is equal to D_i^h .
- Since paths have no cycles, then it can contain at most $N - 1$ arcs. It follows that,

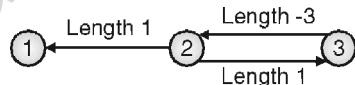
$$D_i^N = D_i^{N-1}, \text{ for all } i$$

- Implying that the algorithm terminates after at most N iterations.
- Note that the preceding proposition is valid even if there is no path from some nodes i to node 1 in the original network. Upon termination, we will simply have for those nodes $D_i^h = \infty$.

7. To estimate computation required to find the shortest path lengths, we note that in the worst case, the algorithm must be iterated N times, each iteration must be done for $N - 1$ nodes and for each node the minimization must be taken over no more than $N - 1$ alternatives. Thus the amount of computation grows at worst like N^3 , which is written as $O(N^3)$.

8. Generally, the notation $O(P(N))$, where $P(N)$ is a polynomial in N, is used to indicate a number depending on N that is smaller than $Cp(N)$ for all N, where C is some constant independent of N. Actually, a more careful accounting shows that the amount of computation is $O(mA)$, where A is the number of arcs and m is the number of iterations required for termination (m is also the maximum number of arcs contained in a shortest path).

9. The example in Fig. 8.8.2 shows the effect of negative length cycles not involving node 1 and illustrates that one can test for existence of such cycles simply by comparing D_i^N with D_i^{N-1} for each i.



(G-1377) Fig. 8.8.2 : Graph with a negative cycle. The shortest path length from 2 to 1 is 1

The Bellman-Ford algorithm gives $D_2^2 = -1$ and $D_2^3 = -1$, indicating the existence of a negative length cycle.

As implied by part (b) of the preceding proposition, there exists such a negative length cycle if and only if $D_i^N < D_i^{N-1}$ for some i.

Bellman's equation and shortest path construction :

1. Assume that all cycles not containing node 1 have non-negative length and denote by D_i the shortest path length from node i to 1. Then upon termination of Bellman-Ford algorithm, we obtain

$$D_i = \min_j [d_{ij} + D_j], \text{ for all } i \neq 1 \quad \dots(8.8.6)$$

$$D_1 = 0 \quad \dots(8.8.7)$$

This is called Bellman's equation and expresses that the shortest path length from node i to 1 is the sum of the length of the arc to the node following i on the shortest



path plus the shortest path length from that node to node 1.

2. From this equation it is easy to find the shortest paths (as opposed to the shortest path lengths) if all cycles not including node 1 have a positive length (as opposed to zero length). To do this, select for each $i \neq 1$, one arc (i, j) that attains the minimum in the equation.

$D_i = \min_j [d_{ij} + D_j]$ and consider the subgraph consisting of these $N - 1$ arcs as shown in Fig. 8.8.3.

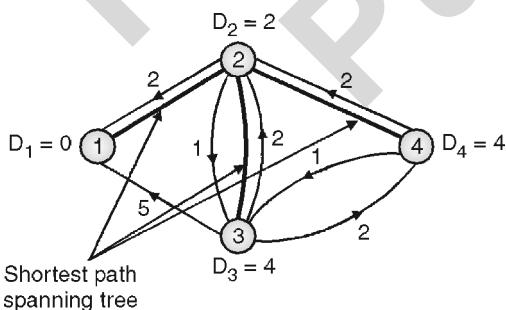
3. To find the shortest path from any node i , start at i and follow the corresponding arcs of subgraph until node 1 is reached. Note that the same node cannot be reached twice before reaching node 1, since a cycle would be formed that (on the basis of equation $D_i = \min_j [d_{ij} + D_j]$) would have zero length let $(i_1, i_2, \dots, i_k, i_1)$ be the cycle and add the equations.

$$D_{i_1} = d_{i_1 i_2} + D_{i_2} \dots D_{i_{k-1}} = d_{i_{k-1} i_k} + D_{i_k}$$

$$D_{i_k} = d_{i_k i_1} + D_{i_1}$$

Obtaining $[d_{i_1 i_2} + \dots + d_{i_k i_1}] = 0$

4. Since the subgraph connects every node to node 1 and has $N - 1$ arcs, it must be a spanning tree. We call this subgraph the shortest path spanning tree and not that it has a special structure of having a root (node 1), with every arc of the tree directed toward the root.



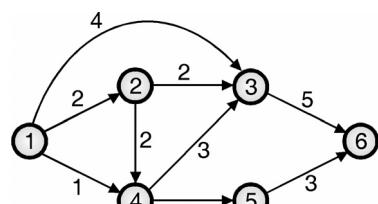
(G-1378) Fig. 8.8.3

5. Using the preceding construction, it can be shown that if there are no zero (or negative) length cycles, then Bellman's Equation (8.8.6) and (8.8.7) (viewed as a system of N equations with N unknowns) has a unique solution. This fact is useful when we consider the

Bellman-Ford algorithm starting from initial conditions other than ∞ [Cf Equation (8.8.2)].

- For a proof we suppose that \tilde{D}_i , $i = 1, \dots, N$, are another solution of Bellman's Equation (8.8.6) and (2) with $\tilde{D}_1 = 0$ and we show that \tilde{D}_i are equal to the shortest path lengths D_i . Let us repeat the path construction of the preceding paragraph with \tilde{D}_i replacing D_i .
- Then \tilde{D}_i is the length of the corresponding path from node i to node 1, showing that $\tilde{D}_i \geq D_i$. To show the reverse inequality, consider the Bellman-Ford algorithm with two different initial conditions.
- The first initial condition is $D_i^0 = \infty$, for $i \neq 1$ and $D_1^0 = 0$, in which case the true shortest path lengths D_i are obtained after at most $N - 1$ iterations, as shown earlier.
- The second initial condition is $D_i^0 = \tilde{D}_i$, for all i , in which case \tilde{D}_i is obtained after every iteration (since the \tilde{D}_i solve Bellman's equation). Since the second initial condition is, for every i , less than or equal to the first, it is seen from the Bellman-Ford iteration $D_i^{h+1} = \min_j [d_{ij} + D_j^h]$ that $\tilde{D}_i \leq D_i$ for all i .
- Therefore $\tilde{D}_i = D_i$, and the only solution of Bellman's equation is the set of the true shortest path lengths D_i . It is also possible to show that if there are zero length cycles not involving node 1, the Bellman's equation has a nonunique solution.
- It turns out that the Bellman-Ford algorithm works correctly even if the initial conditions D_i^0 for $i \neq 1$ are arbitrary numbers and the iterations are done in parallel for different nodes in virtually any order.

Ex. 8.8.1 : Apply Bellman Ford algorithm to given network as shown in Fig. P. 8.8.1 and find the least cost path between source node 1 to other nodes.



(G-1491) Fig. P. 8.8.1

**Soln. :**

Let node 1 → A, 2 → B, 3 → C, 4 → D, 5 → E, 6 → F

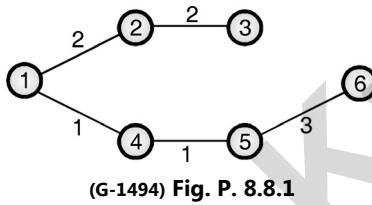
Node 1 is source node.

- Distance from node 1 to all other nodes is as shown in Table P. 8.8.1.

Table P. 8.8.1

Node	1 arc distance	2 arcs distance	3 arcs distance
A	0	0	0
B	2	-	-
C	4	4 (Due to B)	7 (Due to D)
D	1	4 (Due to B)	-
E	∞	2 (Due to D)	5 (Due to D)
F	∞	9 (Due to C)	5 (Due to E)

- Shortest path from node 1 to all other nodes using Bellman Ford algorithm is as shown in Fig. P. 8.8.1.

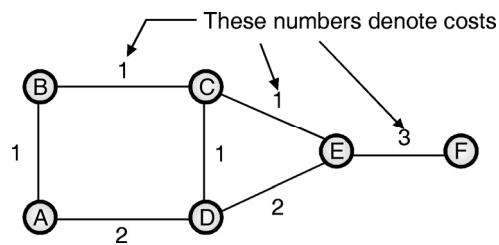
**(G-1494) Fig. P. 8.8.1****8.8.2 Dijkstra's Algorithm :**

- Dijkstra's algorithm is used for computing the shortest path from the **root** node to every other node in the network. The root node is defined as the node corresponding to the router where the algorithm is being run.
- The total number of nodes are divided into two groups namely the P group and T group. In the P group we have those nodes for which the shortest path has already been found.
- In T group the remaining nodes are placed. The path to every node in the T group should be computed from a node which is already present in group P.
- We should find out every possible way to reach an outside node by a one hop path from a node which is already present in P and choose the shortest of these paths as the path to the desired node.
- As stated earlier we define two sets P (permanent) and T (temporary) of the nodes. In set P we have nodes to which the shortest path has already been found and in

set T we have nodes to which we are considering the shortest paths.

- At the time of starting, P is initialized to the current node and T is initialized to null.
- The algorithm then repeats the following steps :
- 1. Start from the desired node say p. Write p in the P set.
- 2. For this node p, add each of its neighbours n to T set. The addition of these nodes in T will have to satisfy the following conditions :
 - If the neighbouring node (say n) is not there in T then add it annotating it with the cost to reach it through p and p's ID.
 - If n is already present in T and the path to n through p has a lower cost, then remove the earlier instance of n and add the new instance annotated with the cost to reach it through p and p's ID.
 - Pick up the neighbour n which has the smallest cost in T, and if it is not present in P then add it to P. Use its annotation to determine the router p to use to reach n.
 - Stop when T is empty.
- This algorithm will be clear after solving the following example.

Ex. 8.8.2 : For the network shown in Fig. P. 8.8.2(a), show the computations at node A using the Dijkshtra's algorithm.

**(G-451) Fig. P. 8.8.2(a) : Given network****Soln. :****Step 1 :**

- Since the computations are to be done at node A, the starting node will be A. We enter this node into group P as shown in Table P. 8.8.2(a).
- We add the neighbouring nodes B and D in group T alongwith the costs to reach them through A as shown in Table P. 8.8.2(a).

(G-451(a)) Table P. 8.8.2(a)

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)

A.



Note : B(A,1) means B is reached by A, and the cost is 1. Similarly D(A,2) means D is reached by A and the cost is 2.

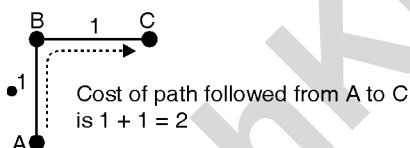
Step 2 :

- Now pick up the neighbour with the smallest cost and add it to P set. Here the neighbour with smallest cost is B. So let us add B(A,1) to P group as shown in Table P. 8.8.2(b).
- As B is added to P group, we have to add its neighbour i.e. C to the T group, as shown in Table P. 8.8.2(b).

(G-452) Table P. 8.8.2(b)

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)
A,B(A,1)	D(A,2),C(B,2)

- Note that D(A,2) has remained in T group as it is but C(B,2) is a new entry. C(B,2) means C is reached by A via B with a cost of 2. The cost is 2 due to the path followed from A to B and then to C, as illustrated in Fig. P. 8.8.2(b).



(G-453) Fig. P. 8.8.2(b)

Step 3 :

- Now pick up the neighbour in T set with the smallest cost in Table P. 8.8.2(b) and add it to the P set. Here we choose neighbour D because it is the immediate neighbour of A.
- Since D is added to P group, we have to add its neighbours i.e. C and E to the T group as shown in Table P. 8.8.2(c). Note that C(B,2) goes as it is, and E(D,4) is a new entry to Table P. 8.8.2(c). But C(D,3) can not be entered because its cost is 3.

(G-454) Table P. 8.8.2(c)

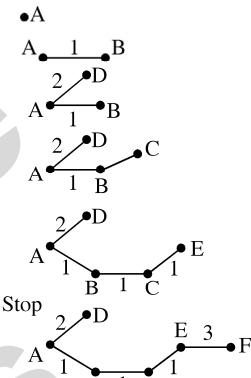
Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)
A,B(A,1)	D(A,2),C(B,2)
A,B(A,1),D(A,2)	E(D,4),C(B,2)

- Where E(D,4) means E is reached by A via D and the cost is 4.

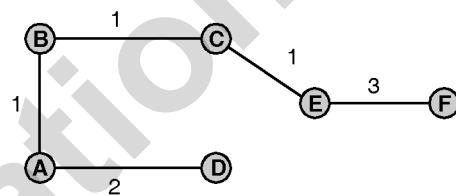
- Similarly we can proceed further. The final table is as shown in Table P. 8.8.2(d).

(G-455) Table P. 8.8.2(d) : Final table

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)
A,B(A,1)	D(A,2),C(B,2)
A,B(A,1),D(A,2)	E(D,4),C(B,2)
A,B(A,1),D(A,2)	E(C,3)
A,B(A,1),D(A,2),C(B,2)	E(D,4) can not be included
A,B(A,1),D(A,2),C(B,2)	F(E,6)
A,B(A,1),D(A,2),C(B,2)	F(E,7) can not be included
A,B(A,1),D(A,2),C(B,2),E(C,3),F(E,6)	Empty (NULL)

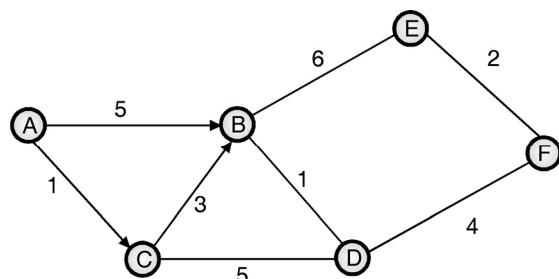


- The shortest paths from A to all other nodes are as shown in Fig. P. 8.8.2(c).



(G-456) Fig. P. 8.8.2(c) : Shortest paths from A to all other nodes

- Ex. 8.8.3 :** For the network shown in Fig. P. 8.8.3(a) show the computations at node A using the Dijkshtra's algorithm.



(G-457) Fig. P. 8.8.3(a) : Given network

Soln. :

Step 1 :

- The starting node is A. Enter it in to group P as shown in Table P. 8.8.3(a).
- Add the neighbours B and C to the temporary group T.

(G-457(a)) Table P. 8.8.3(a)

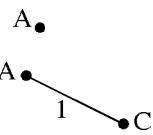
Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)

**Step 2 :**

- Now pick up the neighbour with smallest cost i.e. C and add it to group P.
- As C is added to P group, we have to add D i.e. the neighbour of C to the T group as shown in Table P. 8.8.3(b).

(G-458) Table P. 8.8.3(b)

Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)
A, C(A,1)	B(A,5),D(C,6),B(C,4)



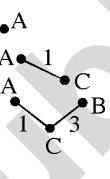
- B(C, 4) is another entry in T group which shows that B is approached by A via C and the cost is 4.

Step 3 :

- Now move B(C,4) from T to P group and add neighbours E and D to the T group as shown in Table P. 8.8.3(c).
- Note that E(B,10) corresponds to the route A-C-B-E with a cost $1 + 3 + 6 = 10$. Do not use the route A-B-E because the associated cost is $5 + 6 = 11$.

(G-459) Table P. 8.8.3(c)

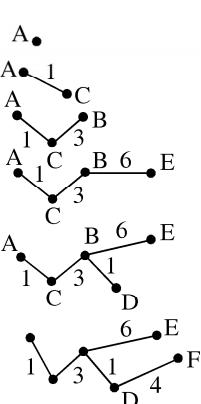
Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)
A, C(A,1)	D(C,6),B(C,4)
A, C(A,1),B(C,4)	D(C,6),E(B,10)

**Step 4 :**

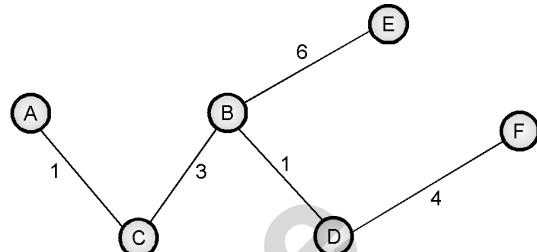
- Now continue in the same manner to get the final table as shown in Table P. 8.8.3(d).

(G-460) Table P. 8.8.3(d) : Final table

Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)
A, C(A,1)	D(C,6),B(C,4)
A, C(A,1),B(C,4)	D(C,6),E(B,10)
A, C(A,1), B(C,4), D(C,6)	E(B, 10) F(D, 10)
A, C(A,1), B(C,4), D(C,6) E(B,10)	F (D, 10)
A, C(A,1), B(C,4), D(C,6) E(B,10), F(D,10)	Null (Stop)



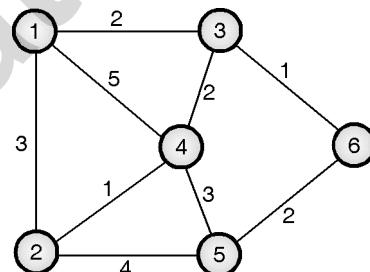
- The shortest path from A to other nodes is shown in Fig. P. 8.8.3(b).



(G-461) Fig. P. 8.8.3(b) : Shortest paths from A to all other nodes

- Dijkstra's algorithm is most suitable for the dense networks and it is particularly useful for the parallel implementation, i.e. when the scan operation is carried out in parallel.
- The disadvantages are that it does not take any advantage of sparsity well and it is only appropriate for the networks with positive arc lengths.

Ex. 8.8.4 : Write Dijkstra's algorithm. Find shortest path Fig. P. 8.8.4(a) to destination node 6.



(G-1383) Fig. P. 8.8.4(a)

Soln. :

For Dijkstra's algorithm refer section 8.8.2.

Let Node 1 → A, 2 → B, 3 → C, 4 → D, 5 → E, 6 → F

Step 1 :

- The starting node is A. Enter it into group P as shown in Table P. 8.8.4(a).
- Add neighbours B, C and D to the temporary group T.

Table P. 8.8.4(a)

Permanent (P)	Temporary (T)
A	B (A, 3), C(A, 2) D(A, 5)

Step 2 :

- Now pick up the neighbour with smallest cost i.e. c and add it to group P.



- As C is added to P group, we have to add neighbours of C to T group as shown in Table P. 8.8.4(b).
- D(C, 4) is another entry in T group which shows that D is approached by A via C and the cost is 4.

(G-2713) Table P. 8.8.4(b)

Permanent (P)	Temporary (T)
A	B(A, 3), C(A, 2), D(A, 5)
A, C(A, 2)	B(A, 3), D(A, 5), D(C, 4), F(C, 3)

Step 3 :

- Now move B(A, 3) from T to P and add neighbours D and E to T group as shown in Table P. 8.8.4(c).

Table P. 8.8.4(c)

Permanent (P)	Temporary (T)
A	B(A, 3), C(A, 2), D(A, 5)
A, C(A, 2)	B(A, 3), D(C, 4), F(C, 3)
A, C(A, 2), B(A, 3)	D(C, 4), F(C, 3), D(B, 4), E(B, 7)

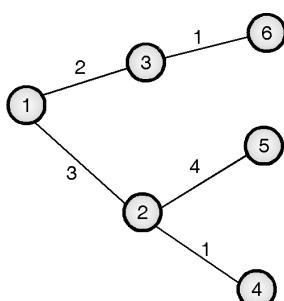
Step 4 :

- Now continue in the same manner to get the final table as shown in Table P. 8.8.4(d).

Table P. 8.8.4(d) : Final table

Permanent (P)	Temporary (T)
A	B(A, 3), C(A, 2), D(A, 5)
A, C(A, 2)	B(A, 3), D(C, 4), F(C, 3)
A, C(A, 2), B(A, 3)	D(C, 4), F(C, 3), D(B, 4), E(B, 7)
A, C(A, 2), B(A, 3), D(B, 4)	F(C, 3), E(B, 7)
A, C(A, 2), B(A, 3), D(B, 4), E(B, 7)	F(C, 3) F(E, 9)
A, C(A, 2), B(A, 3), D(B, 4), E(B, 7), F(C, 3)	Null (stop)

- Shortest path from node 1 to other nodes is shown in Fig. P. 8.8.4(b).



(G-1384) Fig. P. 8.8.4(b) : Shortest path from 1 to all other

8.9 Path Vector Routing :

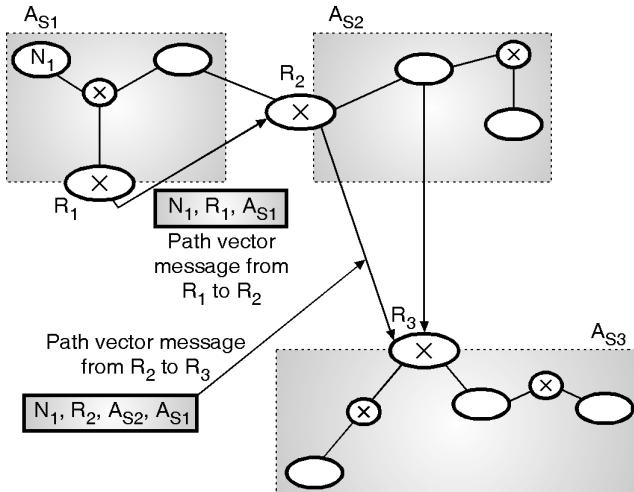
- It is different from both distance vector routing and link state routing.
- Table 8.9.1 shows the example of a path routing table. Each entry in the routing table will have the information about the destination network, the next router and the path to reach the destination.

Table 8.9.1 : Path vector routing table

Network	Next router	Path
N01	R01	AS 12, AS 21, AS 56
N02	R08	AS 20, AS 57, AS 06
.	.	.
.	.	.
.	.	.

8.9.1 Path Vector Messages :

- The autonomous boundary routers participate in path vector routing.
- Their job is to advertise the reachability of networks present in their A.S. to the neighbour autonomous boundary router.
- Each router that receives a path vector message verifies whether or not the advertised path is according to its policy.
- Such a policy is made up of rules that are imposed by the router controlling administrator.
- If yes then the router will update its routing table and will modify the message before it is sent to the next neighbour.
- In the modified message it sends its own AS number and replaces the next router entry with its own identification. This process is demonstrated in Fig. 8.9.1.
- Fig. 8.9.1 shows an internet containing three autonomous systems A_{S1} through A_{S3} .
- Router R_1 sends a path vector message to advertise that it is reachable to network N_1 .
- Router R_2 on receiving this message will update its routing table. It then adds its own autonomous system (A_{S2}) to the path, inserts itself as the next router and sends this message to router R_3 as shown in Fig. 8.9.1.



(G-1788) Fig. 8.9.1 : Path vector messages

8.9.2 Loop Prevention :

- When a message is received, a router checks it to see if its autonomous system is in the path list to the destination.
- If it is present it indicates looping is involved which is undesirable and the message is ignored.
- In this way the looping problem and the associated instability which is present in distance vector routing is avoided in path vector routing.

8.9.3 Path Attributes :

- The path is specified in terms of attributes. Each attribute gives some information about the path.
- Hence the list of attributes helps the receiving router to make a better decision about when to apply its policy.
- Attributes are of two types :
 1. A well known attribute
 2. An optional attribute
- An attribute is called as a well known attribute if it is recognised by every BGP router.
- An optional attribute is the one that need not be recognised by every BGP router.
- The well known attributes are further classified into two categories :
 1. Well known mandatory attributes
 2. Well known discretionary attributes.
- The optional attributes also are classified into two types
 1. An optional transitive attribute
 2. An optional nontransitive attribute.

8.10 Unicast Routing Protocols :

- We can define the unicast communication as the communication between one sender and one receiver.
- In short it is a one to one communication.
- We have already discussed about how the Internet has been divided in **administrative areas** called **Autonomous Systems** which helps in handling the exchange of routing information efficiently.
- In the following sections we are going to discuss some important routing protocols.

8.10.1 Routing :

- An Internet consists of many networks connected to each other by routers.
- A datagram passes through different routers when it travels from the source to destination.

8.10.2 Cost or Metric :

- As a router is connected to many networks it has to make a decision when it receives a packet from one of these networks, as to which network it should pass this packet to ?
- The router makes this decision on the basis of **Optimization**.
- That means it finds out which path is an optimum path to send the packet. But how does it define the term **optimum** ?
- One way is that a **cost** is assigned for passing through a network. This cost is also called as the **metric**.
- In connection with finding the optimum path, the network having a high cost is considered to be **bad** and to have a low cost is considered to be **good**.
- So in order to maximize the throughput the router should choose the networks (paths) having low costs.
- Similarly in order to minimize the delay, the router must choose the paths having low costs.

8.10.3 Routing Tables :

- The routing table for a host or a router consists of an entry for each destination, or a combination of destinations to route the IP packets.
- Routing tables can be of two types :
 1. Static routing tables
 2. Dynamic routing tables



1. Static routing table :

- The information in the static routing tables is entered manual.
- The route of a packet to each destination is entered into the table by the administrator.
- This routing table cannot update itself automatically.
- It has to be changed manually as and when required.
- Hence static routing table is useful only for small networks.

2. Dynamic routing table :

- The dynamic routing tables can get automatically updated by using a dynamic routing protocol such as RIP, OSPF or BGP.
- The structure of a dynamic routing table is shown in Table 8.10.1.

Table 8.10.1 : Format of dynamic routing table

Mask	Network address	Next hop address	Interface	Flags	Reference count	Use

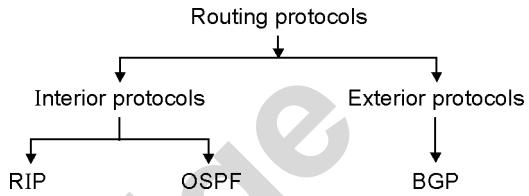
8.11 Routing Protocols :

- Routing protocols are designed on the basis of the demand for dynamic routing tables.
- The router in an Internet are supposed to inform each other about changes.
- Routing protocols combine the rules and procedures which allow the routers to exchange information about these changes between themselves.
- We can divide the routing protocols into two categories, **interior protocols** and **exterior protocols**.
- We can define an **interior protocol** as the one that handles the **intradomain routing**.
- Similarly an exterior protocol is defined as the one which handles the **interdomain** routing.

8.11.1 Unicast Routing Protocols :

- Various unicast routing protocols are shown in Fig. 8.11.1.

- The popular interior protocols are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).
- Whereas the exterior protocol used popularly is BGP (Border Gateway Protocol).



(G-497) Fig. 8.11.1 : Unicast routing protocols

- RIP and OSPF are used to upgrade the routing tables inside an A.S. and BGP is used for upgrading the routing tables for the routers which join multiple A.S. together.

8.12 RIP (Routing Information Protocol) :

- RIP is used for updating the routing tables.
- The routing updates are exchanged between the neighbouring routers after every 30 seconds with the help of the RIP response message.
- These messages are also known as the RIP advertisements.
- These messages are sent by the routers or hosts. They contain a list of multiple destinations within an Autonomous System (AS).
- RIP is an interior routing protocol used inside an Autonomous System (AS).
- Its operation is based on distance vector routing.
- In the distance vector routing each router periodically shares its knowledge about the whole Internet with its neighbours.
- As stated earlier, RIP is a very simple intradomain or interior routing protocol which works inside an **Autonomous System (AS)**.
- RIP implements the distance vector routing with the following considerations :
 1. In an A.S. it has to deal with routers and networks (links) and not the nodes.
 2. Now the destination in a routing table is a network. That is why, the network address is defined in the first column.



3. The **metric** used in RIP is called as the **hop count** and it is very simple. It is defined as the number of links a packet has to travel to reach its destination.
4. In RIP, the value of **infinity** is decided to be equal to 16. That is why the maximum **hop count** for any route inside an A.S. using RIP can be 15.
5. The next node column is used to define the address of the router to which the packet is to be dispatched.

Routing table :

- A typical routing table is shown in Table 8.12.1.
- Every router is supposed to keep such a table with it.

Table 8.12.1 : Routing table

Destination	Hop count	Next router	Other information

- Destination column consists of the destination network address.
- The hop count column consists of the shortest distance to reach the destination and the next router column consists of the address of the next router to which the packet is to be forwarded.
- The other information in Table 8.12.1 may include information such as subnet mask or the time this entry was last updated.

8.12.1 RIP Updating Algorithm :

- The routing table is updated when a RIP response message is received as stated earlier.
- The updating algorithm used by RIP is as follows.

RIP updating algorithm :

1. RIP response message is received.
2. Add one hop to the hop count for each advertised destination.
3. Repeat the following steps for each advertised destination :
- Add the advertised information to the table if the destination is not present in the routing table.
- Replace entry in the table with the advertised one if the next hop field is same.

- Replace entry in the routing table if advertising hop count is smaller than one in the table.
- 4. Return.

8.12.2 Initializing the Routing Table :

- When a new router is added to a network it initialises its routing table.
- Such a table consists of the information only about the directly attached networks and the corresponding hop counts.
- The next hop field which identifies the next router is empty.

8.12.3 Updating the Routing Table :

- When RIP messages are received, each routing table is updated using the RIP updating algorithm as discussed earlier.

8.12.4 RIP Operation :

- RIP work is a combination of a routing database that stores information on the fastest route from computer to computer, an update process that enables each router to tell other routers which route is the fastest from its point of view, and an update algorithm that enables each router to update its database with the fastest route communicated from neighboring routers.
- Each router on the Internet keeps a database that stores the following information for every computer in the same RIP network :
- **IP address** : The Internet Protocol address of the computer.
- **Gateway** : The best gateway to send a message addressed to that IP address.
- **Distance** : The number of routers between this router and the router that can send the message directly to that IP address.
- **Route change flag** : A flag that indicates that this information has changed used by other routers to update their own databases.
- **Timers** : Various timers.
- At regular intervals each router sends an update message which has full information about its routing



database to all the other routers that are directly connected to it.

- Some routers will send this message as often as every 30 seconds, so that the network will always have up-to-date information.
- RIP uses the UDP network protocol because of its efficiency and there are no problems if a message gets lost due to any reason.
- This is because the next update will be coming in a short time.

8.12.5 RIP Message Format :

- RIP messages can be broadly classified into two types : messages that deliver routing information and messages that request routing information.
- Both use the same format which consists of a fixed header followed by an optional list of network and distance pairs.

RIP version 1		
Command	Version	Reserved
Family		All zeros
Network address		
All zeros		
All zeros		
Distance		
Repeat of last 20 bytes ...		

(G-1998) Fig. 8.12.1 : RIP message format

- The summary of the RIP packet format fields illustrated in Fig. 8.12.1, is as follows :

1. Command :

- Indicates whether the type of the packet i.e. a request or a response.
- The request asks that a router send all or part of its routing table.
- The response can be an unsolicited regular routing update or a reply to a request.
- Responses contain routing table entries. Multiple RIP packets are used to convey information from large routing tables.

2. Version :

- This field specifies the RIP version used. This field can signal different potentially incompatible versions.

3. Zero :

- This field is not actually used by RFC 1058 RIP; it was added just to provide backward compatibility with the older versions of RIP. Its name actually indicates its defaulted value: zero.

4. Family :

- This field is used to specify the address family used. RIP is designed to carry routing information for several different protocols.
- Each entry has an address-family identifier to indicate the type of address being specified.
- For example the value of AFI for IP is 2. Similarly different values indicate different protocols.

5. Network address :

- The network address field is used for defining the address of the destination network.
- In RIP this field is 14 bytes long, so that it can be used for any protocol.
- But the IPv4 address is only 4 byte long. Hence the remaining space in the address field is filled with zeros.

6. Distance :

- This field indicates the number of hops (routers) that have been traversed in the trip to the destination.
- This value is between 1 and 15 for a valid route, or 16 for an unreachable route.

8.13 Request and Response Messages (RIP) :

- RIP has two types of messages namely Request and Response Messages.

8.13.1 Request Message :

- The request message is created in the following two situations :
 1. It is created by a router which has just come up.
 2. Or it is created by a router which has some time out entries.
- In a request message, information about some specific entries or all the entries is asked.



- Fig. 8.13.1(a) shows the format of the request message for one and Fig. 8.13.1(b) shows the format of request message for all.

Repeated	Com. 1	Version	Reserved
	Family	All zeros	
	Network address		
	All 0s		

(G-2145) (a) Format of request message (RIP) for one

Fig. 8.13.1

Repeated	Com. 1	Version	Reserved
	Family	All zeros	
	All 0s		

(G-2146) (b) Format of request message (RIP) for all

Fig. 8.13.1

8.13.2 Response Message :

- Response message in RIP can be one of the following two types :
 1. Solicited response or 2. Unsolicited response.

Solicited response :

- A **solicited response** is the one which is sent only as an answer to a request message. It carries with it the information about the destination specified in the request message.

Unsolicited response :

- An **unsolicited response**, is not sent only once but it is sent periodically (every 30 seconds or so) when there is any change in the routing table. This response is also called as the update packet.

8.13.3 Timers in RIP :

- RIP uses three different timers as follows for supporting its options.

 1. The **periodic timer** to control the process of sending messages.
 2. The **expiration timer** is used for governing the validity of a route.
 3. The **garbage collection timer** is used for advertising the failure of a route.

1. Periodic Timer :

- The task of the periodic timer is to control the advertising of the update messages regularly.
- As per protocol specifications, this timer should be set to 30 sec. but practically it is set randomly between 25 and 35 sec. Each router has one periodic timer.
- This timer counts down from the set value (25 to 35 sec.) and sends an update message when its count reaches a zero.
- Then the timer is set once again to a random value between 25 and 35 seconds.

2. Expiration Timer :

- The responsibility of expiration timer is to govern the validity of a route.
- When a router gives out the update information about a route, the value of this timer is set at 180 sec or 3 minutes.
- This timer is reset, everytime a new update for that route is received, which under normal working conditions happen after every 30 sec.
- But due to some problem on the Internet, if a new update for that route is not received within 180 sec, then that route is considered expired and the hop count of that route is set to 16.
- This is an indication that the destination is not reachable.
- There is a separate expiration timer for each route.

3. Garbage Collection Timer :

- The router does not purge a particular route from its table even when the information about that route becomes invalid. Instead the router continues to advertise that route by increasing its metric value to 16 (destination is not reachable).
- At the same time, the router sets another timer called **garbage collection timer** to 120 sec. for this route.
- As soon as this count goes to zero, that route is purged from the router table. Due to this timers the neighbours become aware that a particular route has become invalid, before its purging.

4. Disadvantages of RIPv1 :

- Some of the important disadvantages of the original RIP version i.e. RIPv1 are as follows :



1. RIPv1 only understands the shortest route to a destination, which is based on simple count of number of router hops.
2. It depends on other routers for computed routing updates.
3. Routing tables can get large and these are broadcasted every 30 seconds.
4. Distances are based on hops, not on real costs (such as the speed of link).
5. It continues to be a router to router configuration that means each router is fully dependent on its next router to implement the same options.
6. If we solve one problem another appears.

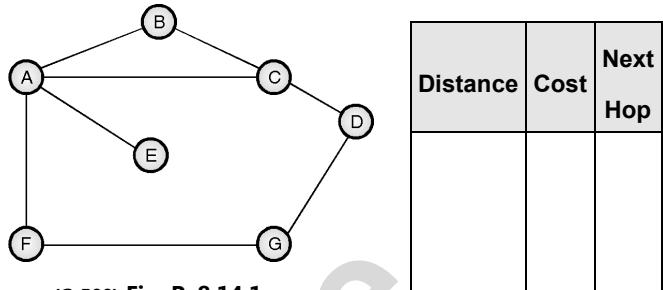
8.14 RIP Version 2 :

- In November 1994, RIP was modified with some additions (extensions) to overcome some of its shortcomings.
 - RIP version 1 is still being used on many routers and continues to outnumber OSPF networks.
 - The modified RIP is called RIP version 2 protocol.
 - Version 2 is backward compatible with version 1 and contains all of the capabilities of the version 1 protocol.
- RIP version 2 implemented the following features :

Features :

- Authentication by means of a simple text password.
- Subnet masking used.
- Multicasting used to allow for variable-length subnet masks to be implemented.
- Route tag-to provide a method of separating RIP routes from externally learned routes.
- Compatibility switch-to allow for interoperability with version 1 routers Notice that the same format is used for RIPv1 and RIPv2.

Ex. 8.14.1 : Complete the final routing table at node A using RIP protocol for the following network.
Assume the cost of hop count.



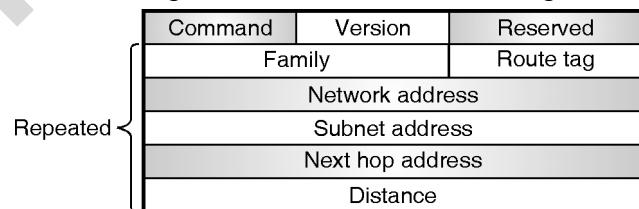
Soln. :

Table P. 8.14.1 : Routing table at A

Destination	Cost (hop count)	Next Hop (Next router)
B	1	B
C	1	C
E	1	E
F	1	F
D	2	C
G	2	F

8.14.1 Message format (RIPv2) :

- The message format of RIPv2 is as shown in Fig. 8.14.1.



(G-2147) Fig. 8.14.1 : Message format of RIPv2

New Fields :

- There are some new fields in the message format of RIPv2 as compared to that in RIPv1. They are as follows :
 1. Route tag
 2. Subnet mask
 3. Next hop address.
- 1. **Route tag** : This new field is useful in containing information such as autonomous system number. Using this field, we can enable RIP to receive information from an interdomain protocol.



2. **Subnet mask :** This field is 4 byte long and it contains the subnet mask or prefix. This shows that the classless addressing and CIDR is supported by the RIPv2.
3. **Next-hop address :** This new field contains the address of the next hop. This feature is useful in a situation where the same network is shared by two autonomous systems for example a backbone. With the help of this field, the message can define a router to which the packet is to be sent next. Note that this router can be a part of the same A.S. or some other A.S.

Classless Addressing :

- The most important difference between the two versions of RIP is that RIPv1 can support only the classful addressing, whereas RIPv2 can also support the classless addressing.
- Due to the additional field called **subnet mask**, it is possible to define a network prefix length in RIPv2. Hence classless addressing becomes possible.

8.14.2 Authentication :

- Authentication is a safety measure taken by RIPv2 to ensure the protection of message against unauthorized advertisement.
- For authentication, it is not necessary to add any extra field to the packet.
- Instead the authentication information is done as the first entry of the message.
- The value of $FFFF_{16}$ is entered in the family field which indicates that the entry is not the routing information but the authentication information, as shown in Fig. 8.14.2.
- The authentication field in Fig. 8.14.2 is used for defining the authentication protocol and the next field carries the actual authentication data.

Command	Version	Reserved
0x FFFF		Authentication type
Authentication data (16 bytes)		
:		

(G-2148) Fig. 8.14.2 : Authentication

8.14.3 Multicasting :

- In RIPv1 broadcasting is used for sending RIP message to all the neighbours.

- Due to broadcasting of the message, all the routers as well as hosts connected to the network would receive the RIP message.
- But in RIPv2 an all round **multicast** address is used to send the RIP messages only to the RIP routers on the network.

8.14.4 Encapsulation :

- The UDP is used to encapsulate the RIP messages. That means RIP message is inserted into the UDP user datagram.
- There is no field in RIP message which can indicate the length of the message.
- The length has to be determined from the UDP packet. The well known port 520 has been assigned to RIP in UDP.

8.14.5 Problems in RIP :

SPPU : Dec. 15

University Questions

Q. 1 How to overcome problems in RIP ?

(Dec. 15, 4 Marks)

- RIP is the most used Internet interior routing protocols. It is based on the distance vector routing principle.
- RIP has many limitations. Some of them are as follows :
 1. **Width restriction :** RIP uses a 4-bit metric to count router hops to the destination. For RIP infinity is defined as 16 which corresponds to 15 hops.
 2. **No direct subnet support :** RIP came into existence prior to subnetting and has no direct support for it. We can use it in the subnetted environment with some restrictions.
 3. **Bandwidth consumptive :** An RIP router will broadcast lists of networks and subnets it can reach after every 30 seconds. This will consume a large amount of bandwidth.
 4. **Difficult to diagnos fault :** Like any other distance vector routing protocols, RIP also is difficult to debug.
 5. **Weak security :** RIP does not have any security features of its own.
 6. **Looping problem :** Being based on distance vector principle the RIP faces the looping (routing loop) problem.

**Remedies :**

- Some of the above mentioned problems are overcome with RIP2 while the looping problem can be overcome by using either a link state routing protocol like OSPF or a newer distance vector routing protocol like BGP.

8.15 OSPF :**SPPU : Dec. 06, May 18, Dec. 19****University Questions.**

Q. 1 Discuss the advantages and disadvantages of OSPF and BGP routing algorithms.

(Dec. 06, 8 Marks)

Q. 2 Explain with neat diagram OSPF routing protocol.

(May 18, Dec. 19, 6 Marks)

- The long form of OSPF is Open Shortest Path First protocol.
- This is another interior routing protocol. It is an intradomain protocol and it is based on the link state routing.
- For handling the routing efficiently and in a timely manner, the OSPF divides an A.S. into areas.

Area :

- Networks, hosts and routers are collectively called as an area.
- An autonomous system can be imagined to be made of various areas.
- All the networks inside an area should be connected.

Area border routers :

- These are special type of routers which are used at the borders of an area.
- These routers summarize the information about the area and sent it to the other areas.

Backbone :

- A special area inside an autonomous system is called as backbone.
- All the areas inside an A.S. should be connected to the backbone.
- So backbone is the primary area and other areas are known as secondary areas.

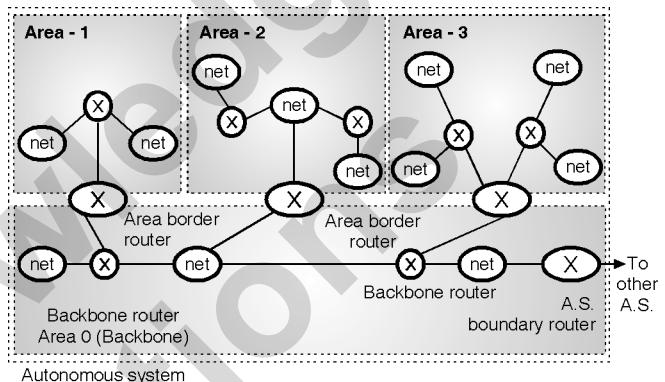
Backbone routers :

- The routers inside the backbone are called as the backbone routers.

- But a backbone router can also work as an area border router.
- If the connectivity between a backbone and an area is broken, due to some problem, then the administration should create a **virtual link** between routers so that the backbone can continue to function as primary area.

Area identification :

- Each area has an area identification.
- The area identification of the backbone is zero. An autonomous system is as shown in Fig. 8.15.1(a).

**(G-1786) Fig. 8.15.1(a) : Autonomous system****Disadvantages of the RIP protocol :**

- The maximum distance between any two stations (the metric, measured in router hops) is 15 hops.
- A destination (network ID) whose hop count is 16 or more is considered to be nonreachable.
- The cost to a destination network is measured in terms of number of hops.
- RIP determines a route based on a hop count that does not take into consideration any other criteria other than the number of routers between the source and destination networks.
- Due to this approach two-hop high-speed network will be ignored and a one-hop low-speed link would be used instead.
- We can make a router to take a better path by adjusting the hop-count metric on the router port, but this reduces the available diameter.
- RIP updates its entire table on a periodic basis using the broadcast address. (RIPv1; RIPv2 uses multicast or broadcast). But this would consume bandwidth.
- RIP sends its update with the help of a 576 byte datagram. If there are more entries than 512 bytes, then multiple datagrams must be sent.



- The biggest drawback of RIP is its slow convergence. In the worse case, a RIP update can take over 15 minutes end to end. This can lead to black holes, loops, etc.
- RIPv1 does not support VLSM.

Remedies (What OSPF could do) :

- The first shortest-path-first routing protocol was developed and used in the ARPAnet packet switching network all the way back in 1978.
- This research work was developed and used in many other routing protocol types and prototypes.
- One of those is OSPF .
- OSPF provides solutions to most of the drawbacks of RIP.
- Using OSPF we can scale up the routing architecture well beyond the maximum 16 hops supported by RIP.
- Rather than exchanging node (and network) reachability information, OSPF routers exchange link state information.
- Through the link state information, each router maintains its own copy of the network topology.
- From this link-state database, it is possible to find the shortest routing path.
- For those of you that are familiar with the OSI routing scheme, many of the features supported by OSPF are similar to the OSI IS-IS routing protocol.
- The original versions of OSPF are actually derived from some of the earlier versions of the IS-IS protocol.

8.15.1 Features of OSPF :**1. Type of service routing :**

- It is possible to configure different routers to support different types of service requirements.
- For example, one router can be configured for high-throughput, while the other one is configured to support minimal delivery delay for some other application.

2. Load balancing :

- When multiple routes are available, traffic can be evenly distributed over the routes.
- This would obviously result in a higher network efficiency.

3. Subdivision of autonomous systems :

- It is possible to further divide the system into logical areas.
- This would improve the management of large autonomous systems.

4. Security :

- The data exchanges in OSPF are authenticated. Inadvertent or malicious transmissions from foreign routing nodes are discarded.
- Only those hosts intended for the routing network are included.
- The network isn't vulnerable to the threat of having routing tables corrupted by faulty route information.

5. Host :

- OSPF supports specific, network and subnetwork routing.

6. Special features are provided to support LAN environments :

- Although the relationships between routers are maintained on a logical link basis, link state transmissions are minimized by the architecture. **Designated gateways** are responsible for transmitting the link state information for all information in their local area.

7. OSPF is an open specification :

- The OSPF has been published as an RFC and not defined as a defacto standard such as RIP.
- Therefore anyone can implement the standard, without paying royalties.
- This has been done to encourage many vendors to use it so that the users are not locked into a single vendor's equipment.

8. OSPF area :

- OSPF divides the network into groups, called an **area**. The topology of an area is not known to the rest of the Autonomous System.
- This technique minimizes the routing traffic required for the protocol.
- When multiple areas are used, each area has its own copy of the topological database.



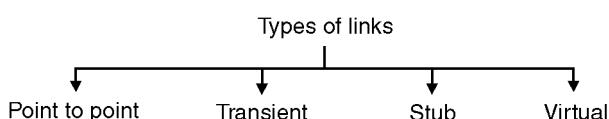
- Several concepts have been incorporated in the OSPF algorithm.
- The RIP treated an autonomous system as a monolithic collection of routes and subnets, but OSPF introduces the concept of areas.
- The concept of hiding the routing information within a OSPF routing domain (Internet autonomous system) has also been introduced.
- After dividing an autonomous system into a collection of logical areas, the OSPF can support different types of routing nodes (routers) such as internal routers, area border routers, backbone routers, and Autonomous System (AS) boundary routers. (See Fig. 8.15.1(a)).
- The protocols used to support OSPF routing include database broadcast packets and link state change broadcasts.
- A "Hello" protocol is used to detect changes in the availability of adjacent routers.

8.15.2 Metric :

- The cost assigned to each route by an OSPF administrator is called as metric of that route.
- In the OSPF protocol the metric can be based on a type of service.
- A router can have multiple routing tables which are based on different types of service.

8.15.3 Types of Links :

- In the OSPF protocol terminology, a connection is called as a link.
- OSPF defines four types of links called point to point, transient link, stub link and virtual links as shown in Fig. 8.15.1(b).

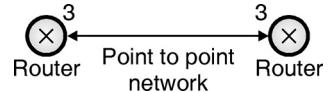


(G-501) Fig. 8.15.1(b) : Types of links

1. Point to point link :

- A point to point link is defined as the link (connection) that directly connects two router without any other host or router present in between.
- An example of such a link is two routers connected by a telephone line.

- Each router has only one neighbour at the other side of the link. This is shown in Fig. 8.15.2.

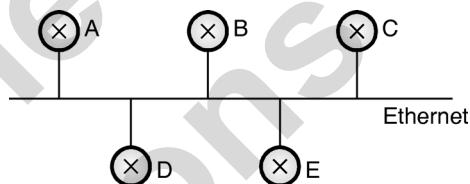


(G-502(a)) Fig. 8.15.2 : Point to point link

- It is not necessary to assign any network address to this link.
- The metric are shown at the two ends of the link and they are generally the same.

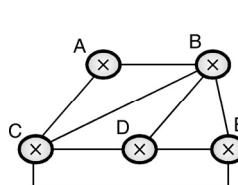
2. Transient link :

- It is a network having many routers attached to it as shown in Fig. 8.15.3.

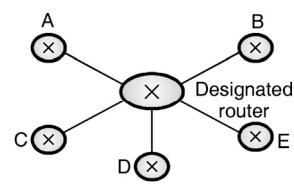


(G-503) Fig. 8.15.3 : Transient link

- All LANs and some WANs are of this type.
- A, B, C etc. are the routers. Each router has several neighbours.
- The relationship between the neighbouring routers is as shown in Fig. 8.15.4(a).
- Each router has been connected to every other neighbour.
- But this arrangement is extremely non- efficient and non-realistic. In order to make it more efficient and realistic, the configuration of Fig. 8.15.4(b) should be used. This is known as the transient network.
- The designated router is assigned to perform two tasks, one as a true router and the other as a designated router.
- Due to the realistic arrangement of Fig. 8.15.4(b) every router has only one neighbour i.e. the designated router (network), however the designated router has multiple (5 in this case) neighbours.



(a) Unrealistic representation



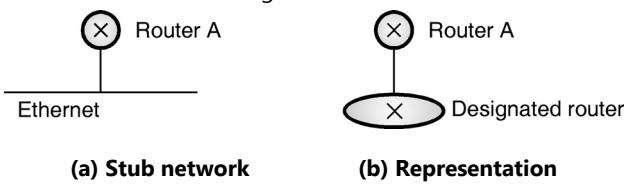
(b) Realistic representation

(G-1787) Fig. 8.15.4

- The realistic arrangement reduces the number of announcement that each router has to make to a small number as compared to the unrealistic arrangement.
 - Note that there is a metric from each node to designated router and there is no metric from the designated router to any other node.

3. A stub link :

- A stub link is a network that is connected to only one router as shown in Fig. 8.15.5.



(G-504) Fig. 8.15.5

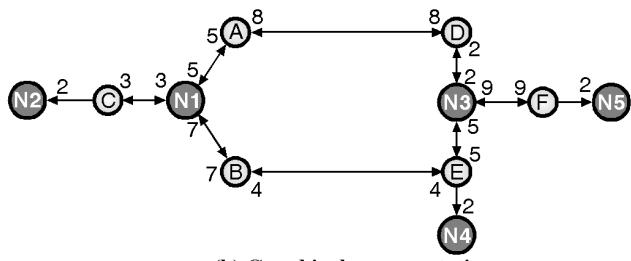
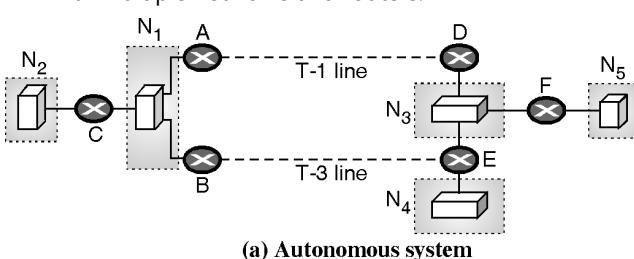
- The stub network of Fig. 8.15.5(a) is a special case of transient network.
 - The data packets use the same link to enter and leave the network.
 - This situation can be represented by using router A as a node and by replacing the network by a designated router as shown in Fig. 8.15.5(b).
 - The link connecting router A and the designated router is unidirectional from router to network.
 - When this link gets damaged the administration can create a virtual link between the two routers.

8.15.4 Virtual Link :

- The administration can create a **virtual link** between two routers, when a link between them gets broken due to some reason.
 - Such a virtual link could be over a longer path which would go through many routers.

8.15.5 Graphical Representation :

- Let us now discuss about representing an A.S. graphically. Consider Fig. 8.15.6(a) which is a small A.S. with multiple networks and routers.



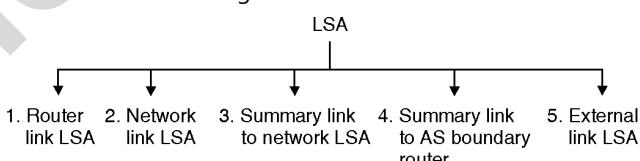
(b) Graphical representation

(G-2115) Fig. 8.15.6 : A.S. and its graphical representation

- There are some point to point networks, and transient as well as stub networks.
 - The symbols such as N_1 and N_2 are used for the transient and stub networks.
 - No identity should be attached to the point to point networks.
 - The graphical representation of the A.S. as seen by OSPF has been shown in Fig. 8.15.6(b).

8.15.6 Link State Advertisements (LSAs) :

- Each entity in a network distributes the Link State Advertisements (LSAs). An LSA announces the states of entity links.
 - Different types of LSAs depending on the type of entity are as shown in Fig. 8.15.7.



(G-505) Fig. 8.15.7 : Types of LSAs

1 Router Links :

- The router produced a router links advertisement for its own area.
 - The advertisement describes the collected states of the router's links to the area.
 - This advertisement also indicates the type of the router i.e. whether it is an area border router or an AS boundary router.

2 Network Links

- A network link advertisement is produced for every transit multi-access network.
 - This advertisement is produced by the designated router for the transit network.



- It describes all the OSPF routers fully adjacent to the designated router.

3. Summary Links :

- Summary Link advertisements describe a single route to a destination.
- The destinations described are external to the area but internal to the Autonomous System.
- Some condensing of routing information occurs when creating these summary link state advertisements.

4. AS Summary Links :

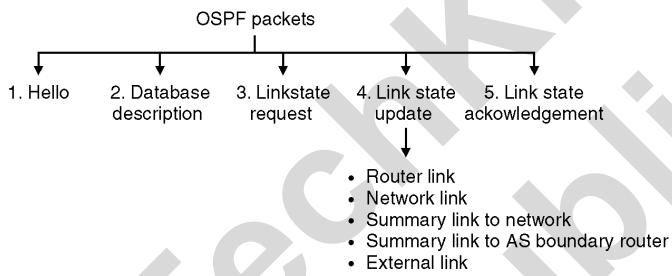
- These are like summary link advertisements but they describe routes to Autonomous System boundary routers.

5. AS External Links :

- AS external advertisements describe routes external to the Autonomous System.

8.15.7 OSPF Packet Types :

- Different types of OSPF packets are as shown in Fig. 8.15.8.



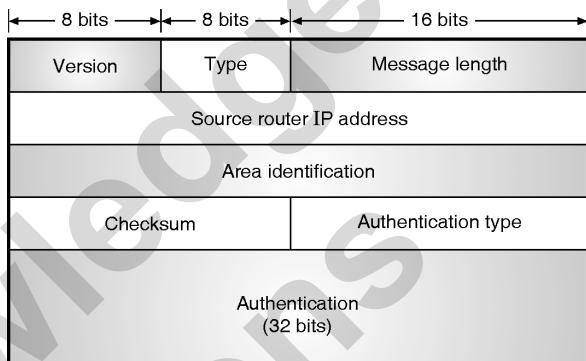
(G-506) Fig. 8.15.8 : OSPF packet types

- The OSPF protocol runs directly over IP, and uses the assigned number 89.
- Each OSPF packet consists of an OSPF header followed by the body of a particular packet type.
- OSPF packets need to be sent to specific IP addresses in nonbroadcast multi-access networks.
- The OSPF operation consist of following stages :
- Neighbours are discovered by means of sending the Hello messages and designated routers are elected in multi-access networks.
- Adjacent routers are identified and link state databases are synchronized.
- Link State Advertisements (LSA) are exchanged among the adjacent routers so as to maintain the topological

databases and also to advertise interarea and interAS routes.

- The routers use the information in the database to generate routing tables.
- All OSPF packets have the same common header which is as shown in Fig. 8.15.9.
- This header is same for all the five packet types of OSPF.

Common Header :



(G-2116) Fig. 8.15.9 : OSPF common header

- Various fields in the OSPF packet header are as follows :

Version :

- The contents of this 8-bit field tells us about the version of the OSPF protocol. It is currently version 2.

Type :

- This 8-bit field defines the type of the packet. There are five types of OSPF packets and they can defined by adjusting the contents of the type field from 1 to 5.

Message length :

- This 16-bit field defines the length of the total message which includes the header as well as the body.

Source router IP address :

- This 32-bit field defines the IP address of the router that sends the packet.

Area identification :

- This 32-bit field defines the area within which the routing takes place.

Checksum :

- This field is used for error detection on the entire packet excluding the authentication type and authentication data field.

Authentication type :

- This 16-bit field defines the authentication method used in this area.



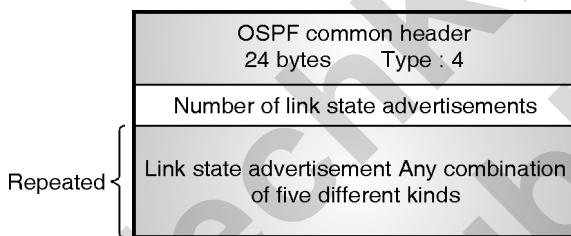
- At this time, two types of authentication are defined : A 0 in this field shows that no authentication is being used and a 1 represents the use of password for authentication.

Authentication :

- This 64-bit field is the actual value of the authentication data.
- In the future, when more authentication types would be defined, this field will contain the result of the authentication calculation.
- For now, if the authentication type is 0, this field is filled with 0s.
- If the type is 1, this field carries an eight-character password.

8.15.8 Link State Update Packet :

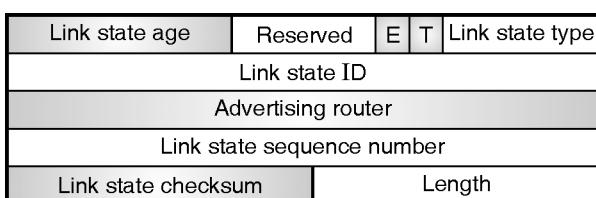
- The heart of OSPF operation is the link state update packet.
- So let us discuss that first. A router uses this packet, to advertise the states of its links.
- Fig. 8.15.10 shows the general format of the link state update packet.



(G-2117) Fig. 8.15.10 : Format of link state update packet

- Each update packet may contain many different LSAs.
- Fig. 8.15.11 shows the general header which is common to all five types of LSAs.

8.15.9 General LSA Header :



(G-2118) Fig. 8.15.11 : LSA general header

- Let us discuss various fields of LSA general header.
- 1. Link state age :**
- This field is useful in indicating the time (in seconds) elapsed from the instant of generation of this message.

- This type of message travels from router to router which is called as flooding.

- At the instant of creation of this message by a router, the value of this field is 0.

- But everytime a router forwards this message, the cumulative value of this field.

2. E Flag :

- This is a 1 bit flag. If E = 1 then it indicates that the area is a **stub area**.

- The area that is connected to the backbone by only one path is called as the stub area.

3. T Flag :

- This is also a 1 bit flag. If T = 1, then it indicates that it is possible for the router to handle multiple services.

4. Link state type :

- This field is used for defining the LSA type.

- There are five different types of advertisements as follows :

- Router link
- Network link.
- Summary link to network.
- Summary link to A.S. boundary router.
- External link.

5. Link state ID :

- The contents of this field are dependent on the type of link, as shown in Table 8.15.1.

Table 8.15.1

Type	Link	Link state ID
1.	Router link	IP address of router
2.	Network link	IP address of designated router.
3.	Summary link to network.	Address of the network
4.	Summary link to AS boundary router	IP address of AS boundary router.
5.	External link	Address of external Network

6. Advertising router :

- The field contains the IP address of the router which advertises this message.

7. Link state sequence number :

- This field contains a sequence number that is assigned to each link state update message.



8. Link state checksum :

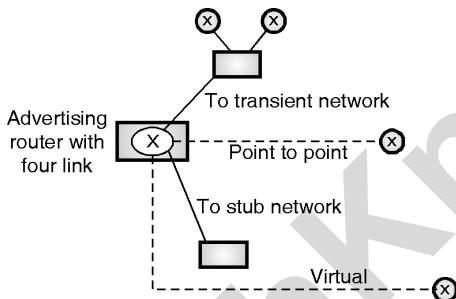
- The contents of this field is not the usual checksum. But the value of this field is calculated on a special type called as **Fletcher's checksum**.
- This method of calculating checksum considers the whole packet except for the age field to calculate the checksum.

9. Length :

- This field is used for defining the length of the whole packet, in bytes.

8.15.10 Router Link LSA :

- The links of a true router are defined by a router link.
- This advertisement is used by a true router to announce information about all its links and at the same time about the neighbours.
- A router link has been shown in Fig. 8.15.12.

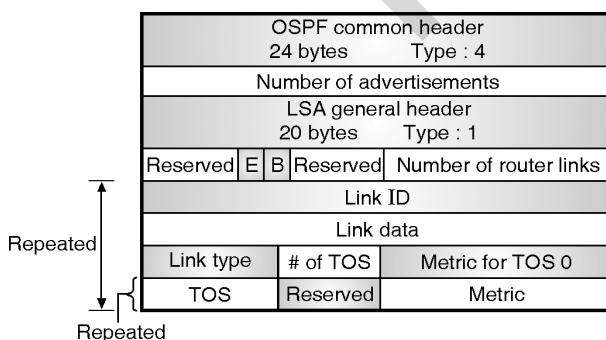


(G-2119) Fig. 8.15.12 : Router link

- The router link LSA is used for advertising all the links of a true router.

8.15.11 Router Link Packet :

- Fig. 8.15.13 shows the format of router link packet. Let us discuss its various fields.



(G-2120) Fig. 8.15.13 : Format of router link LSA

1. Link ID :

- The contents of this field are dependent on the type of link.

- Different link identifications on the basis of link type are as shown in Table 8.15.2.

Table 8.15.2

Link type	Link identification	Link data
Type 1 : Point to point	Address of neighbor router	Interface number
Type 2 : Transient	Address of designated router	Router address
Type 3 : Stub.	Network address	Network mask
Type 4 : Virtual	Address of neighbor router	Router address

2. Link data :

- The contents of this field give additional information about the link.
- Therefore the contents of this field are dependent on the type of link as shown in Table 8.15.2.

3. Link type :

- As shown in Table 8.15.2, OSPF defines four types of links on the basis of the type of network, the router is connected to.

4. Number of types of service (TOS) :

- The contents of this field are used for defining the number of types of services that are announced for each link.

5. Metric for TOS 0 :

- The default type of service is TOS 0. This field is used for defining the metric for the default service.

6. TOS :

- The contents of this field are used for defining the type of service.

7. Metric :

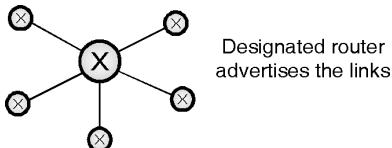
- The contents of this field are used for defining the metric for corresponding TOS.

8.15.12 Network Link LSA :

- The links of a network are defined by a network link LSA.
- A designated router distributes this type of LSA packets on behalf of the transient network.

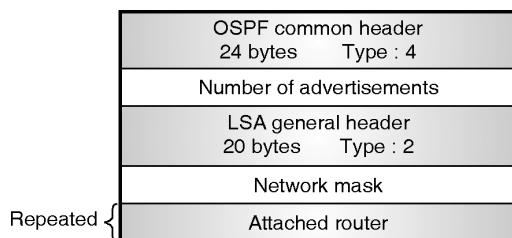


- This packet is used for announcement of existence of all the routers to the network as shown in Fig. 8.15.14.



(G-2121) Fig. 8.15.14 : Network links

- Fig. 8.15.15 shows the format of network link advertisement.



(G-2122) Fig. 8.15.15 : Network link advertisement format

- The important fields of the network link LSA are as given below.

1. Network mask :

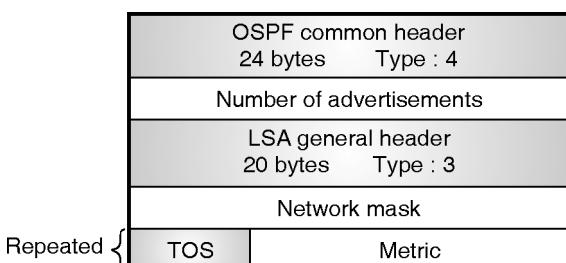
- The contents of this field are used for defining the network mask.

2. Attached router :

- The contents of this field are used for defining the IP addresses of all the attached routers.
- This field is a repeated field.

8.15.13 Summary Link to Network LSA :

- Inside an area, the router link and network link advertisements provide ample information about the router links and network links to a router.
- But this information is not enough. In addition to this, a router is also supposed to know about the network outside its area. This information is provided by the **border routers**.



(G-2123) Fig. 8.15.16 : Format of summary link to network LSA

- An area border router receives router link and network link advertisements and create a routing table for each area because it is simultaneously active in more than one areas.

- Fig. 8.15.16 shows the format of the summary link to network LSA.

- The important fields in this are as follows :

1. Network mask :

- The contents of this field are used for defining the network mask.

2. TOS :

- The contents of this field are used to define the type of service.

3. Metric :

- The contents of this field are used for defining the metric for the type of service stated in the TOS field .

8.15.14 Summary Link to AS Boundary Router LSA :

- The previous advertisement was designed to let every router know the cost to reach all the networks that belong to an A.S.
- But what if a router inside an AS wants to send a packet outside the AS ?
- In order to accomplish this, the router must know the path (route) to an autonomous boundary router.
- This information is provided by the summary link to AS boundary router.
- The area boundary routers will simply flood their areas with this information.
- This packet contains the information about the route to an AS boundary router.
- Fig. 8.15.17 shows the format for summary link to AS boundary router LSA.
- Its primary objective of this packet is to define the network to which the AS boundary router has been attached.
- The fields in this format are same as those in the summary link to the network advertisement message.



Repeated {	OSPF common header 24 bytes Type : 4	
	Number of advertisements	
	LSA general header 20 bytes Type : 4	
	All 0s	
	TOS	Metric

(G-2124) Fig. 8.15.17 : Summary link to AS boundary router LSA

8.15.15 External Link LSA :

- We have seen how the previous advertisement makes each router to know about the route to an AS boundary router.
- But only this much information is not sufficient because a router inside an AS would also like to know about the networks available outside the AS.
- This information is provided by the external link advertisement.
- The cost of each network outside the AS is made available (flooded) by the AS boundary router inside that AS, with the help of a routing table created by an inter domain routing protocol.
- This is accomplished by announcing one single network through an advertisement.
- A separate announcement is made for each network.
- Fig. 8.15.18 shows the format of external link LSA.
- This format is very similar to the summary link to the AS boundary router LSA but there are two additional fields.

Repeated {	OSPF common header 24 bytes Type : 4	
	Number of advertisements	
	LSA general header 20 bytes Type : 5	
	Network mask	
	TOS	Metric
	Forwarding address	
	External route tag	

(G-2125) Fig. 8.15.18 : External link LSA

- These two additional fields are as follows :
1. **Forwarding address :**
 - The contents of this field define the address of a forwarding router which is defined by the AS boundary router.
 - This forwarding router may prove to be a better forwarding destination.

2. **External route tag :**

- This field contents are used by other protocols except OSPF.

8.15.16 Other Packets :

- There are four other packet types in OSPF.
- They are essential for the operation of the protocol even though they are not used as LSAs.

They are as follows :

1. **Hello** : Used to discover and maintain neighbours.
 2. **Database Description** : Used to form adjacencies. The router summarizes all its link state advertisements and passes this information, via database description packets to the router with which it is forming an adjacency.
 3. **Link State Request** : After the database description packets have been exchanged with a neighbour, the router may think that link state advertisements it requires to update or complete the topological database. Link state request packets are sent to the neighbour in order to request for these link state advertisements.
 4. **Link State Update** : It is used for transmission of link state advertisements between routers. This could be in response to a link state request packet or to flood a new or more recent link state advertisement.
 5. **Link State Acknowledgment** : It is used to make the flooding of link state advertisements reliable. Each link state advertisement received is explicitly acknowledged.
- ### 8.15.17 Encapsulation :
- The IP datagram acts as a carrier for the OSPF packet.
 - That means the OSPF packet is encapsulated in the IP datagram.
 - An OSPF packet carrier with it the acknowledgement mechanism for flow and error controls.
 - Thus OSPF does not need a transport layer protocol for provision of these services.



8.15.18 Comparison between RIP and OSPF :

SPPU : May 07

University Questions

Q. 1 Compare and contrast the advertisement used by RIP and OSPF routing protocols.

(May 07, 6 Marks)

Function/Feature	RIPv1	RIPv2	OSPF
Standard number	RFC 1058	RFC 1723	RFC 2178
Link-state protocol	No	No	Yes
Large range of metrics	Hop count (16=Infinity)	Hop count (16=Infinity)	Yes, based on 1-65535
Update policy	Route table every 30 seconds	Route table every 30 seconds	Link-state changes, or every 30 [minutes]
Update address	Broadcast	Broadcast, multicast	Multicast
Dead interval	300 seconds total	300 seconds total	300 seconds total, but usually much less
Supports authentication	No	Yes	Yes
Convergence time	Variable (based on number of routers X dead interval)	Variable (based on number of routers X dead interval)	Media delay + dead interval
Variable-length subnets	No	Yes	Yes
Supports supernetting	No	Yes	Yes
Type of Service (TOS)	No	No	Yes
Multipath routing	No	No	Yes
Network diameter	15 hops	15 hops	65535 possible
Easy to use	Yes	Yes	No

8.16 Border Gateway Protocol (BGP) :

SPPU : Dec. 06, Dec. 07

University Questions

Q. 1 Discuss the advantages and disadvantages of OSPF and BGP routing algorithms.

(Dec. 06, 8 Marks)

Q. 2 What is BGP? Explain the operation of BGP with suitable example.

(Dec. 07, 6 Marks)

- BGP is an exterior routing protocol. It is a unicast routing protocol.
- It is used for the interautonomous system routing i.e. routing among different ASs.
- It was introduced in 1989 and has four versions. BGP operation takes place on the basis of the routing method called **path vector routing**.
- This principle is used because the distance vector routing and link state routing do not prove to be much suitable for interautonomous system routing.

8.16.1 Types of Autonomous Systems :

- We have already discussed about autonomous systems. Now let us discuss about their types.
- The three categories of autonomous systems are as follows :

1. Stub AS 2. Multihomed AS 3. Transit AS.

1. Stub AS :

- A stub AS is that type of AS which has only one connection to another AS.
- The hosts in the AS can send and receive data traffic to the hosts belonging to other AS.
- But note that data traffic cannot pass through a stub AS.
- In other words the stub traffic can be either a source or sink.

2. Multihomed AS :

- An AS which has more than one connection to other ASs is known as multihomed AS.
- But it is interesting to note that a multihomed AS is still only a source or sink for data traffic.
- For a host in multihomed AS, it is possible to send and receive data traffic to from more than one AS.



- But it does not allow the **transient traffic**.
- That means, the multihomed AS does not allow the data traffic coming from one AS to just pass through to the other AS.

3. Transit AS :

- An AS which is a multihomed AS but also allows the transient data traffic is called as **transit AS**.

8.16.2 CIDR :

- A Classless interdomain addressing is used in BGP. That means BGP makes use of the prefix (As discussed earlier) for defining a destination address.

8.16.3 Path Attributes :

- The path for a destination address can be presented as a list of **attributes**.
- We get some information from each attribute about the path.
- The receiving router takes the help of this list of attributes for making a better decision when applying its policies.

8.16.4 Types of Attributes :

- There are two categories of attributes :
 1. A well known attribute.
 2. An optional attribute.
- Every BGP router must recognize the **well known** attribute whereas the **optional attribute** is the one which need not be recognized by every router.
- The well known attributes are further classified into two types namely **mandatory** and **discretionary**.
- We define the well known mandatory attribute as the one which must appear in the description of router.
- On the other hand a well known discretionary attribute can be defined as the one which must be recognized by each router, but it need not be included in every update message.
- We can also subdivide the optional attributes into two categories as : **transitive** and **nontransitive** optional attributes.
- We may define the optional transitive attribute as the one which should be passed to next router that has not implemented this attribute.

- Similarly an optional nontransitive attribute is defined as the one which must be discarded if the receiving router has not implemented it.

8.17 BGP Sessions :

- In a BGP **session**, the two routers using BGP exchange routing information between them.
- So we can define a session as **connection** which has been established between two BGP routers in order to exchange the routing information.
- In order to ensure a reliable session the BGP uses services of TCP.
- The speciality of such a connection that it lasts for a longer time until something unusual happens.
- Therefore the BGP sessions are called as the **semipermanent connections**.

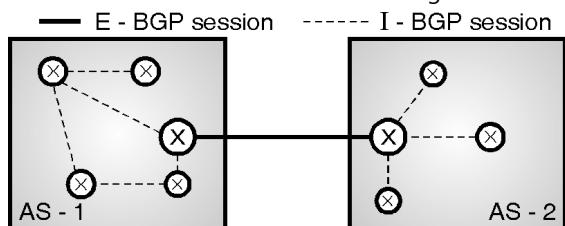
8.17.1 External and Internal BGP :

SPPU : Dec. 07

University Questions

- Q. 1** What is BGP? Explain the operation of BGP with suitable example. **(Dec. 07, 6 Marks)**

- There are two types of BGP sessions as follows :
 1. External BGP (E-BGP) session.
 2. Internal BGP (I-BGP) session.
- We can use the **E-BGP** session for exchanging information between two nodes which are present in two different ASs. This is as shown in Fig. 8.17.1.



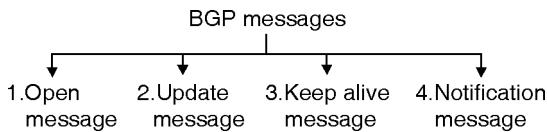
(G-2126) Fig. 8.17.1 : E-BGP and I-BGP sessions

- In Fig. 8.17.1, the session (connection) shown between AS-1 and AS-2 is E-BGP session. It is shown by a bold line.
- The two speaker routers A₁ and B₁ will exchange all the information which is known to them over the E-BGP session.
- But these routers collect information from the other routers belonging to their own A.S. using the I-BGP sessions shown by dotted lines in Fig. 8.17.1.



8.17.2 Types of Messages :

- BGP uses four different types of messages, as shown in Fig. 8.17.2.



(G-508) Fig. 8.17.2 : BGP message types

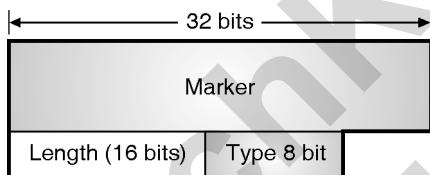
8.17.3 Packet Format :

SPPU : May 13

University Questions

Q. 1 Explain border gateway protocol with message format. **(May 13, 8 Marks)**

- All BGP message types use the basic packet header. Open, update, and notification messages have additional fields, but keep-alive messages use only the basic packet header.
- Fig. 8.17.3 illustrates the fields used in the BGP header. Each BGP packet contains a header whose primary purpose is to identify the function of the packet in question.



(G-2127) Fig. 8.17.3 : BGP packet header format

- Different important fields in the BGP packet header are as follows :

Marker :

- This is a 32 bit field. It contains an authentication value that the message receiver can predict.

Length :

- This is a 16 bit field which indicates the total length of the message in bytes.
- The value of the length field must be between 19 and 4096.

Type :

- Type is an 8-bit field which specifies the message type as one of the following :
 - Open
 - Update
 - Notification
 - Keep-alive

8.17.4 Open Message :

SPPU : May 13

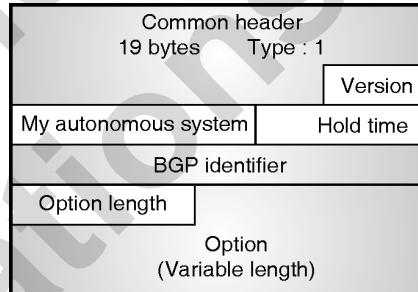
University Questions

Q. 1 Explain border gateway protocol with message format. **(May 13, 8 Marks)**

- This message is used by a router running BGP to create a neighbourhood relationship.
- To do so the router opens a TCP connection with a neighbor router and sends an **open message** to it.
- If the neighbor router is interested then it responds by sending a **keepalive message** which is an indication that the relationship between these two neighbor routers has been established.

Format :

- Fig. 8.17.4 shows the format of the open message.



(G-2128) Fig. 8.17.4 : Format of open message

- The important fields of the open message are as follows:

1. Version :

- The contents of this 1-byte long field define the version of BGP. The current version of BGP is 4.

2. My autonomous system :

- The contents of this 2-byte (16 - bit) field are used to define the autonomous system number.

3. Hold time :

- The contents of this 2-byte field specify the maximum amount of time in seconds that can elapse until one of the routers receives either a **keepalive** or **update** message from the other.
- If a router does not receive any of these messages during the hold time, then the other router is considered to be **dead**.

4. BGP identifier :

- The contents of this 4-byte long field defines the router which has sent the open message.

5. Option length :

- This one byte field is used for defining the length of the total option parameters.



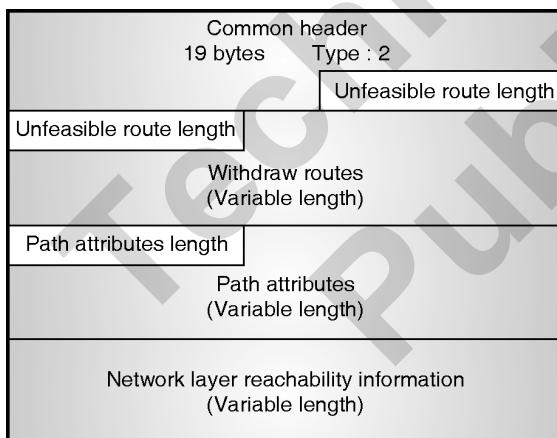
- The value of this field is zero if there are no option parameters.
- 6. Option parameters :**
- This is a variable length field which contains the option parameters.
 - The nonzero value of option parameter length field is an indication that there are some option parameters.
 - **Authentication** is the only option parameter defined so far.

8.17.5 The Update Message : SPPU : May 13

University Questions

Q. 1 Explain border gateway protocol with message format. (May 13, 8 Marks)

- This is the most important message in BGP. This message is used by the routers for the following two purposes :
 1. In order to withdraw a previously advertised destination.
 2. In order to announce a route to a new destination.
- The BGP can withdraw more than one previously advertised destinations but in a single update message, it can advertise only **one** new destination.
- Fig. 8.17.5 shows the format for the update message.



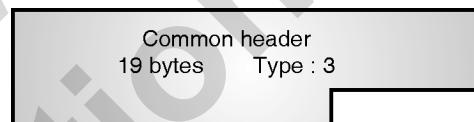
(G-2129) Fig. 8.17.5 : Format of update message

- The important fields in the update message are as follows :
 1. **Unfeasible route length** : This 2-byte long field is used for defining the length of the next field.
 2. **Withdrawn routes** : The contents of this variable length field gives the list of all the previously advertised routes which should be deleted.
 3. **Path attribute length** : The contents of this 2-byte long field defines the length of the next field.

4. **Path attributes** : The contents of this field are used for defining the attributes of the path (route) whose reachability is announced in this update message.
5. **Network layer reachability information** : The contents of this variable length field, are used for defining the network which is actually advertised in this update message. BGP4 supports classless addressing and CIDR.

8.17.6 Keepalive Message :

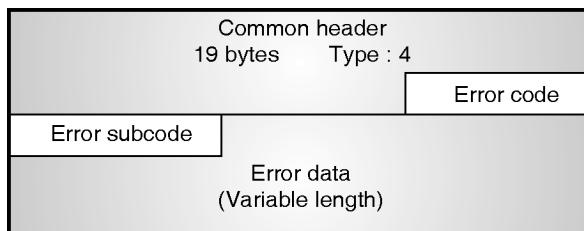
- The keepalive messages are regularly exchanged by all the routers running the BGP protocol, to tell each other that they are alive.
- The format of keepalive message is as shown in Fig. 8.17.6 which shows that it consists of only the common header.



(G-2130) Fig. 8.17.6 : Format of keepalive message

8.17.7 Notification Message :

- A router sends the notification message whenever it detects an error condition or when a router wants to terminate the connection.
- Fig. 8.17.7 shows the format of the keepalive message.



(G-2131) Fig. 8.17.7 : Notification message

- The notification message has the following important fields :
 1. **Error code** : The contents of this 1-byte field are used for defining the category of error.
 2. **Error subcode** : The contents of this 1-byte field are used to further define the type of error in each category.
 3. **Error data** : The contents of this field can be used for giving more diagnostic information about the error.



8.17.8 Encapsulation :

- BGP messages are encapsulated in TCP segments by using the well known port 179.
- The error control and flow control are therefore not needed.
- After opening a TCP connection, the update, keepalive and notification messages are exchanged until a notification message is sent.

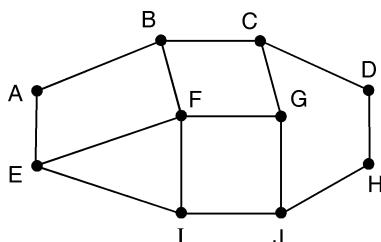
8.17.9 How does BGP Solve the Count to Infinity Problem ?

SPPU : May 07

University Questions

Q. 1 How BGP protocol solves the count to infinity problem ? **(May 07, 6 Marks)**

- The BGP is basically a distance vector protocol.
- But it is very much different from the most other protocols such as RIP.
- Instead of maintaining just the cost of each destination, each BGP router keeps track of the path used.
- Similarly instead of periodically giving each neighbour its estimated cost to each possible destination, each BGP router tells its neighbour the exact path that it is using.
- Fig. 8.17.8 shows a set of BGP routers and Table 8.17.1 shows the information that router F receives from its neighbours about "D".
- BGP can solve the count to infinity problem easily.
- This can be explained as follows : Suppose that the router G in Fig. 8.17.8 crashes, or if the line FG becomes faulty, then router F receives routes from the remaining three neighbours i.e. B, I and E.



(G-512) Fig. 8.17.8 : A set of BGP router

- As shown in Table 8.17.1, these routes are BCD, IFGCD and EFGCD.

Table 8.17.1 : Information received by F from neighbours about D

Neighbour	Information
B	I use path BCD to reach D.
G	I use path GCD to reach D.
I	I use path IFGCD to reach D.
E	I use path EFGCD to reach D.

- Looking at these routes, router F immediately understands that, the routes IFGCD and EFGCD are useless because they pass through F itself.
- So it decides to choose FBCD path as a new route. This avoids the count-to-infinity problem.

8.18 Interior Gateway Routing Protocol (IGRP) :

- In the mid-1980's Cisco Systems developed the Interior Gateway Routing Protocol (IGRP).
- Interior Gateway Routing Protocol is a distance vector routing protocol which provides routing within an autonomous system (AS).
- In the mid-1980s, the Routing Information Protocol (RIP) was the most popular Interior Gateway Routing Protocol.
- Though RIP was useful for routing within a small to moderate size homogeneous internetworks, it becomes difficult in the large networks due to growth of network.
- For the larger networks RIP protocol is replaced by IGRP protocol Due to its robustness property.
- Initially IGRP implementation was worked in Internet Protocol (IP) networks.
- It was designed to work in any network environment. After that it started to run in the OSI Connectionless-Network Protocol networks.
- In the early 1990's Cisco developed Enhanced IGRP (EIGRP) To improve the operating efficiency of IGRP.

8.18.1 Characteristics of IGRP Protocol :

- The characteristics of the IGRP are as follows :
- 1. IGRP is a Distance vector routing protocol.



2. In IGRP a routing update message is sent at regular intervals (i.e every 90 seconds) to each of its neighboring routers.
3. It uses multipath routing.
4. For automatic calculation of best possible route it uses either the administrator set or the default weightings.
5. IGRP uses composite metric based on the bandwidth and delay.
6. To determine the best path to a particular destination, it uses the Bellman-Ford Distance Vector routing algorithm.
7. It supports only Internet Protocol (IP) routing.
8. IGRP routes have an administrative distance of 100.
9. It supports a maximum of 100 hops. This value can be adjusted to a maximum of 255 hops.

8.18.2 Stability Features of IGRP :

- To improve the stability of IGRP, it provides the following stability features :
 1. **Hold-downs** : These are used to prevent regular update messages from improper restoration of a route which might have gone bad.
 2. **Split horizons** : This rule helps to prevent the routing loops. They provide extra algorithm stability.
 3. **Poison reverse updates** : The split horizons should prevent the routing loops between adjacent routers, poison reverse updates are proposed to overcome the larger routing loops. To remove the route and place it in hold-down, Poison reverse updates are sent.

8.18.3 IGRP Timers :

- IGRP has four basic timers :
 1. **Update Timer (default 90 seconds)** : This timer indicates how often the router will send out a routing table update.
 2. **Invalid Timer (default 270 seconds)** : This timer indicates how long a route will remain in a routing table before being marked as invalid, if there are no new updates about this route.
 3. **Hold down Timer (default 280 seconds)** : This timer indicates how long IGRP will suppress a route that it has

placed in a hold-down state. It specifies the hold-down period. Until the hold-down timer expires, IGRP will not accept any new updates for routes in a hold-down state.

4. **Flush Timer (default 630 seconds)** : This timer indicates how long a route can remain in a routing table before being flushed out.

8.19 Enhanced IGRP (EIGRP) :

- Cisco introduced an improved version of IGRP known as EIGRP which combines the advantages of link state protocols and distance vector protocols.
- EIGRP offers compatibility and flawless interoperation with IGRP routers.
- Enhanced IGRP includes the Diffusing Update Algorithm (DUAL).

8.19.1 Features of Enhanced IGRP (EIGRP) :

- EIGRP includes the following features :
 1. **Fast convergence** :
 - To achieve the convergence quickly Enhanced IGRP uses DUAL.
 - Routing tables of all the neighbors are stored in a router running Enhanced IGRP. So that alternate routes are adapted quickly.
 - If no suitable route exists, EIGRP queries its neighbors to find out an alternate route.
 - These queries broadcasts until an alternate route is found.

2. **Variable length subnet masks** :

- Enhanced IGRP consists of full support for the subnet masks with variable lengths.
- On a network number boundary subnet routes are automatically summarized.

3. **Partial, bounded updates** :

- EIGRP does not make periodic updates. When the metric for a route changes, they send partial updates only.
- Due to automatic propagation of partial updates only the routers which need an information is updated. Due to this ability



- Enhanced IGRP consumes significantly less bandwidth as compared to the IGRP.
- 4. Multiple network-layer support :**
- EIGRP provides the support for IP, AppleTalk, and Novell NetWare.
 - Routes learned from OSPF, Routing Information Protocol (RIP), Exterior Gateway Protocol (EGP), or Border Gateway Protocol (BGP) are redistributed in the IP implementation.
 - The routes learned from the Routing Table Maintenance Protocol (RTMP) are redistributed in the AppleTalk implementation.
 - The routes learned from Novell RIP or Service Advertisement Protocol (SAP) are redistributed in the Novell implementation.

8.19.2 Enhanced IGRP Technologies :

- Enhanced IGRP features four new technologies :
- 1. Neighbor discovery / recovery :**
- This technology is used by the routers to learn dynamically about other routers on their networks that are directly attached.
 - Routers should also find out when their neighbors become inoperative or unreachable.
 - By sending small hello packets periodically this process is achieved with low overhead.
 - Until a router receives hello packets from a neighboring router, it assumes that the neighbor is active and the routing information can be exchanged.
- 2. Reliable Transport Protocol (RTP) :**
- For guaranteed, ordered delivery of enhanced IGRP packets to all neighbors, this protocol is responsible.
 - RTP supports intermixed transmission of multicast or unicast packets.
 - For the efficiency purpose, only certain enhanced IGRP packets are reliably transmitted.
 - A single multicast hello packet is sent by EIGRP which contains an indicator that informs the receivers that no need of packet acknowledgement.
 - Other types of packet like update, indicates the packet that acknowledgment is needed.

- When unacknowledged packets are pending, RTP has a provision for sending multicast packets quickly.

- This will help to ensure that, convergence time remains low in the presence of varying speed links.

3. DUAL finite state machine :

- It represents the decision process for all route calculation.
- The routes advertised by all neighbors are tracked by this process.
- To choose an efficient, loop-free path, DUAL uses distance information and based on the feasible successors it selects routes for insertion in a routing table.
- A feasible successor is a neighboring router used for forwarding of a packet having a least-cost path to a destination.
- This router is not a part of the routing loop.
- If there is change in the topology or if a neighbor changes a metric, DUAL will check for feasible successors.
- If change occurs, it uses it to avoid unnecessarily route diffusing computation.
- If there are no feasible successor found but still neighbors advertise the destination, to determine a new successor diffusing computation should occur.
- Though re-computation is not processor intensive, it affects the convergence time, so it is beneficial to avoid unnecessary re-computations.

4. Protocol-dependent modules :

- For network-layer protocol-specific requirements protocol dependent modules are responsible. e.g For transmitting and receiving EIGRP packets encapsulated in IP, the IP-EIGRP module is responsible.
- In order to make the routing decisions, IP-EIGRP asks DUAL, and the results is stored in the IP routing table. IP-EIGRP redistributes the routes learned by other IP routing protocols.

8.19.3 Routing Concepts in EIGRP :

- Following are the fundamental concepts on which EIGRP relies :



- | | |
|---------------------|--------------------|
| 1. Neighbour tables | 2. Topology tables |
| 3. Route states | 4. Route tagging |

1. Neighbour Tables :

- When a router finds out a new neighbor, it records the address of neighbor and it interface an entry in the neighbor table.
- For each protocol-dependent module a single neighbor table exists.
- A hold time is advertised when a neighbor sends a hello packet.
- Within the hold time if a hello packet is not received, then hold time expires and the topology change is informed to DUAL.
- An information required for the RTP is also included in the neighbor table entry.
- To match acknowledgments with the data packets **Sequence numbers** are used.
- In order to detect an out-of-order packets, the last sequence number received from the neighbor is recorded.
- To queue packets for possible retransmission, a transmission list is used.
- To calculate the best possible retransmission interval Round-trip timers are used in the neighbor-table entry.

2. Topology Tables :

- All destinations advertised by the neighboring routers are included in the topology tables.
- Every entry in the topology table consists of the destination address and a list of neighbors that have advertised the destination.

3. Route States :

- For a destination, a topology table entry can exist in an active or passive state.
- If the router is performing a recomputation, a destination is said to be in an active state.
- If the router is not performing a recomputation a destination is said to be in the passive state.
- A destination will not go into the active state, if the feasible successors are always available which avoids the recomputation.
- The router starts the recomputation by transmitting a query packet to each of its neighboring routers.

- A reply packet is sent by the neighboring router which indicates that it has a feasible successor for the destination.
- It will send a query packet which indicates that it will participate in the recomputation.
- In the active state of a destination, a router cannot change the information of destination's routing-table.
- The topology-table entry for the destination returns to the passive state after receiving a reply from each neighboring router, then the router can select a successor.

4. Route Tagging :

- EIGRP supports internal and external routes. Internal routes begin within an EIGRP AS.
- Hence, a directly attached network which is configured to run EIGRP is considered an internal route.
- This information is propagated throughout the Enhanced IGRP AS.
- External routes exist in the routing table as a static route or they are learned by another routing protocol.
- External routes are tagged independently with the identity of their origin.
- External routes are tagged with the information such as Router ID of the EIGRP router that reallocate the route, AS number of the destination, Configurable administrator tag, ID of the external protocol, Metric from the external protocol and Bit flags for default routing.

8.19.4 Packet Types in Enhanced IGRP :

- Following packet types are used in the enhanced IGRP :
 1. **Hello packet** : These are multicast packets for neighbour discovery/recovery and there is no need of acknowledgment.
 2. **Acknowledgment packet** : It is a hello packet which has no data. It consists of a nonzero acknowledgment number and they are always sent by using a unicast address.
 3. **Update packet** :
 - To convey the reachability of destinations these packets are used.
 - Unicast update packets are sent if a new neighbour is found.



- So that the neighbour can build up its topology table.

4. Query and reply :

- Query and reply packets are always multicast and unicast respectively.
- When a destination has no feasible successors query and reply packets are sent.
- If the feasible successors exists there is no need to recompute the route.
- This is informed to the originator by sending the reply packets in response to query packets.
- Query and reply packets are reliably transmitted.

5. Request packet :

- To obtain the specific information from one or more neighbors, request packets are sent.
- These can be multicast or unicast packets which are used in route server applications. Request packets are unreliable.

8.19.5 Comparison between IGRP and EIGRP:

- Table 8.19.1 shows the comparison between IGRP and EIGRP.

Table 8.19.1

Sr. No	Parameter	IGRP	EIGRP
1.	Long Form	Interior Gateway Routing Protocol	Enhanced Interior Gateway Routing Protocol
2.	Supported Addressing	Classful	Classless
3.	Least hop count	255	256
4.	Convergence	Slow	Fast
5.	Bits provided for bandwidth and delay	24	32
6.	Algorithm used	Bellman Ford	Diffusing Update Algorithm (DUAL)
7.	Administrative distance	100	90
8.	Bandwidth required	More	Less

Review Questions

- Q. 1 Write short notes on : Hierarchical routing.
- Q. 2 Write short notes on : Multicast routing.
- Q. 3 What is unicast routing ?
- Q. 4 What is multicast routing ?
- Q. 5 Define the following :
1. Intradomain routing.
 2. Interdomain routing.
- Q. 6 Explain the following terms :
1. Unicast routing
 2. Broadcast routing and
 3. Multicast routing.
- Q. 7 State the optimality principle.
- Q. 8 What is the difference between static and dynamic routing algorithms ?
- Q. 9 Explain distance vector routing algorithm.
- Q. 10 What is looping in DVR ?
- Q. 11 Write a short note on : Count to infinity problem.
- Q. 12 Explain the link state routing algorithm.
- Q. 13 Compare DVR and LSR.
- Q. 14 Explain the Bellman Ford algorithm.
- Q. 15 What is PVR ?
- Q. 16 Explain the RIP updating algorithm.
- Q. 17 Describe the RIP message format.
- Q. 18 What is OSPF ? Is it intradomain or interdomain protocol ?
- Q. 19 State disadvantages of RIP. How are they overcome using OSPF ?
- Q. 20 State and explain important features of OSPF (any four).
- Q. 21 Compare RIP and OSPF.
- Q. 22 What is BGP ? Explain its packet format.
- Q. 23 How does BGP solve the count to infinity problem ?
- Q. 24 State the names of three intradomain routing protocols.
- Q. 25 Explain IGRP.
- Q. 26 Explain EIGRP.

Unit VI

Chapter 9

Transport Layer-Services and Protocols

Syllabus

Transport layer services (Duties), TCP : COTS, TCP header, Services, Segments, Connection establishment, Flow control, Congestion control, Congestion control algorithms, Leaky bucket, Token bucket and QoS, Timers, UDP : CLTS, UDP header, Datagram, Services, Applications, Socket : Primitives, TCP & UDP sockets.

Case study : Client server model using simple socket programming.

Case study on transport layer security - Firewall (Stateless Packet filtering), Stateful, Application.

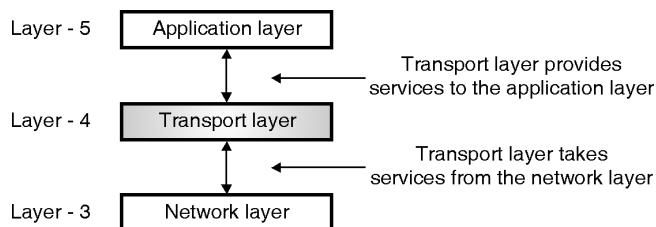
Chapter Contents

9.1	Introduction	9.13	A TCP Connection
9.2	Transport Layer Duties and Functionalities	9.14	Flow Control
9.3	Transport Layer Services	9.15	Congestion Control
9.4	Transport Layer Protocols	9.16	Congestion Control in Datagram Subnets
9.5	User Datagram Protocol (UDP)	9.17	Quality of Service (QoS)
9.6	UDP Services	9.18	TCP Congestion Control
9.7	UDP Applications	9.19	TCP Timer Management
9.8	UDP Features	9.20	Comparison of UDP and TCP
9.9	Transmission Control Protocol (TCP)	9.21	Sockets
9.10	TCP Services	9.22	Case study :Socket Programming with TCP
9.11	Features of TCP	9.23	University Questions and Answers
9.12	The TCP Protocol		



9.1 Introduction :

- The transport layer is the core of the Internet model.
- The application layer programs interact with each other using the services of the transport layer.
- Transport layer provides services to the application layer and takes services from the network layer.
- Fig. 9.1.1 shows the position of the transport layer in the 5-layer internet model.



(G-592) Fig. 9.1.1 : Position of transport layer

- The transport layer is fourth layer in this model. It connects the lower three layers to upper three layers of an OSI layer.

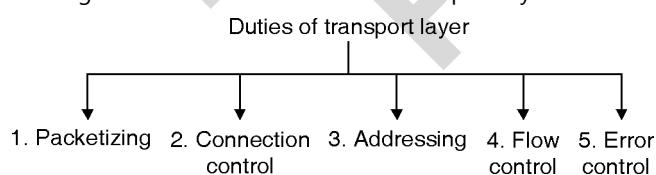
9.2 Transport Layer Duties and Functionalities :

SPPU : Dec. 13

University Questions

Q. 1 Explain duties of transport layer and differentiate between connection-oriented and connection-less service. **(Dec. 13, 9 Marks)**

- Transport layer is meant for the process to process delivery and it is achieved by performing a number of functions.
- Fig. 9.2.1 lists the functions of a transport layer.



(G-1407) Fig. 9.2.1 : Duties of transport layer

1. Packetizing :

- The transport layer creates packets with the help of encapsulation on the messages received from the application layer. Packetizing is a process of dividing a long message into smaller ones.
- These packets are then encapsulated into the data field of the transport layer packet. The headers containing source and destination address are then added.

- The length of the message which is to be divided can vary from several lines (e-mail) to several pages.
- But the size of the message can become a problem. The message size can be larger than the maximum size that can be handled by the lower layer protocols.
- Hence the messages must be divided into smaller sections. Each small section is then encapsulated into a separate packet.
- Then a header is added to each packet to allow the transport layer to perform its other functions.

2. Connection control :

- Transport layer protocols are divided into two categories :
 1. Connection oriented.
 2. Connectionless.

Connection oriented delivery :

- A connection oriented transport layer protocol establishes a connection i.e. virtual path between sender and receiver.
- This is a virtual connection. The packet may travel out of order.
- The packets are numbered consecutively and communication is bi directional.

Connectionless delivery :

- A connectionless transport protocol will treat each packet independently.
- There is no connection between them. Each packet can take its own different route.

3. Addressing :

- The client needs the address of the remote computer it wants to communicate with.
- Such a remote computer has a unique address so that it can be distinguished from all the other computers.

4. Flow and error control :

- For high reliability the flow control and error control should be incorporated.
- **Flow control :** We know that data link layer can provide the flow control. Similarly transport layer also can provide flow control. But this flow control is performed end to end and not across a single link.



- Error control :** The transport layer can provide error control as well. But error control at transport layer is performed end to end and not across a single link. Error correction is generally achieved by retransmission of the packets discarded due to errors.

Congestion control and QoS :

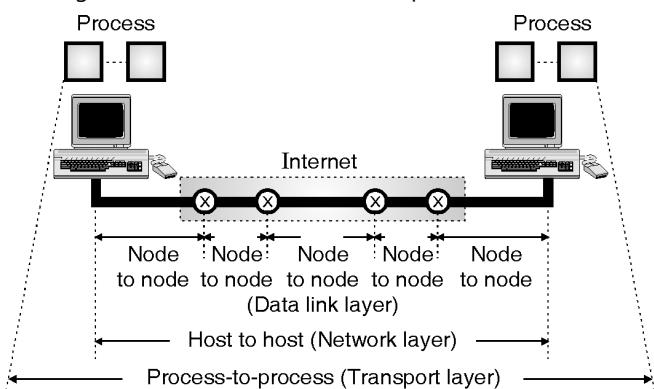
- The congestion can take place in the data link, network or transport layer.
- But the effect of congestion is generally evident in the transport layer.
- Quality of Service (QoS) can be implemented in other layers but its actual effect is felt in the transport layer.
- The transport layer enhances the QoS provided by the network layer.

9.3 Transport Layer Services :

- In this section we are going to discuss the services provided by the transport layer.

9.3.1 Process-to-Process Communication :

- The data link layer performs a node to node delivery.
- The network layer carries out the datagram delivery between two hosts (host to host delivery).
- But the real communication takes place between two processes or application programs for which we need the **process-to-process delivery**.
- The transport layer takes care of the **process-to-process delivery**.
- In this a packet from one process is delivered to the other process.
- The relationship between the communicating processes is the client-server relationship.
- Fig. 9.3.1 demonstrates the three processes.



(G-594) Fig. 9.3.1 : Types of data deliveries

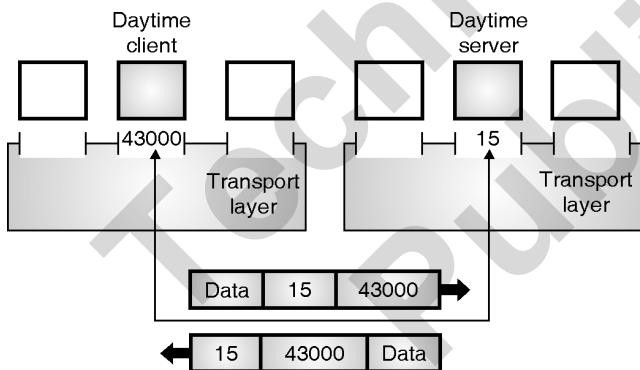
- There is a difference between host-to-host communication and process to process communication that we need to understand clearly.
- The host to host (computer to computer) communication is handled by the network layer.
- But this communication only ensures that the message is delivered to the destination computer. But this is not enough.
- It is necessary to handover this message to the correct process. The transport layer will take care of this.

9.3.2 Addressing : Port Number :

- There are several ways of achieving the process-to-process communication, but the most common method is using the client-server paradigm.
- Client** is defined as the process on the local host.
- It needs services from another process called **server** which is on the other (remote) host.
- Both client and server have the same name. Some of the important terms related to the client-server paradigm are :
 1. Local host
 2. Remote host
 3. Local process
 4. Remote process
- We can use the IP addresses to define the local host and remote host.
- But this is not enough to define a process.
- In order to define a process, we have to use one more identifier called **Port Numbers**.
- In TCP/protocol suite, the port numbers are integers and they are numbered between 0 and 65,535.
- At the data link layer we need a MAC address, at the network layer we need to use an IP address.
- A datagram uses the destination IP address to deliver the datagram and uses the source IP address for the destination's reply.
- At the transport layer a transport layer address called a **port number** is required to be used to choose among multiple processes running on the destination host.
- The destination port number is required to make the packet delivery and the source port number is needed to return back the reply.



- In the Internet model, the port numbers are 16 bit integers.
- Hence the number of possible port numbers will be $2^{16} = 65,535$ and the port numbers range from 0 to 65,535.
- The client program identifies itself with a port number which is chosen randomly.
- This number is called as **ephemeral port number**. Ephemeral means short lived. It is used because life of a client is generally short.
- The server process should also identify itself with a port number but this port number can not be chosen randomly.
- The Internet uses universal port numbers for servers and these numbers are called as **well known port numbers**.
- Every client process knows the well known port numbers of the pre identified server process.
- For example, a Day time client process can use an ephemeral (temporary) port number 43000 for identifying itself, the Day time server process must use the well known (permanent) port number 15. This is illustrated in Fig. 9.3.2.



(G-595) Fig. 9.3.2 : Concept of port numbers

What is difference between IP addresses and port numbers ?

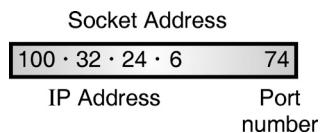
- The IP addresses and port numbers have altogether different roles in selecting the final destination of data.
- The destination IP address is used for defining a particular host among the millions of hosts in the world.
- After a particular host is selected, the port number is used for identifying one of the processes on this selected host.

IANA Ranges :

- The port numbers are divided into three ranges by IANA (International Assigned Number Authority).
- The ranges are as follows :
 1. Well known ports
 2. Registered ports
 3. Dynamic or private ports.
- 1. Well known ports :** The ports from 0 to 1023 are known as well known ports. They are assigned as well as controlled by IANA.
- 2. Registered ports :** The ports from 1024 to 49,151 are neither controlled nor assigned by IANA. We can only register them with IANA to avoid duplication.
- 3. Dynamic or private ports :** The ports from 49,152 to 63,535 are known as dynamic ports and they are neither controlled nor registered.
- They can be used by any process. Dynamic ports are also known as private ports and dynamic port are called as ephemeral ports.

Socket Address :

- Process to process delivery (transport layer communication) has to use two addresses, one is IP address and the other is port number at each end to make a connection. Hence a process to process delivery uses the combination of these two.
- The combination of IP address and port number is as shown in Fig. 9.3.3 and it is known as the socket address.



(G-1548) Fig. 9.3.3 : Socket address

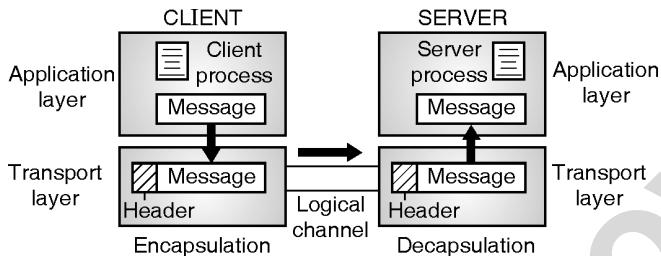
- The client socket address defines the client process uniquely whereas the server socket address defines the server process uniquely.
- A transport layer protocol requires the client socket address as well as the server socket address.
- These two addresses contain four pieces.
- These four pieces go into the IP header and the transport layer protocol header.



- The IP header contains the IP addresses while the UDP and TCP headers contain the port numbers.
- If we want to use the transport layer services in the Internet, then we have to use a pair of socket addresses namely the clients socket address and the server's socket address.

9.3.3 Encapsulation and Decapsulation :

- The transport layer carries out the **Encapsulation** of the message at the sending end and then **Decapsulation** at the receiving end when two computers communicate. This process has been illustrated in Fig. 9.3.4.



(G-2012) Fig. 9.3.4 : Encapsulation and decapsulation

Encapsulation :

- At the sending end the process that has a message to send, will pass it to the transport layer alongwith a pair of socket addresses and some additional information.
- The transport layer adds its own header to this data. This packet at the transport layer in the Internet is known by different names such as **user datagram, segment or packet**.

Decapsulation :

- When the segment or datagram arrives at the receiving end, the header is isolated and destroyed, and the message is delivered to the process running at the application layer as shown in Fig. 9.3.4.
- The socket address of the sender process is then handed over to the destination process.

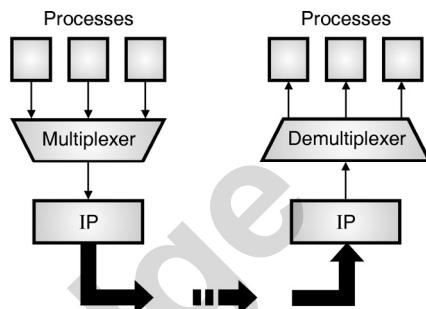
9.3.4 Multiplexing and Demultiplexing :

SPPU : May 06, Dec. 16

University Questions

- Q. 1** Explain the multiplexing technique used in transport layer. **(May 06, 8 Marks)**
- Q. 2** Explain multiplexing technique at transport layer. **(Dec. 16, 4 Marks)**

- The addressing mechanism allows multiplexing and demultiplexing taking place at the transport layer as shown in Fig. 9.3.5.



(G-597) Fig. 9.3.5 : Multiplexing and demultiplexing

Multiplexing :

- At the sending end, there are several processes that are interested in sending packets.
- But there is only one transport layer protocol (UDP or TCP).
- Thus it is a many processes-one transport layer protocol situation.
- Such a many-to-one relationship requires multiplexing.
- The protocol first accepts messages from different processes.
- These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it.
- Then the transport layer adds header and passes the packet to the network layer as shown in Fig. 9.3.5.

Demultiplexing :

- At the receiving end, the relationship is one as to many. So we need a demultiplexer.
- First the transport layer receives datagrams from the network layer.
- The transport layer then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

9.3.5 Flow Control :

- If the packets produced by the sender are at a rate X and the receiver is receiving them at a rate Y, then for $X = Y$, there will be a perfect balance observed in the system.
- But if X is higher than Y (source is producing packets at a rate which is higher than the rate at which the receiver



- is accepting them), then the receiver can be overwhelmed and has to **discard** some packets.
- And if X is less than Y (i.e. source is producing packets at slower rate than the rate of acceptance at the receiver) then system becomes **less efficient**.
 - Flow control is related to the situation in which $X > Y$ because it is very important to prevent data loss (due to discarding of packets) at the receiver site.

Pushing and pulling for flow control :

- There are two different ways of delivering the packets produced by the sender to the receiver.
- They are pushing or pulling.

1. Pushing :

- If the sender is sending the packets soon as they are produced, without receiving any prior request from the receiver then this type of delivery is called as **pushing**. Fig. 9.3.6(a) illustrates this concept.

2. Pulling :

- If the sender sends the produced packets only when they are requested by the receiver then the delivery is called as **pulling**. Fig. 9.3.6(b) illustrates the principle of pulling.



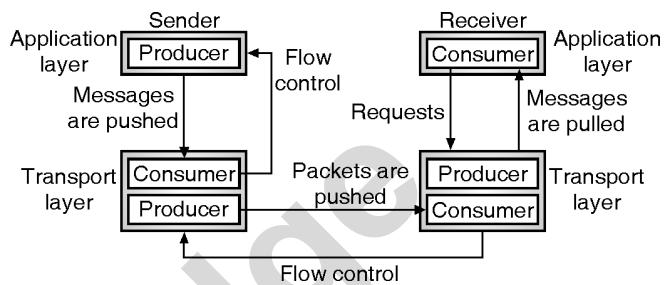
(G-2013) Fig. 9.3.6 (a)

(G-2013) Fig. 9.3.6 (b)

- In case of **pushing** type delivery, if the packets are being sent at a higher rate than that of receiving, then the receiver will be **overwhelmed**, and some received packets will have to be discarded.
- In order to avoid discarding of packets, the **flow control** will have to be exercised.
- For this the receiver has to warn the sender to stop the delivery when it is overwhelmed and it has to inform the sender again to start delivery when it (receiver) is ready, to receive the packets.
- In case of **pulling type delivery**, the receiver is actually pulling the packets from the sender.
- It requests for the packets when it is ready. Therefore the flow control is not required in this case.

9.3.6 Flow Control at Transport Layer :

- The concept of flow control at transport layer has been illustrated in Fig. 9.3.7.



(G-2014) Fig. 9.3.7 : Flow control at transport layer

- It shows the communication taking place between a sender and a receiver.
- As shown in Fig. 9.3.7, there are four entities involved in this communication. They are as follows :
 1. Sender process.
 2. Sender transport layer.
 3. Receiver process.
 4. Receiver transport layer.
- We will discuss the flow control by considering the sending and receiving ends separately.

Sending end :

- The first entity on the sending end is the **sender process**, at the application layer. It works only as a **producer** which produces chunk of messages and pushes them to the transport layer on the sending end, as shown in Fig. 9.3.7.
- The second entity on the sending end is the **sender transport layer**. It has two different roles to play.
 - First it acts as a **customer** and consumes all the messages produced and pushed by the producer.
 - Then it encapsulates those messages into packets and pushes them to the receiver transport layer as shown in Fig. 9.3.7. Here it acts as a **producer**.

Receiving end :

- The first entity on the receiving end is the **receiver transport layer**. It also has two different roles to play.
 - It acts as a **consumer** for the packets pushed by the senders transport layer and it also acts as the **producer**.
 - It has decapsulate the messages and deliver them to the application layer as shown in Fig. 9.3.7.



- However the delivery of decapsulated messages to the application layer is a **pulling type delivery**.
- That means the transport layer waits till the application layer process requests for the decapsulated messages.

Flow control :

- As shown in Fig. 9.3.7, the flow control is needed for atleast two cases.
- First is from transport layer of sender to the application layer of sender.
- And secondly form the transport layer of receiver to the transport layer of sender.

Buffers :

- It is possible to implement the flow control in many different ways.
- One of the ways of implementation is to use two **buffers** one each at the sending and receiving transport layers.
- A **buffer** is nothing but a set of memory locations which can temporarily hold (store) packets.
- It is possible to exercise flow control communication by sending signals from the consumer to producer.
- The **flow control** at the **sending end** takes place as follows :
 - As soon as the buffer at the transport layer becomes full it sends the stop message to its application layer in order to stop the chunk of messages that are being pushed into the buffer.
 - The second flow control takes place at the receiver transport layer as follows :
 - As soon as the buffer at receiver transport layer becomes full, it will inform the sender transport layer to stop pushing the packets.
 - Whenever the buffer becomes partially empty, it again informs the sender transport layer to start sending the packets again.

9.3.7 Error Control :

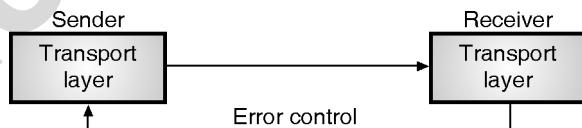
Need of error control :

- In the Internet, the network layer protocol IP has the responsibility to carry the packets from the transport layer at the sending end to the transport layer at the receiving end.

- But IP is unreliable. Therefore transport layer should be made reliable, in order to ensure reliability at the application layer.
- We can make the transport layer reliable by adding the **error control service** to the transport layer.

Duties of error control mechanism :

- Following are the important responsibilities of the error control mechanism introduced at the transport layer :
 1. To find and discard the corrupted packets.
 2. To keep the track of lost and discarded packets and to resend them.
 3. Identify the duplicate packets and discard them.
 4. To buffer out of order packets until the missing packets arrive.
- In the error control process, only the sending and receiving transport layers are involved.
- That means it is assumed that the chunk of messages exchanged between the application layers and transport layers are error free.
- The concept of error control at the transport layer level is demonstrated in Fig. 9.3.8.



(G-2015) Fig. 9.3.8 : Concept of error control at the transport layer

- The receiving transport layer manages the error control by communicating with the sending transport layer about the problem.

Sequence numbers :

- In order to exercise the error control at the transport layer following two requirements should be satisfied :
 1. The sending transport layer should know about the packet which is to be resent.
 2. The receiving transport layer should know about the packets which are duplicate or the ones that have arrived out of order.
- The requirements can be satisfied only if each packet has a unique **sequence number**.



- If a packet is either corrupted or lost the receiving transport layer will somehow inform the sending transport layer about the sequence number of those packets and request it to resend those packets.
- Due to the unique sequence number assigned to each packet it is possible for the receiving transport layer to identify the duplicate packets received.
- The out of order packets can also be recognized by observing gaps in the sequence numbers of the received packets.
- Packet numbers are given sequentially. But the length of the sequence number cannot be too long because the sequence number is to be included in the header of the packets.
- If the header of a packet allows "m" bits per sequence number, then the range of sequence number will be from 0 to $2^m - 1$. For example if m = 3 then the range of sequence numbers will be from 0 to 7.
- Thus sequence numbers are modulo 2^m .

Acknowledgement :

- The receiver side can send an acknowledgement (ACK) signal corresponding to each packet or each group of packets which arrived safe and sound.
- The question is what happens if a received packet is corrupted ? The answer is that the receiver simply discards the corrupted packet and does not send any ACK signal for it.
- The sender can detect a lost packet with the help of a timer. A timer is started at the sending end as soon as a packet is sent.
- If the ACK does not arrive before the expiry of the timer, then the sender treats the packet to be either lost or corrupted and resends it.
- The receiver silently discards the duplicate packets. It will either discard the out of order packets or stored until the missing packet is received.
- Note that every discarded packet is treated as a lost packet by the sender.

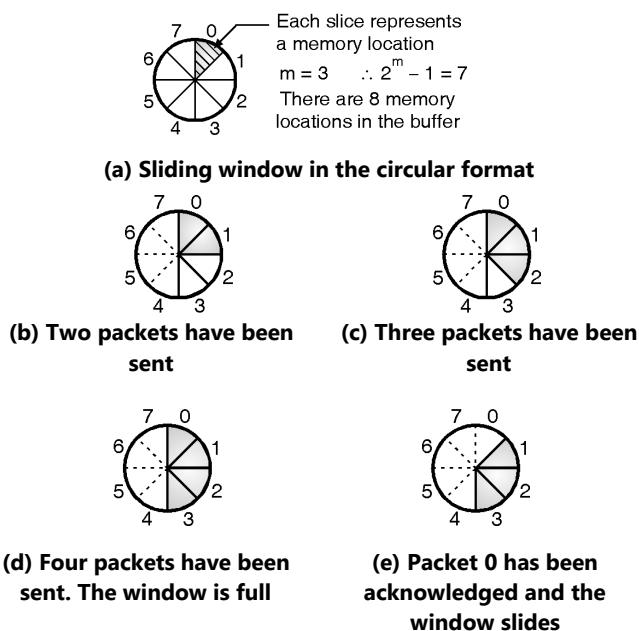
9.3.8 Combination of Flow and Error Control :

- Till now we have discussed the following important concepts :

1. We need to use buffers at the sending and receiving ends for exercising the flow control.
 2. Also we have to use the sequence numbers and acknowledgements for exercising the error control.
- We can combine these two concepts together by using two numbered buffers one at the sender and the other at the receiver, in order to exercise a combination of flow and error control.
 - At the sending end, when a packet, is prepared to be sent, the number of the next free location (x) in the buffer is used as the sequence number of that packet.
 - As soon as the packet is sent, its copy is stored at location (x) in the sending end buffer and the sender waits for the acknowledgement from the receiver.
 - On reception of the acknowledgement of the sent packet, the copy of that packet is purged to make the memory location (x) free again.
 - At the receiver, when a packet having a sequence number "y" arrives, it is stored at the memory location "y" in the receiver buffer until the receiver application layer is ready to receive it.
 - The receiver will send the ACK message back to sender to inform it that packet "y" has arrived.

Sliding window :

- As the sequence numbers are modulo 2^m , we can use a circle as shown in Fig. 9.3.9 to represent the sequence number from 0 to $2^m - 1$.
- We can represent the buffer as a set of slices, called as the **sliding window** which will occupy a part of the circle at any time.
- In Fig. 9.3.9, we have assumed that m = 3. Therefore $2^m - 1 = 7$ and the sequence numbers are from 0 to 7.
- Hence the number of memory locations in a buffer will also be 8 i.e. 0 to 7.
- The sliding windows will correspond to the sender as well as receiver.
- On the sending side, when a packet is sent we will mark the corresponding slice.
- Therefore when marking of all the slices is done, it means the **sending buffer is full**, and it cannot accept any further messages from the application layer as shown in Fig. 9.3.9(d).



(G-2017) Fig. 9.3.9

- When the acknowledgement for segment "0" arrives at the sending end, the corresponding segment (segment 0) is unmarked and window slides ahead by one slice as shown in Fig. 9.3.9(e).
- The size of the **sending window** is 4.
- Note that the sliding window is just an abstraction. In actual practice, computer variables are used to hold the sequence number of the next packet to be sent and the last packet sent.

Sliding window in the linear format :

- This is another way to diagrammatically represent a sliding window. It is as shown in Fig. 9.3.10.
- | | |
|---|---|
| 6[7]0[1 2 3 4]5[6 7]1[] | 6[7]0[1 2 3 4]5[6 7]1[] |
| (a) Two packets have been sent | (b) Three packets have been sent |
| 6[7]0[1 2 3 4]5[6 7]1[] | 6[7]0[1 2 3 4]5[6 7]1[] |
| (c) Four packets have been sent. The window is full. | (d) Packet 0 has been acknowledged and the window slides |

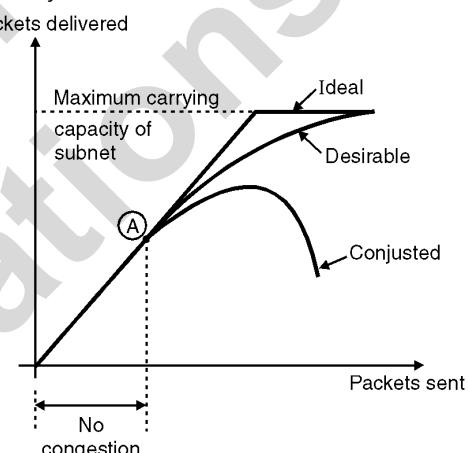
(G-2075)Fig. 9.3.10 : Sliding windows presented in the linear format

- The principle of this type of sliding window is same as that of the circular representation.
- The linear format is the most preferred format. It needs less space on paper.
- Fig. 9.3.10(a), (b), (c) and (d) are the sliding windows presented in the linear format corresponding to

Figs. 9.3.9(b), (c), (d) and (e) respectively in the circular presentation.

9.3.9 Congestion Control :

- An important issue in a packet switching network is congestion.
- If an extremely large number of packets are present in a part of a subnet, the performance degrades. This situation is called as congestion.
- Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network (i.e. the number of packets a network can handle).
- Fig. 9.3.11 explains the concept of congestion graphically.



(G-473) Fig. 9.3.11 : Concept of congestion

- Upto point A in Fig. 9.3.11, the number of packets sent into the subnet by the host is within the capacity of the network.
- So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place.
- But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.
- As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens.
- At very high traffic, the performance collapses completely and almost all packets are lost.
- This is the worst possible congestion.

**Need of congestion control :**

- We may define the **congestion control** as the mechanisms and techniques to control the congestion and keep the load below the capacity.
- It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.
- Congestion will result in long queues, which results in buffer overflow and loss of packets.
- So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

Causes of congestion :

- Congestion happens in any network due to waiting, and due to the abnormality in the flow.
- It also occurs due to the fact that routers and switches have queues at the buffers which store packet before and after their processing.

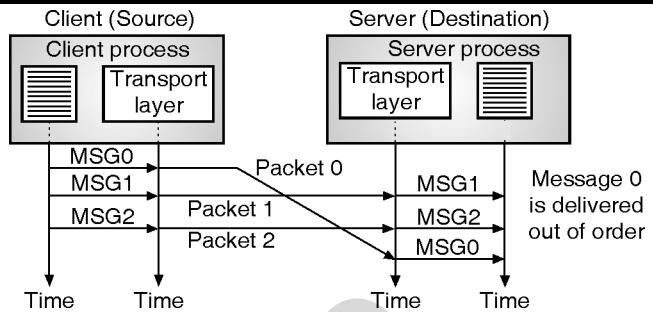
9.3.10 Connectionless and Connection Oriented Services(CLTS& COTS) :**SPPU : Dec. 13****University Questions**

Q. 1 Explain the duties of transport layer and differentiate between connection oriented and connectionless service. **(Dec. 13, 9 Marks)**

- A transport layer protocol is capable of providing two types of services :
 1. Connectionless services.
 2. Connection oriented services.
- The meaning of the words connectionless and connection oriented is different at the transport layer than that at the network layer.
- A connectionless service at the network layer means different datagrams of the same message following different paths.
- However at the transport layer, the meaning of connectionless service is independency between different packets.
- On the other hand a connection oriented service means the packets are interdependent.

Connectionless Transport service (CLTS) :

- Refer Fig. 9.3.12 to understand the concept of connectionless service.

**(G-2018) Fig. 9.3.12 : Concept of connectionless service**

- The source process at the application layer first divides its message in chunks of data the size of which is acceptable to the transport layer.
- These data chunks are then delivered to the transport layer one by one. These chunks are treated as independent units by the transport layer.
- Every data chunk arriving from the application layer is encapsulated in a packet by the transport layer and sent to the destination transport layer as shown in Fig. 9.3.12.

Out of Order Delivery :

- In Fig. 9.3.12 we have considered three chunks of independent messages 0, 1 and 2. As the corresponding packets also are independent of each other and as they are free to follow their own path, these packets can arrive out of order at the destination as shown in Fig. 9.3.12.
- Naturally they are delivered to server process in an out of order manner.
- As seen in Fig. 9.3.12, at the sending end (client) the three chunks of messages 0, 1 and 2 are delivered to the transport layer in the order 0, 1, 2.
- But packet 0 travels a longer path and undergoes an extra delay.
- Therefore the packets are not delivered in order at the destination (server) transport layer.
- Therefore the message chunks delivered to the server process will also be out of order (1, 2, 0).
- If these chunks are of the same message then due to their out of order delivery the server will receive a strange message.

One packet is lost :

- The UDP packets are not numbered. So if one of the packets is lost, then the receiving transport layer will not have any idea about the lost packet.

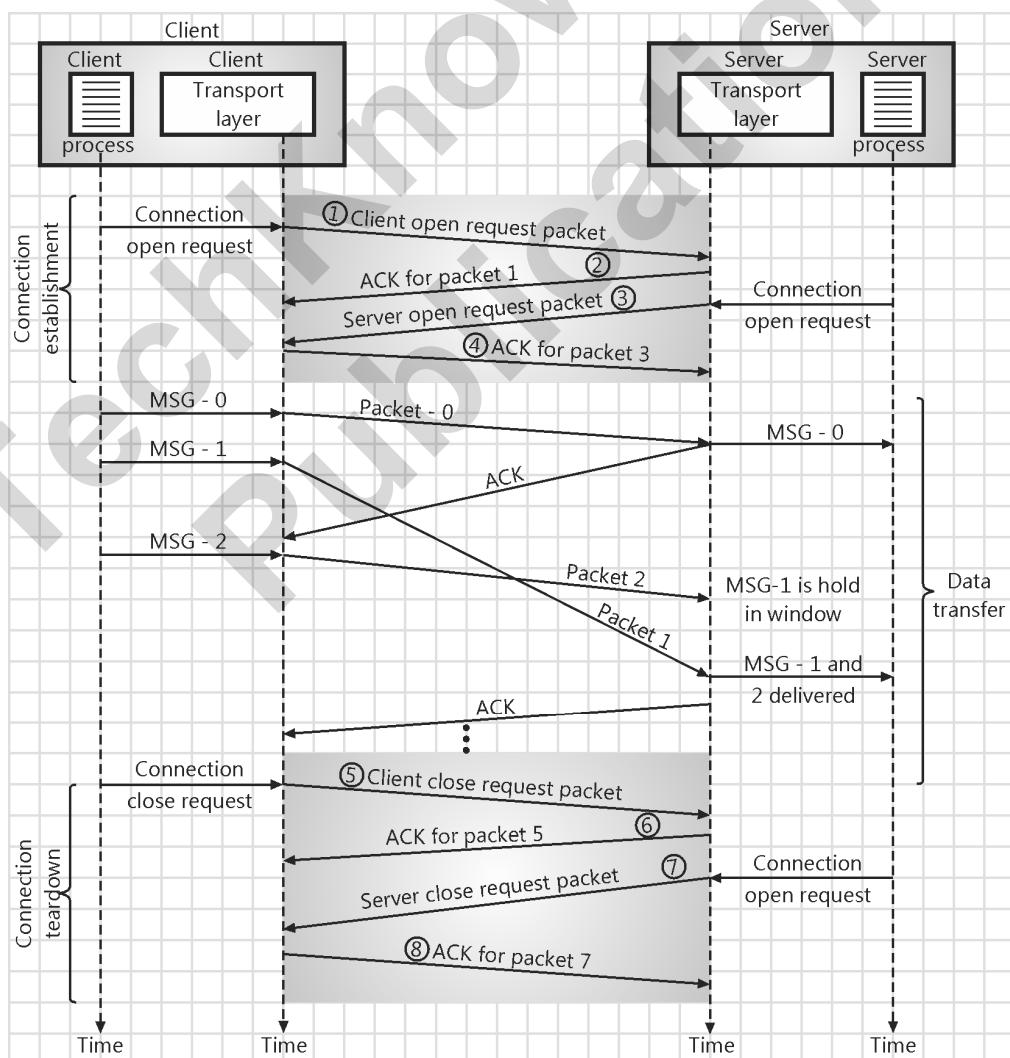


- It will simply deliver the received chunks of messages to the server process.
- The above problems arise due to **lack of coordination** between the two transport layers.
- Due to this lack of co-ordination it is not possible to implement flow control, error control or congestion control in the connectionless service.

Connection Oriented Transport Service (COTS) :

- As we know, there are three stages involved in the connection oriented service. They are :
 1. Connection establishment.
 2. Exchange of data.
 3. Connection teardown.
- The connection oriented service is present at the network layer as well, but it is different from that at the transport layer.y

- At the network layer, the meaning of connection oriented service involves the co-ordination between the hosts on either sides and all the routers between them.
- But at the transport layer, the meaning of connection oriented service is the end to end service that involves only the two hosts.
- Refer Fig. 9.3.13 to understand the concept of connection oriented service at the transport layer.
- In Fig. 9.3.13, all the three stages namely connection establishment, data exchange and connection teardown have been shown.
- It is important to note that it is possible to implement the flow control, error control and congestion control in the connection oriented service.



(G-2076) Fig. 9.3.13 : Concept of connection oriented service



Comparison of Connection Oriented and Connectionless Services :

Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection needs to be established	Connection need not be established
6.	Delays	More	Less
7.	Overheads	Less	More
8.	Packets travel	Sequentially	Randomly
9.	Congestion due to overloading	Not possible	Very much possible

9.3.11 Reliability at Transport Layer Versus Reliability at DLL :

SPPU : Dec. 14

University Questions

Q. 1 Explain how to achieve reliability at transport layer.
(Dec. 14, 4 Marks)

- The transport layer services can be of two types :
 1. Reliable services
 2. Unreliable services.

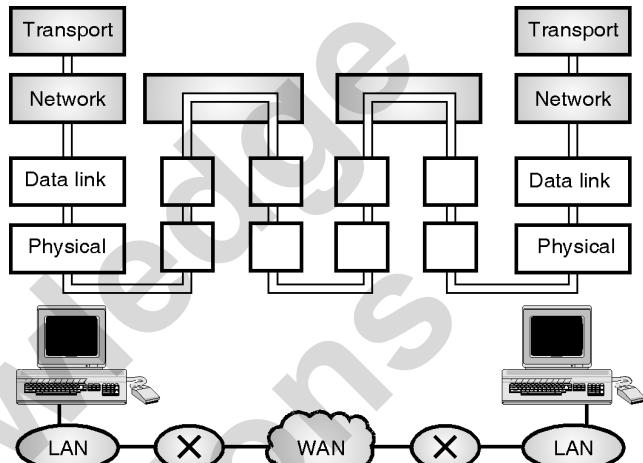
Reliable services :

- If the application layer program needs reliability then the reliable transport layer protocol is used which implements the flow and error control at the transport layer. But this service will be slow and more complex.

Unreliable services :

- But some application layer programs do not need reliability because they have their own flow and error control mechanisms. Such programs use an unreliable service.

- UDP is connectionless and unreliable, but TCP is connection oriented and reliable protocol. Both these are the transport layer protocols.
- We need reliability at the transport layer even though data link layer is reliable because the data link can provide reliability for only the node to node delivery.



(G-598) Fig. 9.3.14 : Error control

- The error control at the data link layer does not guarantee error control at the transport layer. The network layer service in the Internet is unreliable. Hence reliability at the transport layer must be ensured independently.
- Therefore flow and error controls are implemented in TCP using the sliding window protocols.
- This is reliability assurance at the transport layer. Note that the error is checked only upto the data link layer by the data link error control system.

9.3.12 Quality of Service (QoS) :

SPPU : May 08, May 11, Dec. 11, May 18, Dec. 19

University Questions

- Q. 1** Define Quality of Service and list the parameters typical to transport layer.
(May 08, May 11, 8 Marks)
- Q. 2** What are the different quality of service parameters present at transport layer ? (Dec. 11, 8 Marks)
- Q. 3** Write a short note on Quality of Service parameter in Transport layer. (May 18, Dec. 19, 4 Marks)

- As mentioned earlier, the QoS parameters are as follows :

**1. Connection establishment delay :**

- The time difference between the instant at which a request for transport connection is made and the instant at which it is confirmed is called as **connection establishment delay**.
- This delay should be as short as possible to ensure better service.

2. Connection establishment failure probability :

- Sometimes the connection may not get established even after the maximum connection establishment delay.
- This can be due to network congestion, lack of table space or some other problems.

3. Throughput :

- It is defined as the number of bytes of user data transferred per second, measured over some time interval.
- Throughput is measured separately for each direction.

4. Transit delay :

- It is the time duration between a message being sent by the transport user from the source machine and its being received by the transport user at the destination machine.

5. Residual error ratio :

- It measures the number of lost or garbled messages as a percentage of the total messages sent.
- Ideally the value of this ratio should be zero and practically it should be as small as possible.

6. Protection :

- This parameter provides a way to protect the transmitted data against reading or modifying it by some unauthorised parties.

7. Priority :

- Using this parameter the user can show that some of its connections are more important (have higher priority) than the other ones.
- This is important when congestions take place. Because the higher priority connections should get service before the low priority connections.

8. Resilience :

- Due to internal problem or congestion the transport layer spontaneously terminates a connection.
- The resilience parameter gives the probability of such a termination.

9.4 Transport Layer Protocols :

- We have discussed a few transport layer services in the previous section.
- By combining a set of these services as per requirement, we can create a transport layer protocol.
- It is important to understand the behavior of these general protocols, before we discuss the transport layer protocols such as UDP and TCP.
- In this section we will discuss the following protocols :
 1. Simple protocol.
 2. Stop and wait protocol.
 3. Go back N (GBN) protocol.
 4. Selective repeat protocol.
 5. Bidirectional protocol. (Piggybacking).

9.4.1 The Internet Transport Protocols (TCP and UDP) :

- The Internet has two main protocols in the transport layer.
- One of them is connection oriented and the other one supports the connectionless service.
- TCP (Transmission Control Protocol) is a connection oriented protocol and UDP (User's Data Protocol) is the connectionless protocol.
- UDP is basically just IP with an additional short header.

9.5 User Datagram Protocol (UDP) :

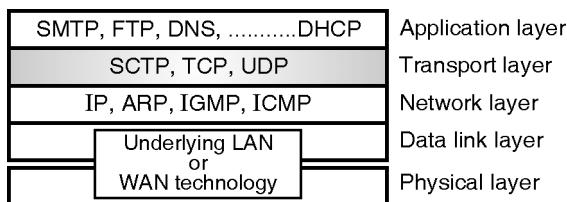
- The User Datagram Protocol is a very simple protocol. It adds little to the basic functionality of IP. Like IP, it is an unreliable, connectionless protocol.
- You do not need to establish a connection with a host before exchanging data with it using UDP, and there is no mechanism for ensuring that data sent is received.
- A unit of data sent using UDP is called a Datagram. UDP adds four 16-bit header fields (8 bytes) to whatever data is sent.



- These fields are : a length field, a checksum field, and source and destination port numbers. "Port number", in this context, represents a software port, not a hardware port.
- The concept of port numbers is common to both UDP and TCP.
- The port numbers identify which protocol module sent (or is to receive) the data.
- Most protocols have standard ports that are generally used for this.
- For example, the Telnet protocol generally uses port 23. The Simple Mail Transfer Protocol (SMTP) uses port 25.
- The use of standard port numbers makes it possible for clients to communicate with a server without first having to establish which port to use.
- The port number and the protocol field in the IP header duplicate each other to some extent, though the protocol field is not available to the higher-level protocols. IP uses the protocol field to determine whether data should be passed to the UDP or TCP module.
- UDP or TCP use the port number to determine which application-layer protocol should receive the data.
- Although UDP isn't reliable, it is still a preferred choice for many applications.
- It is used in real-time applications like Net audio and video where, if data is lost, it's better to do without it than send it again out of sequence.
- It is also used by protocols like the Simple Network Management Protocol (SNMP).

Relationship with other protocols :

- The relationship of UDP with the other protocols and layers of TCP/IP suite is as shown in Fig. 9.5.1.



(G-2019) Fig. 9.5.1 : Relation between UDP and other protocols

- As shown, UDP is located between IP and application layer. It therefore works as an intermediary between application program and the network layer.

9.5.1 Responsibilities of UDP :

- Being a transport layer protocol, the UDP has the following responsibilities :

 1. To create a process to process communication, UDP uses port numbers to accomplish this.
 2. To provide control mechanisms at the transport layer, UDP does not provide flow control or acknowledgements. It provides error detection. The erroneous packet is discarded.
 3. UDP does not add anything to the services of IP except for providing process to process communication.

9.5.2 Advantages of UDP :

- UDP, despite all its simplicity and powerlessness is still used because it offers the following advantages :

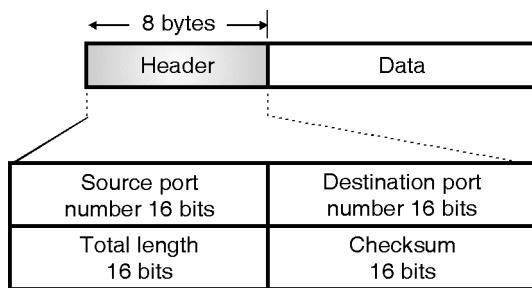
 1. UDP has minimum overheads.
 2. UDP can be easily used if the sending process is not too bothered about reliability.
 3. UDP reduces interaction between sender and receiver.

9.5.3 User Datagram :

- User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable 'best effort' delivery.
- This means that the arrival of packets is not guaranteed, nor is the correct sequencing of delivered packets.
- Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP.
- UDP is also used by applications that typically transmit small amounts of data at one time, for example, the Simple Network Management Protocol (SNMP).
- UDP provides a mechanism that application programs use to send data to other application programs.
- UDP provides protocol port numbers used to distinguish between multiple programs executing on a single device.
- That is, in addition to the data sent, each UDP message contains both a destination port number and a source port number.
- This makes it possible for the UDP software at the destination to deliver the message to the correct application program, and for the application program to send a reply.



- UDP packets are called as **user datagrams**.
- They have a fixed-size header of 8-bytes. The format of user datagram is as shown in Fig. 9.5.2.



(G-624)Fig. 9.5.2 : User datagram format

- The UDP header is divided into the following four 16-bit fields :
- | | |
|---------------------|-----------------|
| 1. Source port | 3. Total length |
| 2. Destination port | 4. Checksum. |

Source Port Number :

- Source port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information.
- If not used, a value of zero is inserted.
- This is a 16 bit field. That means the port numbers can range from 0 to 65,535.
- If the source host is a client, means if a client is sending a request using UDP, then generally a **ephemeral (temporary)** port number is requested by the process and chosen by the UDP.
- If the source host is a server that means if a server is sending a response message, mostly the **well known port** number is used.

Destination Port Number :

- The destination port number also is a 16 bit number and this port number is used by the process running on the destination host.
- If the destination host is a server that means if a client is sending a request to it, then a **well known port** number is used in most cases.
- However if the destination host is a client than means if a server is sending its response to it, then the chosen port number is generally an **ephemeral port** number.

Length :

- It is also a 16 bit field which is used for defining the total length of the UDP datagram including header as well as data.
- Due to 16 bit length it can define a total length of the datagram upto 65,535 bytes.
- However practically the total length of a UDP datagram is much smaller than 65,535 bytes.
- This is because the UDP datagram is to be stored in an IP datagram which itself has a length of 65,535 bytes.
- The **length** field in the UDP datagram is actually not necessary, because this UDP datagram is actually encapsulated in an IP datagram and the IP datagram has its own length field.
- So without using the length field in UDP datagram, we can obtain the length of the UDP datagram as follows :

$$\text{UDP length} = \text{IP length} - \text{IP header length}$$

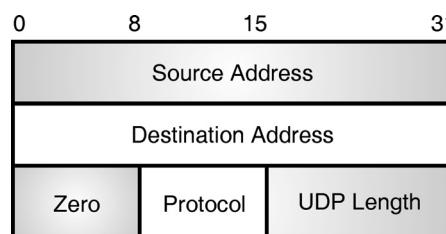
- Note that while delivering the UDP datagram to UDP layer, the IP software drops the IP header.

UDP Checksum :

- This is used to verify the integrity (i.e. to detect errors) of the UDP header.
- The checksum is performed on a "pseudo header" consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

9.5.4 UDP Pseudo Header :

- The purpose of using a pseudo-header is to verify that the UDP packet has reached its correct destination.
- The correct destination consists of a specific machine and a specific protocol port number within that machine.



(G-625) Fig. 9.5.3 : UDP pseudo header

- The UDP header itself specifies only the protocol port number.



- Thus, to verify the destination, UDP on the sending machine computes a checksum that covers the destination IP address as well as the UDP packet.
- At the ultimate destination, UDP software verifies the checksum using the destination IP address obtained from the header of the IP packet that carried the UDP message.
- If the checksum agrees, then it must be true that the packet has reached the intended destination host as well as the correct protocol port within that host.

User Interface :

- A user interface should allow the creation of new receive ports, receive operations on the receive ports that return the data octets and an indication of source port and source address, and an operation that allows a datagram to be sent, specifying the data, source and destination ports and addresses to be sent.

IP Interface :

- The UDP module must be able to determine the source and destination Internet addresses and the protocol field from the Internet header.
- One possible UDP/IP interface would return the whole Internet datagram including the entire Internet header in response to a receive operation.
- Such an interface would also allow the UDP to pass a full Internet datagram complete with header to the IP to send.
- The IP would verify certain fields for consistency and compute the Internet header checksum.

Protocol Application :

- The major uses of this protocol are the Internet Name Server, and the Trivial File Transfer.

Protocol Number :

- This is protocol 17 (21 octal) when used in the Internet Protocol.

Ex. 9.5.1 : The dump of a UDP header in hexadecimal format is as follows :

B C 8 2 0 0 0 D 0 0 2 B 0 0 1 D

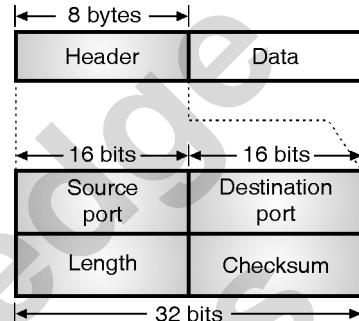
Obtain the following from it :

1. Source port number
2. Destination port number
3. Total length

4. Length of the data.
5. Packet direction.
6. Name of client process.

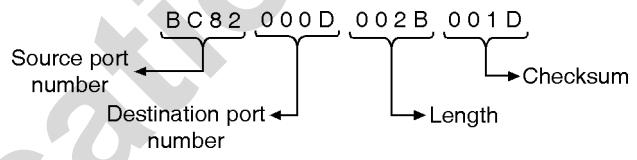
Soln. :

- The standard format of UDP header has been shown in Fig. P. 9.5.1.



(G-2020) Fig. P. 9.5.1 : UDP header format

- Therefore we can split the given UDP header in 4 equal parts as follows :



(G-2021)

1. Source port number = $(BC82)_{16}$...Ans.
2. Destination port number = $(000D)_{16}$...Ans.
3. Total length of UDP packet = $(002B)_{16} = (43)_{10}$ bytes ...Ans.
4. Length of data = Total length – Length of the header.
 $= 43 - 8 = 35$ bytes ...Ans.
5. Destination port number is $(000D)_{16} = (13)_{10}$
- It is a well known port. Hence the direction of UDP packet travel is from client to server.
6. The client process can be obtained from Table 9.6.1 which shows that for well known port number 13, the corresponding client process is "Daytime".

9.6 UDP Services :

- In this section we are going to discuss the following important services provided by the UDP :

1. Process to process communication.
2. Connectionless services.
3. Flow control.
4. Error control.



- 5. Checksum.
- 6. Congestion control.
- 7. Encapsulation and decapsulation.
- 8. Queuing.
- 9. Multiplexing and demultiplexing.

9.6.1 Process to Process Communication :

- We have already discussed the process to process communication in a general sense, earlier in this chapter.
- UDP also does it with the help of sockets which is a combination of IP address and port numbers.
- Table 9.6.1 shows different port numbers used by UDP.
- Some of these ports can be used by UDP as well as TCP.

Table 9.6.1 : Well known ports used with UDP

Port	Protocol	Description
7	Echo	The received datagram is echoed back to sender.
9	Discard	Any received datagram is discarded.
11	Users	Active users.
13	Daytime	Return the day and the current time.
17	Quote	Return the quote of the day.
19	Chargen	To return a string of characters.
53	Nameserver	Domain Name Service (DNS).
67	BOOT PS	This is the server port to download the bootstrap information.
68	BOOT PC	This is the client port to download bootstrap information.
69	TFTP	Trivial File Transport Protocol.
111	RPC	Remote Procedure Call.
123	NTP	Network Time Protocol.
161	SNMP	Simple Network Management Protocol.
162	SNMP	Simple Network Management Protocol (Trap).

9.6.2 Connectionless Services :

- As UDP is a connectionless, unreliable protocol, each user datagram sent using UDP is an independent datagram.

- Different user datagrams sent by the UDP have absolutely no relationship between them.
- This is true even for those datagrams which are originating from the same process and being sent to the same destination.
- The user datagrams do not have any number.
- Also the connection establishment and release are not at all required.
- So each datagram is free to travel any path.
- Only those processes which are sending very short messages can successfully use the UDP.

9.6.3 Flow and Error Control :

- Being a connectionless protocol, UDP is a simple, unreliable protocol.
- It does not provide any flow control, hence the receiver can overflow with incoming messages.
- UDP does not support any other error control mechanism, except for the checksum.
- There are no acknowledgements sent from destination to sender.
- Hence the sender does not know if the message has reached, lost or duplicated.
- If the receiver detects any error using the checksum, then that particular datagram is discarded.

9.6.4 Checksum :

- The calculation of checksum for UDP is different than that for IP.
- In UDP the checksum is calculated by considering the following three sections :
 1. A pseudoheader
 2. The UDP header.
 3. The data coming from the application layer.
- The checksum in UDP is **optional**.
- That means the sender can make a decision of not calculating the checksum.
- If so, then the checksum field is filled with all zeros before sending the UDP packet.
- In case if the calculated checksum is all zeros (when the sender decides to send checksum) then an all 1 checksum is sent.



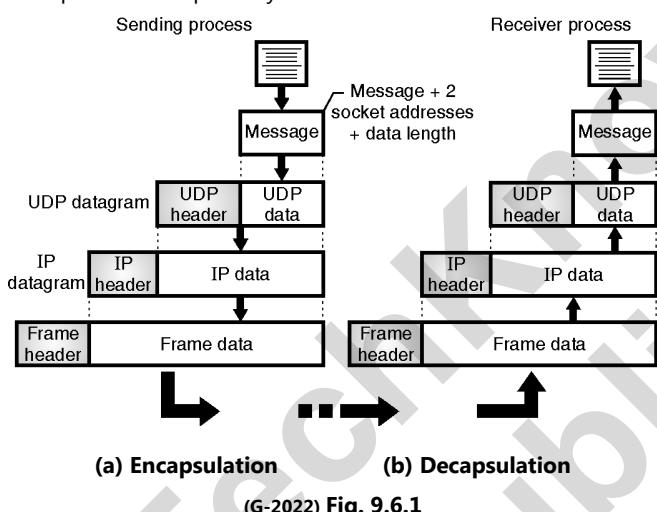
- This solution works without any problem because, a checksum will never have an all 1 value.

9.6.5 Congestion Control :

- UDP does not provide any congestion control.
- It assumes that the UDP packets being small, will not create any congestion.
- But this assumption may not always be correct.

9.6.6 Encapsulation and Decapsulation :

- The UDP encapsulates and decapsulates messages in an IP datagram in order to exchange the message between two communicating processes.
- This is as shown in Fig. 9.6.1. We will discuss the two processes separately.



(G-2022) Fig. 9.6.1

Encapsulation :

- Refer Fig. 9.6.1(a). The message produced by a process is to be sent with the help of UDP.
- The process passes the message and two socket addresses alongwith the length of data to UDP.
- UDP receives this data and adds the UDP header to it as shown.
- This is called as UDP datagram which is passed to IP with the socket address.
- IP adds its own header to UDP datagram as shown. It enters value 17 into the protocol field.
- This is an indication that UDP is being used. The IP datagram is then passed on to the data link layer.
- The DLL adds its own header and possibly a trailer to create a frame and sends it to the physical layer.

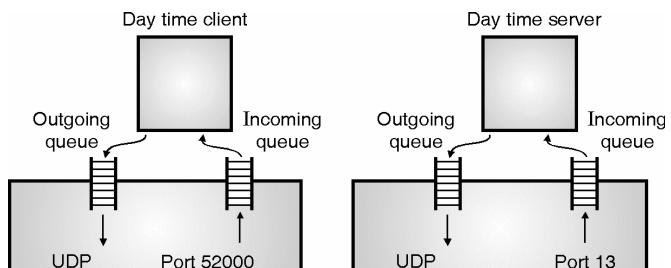
- Finally the physical layer converts these bits into electrical or optical signals and sends them to the destination machine.

Decapsulation :

- Refer Fig. 9.6.1(b) for understanding of the decapsulation process.
- The encoded message arrives at the destination physical layer where it decodes the electrical/optical signals into bits and passes them to the DLL.
- The DLL checks the data using header and trailer.
- The header and trailer are discarded if no errors are found, and the datagram is passed to IP.
- The IP carries out its checking to find the errors and if none are found, the datagram is passed on to UDP, after dropping the IP header.
- The datagram from IP to UDP also contains the sender and receiver IP addresses.
- This entire user datagram is checked by the UDP with the help of checksum.
- If there is no error detected, then the UDP header is dropped and the application data plus senders socket address are handed over to the process.
- The process can use this senders socket address if it wants to respond to the message received.

9.6.7 Queuing :

- The queues in UDP are related with ports as shown in Fig. 9.6.2.



(G-626)Fig. 9.6.2 : Queues in UDP

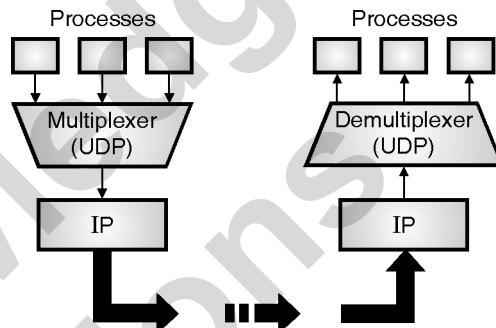
- A process starts at the client site by requesting a port number from the operating system.
- In some implementations both incoming and outgoing queues are created in association with each process.
- Every process gets only one port number and hence it can create one outgoing and another incoming queue.



- The queues function only when the process is running. They are destroyed as soon as the process is terminated.
- The client process uses the source port number mentioned in the request to send message to its outgoing queue.
- UDP removes the queue messages one by one by adding the UDP header and delivers them to IP.
- If the outgoing queue overflows, then operating system tells that client process to wait before sending the next message.
- When the client receives a message, UDP checks if the incoming queue has been created or not.
- If the queue has been created, then the UDP sends the received datagram to the end of the queue.
- If the queue is not present then UDP will simply discard the user datagram.
- If the incoming queue overflows, then UDP discards the user datagram and arranges to send the port unavailable message to the server.
- The mechanism to create the server queue is different. The server creates the incoming and outgoing queues using its well known port as soon as it starts running. The queues exist as long as the server is running.
- When a message is received at the server, the UDP checks if the incoming queue has been created or not.
- If the queue is not present, the UDP discards the user datagram.
- If the queue is present then UDP sends the datagram at the end of the queue.
- If the incoming queue overflows, then UDP drops the user datagram and arranges to send the port unavailable message to the client.
- When the server wants to send a message to client it sends that message to the outgoing queue.
- These messages are then removed one by one after adding the UDP header. They are delivered to IP.
- If the outgoing queue overflows then the operating system will ask the server to wait before it sends the next message.

9.6.8 Multiplexing and Demultiplexing :

- We have discussed the general principle of multiplexing and demultiplexing in the transport layer.
- Now let us see how to apply the same principle to UDP. Imagine that a host is running a TCP/IP protocol suite and that there is only one UDP and a number of processes which would like to use the services of UDP.
- UDP handles such a situation by using the principle of multiplexing and demultiplexing as shown in Fig. 9.6.3.



(G-2023) Fig. 9.6.3 : Multiplexing and demultiplexing

Multiplexing :

- At the sending end, there are several processes that are interested in sending packets.
- But there is only one transport layer protocol (UDP or TCP).
- Thus it is a many processes-one transport layer protocol situation.
- Such a many-to-one relationship requires multiplexing.
- The UDP first accepts messages from different processes.
- These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it.
- Then the UDP adds header and passes the packet to IP as shown in Fig. 9.6.3.

Demultiplexing :

- At the receiving end, the relationship is one to many. So we need a demultiplexer.
- First the UDP layer receives datagrams from the IP.
- The UDP then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.



9.6.9 Comparison of UDP and Generic Simple Protocol :

- In this section we will compare UDP with a simple connectionless transport layer protocol.
- The only difference between the two is that the UDP provides an **optional checksum**.
- If the checksum is added to the UDP packet then at the destination, the receiving UDP can check the packet for any error with the help of the checksum.
- If any error is detected, the receiving UDP will discard that packet, without sending any feedback to the sender.

9.7 UDP Applications :

- Despite being connectionless, unreliable, no flow control, no error control, UDP is still preferred for some applications.
- This is because UDP has some advantages too. An application designer has to sometimes compromise between advantages and drawbacks to get the optimum.
- Here we will discuss some important features of UDP that are useful in designing an application program.

9.8 UDP Features :

9.8.1 Connectionless Service :

- The feature of UDP is that it is a connectionless protocol and that each UDP packet is independent from the other packets, can be considered as an advantage or a disadvantage depending on the requirements of an application.
- In an application, if we want to send only short messages to server and receive short messages from the server.
- Then the above mentioned feature becomes an advantage.
- The feature of being connectionless is an advantage if request and respond each can fit in one single user datagram.
- The overhead (number packets to be exchanged) required to establish and close a connection is zero in case of UDP.

- This can be a very important advantage for some applications.
- Similarly the delay involved with the connectionless delivery is very short as compared to that with the connection oriented delivery.
- Hence the connectionless service provided by UDP is preferred for the applications in which delay is important

9.8.2 Lack of Error Control :

- UDP is an unreliable protocol which does not provide any error control.
- Now this is actually a disadvantage but it becomes an advantage for some applications as explained below.
- If TCP is used for reliable service and if a packet is lost, then TCP will resend it.
- So the receiver transport layer is unable to deliver that part of the message to the application immediately.
- Due to this an uneven delay is introduced between different parts of the messages which is undesirable for some delay sensitive applications.
- This delay is actually a side effect of the reliable operation of TCP.
- Some applications are not affected by this delay but for some others it is very crucial.

9.8.3 Lack of Congestion Control :

- We know that there is no provision for congestion control in UDP.
- But this disadvantage can become an advantage for some applications.
- A good side effect of lack of congestion control is that UDP does not create any additional traffic that is created by TCP for congestion control.
- Hence the UDP is preferred for some congestion prone networks.

9.8.4 Typical Applications of UDP :

1. UDP is suitable for the applications (processes) that have the following requirements :
 - (a) A simple response to request is to be made.
 - (b) Flow and error controls not essential.
 - (c) Bulk data is not to be sent (like FTP).



2. UDP is used for RIP (Routing Information Protocol).
3. UDP is used for management processes such as SNMP.
4. UDP is suitable for the processes having inbuilt flow and error control mechanisms, such as TFTP.
5. UDP is suitable for the multicasting applications.
6. UDP is also used in the real time applications which do not tolerate the uneven delays.

9.9 Transmission Control Protocol (TCP) :

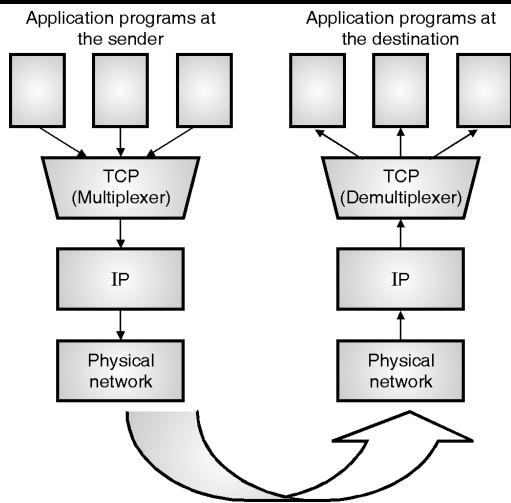
- The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
- Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
- TCP is the layer 4 protocol in the TCP/IP suite and it is a very important and complicated protocol.
- TCP has been revised multiple times in last few decades.
- With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers.
- This service benefits applications because they do not have to chop data into blocks before handing it off to TCP.
- Instead, TCP groups bytes into segments and passes them to IP for delivery.
- TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.
- It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive.
- Bytes not acknowledged within a specified time period are retransmitted.
- The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets.
- A time-out mechanism allows devices to detect lost packets and request retransmission.
- TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence

number that it can receive without overflowing its internal buffers.

- TCP supports a full-duplex operation means that TCP processes can both send and receive at the same time.
- Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

9.9.1 Relationship Between TCP and IP :

- The relationship between TCP and IP is very interesting. Each TCP message gets encapsulated or inserted in an IP datagram and then this datagram is sent over the Internet to the destination.
- IP transports this datagram from sender to destination, without bothering about the contents of the TCP message.
- At the final destination the IP hands over the message to the TCP software running on the destination computer.
- IP acts like a postal service and transfers the datagrams from one computer to the other.
- Thus TCP deals with the actual data to be transferred and IP takes care of transfer of that data.
- Many applications such as FTP, Remote login TELNET etc. keep sending data to TCP software on the sending computer.
- The TCP software acts as a multiplexer at the sending computer.
- It receives data from various applications, multiplexes the data and hands it over to the IP software at the sending end as shown in Fig. 9.9.1.
- IP adds its own header to this TCP packet and creates an IP packet out of it.
- Then this packet is sent to its destination.
- At the destination exactly opposite process will take place.
- The IP software hands over the multiplexed data to the TCP software.
- The TCP software at the destination computer then demultiplexes the multiplexed data and gives it to the corresponding applications as shown in Fig. 9.9.1.

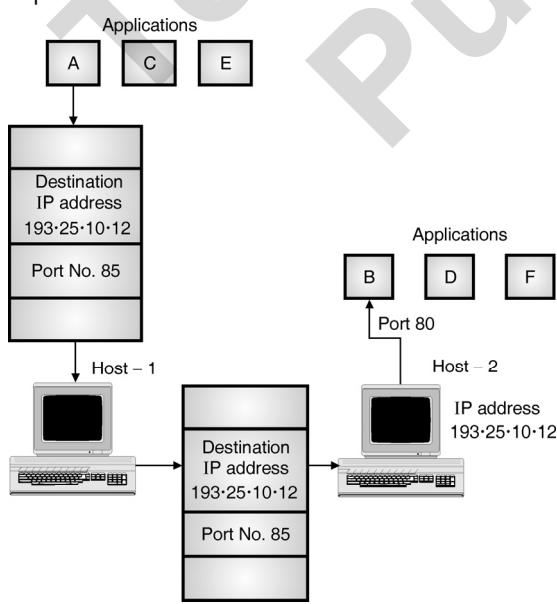


(G-1440) Fig. 9.9.1 : Multiplexing and demultiplexing using TCP

9.9.2 Ports and Sockets :

1. Ports :

- Applications running on different hosts communicate with TCP with the help of ports. Every application has been allotted a unique 16 bit number which is known as a **port**.
- When an application on one computer wants to communicate using a TCP connection to another application on some other computers these ports prove to be very helpful.
- Let an application A on host 1 wants to communicate with an application B on host 2.
- So the process takes place as shown in Fig. 9.9.2 and explained below.

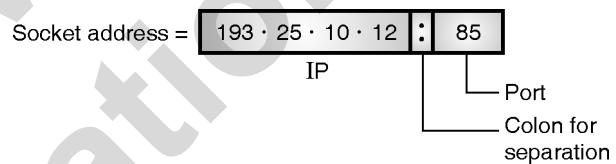


(G-1437) Fig. 9.9.2 : Use of port numbers

- Application A running on computer 1 provides the IP address of computer 2 and the port number corresponding to application B as shown in Fig. 9.9.2.
- Computer 1 communicates with computer 2 using the IP address and computer 2 uses the port number to direct the message to application B.

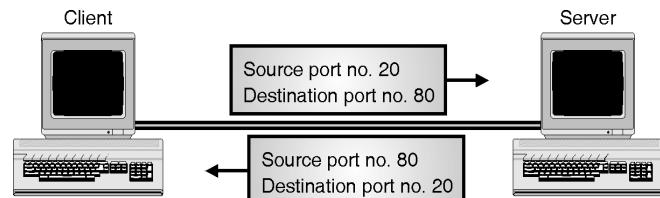
2. Sockets :

- A port is a 16 bit unique number used for identification of a single application.
- But socket address or simply socket would identify the combination of the IP address and the port number concatenated together as shown in Fig. 9.9.3.
- For example if the IP address = 193.25.10.12 and the port number is 85.
- Then this port of this computer will have the following socket address.



(G-1438) Fig. 9.9.3

- So a pair of sockets is required to identify a TCP connection between two applications on two different hosts.
- These two socket addresses specify the end points of the connection as shown in Fig. 9.9.4.



(G-1436) Fig. 9.9.4 : Source and destination port numbers

- Generally the server port numbers are known as the **well known ports**.
- Some of the well known port numbers have already been mentioned for UDP and TCP earlier in this chapter.
- Multiple TCP connections between different applications or same applications on two hosts exist in practice.
- Here the IP addresses of the two hosts are same but the port numbers are different.
- The communication using port numbers is illustrated in Fig. 9.9.4.



9.10 TCP Services :

- Following are some of the services offered by TCP to the processes at the application layer :
 1. Stream delivery service
 2. Sending and receiving buffers
 3. Bytes and segments
 4. Full duplex service
 5. Connection oriented service
 6. Reliable service.
 7. Process to process communication.

9.10.1 Process to Process Communication :

- The TCP uses port numbers as transport layer addresses. Table 9.10.1 shows some well known port numbers used by TCP.
- Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

Table 9.10.1 : Well known ports used by TCP

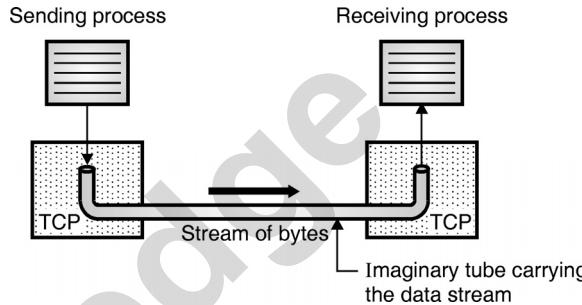
Port	Protocol	Description
7	Echo	Sends received datagram back to sender
9	Discard	Discards any received packet
11	Users	Active users
13	Daytime	Sends the date and the time
17	Quote	Sends a quote of the day
19	Chargen	Sends a string character
20	FTP, Data	File Transfer protocol for data
21	FTP, Control	File Transfer protocol for control
23	TELNET	Terminal network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

9.10.2 Stream Delivery Service :

- TCP is a stream oriented protocol. The sending process delivers data in the form of a stream of bytes and the receiving process receives it in the same manner.

- TCP creates a working environment in such a way that the sending and receiving processes seem to be connected by an imaginary "tube" as shown in Fig. 9.10.1.

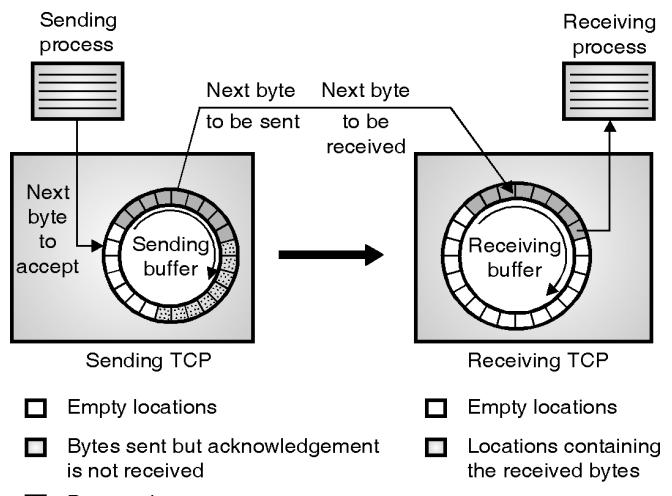
- This is called as stream delivery service.



(G-621)Fig. 9.10.1 : Stream delivery service

9.10.3 Sending and Receiving Buffers :

- The sending and receiving processes may not produce and receive data at the same speed.
- Hence TCP needs buffers for storage of data at both the ends.
- There are two types of buffers used in each direction :
 1. Sending buffer
 2. Receiving buffer.
- A buffer can be implemented by using a circular array of 1 byte locations as shown in Fig. 9.10.2.



(G-622)Fig. 9.10.2 : Sending and receiving buffers

- Fig. 9.10.2 shows the direction of movement of data. The sending buffer has three types of locations :
 1. Empty locations

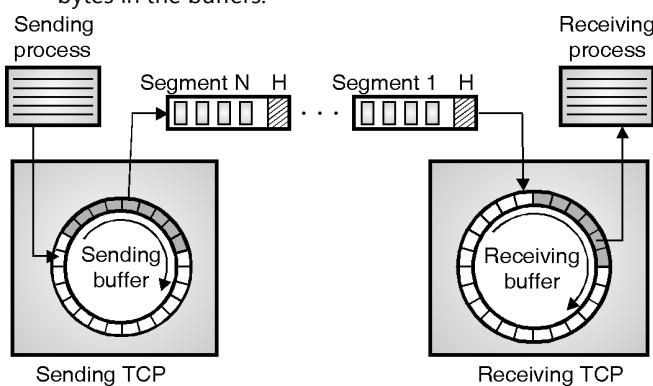


2. Locations containing the bytes which have been sent but not acknowledged. These bytes are kept in the buffer till an acknowledgement is received.
3. The locations containing the bytes to be sent by the sending TCP.
- In practice, the TCP may be able to send only a part of data which is to be sent, due to slowness of the receiving process or congestion in the network.
- The buffer at the receiver is divided into two parts :

 1. The part containing empty locations.
 2. The part containing the received bytes which can be consumed by the sending process.

9.10.4 Bytes and Segments :

- Buffering is used to handle the difference between the speed of data transmission and data consumption.
- But only buffering is not enough. We need one more step before sending the data.
- The IP layer, which provides service to TCP, has to send data in the form of packets instead of stream of bytes.
- At the transport layer, TCP groups a number of bytes to form a packet called a segment.
- A header is added to each segment for the purpose of exercising control.
- The segments are then inserted in an IP datagram and transmitted.
- The entire operation is transparent to the receiving process.
- The segments may be received out of order, lost or corrupted when it reaches the receiving end.
- Fig. 9.10.3 shows the creation of segments from the bytes in the buffers.



(G-623)Fig. 9.10.3

- The segments are not of the same size. Each segment can carry hundreds of bytes.

9.10.5 Full Duplex Service :

- TCP offers full duplex service where the data can flow in both the directions simultaneously.
- Each TCP will then have a sending buffer and receiving buffer.
- The TCP segments can travel in both the directions, therefore TCP provides a full duplex service.

9.10.6 Connection Oriented Service :

- TCP is a connection oriented protocol.
- When process – 1 wants to communicate (send and receive) with another process (process – 2), the sequence of operations is as follows :

 1. TCP of process – 1 informs TCP of process – 2 and create a connection between them.
 2. TCP of process – 1 and TCP of process – 2 exchange data in both the directions.
 3. After completing the data exchange, when buffers on both sides are empty, the two TCPs destroy their buffers to terminate the connection.

- The type of connection in TCP is not physical, it is virtual. The TCP segment is encapsulated in an IP datagram and these packets can be transmitted without following the sequence.
- These segments can get lost or corrupted and may have to be resent.
- Each segment may take a different path to reach the destination.

9.10.7 Reliable Service :

- TCP is a reliable transport protocol and not unreliable like UDP.
- Different acknowledgements are used by the receiver to convey sender the status of data.

9.11 Features of TCP :

- In order to provide the services mentioned in the previous section, TCP has a number of features as follows :



9.11.1 Numbering System :

- The TCP software keeps track of the segments being transmitted or received.
- However in the segment header there is no field for a segment number value.
- But there are fields called sequence number and the acknowledgement number.
- Note that these fields correspond to the byte number and not the segment number.

Byte numbers :

- TCP give numbers to all the data bytes which are transmitted.
- The numbering is independent of the direction of data travel.
- The numbering does not always start from 0, but it can start with a randomly generated number between 0 and $2^{32} - 1$.

Sequence number :

- After numbering the bytes, the TCP assigns a sequence number to each segment that is being transmitted.
- The sequence number for each segment is same as the number assigned to the first byte present in that segment.

Acknowledgement number :

- The TCP communication is duplex.
- So both the communicating processes can send and receive data at the same time.
- Each process will give numbers to the bytes with a different starting byte number.
- Each party also uses an acknowledgement number to confirm the reception of bytes.

The acknowledgement number is cumulative i.e. the receiver takes the number of the last byte received, adds 1 to it and uses this sum as the acknowledgement number.

9.11.2 Flow Control :

- TCP provides flow control (UDP does not). The receiver will control the amount of data to be sent by the sender.
- This will avoid data overflow at the receiver. The TCP uses byte oriented flow control.

9.11.3 Error Control :

- The error control mechanism is inbuilt for TCP. This allows TCP to provide a reliable service.
- The error control mechanism considers a segment as the unit of data for error correction however the byte oriented error control is provided.

9.11.4 Congestion Control :

- TCP takes the congestion in network into account. UDP does not do this.
- The amount of data sent by the sender depends on the following factors :
 1. The receivers decision (flow control).
 2. The network congestion.

Summary of TCP features :

1. TCP is a process-to-process protocol.
2. TCP uses port numbers.
3. It is a connection oriented protocol (creates a virtual connection).
4. It uses flow and error control mechanisms.
5. TCP is a reliable protocol.

9.12 The TCP Protocol :

- Let us take a general overview of the TCP protocol.
- Every byte on a TCP connection has its own 32-bit sequence number.
- These numbers are used for both acknowledgement and for window mechanism.

Segments :

- The sending and receiving TCP entities exchange data in the form of segments.
- A segment consists of a fixed 20 byte header (plus and optional part) followed by zero or more data bytes.

Segment size :

- The segment size is decided by the TCP software. Two limits restrict the segment size as follows :
 1. Each segment including the TCP header, must fit in the 65535 byte IP payload.
 2. Each segment must fit in the **MTU (Maximum Transfer Unit)**. Each network has a maximum transfer unit.



Practically an MTU which is a few thousand bytes defines the upper limit on the segment size.

Fragmentation :

- If a segment is too large, then it should be broken into small segments. Using fragmentation by a router.
- Each new segment gets a new IP header. So the fragmentation by router will increase the overhead.

Timer :

- The basic protocol used by TCP entities is the sliding window protocol.
- A sender starts a timer as soon as a sender transmits a segment.
- When the segment is received by the destination, it sends back acknowledgement alongwith data if any.
- The acknowledgement number is equal to the next sequence number it expects to receive.
- If the timer at the sender goes out before the acknowledgement reaches back, it will **retransmit** that segment again.

Possible problems :

- As the segments can be fragmented, a part of the transmitted segment only may reach the destination with the remaining part lost.
- Segments can arrive out of order.
- Segments can get delayed so much that timer is out and unnecessary retransmission will take place.
- If a retransmitted segment takes a different route than the original segment is fragmented then the fragments of original and retransmitted segments can reach the destination in a sporadic way.
- So a careful administration is required to achieve reliable byte stream.
- There is a possibility of congestion or broken network along the path.
- TCP should be able to solve these problems in an efficient manner.

9.12.1 TCP Segment :

- The TCP segment as shown in Fig. 9.12.1 consists of two parts :
 1. Header
 2. Data

2. Data



(G-1423)Fig. 9.12.1 : TCP segment

9.12.2 The TCP Segment Header :

SPPU : May 11, Dec. 12, May 13, Dec. 14, May 19

University Questions

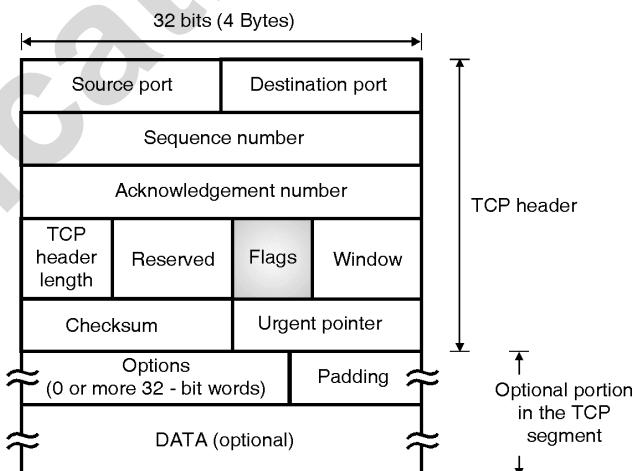
- Q. 1** Explain TCP with its header format.

(May 11, May 13, Dec. 14, May 19, 8 Marks)

- Q. 2** Explain all the fields of TCP header.

(Dec. 12, 10 Marks)

- Fig. 9.12.2 shows the layout of a TCP segment.
- Every segment begins with a 20 byte fixed format header.
- The fixed header may be followed by header options.
- After the options, if any, upto $65535 - 20 - 20 = 65495$ data bytes may follow.
- Note that the first 20 bytes correspond to the IP header and the next 20 correspond to the TCP header.



(G-611)Fig. 9.12.2 : TCP header format

- The TCP segment without data are used for sending the acknowledgements and control messages.

Source port :

- A 16-bit number identifying the application the TCP segment originated from within the sending host.
- The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49,151) and private ports (49,152 through 65,535).
- Port assignments are used by TCP as an interface to the application layer.

**Destination port :**

- A 16-bit number identifying the application the TCP segment is destined for on a receiving host.
- Destination ports use the same port number assignments as those set aside for source ports.

Sequence number :

- A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection.
- After reaching $2^{32} - 1$, this number will wrap around to 0.

Acknowledgement number :

- A 32-bit number identifying the next data byte the sender expects from the receiver.
- Therefore, the number will be one greater than the most recently received data byte.
- This field is only used when the ACK control bit is turned on.

Header length or offset :

- A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer).
- Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes.
- This field is required because the size of the options field(s) cannot be determined in advance.
- Note that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

Reserved :

- A 6-bit field currently unused and reserved for future use.

Control bits or flags :

1. **Urgent pointer (URG) :** If this bit field is set, the receiving TCP should interpret the urgent pointer field.
2. **Acknowledgement (ACK) :** If this bit field is set, the acknowledgement field described earlier is valid.
3. **Push function (PSH) :** If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible.
- An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.

4. **Reset the connection (RST) :** If this bit is present, it signals the receiver that the sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinquished.

5. **Synchronize (SYN) :** When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers.

- This bit is used during the initial stages of connection establishment between a sender and receiver.

6. **No more data from sender (FIN) :** If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window :

- A 16-bit integer used by TCP for flow control in the form of a data transmission window size.
- This number tells the sender how much data the receiver is willing to accept.
- The maximum value for this field would limit the window size to 65,535 bytes, however a "window scale" option can be used to make use of even larger windows.

Checksum :

- A TCP sender computes a value based on the contents of the TCP header and data fields.
- This 16-bit value will be compared with the value the receiver generates using the same computation.
- If the values match, the receiver can be very confident that the segment arrived intact.

Urgent pointer :

- In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible.
- This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options :

- In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver.
- Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits).



- The most common option is the Maximum Segment Size (MSS) option.
- A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option.
- Other options are often used for various flow control and congestion control techniques.

Padding :

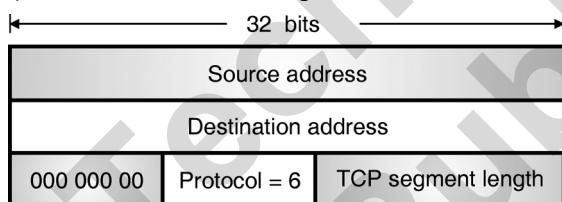
- Because options may vary in size, it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32-bit word boundary as defined by the standard.

Data :

- Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver.
- This field coupled with the TCP header fields constitutes a TCP segment.

9.12.3 Checksum :

- A checksum is provided to ensure extreme reliability. It checksums the header, the data and the conceptual pseudo header shown in Fig. 9.12.3.



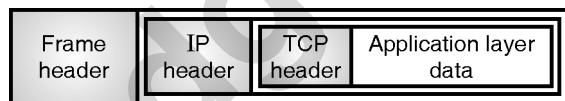
(G-612)Fig. 9.12.3 : The pseudo header included in the TCP checksum

- When the checksum is being computed, the TCP checksum field is set to zero, and the data field is padded out with an additional zero byte if its length is an odd number.
- Then all the 16 bit words are added in 1's complement and then 1's complement of the sum is taken to get the checksum.
- When a receiver performs the calculation on the entire segment including the checksum field, the result has to be zero.
- The pseudo header contains the 32 bit IP address of the source and destination machines, the protocol number

for TCP i.e. 6 and the TCP segment length as shown in Fig. 9.12.3.

9.12.4 Encapsulation :

- The data coming from the application layer is encapsulated in a TCP segment. This TCP segment is then encapsulated in an IP datagram.
- The IP datagram is encapsulated in a frame at the data link layer. The process of encapsulation is shown in Fig. 9.12.4.



(G-2072) Fig. 9.12.4 : Encapsulation

9.13 A TCP Connection :

- TCP is a connection oriented protocol. Such a protocol would establish a virtual path between the sender and the receiver.
- Multiple segments corresponding to the message are then sent over this virtual connection.
- As TCP is using the same single path for the entire path, it can use the same path for acknowledgements and retransmission of damaged or lost packets.
- While discussing the relation between TCP and IP we have seen how TCP uses the services of IP.
- TCP operates at a higher level than IP and the TCP connection is virtual and not physical.
- Though IP delivers the individual segments to the destination, the entire control on the connection is exercised by TCP.
- If a segment is lost or damaged, the TCP makes a decision of its retransmission, and IP does not know anything about it.
- The **three phases** in the connection oriented TCP transmission are as follows :
 1. Connection establishment
 2. Data transfer and 3. Connection termination.

9.13.1 TCP Connection Establishment :

SPPU : Dec. 11, May 12, Dec. 13, May 15, May 19

University Questions

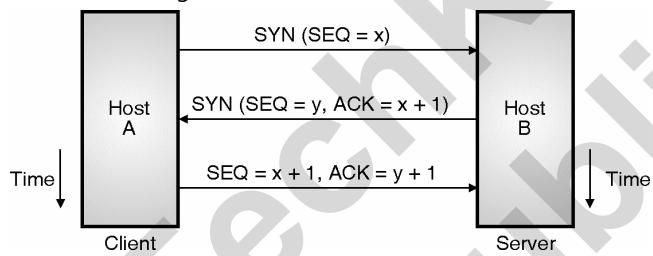
- Q. 1** Explain three way hand shake algorithm for TCP connection establishment.

(Dec. 11, May 12, Dec. 13, 8 Marks)



Q. 2 Describe 3-way handshake for connection establishment in TCP. (May 15, May 19, 6 Marks)

- To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another.
- Connection establishment is performed by using a **three-way handshake** mechanism.
- A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers.
- This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well.
- This is necessary so that packets are not transmitted or re-transmitted during session establishment or after session termination.
- Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving.
- Then, the three-way handshake proceeds in the manner shown in Fig. 9.13.1(a).



(G-613) Fig. 9.13.1(a) : TCP connection establishment (Three-way handshake)

- The requesting end (HOST A) sends a SYN segment specifying the port number of the server that the client wants to get connected to, and the client's initial sequence number (x).
- The server (HOST B) responds with its own SYN segment containing the server's initial sequence number (y).
- The server also acknowledges the client's SYN by acknowledging the client's SYN plus one ($x + 1$). A SYN consumes one sequence number.
- The client must acknowledge this SYN from the server by acknowledging the server's SYN plus one. ($SEQ = x + 1, ACK = y + 1$).
- This is how a TCP connection is established.

9.13.2 Connection Termination Protocol

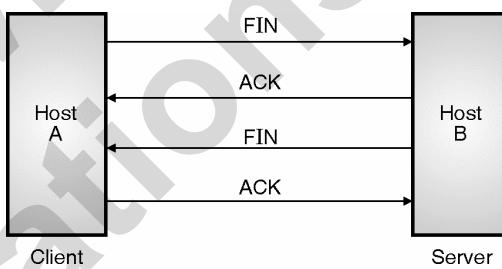
[Connection Release] : **SPPU : Dec. 02**

University Questions

- Q. 1** Explain the modified three-way handshake procedure of connection termination in the TCP.

(Dec. 02, 8 Marks)

- While it takes three segments to establish a connection, it takes four to terminate a connection.
- Since a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), the connection should be terminated in both the directions independently.
- The termination procedure in each direction is shown in Fig. 9.13.1(b).



(G-614) Fig. 9.13.1(b) : TCP termination

- The rule is that either side can send a FIN when it has finished sending data (FIN indicates finished).
- When a TCP program on a host receives a FIN, it informs the application that the other end has terminated the data flow.
- The receipt of a FIN only means there will be no more data flowing in that direction. A TCP can still send data after receiving a FIN.
- The end that first issues the close (e.g., sends the first FIN) performs the active close and the other end (that receives this FIN) performs the passive close.
- Now refer Fig. 9.13.1(b). When the server receives the FIN it sends back an ACK of the received sequence number plus one.
- A FIN consumes a sequence number, just like a SYN.
- At this point the server's TCP also delivers an end-of-file to the application (the discard server).
- The server then closes its connection and its TCP sends a FIN to the client.



- The client's TCP informs the application and sends an ACK to server by incrementing the received sequence number by one.
- Connections are normally initiated by the client, with the first SYN going from the client to the server.
- A client or server can actively close the connection (i.e. send the first FIN).
- But in practice generally the client determines when the connection should be terminated, since client processes are often driven by an interactive user, who enters something like quit to terminate.
- This is how the TCP connection is released.

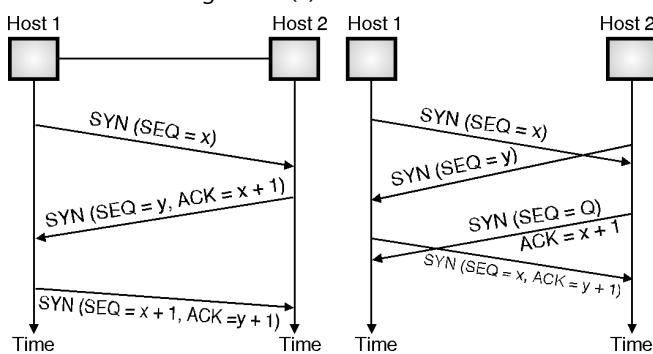
9.13.3 TCP Connection Management :

SPPU : May 02

University Questions

Q. 1 Write short notes on : Connection management in TCP. **(May 02, 6 Marks)**

- Connections are established in TCP by following the three-way handshake technique.
- To establish a connection, one side, say the server, passively waits.
- It executes the LISTEN and ACCEPT primitives, to specify either a particular other side or nobody in particular.
- The other side (client) executes a connect primitive, with the IP and the port specified.
- The other information is the maximum TCP segment size, possible other options and optionally some user data (e.g. a password).
- The CONNECT primitive sends a TCP segment with the SYN bit on and the ACK bit off and waits for a response.
- The sequence of TCP segments sent in the normal case is shown in Fig. 9.13.2(a).



(a) Normal operation

(b) Call collision

(G-615) Fig. 9.13.2 : TCP connection management

- When the segment sent by host - 1 reaches the destination i.e. host - 2 the receiving server checks to see if there is a process that has done a LISTEN on the port given in the destination port field.
- If not, it sends a reply with the RST bit on to reject the connection.
- Otherwise it gives the TCP segment to the listening process, which can accept or refuse (e.g. if it does not like the client) the connection.
- On acceptance a SYN is send, otherwise a RST.
- Note that a SYN segment occupies 1 byte of sequence space so it can be acknowledged unambiguously.

Call collision :

- If two hosts try to establish a connection simultaneously between the same two sockets then the events take place as shown in Fig. 9.13.2(b).
- Under such circumstances only one connection is established. Both the connections can not be established simultaneously because connections are identified by their end points.
- If the first set up results in a connection which is identified by (x, y) and second connection is also set up, then only one table entry will be made i.e. for (x, y).
- For the initial sequence number a clock based scheme is used, with a clock pulse coming after every 4 μ sec.
- For ensuring an additional safety, when a host crashes, it may not reboot for 120 sec which is maximum packet lifetime.
- This is to make sure that no packets from previous connections are still alive and travelling around.

9.13.4 TCP Connection Release :

- A TCP connection is actually a full duplex connection but to understand the connection release we will assume that it is a pair of simplex connections.
- We can then think that each simplex connection is getting terminated independently.
- Releasing a TCP connection is identical on both ends. Each side can send a TCP segment with the FIN bit set, meaning it has no more data to send.
- After receiving a FIN, the Acknowledge (ACK) signal is sent and that direction is shut down, but data may continue to flow indefinitely in the other direction.



- If the sender of FIN does not receive the ACK within 2 maximum packet lifetimes, it releases the connection. The receiver will eventually notice that it receives no more data and time-out as well.
- Normally four TCP segments are required to release a connection i.e. one FIN and one ACK in each direction.
- However the first ACK and second FIN can be combined in the same segment.

Connection reset :

- The connection reset in TCP can take place when TCP at one end done any one of the following :
 1. It may deny a connection request.
 2. It may abort the existing connection.
 3. It may terminate an idle i.e. non operating connection.
- TCP does all the three with the help of the RST (reset flag).

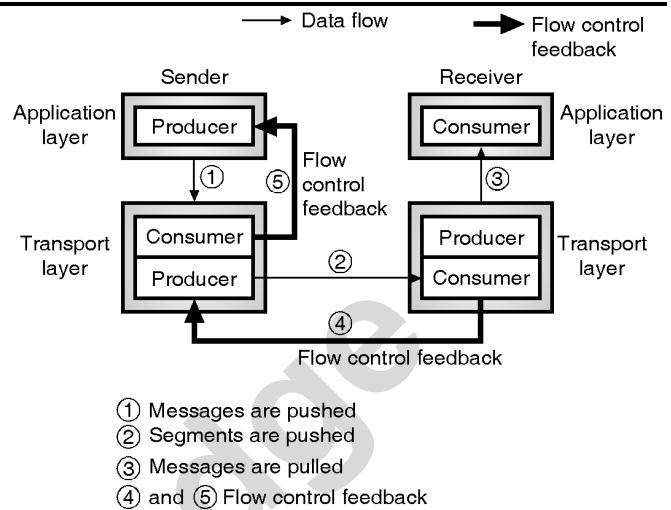
9.14 Flow Control :

SPPU : May 06, May 08, May 09

University Questions

- Q. 1 Explain how TCP provides flow control.
(May 06, May 08, May 09, 8 Marks)**

- The flow control is a technique used for controlling the data rate of the sender so that the receiver is not overwhelmed.
- In TCP the flow control has been kept separate from the error control.
- So when the flow control is being discussed, we will temporarily ignore the error control. i.e. we assume that the data transmission is taking place over an errorfree channel.
- Refer Fig. 9.14.1 which shows the data transfer taking place in only one direction from the sender to receiver.
- We can apply the same principle to the bidirectional data transfer.
- Two different types of signals travel between the sending process and the receiving process in Fig. 9.14.1. They are data and flow control feedback signals.



(G-1802) Fig. 9.14.1 : Data flow and flow control feedback in TCP

- The data flow takes place from the sending process to the sending TCP (denoted by ①), then from sending TCP to receiving TCP (denoted by ②) and finally from receiving TCP to receiving process (denoted by ③).
- Thus flow of data takes place from sender to receiver. But the flow control feedback signals travel from the receiver to sender as shown.
- They flow from receiving TCP to sender TCP (denoted by ④) and from sending TCP to sending process (denoted by ⑤).
- Most TCP versions however, do not provide the flow control feedback facility.
- Instead the receiving process is allowed to pull data from receiving TCP whenever the receiving process becomes ready.
- Thus the receiving TCP controls the sending TCP (due to flow control feedback) and the sending TCP controls the sending process as far as the data rate of the sending process is concerned.
- Consider the flow control feedback path denoted by ⑥ in Fig. 9.14.1.
- This feedback is practically achieved by simply rejecting the data by sending TCP when its window is full.
- So now let us concentrate on the flow control feedback signal from receiving TCP to sending TCP, denoted by path ④ in Fig. 9.14.1. i.e. how does the receiving process control the sending TCP.



9.14.1 Opening and Closing Windows :

- In TCP the flow control is achieved by forcing the sender and receiver to adjust their window sizes.
- The size of the buffer for both sender and receiver will not be changed. It will remain fixed in size.
- Consider the receive window shown in Fig. 9.14.2.
- This window closes by moving its left wall to the right in response to arrival of more bytes from the sender.
- The receive window of Fig. 9.14.2 will open by moving its right wall towards right when the receiver process pulls more bytes from the receiver buffer.
- The send window can open, close or shrink in order to exercise the flow control.
- All the three functions of the send window are controlled by the receiver.
- The send window closes by moving its left wall to the right (see Fig. 9.14.2) in response to a new acknowledgement from the receiver.
- The send window opens by moving its right wall to the right when the advertised receive window size (rwnd) by the receiver allows it to do so.
- The send window may shrink on occasion. It is assumed that this situation does not arise.

9.14.2 Shrinking of Windows :

- As we know, the receiver window does not shrink.
- However the send window can shrink in the event of the receiver defining a value of "rwnd" which results in the shrinking of windows.
- Some versions of TCP do not allow the send window to shrink.
- That means they do not allow the right wall of the send window to move to the left.
- The receiver can prevent the shrinking of send window by maintaining the following relationship between the last and new acknowledgement and the last and new "rwnd" values.

$$(new \text{ ackNo} + new \text{ rwnd}) \geq (last \text{ ackNo} + last \text{ rwnd})$$

↓ ↓

New position of the right wall with respect to sequence number space Old position of the right wall

(G-1803)

- The above relationship shows that the right wall should not move to the left.

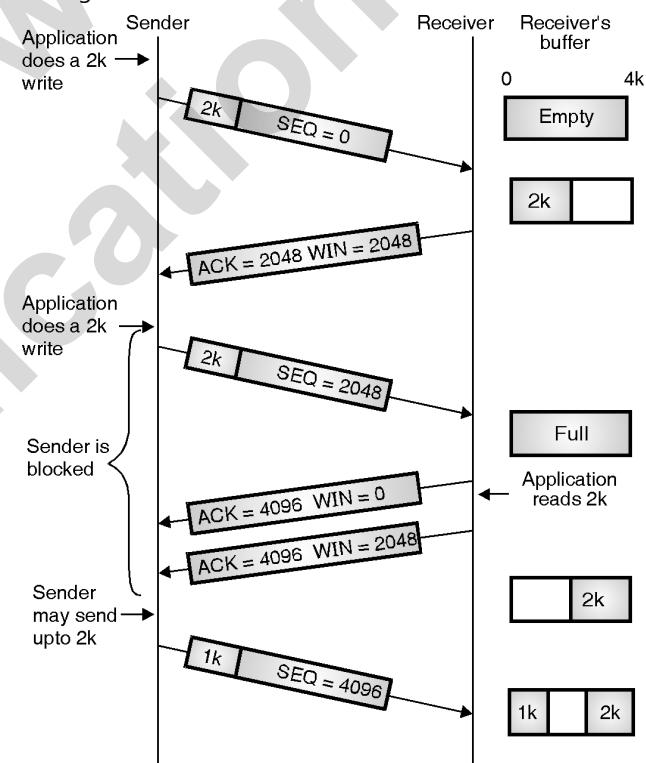
9.14.3 An Example of Flow Control :

SPPU : May 05

University Questions

Q. 1 Discuss flow control and congestion control mechanisms in TCP. (May 05, 8 Marks)

- Let us now see how the window policy is used in transmission policy of TCP protocol.
- Window management in TCP is normally decoupled from the acknowledgements that means acknowledgements are not connected to the TCP window management.
- To understand the window management, refer Fig. 9.14.2.



(G-616) Fig. 9.14.2 : Windows management in TCP

Explanation :

- Let the receiver in Fig. 9.14.2, has a 4 kbyte i.e. 4096 byte buffer space.
- The sender transmits a 2048 byte (2 kbyte) segment with a sequence number SEQ = 0.
- These bytes occupy half space of the receiver's buffer and the receiver will send back acknowledgement of this segment (ACK 2048, WIN = 2048).



- Here WIN = 2048 is the window which tells the sender that an empty buffer space of 2048 is available on the receiver side.
- Now the sender sends another 2k i.e. 2048 bytes segment (SEQ = 2048) which is acknowledged by the receiver (ACK = 4096, WIN = 0) which shows that window = 0 because the receiver buffer space is 0. ACK = 4096 indicates that the receiver has received 4096 bits successfully.
- The sender must now be blocked until the application process on the receiver removes some data from the buffer and some buffer space becomes available.
- As soon as the application on the receiver side reads 2k bytes, the buffer becomes partially empty and an acknowledgement with a window of 2k (ACK = 4096, WIN = 2048) is sent back to sender. Here WIN = 2048 indicates the empty buffer space on the receiver side.
- The sender may send upto 2 kbytes.
- When the window = 0, the sender should not normally send any segment.
- But under two exceptional conditions the sender will continue to send data even when it receives WIN = 0.
 1. First, urgent data may be send, e.g. to allow the user to kill the process running on the other machine.
 2. Second, the sender may send a 1-byte segment to make the receiver reannounce the next byte expected and the window size.
- This is used to prevent the possible confusion if a window announcement gets lost.
- Senders are not supposed to transmit data as soon as the data is obtained from an application.
- The receivers also are not supposed to send acknowledgements as soon as they receive it.
- This is done in order to reduce the usage of the system. One way to reduce the system usage is to use an algorithm called Nagle's algorithm is used.

9.14.4 Silly Window Syndrome :

SPPU : May 09, Dec. 09, Dec. 10, May 12, May 15

University Questions

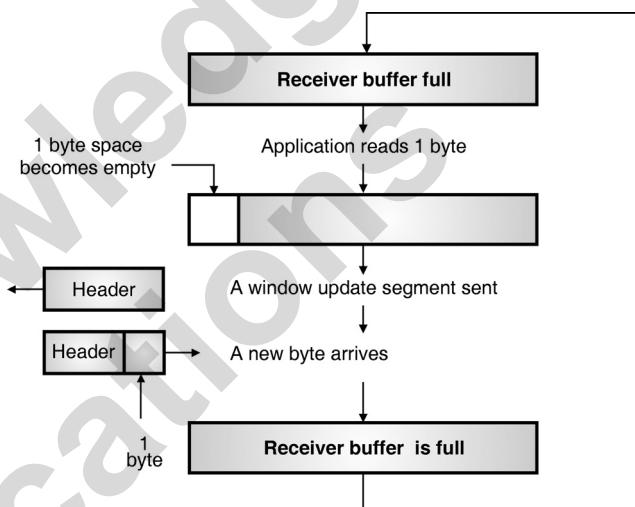
- Q. 1** What is silly-window syndrome ? Explain at-least two methods to overcome it.

(May 09, Dec. 09, 8 Marks)

Q. 2 What is silly window syndrome ? How to overcome it ? **(Dec. 10, May 12, 8 Marks)**

Q. 3 What is silly window syndrome problem ? **(May 15, 4 Marks)**

- This is another problem that can degrade the TCP performance.
- This problem occurs when the sender transmits data in large blocks, but an interactive application on the receiver side reads data 1 byte at a time.
- To understand this problem, refer Fig. 9.14.3.



(G-617) Fig. 9.14.3 : Silly window syndrome

1. Initially the receiver's buffer is full so it sends a window size 0 to block the sender.
2. But the interactive application reads one byte from the buffer. So one byte space becomes empty.
3. The receiving TCP sends a window update to the sender informing that it can send 1 byte.
4. The sender sends 1-new byte.
5. The buffer is full again and the window size is 0. This process can continue forever. This is known as the silly window syndrome.

9.14.5 Nagle's Algorithm :

SPPU : May 07, Dec. 11, May 19

University Questions

- Q. 1** How Nagle algorithm helps in TCP transmission policy ? Explain the Clark's solution to overcome the silly window syndrome.

(May 07, Dec. 11, May 19, 8 Marks)



- The Nagle's algorithm is very simple. It takes into account the speed of transmission of the sender and the speed of the network which is transporting the data. The algorithm is as follows :
 1. The first piece of data received from the sending application program is send by the sending TCP even if it is only 1 byte.
 2. Once the first segment is sent, the sending TCP will wait and accumulate data in the output buffer until either the acknowledgement is received from the receiving TCP or sufficient data is accumulated to fill the maximum size segment.
 3. Step 2 is repeated for the remaining transmission.
- If the sending application program data rate is higher than the speed of data transporting network then the segments are larger (maximum size segments).
- On the other hand if the sending application program is slower than the data transport network, the segments will be smaller than the maximum segment size.

Clark's solution to silly window syndrome :

- Clark suggested a solution to silly window syndrome as follows.
- He suggested that the receiver should not send a window update for 1 byte.
- Instead the receiver must wait until it has a considerable amount of buffer space available and then send the window update.
- To be specific, the receiver should wait until it can handle the maximum window size it has advertised at the time of establishing a connection or its buffer is half empty, whichever is smaller.
- The sender can also help to improve the situation.
- It should not send tiny segments. Instead it must wait and send a full segment or at least one containing half of the receivers buffer size.

9.15 Congestion Control :

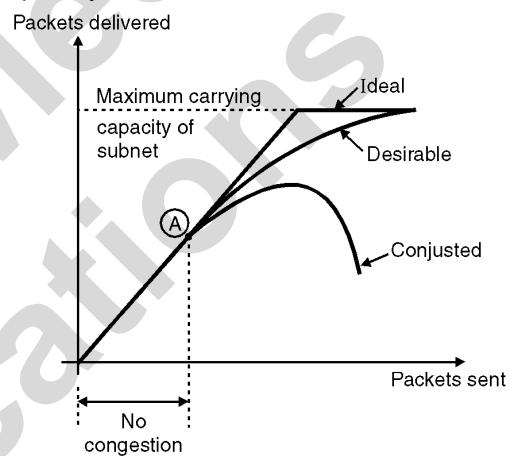
SPPU : May 12, Dec. 13, March 19

University Questions

- Q. 1** What do you mean by congestion ? Explain any two congestion control algorithms in virtual circuit subnets. **(May 12, Dec. 13, 9 Marks)**

Q. 2 What is congestion control ? Explain leaky bucket and token bucket algorithm. **(March 19, 5 Marks)**

- An important issue in a packet switching network is congestion.
- If an extremely large number of packets are present in a part of a subnet, the performance degrades. This situation is called as congestion.
- Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network (i.e. the number of packets a network can handle).
- Fig. 9.15.1 explains the concept of congestion graphically.



(G-473) Fig. 9.15.1 : Concept of congestion

- Upto point A in Fig. 9.15.1, the number of packets sent into the subnet by the host is within the capacity of the network.
- So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place.
- But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.
- As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens.
- At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.

9.15.1 Need of Congestion Control :

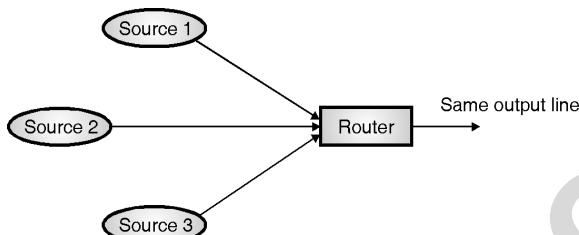
- It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.



- Congestion will result in long queues, which results in buffer overflow and loss of packets.
- So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

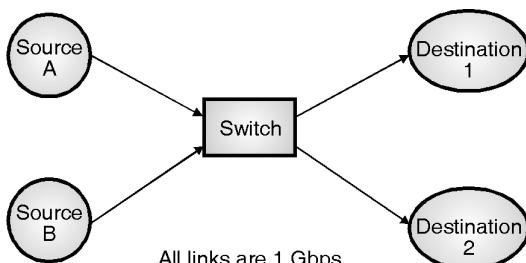
9.15.2 Causes of Congestion :

- Some of the causes of congestion are as follows :
- 1. If suddenly a flow of packets start coming on three or four senders which all needing the same output line. Then a queue will become long. If the memory capacity is not sufficient to hold all these packets, some of them will be lost. This is shown in Fig. 9.15.2(a). This leads to congestion.



(G-474) Fig. 9.15.2(a)

- Note that increasing the memory to infinity also does not solve the problem, in fact it worsens.
- 2. Congestion is caused by slow and low bandwidth links. The problem will be solved when high speed links become available. It is not always the case, sometimes increases in link bandwidth can aggravate the congestion problem because higher speed links may make the network more unbalanced. For the configuration shown in Fig. 9.15.2(b), if both the sources begin to send to destination 1 at their maximum rate, congestion will occur at the switch. Higher speed links can make the congestion condition in the switch worse.



(G-475) Fig. 9.15.2(b) : Network with high speed links

- 3. Congestion is caused by slow processors. The problem will be solved when processor speed is improved. Faster processors will transmit more data in unit time. If

several nodes begin to transmit to one destination simultaneously at their maximum rate, the destination will be overwhelmed soon.

4. Congestion can make itself worse. If a router does not have any free buffers it should ignore (discard) new packets arriving at it. But when a packet is discarded, the sender may retransmit it many times because it is not receiving the acknowledgement of the packet. This multiple transmission of packets will force the congestion to take place at the sending end.

9.15.3 Effects of Congestion :

- Due to congestion, various network parameters get affected.
- The most important network parameters which get affected by congestion are as follows :
 1. Delay
 2. Throughput

1. Delay versus load :

- When the load is very small as compared to the capacity of network, the delay is at its minimum.
- This minimum delay is equal to the sum of propagation delay and processing delay and it is negligible.
- But when load increases and becomes comparable to the network capacity the delay increases sharply due to the addition **waiting time** which gets added to the total delay.
- The delay becomes infinite when the load is greater than the capacity of network.
- The delay increases due to congestion.

2. Throughput versus load :

- Throughput can be defined as number of packets passing through a network per unit time.
- When the load is less than the capacity of network, the throughput increases proportional to the load.
- The throughput is expected to remain constant after it reaches its maximum (capacity of network).
- But practically the throughput reduces sharply as the load reaches its capacity.
- This happens because in the event of congestion, the routers discard some of the packets received by them.
- Thus throughput reduces due to congestion.



9.15.4 Difference between Congestion Control and Flow Control :

SPPU : Dec. 02

University Questions

Q. 1 What is the difference between flow control and congestion control ? **(Dec. 02, 8 Marks)**

- Congestion control makes it sure that the subnet is able to carry the offered traffic i.e. the subnet is able to carry all the packets sent by all the senders to their destinations.
- Congestion control is dependent on the behaviour of all the hosts, all the routers and other factors which reduce the carrying capacity of a subnet.
- On the contrary, the flow control is related to point to point traffic between a sender and its destination.
- Flow control ensures that a fast sender does not send data at a rate faster than the rate at which the receiver can receive it.
- Flow control involves some kind of feedback from the receiver, which can control the sending rate of the sender.

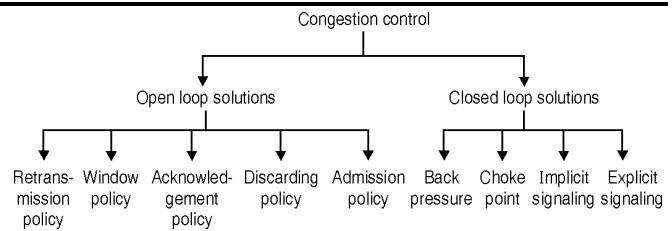
9.15.5 Principle of Congestion Control :

SPPU : May 08

University Questions

Q. 1 What do you mean by congestion ? Discuss the open-loop and closed-loop congestion control mechanism. **(May 08, 8 Marks)**

- The solutions to the congestion problems can be divided into two categories or groups as open loop solutions and closed loop solutions.
- Congestion control refers to the techniques and mechanisms which can either prevent congestion from happening or remove congestion after it has taken place.
- The **open loop congestion** control is based on the prevention of congestion whereas the **closed loop solutions** are for removing the congestion after it has occurred.
- Fig. 9.15.3 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-476) Fig. 9.15.3 : Classification of congestion control schemes

Open loop control :

- Open loop solutions try to solve the congestion issue by excellent design to prevent the congestion from happening.
- Open loop control is exercised by using the tools such as deciding when to accept the new packets, when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points.
- It is important to note that none of these decisions are made on the basis of the current status of a network, as no feedback is being used.

Closed loop control :

- The closed loop congestion control uses some kind of feedback. It takes into account the current status of the network.
- A closed loop control is based on the following three steps :
 1. Detect the congestion and locate it by monitoring the system.
 2. Transfer the information about congestion to places where action can be taken.
 3. Adjust the system operations to correct the congestion.
- Two examples of closed loop control are :
 1. TCP flow control.
 2. BR rate control for an ATM network.

Open loop versus closed loop :

- Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control.
- In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.



- Some people feel that closed loop congestion control schemes are too slow in todays high-speed, large range network.
- Because it takes a long time for feedback to go back to source. Hence before any corrective action takes place thousands of packets have been already lost.
- But on other hand, if the congestion has already taken place and the overload is of long duration, the congestion cannot be released unless the source causing the congestion is asked to reduce its rate.
- Furthermore, ABR service is designed to use any bandwidth that is left over the source must have some knowledge of what is available when it is sending cells.

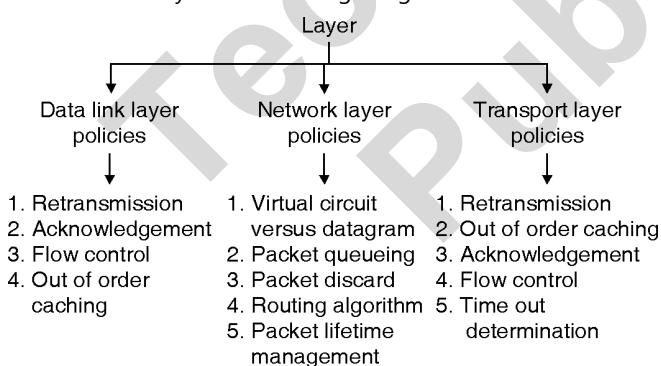
9.15.6 Congestion Prevention Policies :

SPPU : Dec. 08

University Questions

Q. 1 Explain any two congestion prevention policies with suitable example. (Dec. 08, 8 Marks)

- In this section we are going to discuss the open loop congestion control systems.
- These systems try to avoid congestion by using the appropriate policies at different levels.
- Fig. 9.15.4 lists various policies corresponding to different layers for avoiding congestion.



(G-477) **Fig. 9.15.4 : Policies affecting the congestion**

Policies related to data link layer :

1. Retransmission policy :

- The retransmission policy and the retransmission timers must be designed to optimise efficiency and at the same time prevent congestion.
- The retransmission policy deals with how fast a sender times out.

- If a sender times out early then it will retransmit all the packets and such a retransmission can lead to congestion.

- By designing the retransmission policy we can avoid this and prevent congestion.

2. Out of order caching policy :

- If the receivers routinely discard all the packets which are out of order, then retransmission of these packets will take place.
- This will increase the load and result in congestion. So a selective repeat (retransmission) should be adopted to avoid congestion.

3. Acknowledgement policy :

- If each received packet is promptly acknowledged then the acknowledgement packets will increase the traffic.
- If the acknowledgement is delayed (piggybacking) then there is a possibility of time out and retransmission.
- So a tight flow control has to be exercised to avoid congestion.

4. Window policy :

- The type of window at the sender may also affect congestion. The selective repeat window is better than the Go Back N window.

Policies related to network layer :

1. Choice between virtual circuit and datagrams :

- This choice at the network layer will affect the congestion because many congestion control algorithms work only with virtual circuit subnets.

2. Packet queuing and service :

- This policy is related to whether the routers have one queue per input line and one queue per output line or both.
- This policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.

3. Discard policy :

- This policy lays a rule which tells the routers about which packet is to be discarded.
- A good discard policy can prevent congestion and a bad one will worsen the situation.

**4. Routing algorithms :**

- The routing algorithms can spread the traffic over all the lines.
- By doing so it is ensured that none of the lines are overloaded. This will certainly avoid congestion.

5. Package lifetime management :

- This policy decides the maximum time for which a packet may live before being discarded.
- This time should be of adequate value so that congestion can be avoided.

Policies related to transport layer :

- The policies at the transport layer are same as those at the data link layer.
- But at transport layer determining the time out interval is more difficult.
- If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will reduce at the cost of increased response time (network will become slow).

Traffic shaping :

- One of the important reason behind congestion is the bursty nature of the traffic.
- If the traffic has a uniform data rate then congestion would not happen every now and then.
- But due to bursty traffic it can happen regularly.
- Traffic shaping is an open loop control. It prevents the congestion by making the packet transmission rate to be more predictable (bursty traffic is unpredictable).
- Thus traffic shaping will regulate the average rate or the burstiness of data transmission.
- Monitoring a traffic flow is called as **traffic policing**.
- Check if a packet stream (connection) is as per its descriptor, and if it is not as per its descriptor, then give penalty !
- In order to achieve this the network may want to monitor the traffic flow during the connection period.
- The process of monitoring and enforcing the traffic flow is called traffic policing.
- The types of penalties enforced are as follows :
 1. Drop packets that violate the descriptor.

2. Give low priority to the packets violating the descriptor.

9.15.7 Congestion Control in Virtual Circuit Subnets :**SPPU : May 12, Dec. 13****University Questions**

- Q. 1** What do you mean by congestion ? Explain any two congestion control algorithms in virtual circuit subnets. **(May 12, Dec. 13, 9 Marks)**

- All the congestion control techniques discussed till now were open loop techniques.
- Now let us discuss a dynamic technique called **admission control**.

Admission control principle :

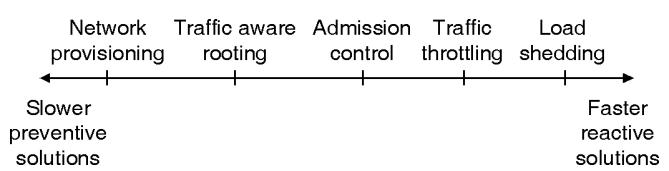
- This technique is used to keep the congestion which has already begun to a manageable level and does not allow it to worsen any further.
- Its principle is as follows : Once congestion has been detected, do not set up any more virtual circuits until the congestion is cleared.
- The advantage of this technique is that it is a simple and easy to carry out control.

Alternative approach :

- An alternative approach to admission control allows the virtual circuits to set up even when a congestion has taken place.
- But carefully route all the new virtual circuits around the area where congestion is already present.

9.15.8 Approaches to Congestion Control :

- The two basic solutions to the problem of congestion are :
 1. Increase the resources
 2. Decrease the load
- These solutions are applied on different time scales in order to either prevent congestion or handle it if it has occurred.



(G-1522) Fig. 9.15.5 : Time scales of approaches to congestion control

**1. Network provisioning :**

- The fundamental way of avoiding congestion is to build a network that is properly matched to the traffic that it is going to carry.
- If the network uses a low bandwidth link along which a heavy traffic is directed, then congestion is most certain to take place.
- We can add resources dynamically when there is congestion.
- For example, we can turn on additional routers and use spare (back up) lines whenever congestion has taken place.
- Another example is purchasing bandwidth on open market as and when congestion occurs. But you can't do it instantly. It takes a long time.
- This is called as **Network Provisioning**. It is a slow preventive solution and happens on a time scale of months.

2. Traffic aware routing :

- If we can not increase the capacity of a network then we should think of utilizing the existing capacity in the best possible way.
- Routers can be tailored to suite traffic patterns that change during the day as network users wake and sleep in different time zones.
- The traffic can be routed over those paths which have less traffic at that time. This is known as traffic aware routing.

3. Admission control :

- Sometimes it is not possible to increase capacity. Then the only possible way to fight congestion is to **decrease the load**.
- As stated earlier, in the virtual circuit networks, new connections are not allowed once congestion has been detected.
- This is a feedback (closed loop) control approach. When the congestion is predicted, the network can deliver feedback to those sources who are responsible for congestion.
- Then these sources would be requested to **reduce** their outputs.
- There are two difficulties faced in this approach :

- 1. It is difficult detect the beginning of congestion.
- 2. It is also difficult to inform the sources to slow down accordingly.

- The **leaky bucket** and **token bucket** methods are examples of admission control.

4. Traffic throttling (Congestion avoidance) :

- In the Internet and many other computer networks, senders adjust their transmission rates and send only that much traffic which a network can readily deliver without causing congestion.
- This is done so as to operate the network just before the beginning point of congestion.
- When congestion is about to happen the senders should be told to **reduce** their transmission and slow down. This technique is an example of **congestion avoidance** principle.
- The first step in traffic throttling is to **detect** the beginning point of congestion and the second step is to tell the senders to slow down.
- Note that traffic throttling approach can be used in both datagram **subnets** as well as **virtual circuit subnets**.
- The onset of congestion can be detected if the routers are made to monitor the following parameters :
 1. Utilization of output links.
 2. Buffering of queued packets inside the router.
 3. Number of packets lost due to inadequate buffering.
- Generally the second parameter is most useful in practice.
- The second task for the routers is that they should deliver timely feedback to the senders.
- Different schemes use different feedback mechanisms. Some of them are as follows :
 1. Choke packets.
 2. Explicit Congestion Notification (ECN).
 3. Hop by Hop back pressure.

5. Load shedding :

- When all other solutions fail to contain congestion, the network has no option but to discard packets that can not be delivered.
- A good policy for selecting which packets to discard can help preventing the congestion collapse.



9.16 Congestion Control in Datagram Subnets :

- Let us now discuss some congestion control approaches which can be used in the datagram subnets (and also in virtual circuit subnets).
- The techniques are :
 1. Choke packets
 2. Load shedding
 3. Jitter control.

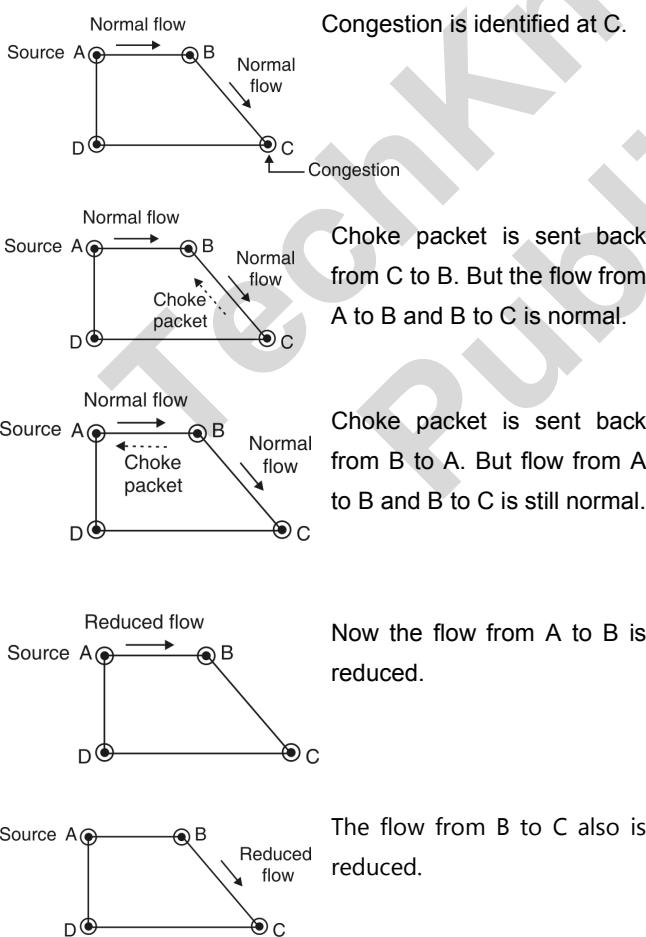
9.16.1 Choke Packets :

SPPU : May 16

University Questions

Q. 1 Explain choke packets and hop by hop choke packets. (May 16, 6 Marks)

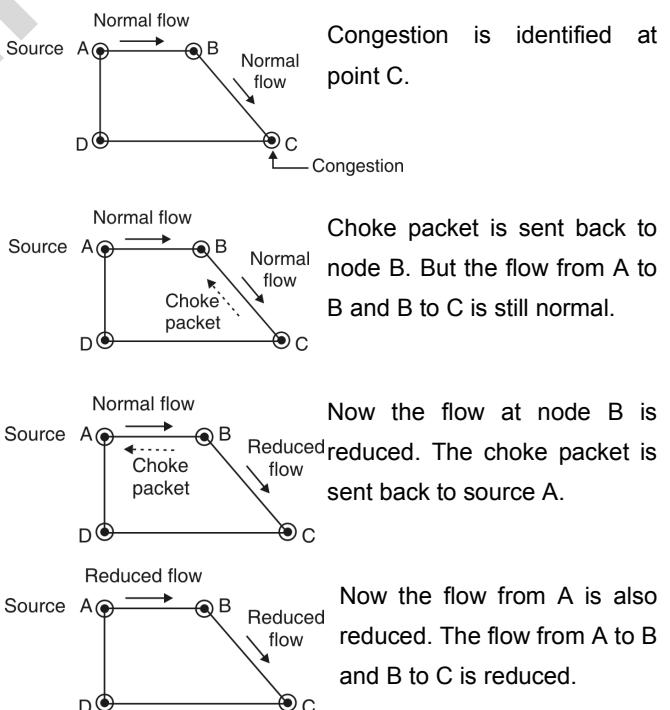
- This approach can be used in virtual circuits as well as in the datagram subnets.
- In this technique each router associates a real variable with each of its output lines.
- This real variable say "u" has a value between 0 and 1 and it indicates the how much is utilization of that line in percentage (60 %, 70 % etc.).



(G-478) Fig. 9.16.1(a) : Choke packet mechanism

- If the value of "u" goes above the threshold then that output line will enter into a "warning" state.
- The router will check each newly arriving packet to see if its output line is in the "warning state".
- If it is in the warning state then the router will send back a **choke packet** signal to the sending host.
- The sender host will not generate any more data packets. This will reduce the congestion.
- Different congestion control algorithm have been proposed, depending on the value of thresholds.
- Depending on the threshold value, the choke packets can contain a mild warning, a stern warning or an ultimatum.
- Another algorithm may use the queue lengths or buffer utilization instead of using the line utilization as a deciding factor.
- The general concept of choke packet mechanism is demonstrated in Fig. 9.16.1(a).
- Fig. 9.16.1(a) shows that, the choke packets have to travel over the entire network, from the point of congestion to the appropriate source (i.e. from C to A).
- Then the action of reducing the flow will take place. The whole process is therefore very much time consuming.

Hop-by-Hop choke packet technique :



(G-479) Fig. 9.16.1(b) : Concept of hop-by-hop choke packet mechanism



- The problem associated with the general choke packet mechanism can be overcome by using another technique called as hop-by-hop choke packet technique.
- This is demonstrated in Fig. 9.16.1(b). In this approach, the choke packets are used at each hop between the destination and source.
- Each node receiving the choke packet will reduce its output flow.
- This will have a more effective and fast control over the overall transmission rate.
- Fig. 9.16.1(b) shows how the transmission rate is reduced at every hop in response to the choke packets.

Disadvantage :

- The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is not compulsory.
- The host may reduce its transmission rate or ignore the choke packets.

Weighted fair queuing :

- The disadvantage of choke packet technique can be overcome with the help of the weighted queuing technique.
- The queuing algorithm was proposed first in 1987.
- In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.

9.16.2 Load Shedding : SPPU : Dec. 06, Dec. 08

University Questions

Q. 1 What is the need of load shedding ? Explain the procedure for load shedding.

(Dec. 06, Dec. 08, 8 Marks)

- Admission control, choke packets, fair queuing are the techniques suitable for light congestion.
- But if these techniques cannot eliminate the congestion, then the load shedding technique is to be used.
- The principle of load shedding states that when the routers are flooded with the packets that they cannot handle, they should simply throw the packets away.

- A router which is flooding with packets due to congestion can discard any packet at random. But there are better ways of doing this.
- The policy for dropping a packet depends on the type of packet.
- For file transfer an old packet is more important than a new packet.
- In contrast for multimedia a new packet is more important than an old one.
- Accordingly a policy is formulated for discarding the packets.
- An intelligent discard policy can be decided depending on the applications.
- It is not possible to implement such an intelligent discard policy without the co-operation from the sender.
- The applications should mark their packets as per priority to indicate how important they are.
- If this is done then when the packets are to be discarded the routers can first drop packets having lower priority (i.e. the packets which are least important).
- Then the routers will discard the packets from next lower class and so on.
- One or more header bits are required to put the priority of a packet.
- In every ATM cell, 1 bit is reserved in the header for marking the priority.
- Every ATM cell is labeled either as a low priority or high priority.

9.17 Quality of Service (QoS) :

SPPU : Dec. 06, Dec. 14

University Questions

Q. 1 List and explain the parameters for quality of service. **(Dec. 06, 8 Marks)**

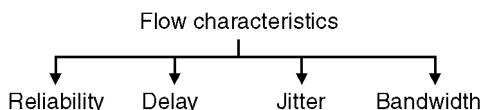
Q. 2 Explain parameters for quality of service in network layer. **(Dec. 14, 6 Marks)**

- The long form of QoS is quality of service and it is an internetworking issue.
- We can informally define quality of service as something flow seeks to attain.



Flow characteristics :

- There are four important characteristics of data flow : reliability, delay, jitter and bandwidth.
- These characteristics are shown in Fig. 9.17.1.



(G-480) Fig. 9.17.1 : Flow characteristics

1. Reliability :

- A data flow must have some level of reliability. Lack of reliability means a packet or acknowledgment, will be lost and retransmission will be required.
- However, each application programs has a different demand for reliability.
- For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

2. Delay :

- Source-to-destination delay is another important flow characteristic.
- Again delay tolerance of different applications will be different.
- In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while file transfer or email are delay tolerant applications.

3. Jitter :

- Jitter is the variation in delay for packets belonging to the same flow. i.e. different packets experience different amounts of delays.
- Real-time audio and video cannot tolerate a large amount of jitter.
- On the other hand, it does not matter if packet carrying information in a file have different delays.
- The transport layer at the destination waits until all packets arrive before delivery to the application layer.

4. Bandwidth :

- Different applications need different bandwidths.
- In video conferencing needs a huge bandwidth whereas an email may not need a large bandwidth.

9.17.1 Techniques for Achieving Good QoS :

- Some of the techniques useful in achieving good QoS are as follows :
 - 1. Buffering
 - 2. Traffic shaping
 - 3. Leaky bucket algorithm
 - 4. Token bucket algorithm
 - 5. Resource reservation
 - 6. Admission control
 - 7. Proportional routing
 - 8. Packet scheduling.

9.17.2 Traffic Shaping :

- One of the important reason behind congestion is the bursty nature of the traffic.
- If the traffic has a uniform data rate then congestion problem will not be very common.
- Traffic shaping is an open loop control of congestion control.
- It manages the congestion by making the packet transmission rate to be more predictable.
- This will make the data rate more uniform and bursty traffic is reduced.
- Thus traffic shaping will regulate the average rate or the burstiness of data transmission.
- The process of monitoring a traffic flow is called as **traffic policing**.
- Here the principle followed is to check if a packet stream (connection) obeys the rules and if it violates the rules then, give penalty !
- For this the network would like to monitor the traffic flow during the connection period.
- The process of monitoring and enforcing the rules to regulate traffic flow is called **traffic policing**.
- Penalty for breaking the rules will be :
 - 1. Drop packets that violate the rules.
 - 2. Give low priority to them.



- **Traffic shaping** is defined as a mechanism to control the amount and rate of the traffic sent to the network.
- The two popularly used traffic shaping techniques are :
 1. Leaky bucket
 2. Token bucket.

9.17.3 Leaky Bucket Algorithm :

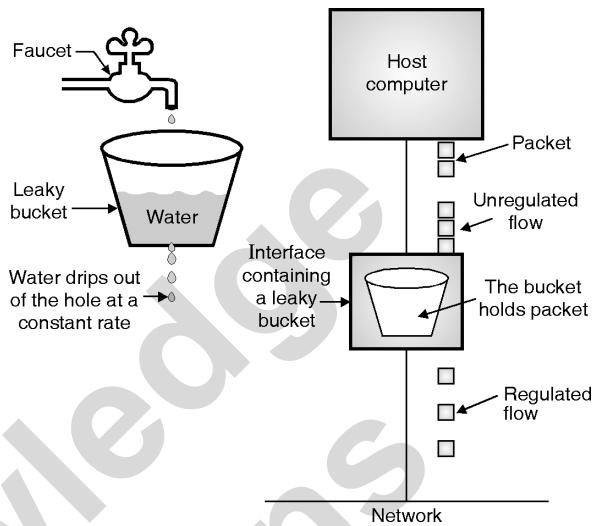
SPPU : May 13, Dec. 13, May 18, Dec. 18, March 19

University Questions

- Q. 1 Explain leaky bucket and token bucket algorithm. **(May 13, May 18, 8 Marks)**
- Q. 2 Explain leaky bucket algorithm. **(Dec. 13, 8 Marks)**
- Q. 3 What is the purpose of Leaky bucket and token bucket algorithms ? Describe working of Token bucket algorithm with reference to CBR, VBR and bursty traffic. **(Dec. 18, 6 Marks)**
- Q. 4 What is congestion control ? Explain leaky bucket and token bucket algorithm. **(March 19, 5 Marks)**

- Leaky bucket algorithm is used to control congestion in network traffic.
- As the name suggests its working is similar to a leaky bucket in real life.
- The principle of leaky bucket algorithm is as follows :
- Leaky bucket is a bucket with a hole at bottom.
- Flow of the water from bucket is at a constant rate (data rate is constant) which is independent of water entering the bucket (incoming data).
- If bucket is full, any additional water entering in the bucket is thrown out (Packets are discarded).
- Same technique is applied to control congestion in network traffic.
- Every host in the network is having a buffer (equivalent to a bucket) with finite queue length.
- Packets which are put in the buffer when buffer is full are thrown away.
- The buffer may send some number of packets per unit time onto the subnet (helpful if packets vary greatly in size) as shown in Fig. 9.17.2.

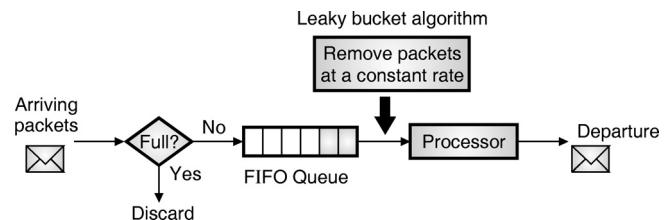
- the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.



(a) (b)
(G-481) Fig. 9.17.2 : Leaky bucket algorithm

Leaky bucket implementation :

- Fig. 9.17.3 shows the implementation of leaky bucket principle. A FIFO (First In First Out) queue is used for holding the packets which is equivalent to the leaky bucket.
- The implementation of Fig. 9.17.3 can be discussed under two different operating conditions, namely :
 1. For packets of fixed size.
 2. For packets of variable size.



(G-482) Fig. 9.17.3 : Implementation of leaky bucket

1. Fixed size packets :

- If the arriving packets are of fixed size (e.g. cells in ATM networks), then the process of Fig. 9.17.3 will allow the removal of a fixed number of packets from the queue corresponding to every tick of the clock.

2. Packets of variable size :

- If the packets at the input of the process are of different size, then the fixed output rate will not correspond to



the number of packets leaving the process but it will correspond to the number of bits leaving the process.

Algorithm :

- The algorithm for variable length packets is as follows :

 1. Initialize a counter to a number "n" at the tick of the clock.
 2. If "n" is greater than the packet size, then send the packet and decrement the counter by the packet size.
 3. Repeat step 2 until "n" becomes smaller than the packet size.
 4. Reset the counter and go back to step 1.

Note : Thus a leaky bucket algorithm shapes the bursty traffic to convert it into a fixed rate traffic. It does so by averaging the data rate. It drops the packets if the bucket (buffer) is full.

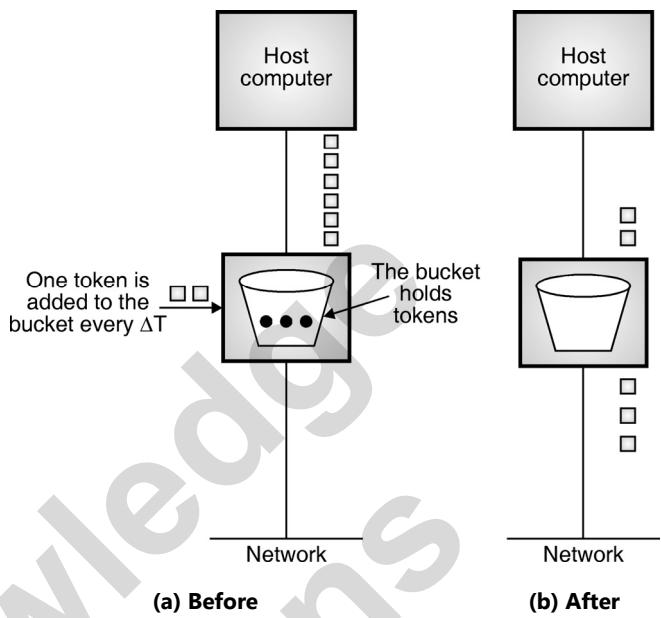
9.17.4 Token Bucket Algorithm :

SPPU : May 13, Dec. 15, May 18, Dec. 18, March 19

University Questions

- Q. 1** Explain leaky bucket and token bucket algorithm. **(May 13, May 18, 8 Marks)**
- Q. 2** How token bucket algorithm works in case of smooth and bursty traffic ? **(Dec. 15, 6 Marks)**
- Q. 3** What is the purpose of Leaky bucket and token bucket algorithms ? Describe working of Token bucket algorithm with reference to CBR, VBR and bursty traffic. **(Dec. 18, 6 Marks)**
- Q. 4** What is congestion control ? Explain leaky bucket and token bucket algorithm. **(March 19, 5 Marks)**

- This algorithm is similar to the leaky bucket but it is possible to vary output rates.
- This is useful when larger burst of traffic is received.
- It enforces a long-term average transmission rate while permitting bounded bursts.
- In this approach, a token bucket is used to which manages the queue regulator that ultimately controls the rate of packet flow into the network.
- A token generator continuously produces tokens at a rate of R tokens per second and puts them into a token bucket with a depth of D tokens as shown in Fig. 9.17.4.



(a) Before

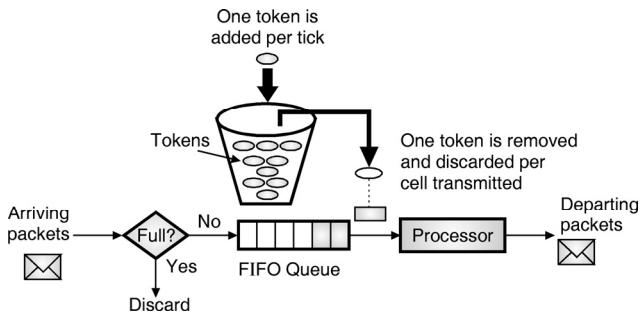
(b) After

(G-483) Fig. 9.17.4 : Token bucket algorithm

- If the token bucket gets full then the extra tokens are discarded.
- Token bucket algorithm is a variant of leaky bucket algorithm discussed earlier. Here the bucket is filled with tokens.
- A packet which grabs and destroys a token is allowed to leave the bucket.
- Due to this mechanism, the packets never get lost but they just have to wait to grab a token.
- At the same time, an unregulated stream of packets arrive and are placed into a packet queue that has a maximum length of L . If the flow delivers more packets than the queue can store, the excess packets are discarded.

Implementation of token bucket :

- Fig. 9.17.5 shows the implementation of token bucket.
- The token bucket can be easily implemented with a counter. The token is initialized to zero.
- Every time a token is added, the counter is incremented by 1 and every time a packet is dispatched, the counter is decremented by 1.
- If the counter contents go to zero, the host cannot send any data.



(G-484) Fig. 9.17.5 : Implementation of token bucket

Note : The token bucket allows the bursty traffic at maximum possible rate.

Token bucket performance :

Let, s = Burst length (seconds),
 c = Bucket capacity (bytes),
 ρ = Token arrival rate (bytes/second),
and m = Maximum source rate (bytes/second)

What is the duration of a maximum-rate burst through a token bucket ?

1. Maximum bytes sent from the token bucket during a burst is, $c + \rho \cdot s$
2. Maximum bytes the source can send during a burst is, $m \cdot s$
3. Setting the two equal and solving for s ,

$$s = \frac{c}{m - \rho}$$

Comparison of Token Bucket and Leaky Bucket :

Sr. No.	Leaky Bucket	Token Bucket
1.	Smooth out traffic by passing packets only when there is a token. Does not permit burstiness.	Token bucket smooths traffic too but permits burstiness.
2.	Leaky bucket discards packets for which no tokens are available. (No concept of queue)	Token bucket discards token when bucket is full, but never discards packets (infinite queue)
3.	Application : Traffic shaping or policing.	Application : Network traffic shaping or rate limiting

9.17.5 Combination of Token Bucket and Leaky Bucket :

- The token bucket and leaky bucket techniques can be combined to obtain the following advantages :
 1. To credit an idle host
 2. To regulate the traffic
- The token bucket is used first followed by the leaky bucket technique.
- The rate of leaky bucket needs to be higher than the rate of tokens dropped in the bucket.

9.17.6 Resource Reservation :

- The data flow is dependent on the following resources :
 1. Buffer
 2. Bandwidth
 3. CPU time
- The QoS can be improved by reserving these resources.
- The QoS model called integrated services operates on the principle of resource reservation, for improvement in QoS.

9.17.7 Admission Control :

- Admission control technique is used by a router or a switch.
- They use this mechanism to accept or reject the data flow based on predefined parameters called flow specifications.
- Before accepting a flow for processing, a router checks the flow specifications and finds out if it is possible to take up and handle this new data flow.
- It does this by comparing its bandwidth, buffer size, CPU speed etc. with the flow specifications.

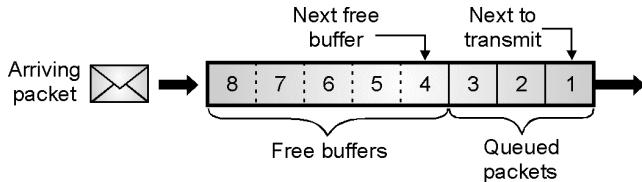
9.17.8 Queuing Disciplines :

- Each router must implement some queuing discipline which decides about how the packets are buffered when they are waiting to get transmitted.
- There are two algorithms commonly used in packet switching networks namely :
 1. First In First Out (FIFO)
 2. Fair Queuing (FQ)



9.17.9 FIFO Queuing :

- The FIFO queuing is also called as First Come First Served (FCFS) Queuing.
- Its idea is simple and illustrated in Fig. 9.17.6.

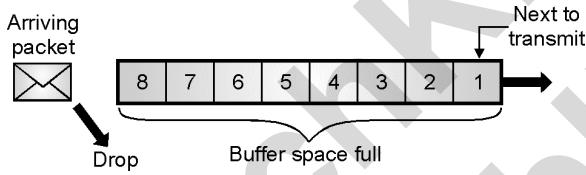


(G-485) Fig. 9.17.6 : FIFO queuing

- The principle of FIFO queuing is, that the packet that arrives first at a router is the packet which is transmitted first.
- In this sense it is First In First Out (FIFO) queuing.
- Fig. 9.17.6 shows a FIFO with "slots" to store upto eight packets.

Discarding of a packet :

- The buffer space at any router is limited. So if a packet arrives when the queue (buffer space) is full, then the router discards that packet as shown in Fig. 9.17.7.

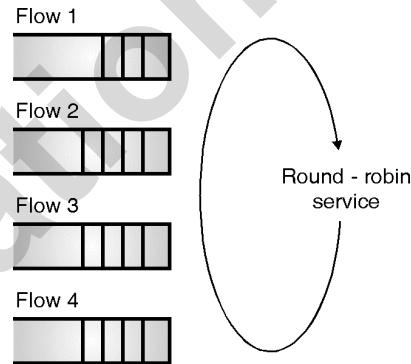


(G-486) Fig. 9.17.7 : Dropping of a packet

- The packet is dropped (discarded) irrespective of which flow the packet belongs to or what is its priority level etc.
- This is sometimes called as "tail drop" because packets which arrive at the tail end of the FIFO are dropped.
- FIFO with tail drop, is the simplest queuing algorithm and so it is the most widely used one.
- A simple type of the basic FIFO queuing is priority queuing.
- In this each packet is marked with a priority.
- The router then implements multiple FIFO queues, one for each priority class.
- The router will always transmit out packets of highest priority queues if that queue is non-empty, then it moves to the next priority queue.

9.17.10 Fair Queuing :

- The disadvantage of FIFO queuing is that there is absolutely no discrimination among the packets being received from different sources. All are treated equally.
- Because the entire congestion control mechanism is implemented at the sources and the FIFO queuing does not have any facility of policing the source behaviour to this mechanism, it is possible that a bad behaved source may occupy large fraction of the network capacity.
- Fair Queuing (FQ) is an algorithm which is proposed to solve this problem.
- It maintains a separate queue for each flow which is being currently handled by the router.
- The router then entertains these queues in the round robin manner as shown in Fig. 9.17.8.



(G-487) Fig. 9.17.8 : Concept of fair Queuing (FQ) at the router

- When a sender sends packets too fast, then its queue is filled up.
- When a queue reaches a particular length, additional packets from that flow are dropped.
- This ensures that any source can not arbitrarily increase its share of the network's capacity.
- The main problem with FQ is that the packets being processed at a router are not of same length.
- Ideally a bit by bit round robin is expected i.e. one bit from flow-1 is transmitted, then one bit from flow-2 and so on. But practically it is not possible.
- The FQ mechanism therefore simulates this behaviour by first determining when a given packet would finish being transmitted if it were being sent using bit by bit round robin, and then using this finishing time to sequence the packets for transmission.

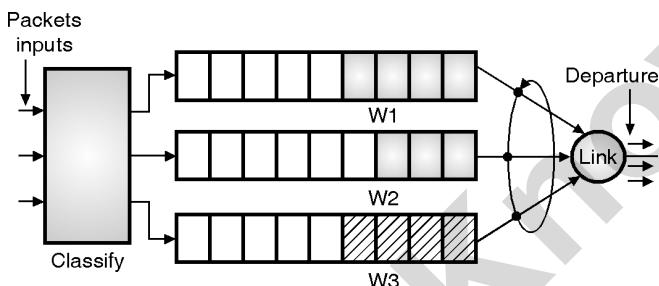


Disadvantages of fair queuing algorithm :

- The problem with this algorithm is that it gives all the hosts the same priority.
- To overcome this problem, the modified algorithm called weighted fair queuing is used.

9.17.11 Weighted Fair Queuing :

- The disadvantage of choke packet technique can be overcome with the help of the Weighted Fair Queuing (WFQ) technique.
- This queuing algorithm was proposed first in 1987.
- In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.
- Refer Fig. 9.17.9 to understand weighted fair queuing.



(G-488) Fig. 9.17.9 : Weighted fair queuing (WFQ)

- The incoming packets are classified into different classes (1, 2, 3 etc) and stored in separate queues (W1, W2, W3 etc.) specifically assigned to them.
- Similar to the round robin technique the WFQ scheduler, will output the packets from W1, W2, and W3 in a sequential manner.
- If a queue is empty the WFQ scheduler will move immediately to the next queue.
- It will always keep the link busy. No empty slots are present on the link.

Difference between round robin and WFQ :

- In round robin the service given to each class is same but in WFQ, each class may receive a different amount of service in any interval of time, depending on the weightage of that class.

9.18 TCP Congestion Control :

SPPU : May 05, Dec. 10, May 13

University Questions

- Q. 1** Discuss flow control and congestion control mechanisms in TCP. **(May 05, 8 Marks)**

Q. 2 Explain congestion control in connection oriented service. **(Dec. 10, 4 Marks)**

Q. 3 Explain TCP congestion control in detail. **(May 13, 9 Marks)**

- We have already discussed the reasons of congestion in networks and the Internet is no exception.
- So there are congestions occurring on Internet too.
- The network layers detects the congestion by looking at the growing queues at the routers and tries to manage it by dropping packets.
- The network layer has to give feedback to the transport layer about the possible congestion because only then the transport layer can reduce the sender's data rate.
- In the Internet, TCP plays a major role in controlling congestion.
- A control law called AIMD (Additive Increase Multiplicative Decrease) can be used in response to binary congestion signals received from the network.
- According to this law, in response to congestion signals the transport protocol should converge to a fair and efficient bandwidth allocation.
- TCP congestion control is based on this approach using a **window** and with a loss of packet used as the binary signal to indicate congestion.

Principle of congestion control :

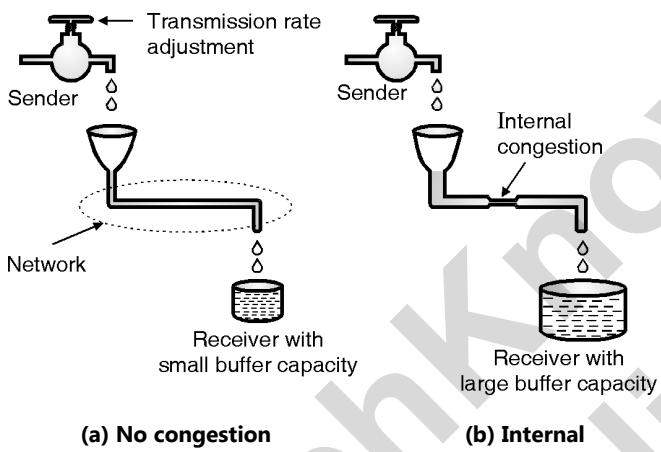
- The basic principle is do not inject a new packet into the network until an old one is delivered.
- TCP tries to do this by dynamically adjusting the window size.
- The steps followed in achieving the congestion control in TCP are as follows :

Step 1 : Detect the congestion :

- This is the first step in congestion control.
- Now-a-days packet loss due to transmission errors is very rare because the optical fiber links are being used. So most transmission time-outs (loss of packets) are due to congestions.
- So all the Internet TCP algorithms assume that time-outs are caused by congestion and so time outs can be used to detect the congestion.

Step 2 : Try to prevent congestion :

- After establishing a connection, a suitable window size is to be chosen.
 - The receiver window size is based on its buffer capacity. If the sender adjusts its transmission rate according to this capacity as shown in Fig. 9.18.1(a), the congestion due to buffer overflow will never take place.
 - Now consider Fig. 9.18.1(b). The sender is slow, the receiver has a large buffer capacity but the problem is low internal carrying capacity of the network.
 - If the sender is too fast, the water will back up and some will be lost (loss of packets) and congestion will take place.



(G-618) Fig. 9.18.1 : Congestion

Conclusion :

- To prevent congestion TCP has to deal with two problems separately – receiver capacity and network capacity.

Solution :

- To deal with the two problems mentioned earlier each sender maintains two windows : the window the receiver has granted (which indicates the receiver capacity) and the **congestion window** (which indicates the network capacity).
 - The first window that indicates the receiver capacity is called as the **flow control window**.
 - The size of the congestion window is equal to the number of bytes the sender may have in the network at any time.

- Hence the corresponding **sending rate** is equal to the ratio of **congestion window size** and the **RTT** of the connection.
 - TCP adjusts the size of window as per the AIMD rule.
 - The **congestion window** is maintained in addition to the **flow control window** (Which specifies the number of bytes that the receiver can buffer).
 - Both these windows are considered simultaneously.
 - Both the windows indicate the number of bytes the sender may transmit and the number can be different.
 - Therefore the number of bytes that may be sent by the sender is the minimum of the two windows.
 - So the effective window is the minimum of what the sender and the receiver both think is all right.

Modern congestion control :

- Modern congestion control was added to TCP in 1988 through the efforts of Van Jacobson.
 - In 1986 due to growing number of Internet users the first **congestion collapse** took place.
 - As a response to this collapse Jacobson approximated an AIMD congestion window and added it to the existing TCP.
 - While doing so he made following two important considerations :
 1. The rate at which the acknowledgements return to the sender is approximately equal to the rate at which packets can be sent over the slowest link in the path. This is the rate a sender wants to use to avoid congestion. This timing is known as **ACK clock** and it is an essential part of TCP. Using ACK clock TCP smoothes out traffic and avoids congestion.
 2. The second consideration was that AIMD rule will take a very long time to reach the desired operating point on fast networks if the congestion window is started from a small value. The start up time can be reduced by using a large initial window. But a too large starting window would cause congestion in slow or short links.
 - Hence Jacobson mixed both linear and multiplicative increase in the window size in his solution to resolve congestion. This modified algorithm is known as the **slow start** algorithm.

9.18.1 Slow Start Algorithm :

SPPU : Dec. 03, Dec. 04

University Questions

Q. 1 How does congestion build up over communicating networks ? Explain use of the slow start algorithm to prevent occurrence of congestion ?

(Dec. 03, 8 Marks)

Q. 2 List and explain congestion handling techniques provided by TCP. **(Dec. 04, 8 Marks)**

(Dec. 04, 8 Marks)

1. After establishing a connection, the sender initialises the congestion window to the size which is equal to the maximum segment in use on the connection. It then sends one maximum segment.
 2. If this segment is acknowledged by the receiver indicating no congestion, it adds bytes corresponding to one full segment to the congestion window. So now the congestion window size is equal to two maximum size segments. The sender then sends two segments.
 3. As each of these segments is acknowledged indicating that there is no congestion, the size of congestion window is increased by one maximum segment size. This is shown in Fig. 9.18.2. This is the exponential growth of the congestion window size.
 4. When the congestion window is of n segments, if all n segments are acknowledged before time-out takes place, the congestion window is increased by the byte count corresponding to n segments.
 5. But there is a limit on the exponentially growing congestion window. The congestion window stops growing as soon as either the time-out occurs or the receiver's window size is reached.
 6. If the congestion window can grow to 1024 (1 kbyte) byte, 2048 byte, but a burst of 4096 bytes gives a time-out then we have to set the congestion window at 2048 in order to avoid congestion.
 7. Once this is done, no data bursts longer than 2048 bytes will be sent by the sender even if receiver grants a wider window.
 8. The name of this algorithm is slow algorithm and it is required to be supported by all the TCP implementations.

9.18.2 Internet Congestion Control

Algorithm :

SPPU : Dec. 04

University Questions

Q. 1 List and explain congestion handling techniques provided by TCP. **(Dec. 04, 8 Marks)**

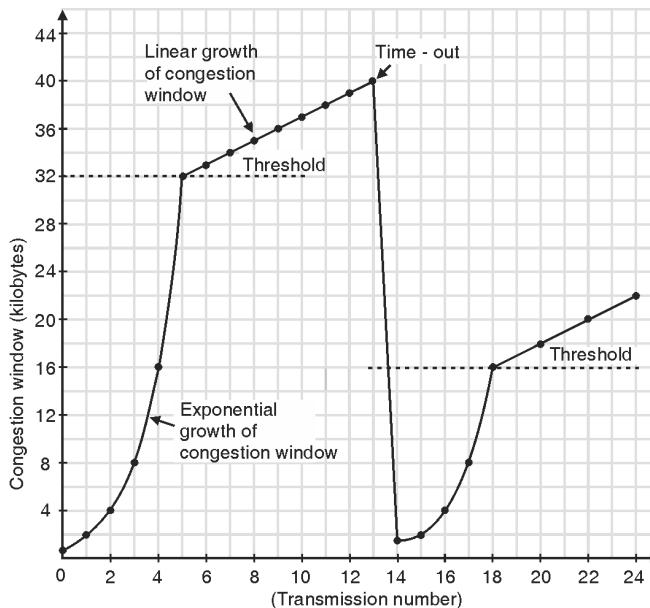
- Till now only two parameters have been used namely receiver window and congestion window.
 - But in the algorithm we are going to discuss, a third parameter called **threshold** is used.
 - Initially the threshold is set to 64 kbyte.
 - When the time-out occurs, the threshold is set to half of the current congestion window i.e. 32 k bytes and the congestion window is reset to one maximum segment.
 - The slow start algorithm is then used to find what the network can handle.
 - But most importantly the exponential growth of the congestion window is stopped as soon as it reaches the **threshold**.
 - After this point (threshold point), the congestion window grows linearly (and not exponentially) by one maximum segment for each burst instead of one per segment. This is illustrated in Fig. 9.18.2.
 - Table 9.18.1 is used to plot the graph of Fig. 9.18.2. See how the threshold point acts as the boundary of the exponential growth and linear growth of the congestion window.

(G-619(a)) Table 9.18.1

Transmission number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
Congestion window kilobytes	2	4	8	16	32	33	34	35	36	37	38	39	40	1	...

Exponential growth Linear growth

- The maximum segment size here is 1024 i.e. 1 kbyte. Initial value of congestion window was 64 k, but time-out occurs. So threshold is set to 32 k and congestion window to 1 k at 0. (Original point in Fig. 9.18.2)
 - Then the congestion window grows exponentially till the congestion window size reaches the threshold of 32 k.



(G-619) Fig. 9.18.2 : Internet congestion control algorithm

- The threshold occurs at 32 k and the congestion window grows linearly after this point.
- The time-out occurs as the 13th transmission. Therefore the new threshold is set to half the current window (i.e. at 16 k) and slow start is initiated again. The process will repeat thereafter.
- If no more time-outs occur, the size of congestion window continues to grow upto the size of the receiver window.

9.18.3 Congestion Avoidance (Additive Increase) :

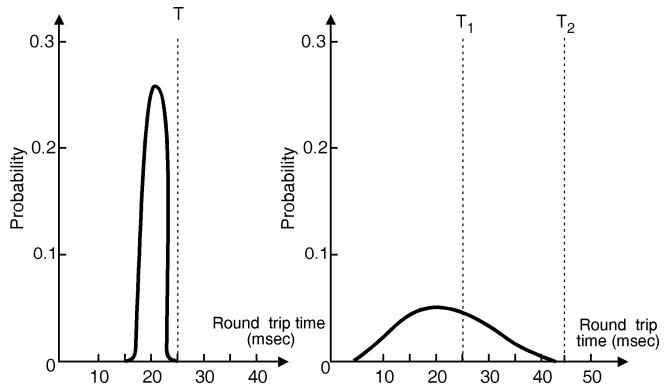
- In the slow start algorithm discussed earlier, the size of the congestion window initially increases exponentially (upto the threshold).
- In order to avoid congestion before it happens, we have to slow down such an exponential growth.
- TCP defines another algorithm called **congestion avoidance** which is based on the principle of additive increase of the congestion window and not the exponential one.
- When the size of the congestion window reaches the slow start threshold, the slow start phase will stop and additive increase phase begins.
- In this algorithm, corresponding to every acknowledgement, the size of the congestion window is increased by 1 as shown in Fig. 9.18.2.

9.19 TCP Timer Management :

- The TCP, at least conceptually uses more than one timers.
- But the most important of them is the **Re-transmission Timer (RTO)**.
- This timer is started as soon as a segment is sent.
- The timer is stopped if the acknowledgement corresponding to the sent segment is received, before the timer expires.
- But if the timer times out before the arrival of an "ack" signal then that segment is re-transmitted and the timer is started again.

What should be the time-out interval ?

- The most important question about the re-transmission timer is that how long should the time-out interval be ?
- The answer to this question is difficult in the transport layer as compared to that in the data link protocol.
- Fig. 9.19.1 shows the probability density function for the time taken by data link and TCP segment acknowledgements.
- Determining the Round Trip Time (RTT) to destination is not simple and even if we know it, deciding the value of time-out is difficult.
- Refer Fig. 9.19.1(b). If the value of time-out is too small (T_1 for example) then unnecessary re-transmission will take place.



(G-620) Fig. 9.19.1 : Probability density of acknowledgement arrival times

- If time-out is too long say T_2 , then the performance will degrade because re-transmission will be delayed for the long time whenever a packet is lost.



- The solution to this problem is to use a highly dynamic algorithm which adjusts the time-out interval constantly.
- This adjustment is based on continuous measurement of network performance.

9.19.1 Jacobson's Algorithm :

- This is the algorithm, generally used by the TCP.
- For each connection, TCP maintains a variable Round Trip Time (RTT) which is also called as SRTT (Smoothed Round Trip Time).
- Its value will be equal to the best current estimate of the round trip time to the desired destination.
- When a segment is sent, timer is started. This is to measure the time required to receive ACK and to trigger re-transmission if ACK takes too long to come.
- If the acknowledgement returns back before timer goes out, then TCP measures the time taken by the ACK (say R) and adjusts SRTT to a new value using the following equation,

$$\text{SRTT} = \alpha \text{ SRTT} + (1 - \alpha) R \quad \dots(9.19.1)$$

- Here α is called as smoothing factor. Typically $\alpha = 7/8$.
- Even if a good value of SRTT is given, it is not easy to choose the time-out.
- In the initial implementations of TCP the value of SRTT was chosen to be equal to $2 \times \text{RTT}$.
- But practical observations showed that such a constant value was not flexible enough in the events of increased loads.
- When the load approaches capacity (maximum value); the delay becomes large and varies to a large extent. This can initiate retransmission when the original packet is still alive.
- Jacobson fixed this problem by making the time out value sensitive to the variance in RTT as well as the smoothed round trip time SRTT.
- In order to implement this change, we need to keep track of another smoothed variable called RTTVar (Round Trip Time VARIation) which is updated by the following formula,

$$\text{RTTVar} = \beta (\text{RTTVar}) + (1 - \beta) |\text{SRTT} - R| \quad \dots(9.19.2)$$

- The typical value of $\beta = 3/4$. The retransmission timeout RTO is set by the following expression,

$$\text{RTO} = \text{SRTT} + (4 \times \text{RTTVar}) \quad \dots(9.19.3)$$

- The choice of multiplying factor 4 in the above expression is arbitrary.
- The retransmission timer is also held to a minimum of 1 second regardless of the estimates.
- This value is chosen on the basis of measurements to prevent spurious retransmissions.

9.19.2 Karn's Algorithm :

- A problem in Jacobson's algorithm is that of measuring the value of R (time taken by the ACK), when a segment times out and is sent again.
- This happens because when the ACK comes in, it is not clear whether it corresponds to the original transmission or to the re-transmission.
- If the guessing goes wrong it can seriously affect the value of RTO.
- Phil Karn made a simple proposal to solve this problem. He suggested not to update estimates on any segments that have been re-transmitted.
- In addition the timeout is doubled on each successive re-transmission until the segments get through for the first time.
- This is known as **Karn's algorithm** and most TCP implementations use it.

9.19.3 Other Timers in TCP :

SPPU : Dec. 08, Dec. 16, May 18, Dec. 18

University Questions

- Q. 1** Give two functions of four different timers used in TCP. **(Dec. 08, 8 Marks)**
- Q. 2** Why three timers are required in TCP timer management ? **(Dec. 16, 6 Marks)**
- Q. 3** Explain different timers used in TCP. **(May 18, Dec. 18, 4 Marks)**

Persistence timer :

- The second timer in TCP is called **persistence timer**.
 - It is designed to solve the following problem :
1. The receiver sends an ACK with window size = 0. So the sender will wait for the receiver's buffer to have some free space.



2. After the receiver buffer becomes partially empty it sends a window update to the sender asking it to send.
3. But the packet containing this window update is lost on its way to sender.
4. So both sender and receiver will be waiting for ever.
 - To solve this problem, the persistence timer is used. If it goes off, then sender transmits a probe to the receiver.
 - The receiver sends the window size in response to this probe.
 - If the window size is still zero then the persistence timer is set again and the cycle repeats. But if the window size is nonzero then sender can send data.

Keepalive timer :

- This is the third timer in TCP. It is used when a connection is idle for a long time.
- When a connection is idle for a very long time, the Keepalive timer may go off.
- This will cause one side to check if the other side is still there.
- If the other side does not respond, then the connection is terminated.

Timer for TIMED WAIT state :

- This timer is used in the TIMED WAIT state while closing.
- This timer is set to a time equal to twice the maximum packet lifetime to ensure that after closing a connection all the packets created by it die off.

Ex. 9.19.1 : If the round trip time is 30 msec and following acknowledgements come in after 26, 32 and 24 msec respectively, What is the new RTT estimate using the Jacobson algorithm ?
Assume suitable value of α .

May 07, 8 Marks

Soln. :

Given : RTT = 30 msec, M = 26, 32, 24 msec

Choose : $\alpha = 7/8$

1. For M = 26 msec :

$$\begin{aligned} D &= \alpha D + (1 - \alpha) | RTT - M | \\ \therefore (1 - \alpha) D &= (1 - \alpha) | RTT - M | \\ \therefore D &= | RTT - M | = | 30 - 26 | = 4 \text{ msec} \\ \therefore \text{Time out} &= RTT + 4D = 30 \text{ ms} + (4 \times 4) = 46 \text{ msec} \end{aligned}$$

2. For M = 32 msec :

$$\begin{aligned} D &= | RTT - M | = | 30 - 32 | = 2 \text{ msec} \\ \therefore \text{Time out} &= RTT + 4D = 30 + (4 \times 2) = 38 \text{ msec} \end{aligned}$$

3. For M = 24 msec :

$$\begin{aligned} D &= | RTT - M | = | 30 - 24 | = 6 \text{ msec} \\ \therefore \text{Time out} &= 30 + (4 \times 6) = 54 \text{ msec} \end{aligned}$$

9.20 Comparison of UDP and TCP :

Characteristic / Description	UDP	TCP
General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics;



Characteristic / Description	UDP	TCP
		congestion avoidance algorithms.
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols.
Well-Known Applications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions).	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions).
Error control	Only checksum.	Provided.

9.21 Sockets :

SPPU : Dec. 11, May 12, Dec. 12, May 13, Dec. 13, Dec. 18, March 19

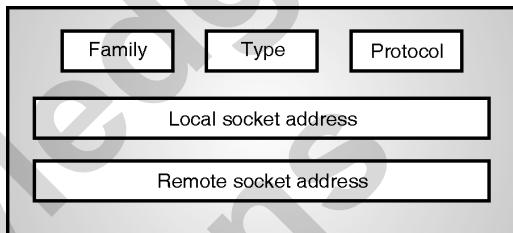
University Questions

- Q. 1** What is a socket ? Explain various socket primitives used in client-server interaction (for both TCP and UDP). Explain different types of sockets with example. **(Dec. 11, 8 Marks)**
- Q. 2** What is a socket ? Explain various socket primitives used in client-server interaction. **(May 12, Dec. 12, 10 Marks, May 13, Dec. 18, March 19, 8 Marks)**
- Q. 3** What is socket ? Explain various socket primitives used in TCP. **(Dec. 13, 9 Marks)**

- The socket interface was originally based on UNIX.
- It defines a set of system calls or procedure.
- The communication structure that we need in socket programming is called as a **socket**.
- A socket acts as an end point.
- Two processes can communicate if and only if both of them have a socket at their ends.

Socket structure :

- Fig. 9.21.1 shows a simplified socket structure.



(G-601) Fig. 9.21.1 : Socket structure

- Various fields in the socket structure are as follows :

 1. **Family** : This field is used for defining the protocol group such as IPv4 or IPv6, UNIX domain protocol etc.
 2. **Type** : This field is used for defining the type of socket such as stream socket, packet socket or raw socket.
 3. **Protocol** : This field is usually set to zero for TCP and UDP.
 4. **Local socket address** : It is used for defining the local socket address. This address is a combination of local IP address and the port address of the local application program.
 5. **Remote socket address** : It is used for defining the remote socket address which is a combination of remote IP address and the port address of the remote application program.

9.21.1 Socket Types :

SPPU : Dec. 11, Dec. 12, May 13

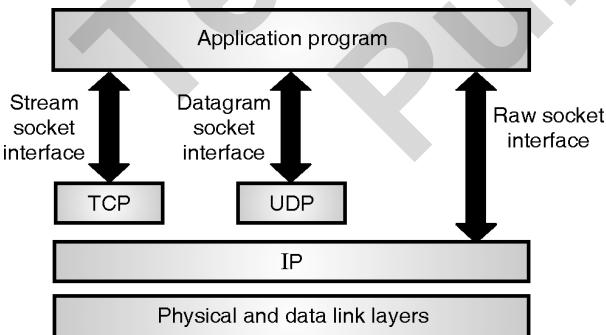
University Questions

- Q. 1** What is a socket ? Explain various socket primitives used in client-server interaction (for both TCP and UDP). Explain different types of sockets with example. **(Dec. 11, 8 Marks)**
- Q. 2** Explain with example various types of sockets. **(Dec. 12, 8 Marks)**



Q. 3 How will you differentiate a stream socket from a raw socket ? How data transmissions happen in a datagram mode ? **(May 13, 8 Marks)**

- There are three types of sockets :
 1. The stream socket
 2. The packet socket
 3. The raw socket
 - All these sockets can be used in TCP/IP environment. Let us discuss them one by one.
- 1. Stream socket :**
- This is designed for the connection oriented protocol such as TCP.
 - The TCP uses a pair of stream sockets one each on either ends for connecting one application program to the other across the Internet.
- 2. Datagram socket :**
- This type of socket is designed for the connectionless protocol such as UDP.
 - UDP uses a pair of datagram sockets for sending a message from one application program to another across the Internet.
- 3. Raw socket :**
- Raw sockets are designed for the protocols like ICMP or OSPF, because these protocols do not use either stream packets or datagram sockets.
 - Fig. 9.21.2 shows the three types of socket types.



(G-602) Fig. 9.21.2 : Type of sockets

9.21.2 Socket Primitives :

SPPU : May 13, Dec. 13, Dec. 14, Dec. 18, March 19

University Questions

Q. 1 What is a socket ? Explain various socket primitives used in client-server interaction.
(May 13, Dec. 18, March 19, 8 Marks)

Q. 2 What is socket ? Explain various socket primitives used in TCP. **(Dec. 13, 9 Marks)**

Q. 3 Explain all socket primitives used by client. **(Dec. 14, 6 Marks)**

- Table 9.21.1 lists various transport primitives used in Berkeley UNIX for TCP.

Table 9.21.1

Sr. No.	Primitive	Meaning
1.	SOCKET	Create a new communication end point.
2.	BIND	Provide a local address to a socket
3.	LISTEN	Show willingness to accept connections
4.	ACCEPT	Block the caller as long as a connection attempt does not arrive
5.	CONNECT	Attempt to establish a connection
6.	SEND	Send data
7.	RECEIVE	Receive data
8.	CLOSE	Release the connection

- The first four primitives in the Table 9.21.1 are executed in the same order by the server.
- The SOCKET primitive creates a new end point and allocates table space for it within the transport entity.
- The newly created sockets do not have addresses. These are assigned using the BIND primitive.
- The LISTEN primitive allocates space to queue the incoming calls in case if several clients wish to connect at the same time.
- To block waiting for an incoming connection, the server executes an ACCEPT primitive.
- When a TPDU requesting for a connection arrives, the transport entity creates a new socket and returns a file descriptor for it.
- These were the primitives corresponding to server side. Now let us consider the client side.
- On the client side also a socket needs to be created first using the SOCKET primitive, however the BIND is not required.



- The **CONNECT** primitive blocks the caller and initiates the connection process.
- When it completes (which is indicated by an appropriate TPDU received from the server), the client process is unblocked and the connection is established.
- After this both the sides can use **SEND** and **RECEIVE** primitives to send and receive data.
- In order to release the connection, both sides have to execute a **CLOSE** primitive.

Steps followed for Socket Programming :

- The steps followed for the socket programming are as follows :

Server side :

1. Server creates a socket and checks for errors using SOCKET.
2. Assign address to the newly created socket using BIND.
3. Use the LISTEN to allocate space for the queue which is used for the incoming calls.
4. Execute an ACCEPT for blocking the waiting incoming connections.

Client side :

1. Create a socket using SOCKET.
2. Use CONNECT to initiate connection process.
3. Establish the connection.

9.21.3 Connectionless Iterative Server :**SPPU : Dec. 08, May 11, May 13****University Questions**

- Q. 1** How will you differentiate a stream socket from a raw socket ? How data transmissions happen in a datagram mode ? **(Dec. 08, May 13, 8 Marks)**
- Q. 2** Explain the significance of 'bind' socket system call. Does it apply to all sockets at server and client ? What parameters are specified by its various arguments ? **(May 11, 10 Marks)**

- Let us now discuss connectionless, iterative client-server communication using UDP and datagram sockets.
- The server that uses UDP is usually connectionless iterative. So the server serves one request at a time.

- A server gets the request received in a packet from UDP, it processes the request and gives the response to UDP to send it to the client.
- The server does not pay any attention to the other packets.
- The other packets are stored in a queue waiting for the service. They are processed one by one.
- The server uses one single port for this purpose, the well known port.
- All the packets arriving at this port will wait in line to be served.

Server functions :

- The server performs the following functions :
1. **Create a socket** : The server asks the operating system to create a socket.
 2. **Bind** : The server asks the operating system to enter information in the socket related to the server. This is called as binding the server socket.
 3. **Repeat** : The server repeats the following steps for infinite number of times.
 - (a) Receive a request
 - (b) Process : The request is processed by the server.
 - (c) Send : The response is sent to the client.

Clients functions :

- The client performs following functions :
1. **Create a socket** : The client asks the operating system to create a socket. There is no need of binding.
 2. **Repeat** : The client repeats the following steps as long as it has requests.
 - (a) **Send** : Client asks the operating system to send a request.
 - (b) **Receive** : Client asks the operating system to wait for the response and deliver it when it has arrived.
 3. **Destroy** : When the client does not have any more requests, it asks the operating system to destroy the socket.



9.21.4 Connection Oriented Concurrent

Server : SPPU : Dec. 08, May 11, May 13

University Questions

- Q. 1** How will you differentiate a stream socket from a raw socket ? How data transmissions happen in a datagram mode ? **(Dec. 08, May 13, 8 Marks)**
- Q. 2** Explain the significance of 'bind' socket system call. Does it apply to all sockets at server and client ? What parameters are specified by its various arguments ? **(May 11, 10 Marks)**

- The connection oriented concurrent client server communication uses TCP and stream socket.
- The servers using TCP are normally of concurrent type. That means a server is serving many clients at the same time.
- The type of communication is connection oriented. Once a connection is established, it remains established until entire stream of bytes is processed. After that the connection is terminated.
- The server must have one buffer for each connection.
- The bytes from the client are stored in buffers and handled concurrently by the server.
- In order to provide this type of server, the concept of parent and child server is used.

Parent server :

- A parent server is the server running infinitely and accepting connections from clients. It uses the well known port.
- After establishing a connection, the parent server creates a new server called as a child server and an ephemeral port to allow the **child server** to handle the client.

Server function :

- The server performs following functions :
- 1. Create a socket :** The server asks the operating system to create a socket.
 - 2. Bind :** The server asks the operating system to enter information in the socket.
 - 3. Listen :** The server asks the operating system to be passive and listen to the client which needs to be connected to this server. This is because TCP is a

connection oriented protocol so a connection needs to be made before transferring the data.

- 4. Repeat :** The server repeats the steps given below infinitely.

(a) Create a child : When a child requests a connection, the operating system creates a temporary child process and assigns the duty of serving the client to the child. The parent process is then free for listening to new clients.

(b) Create a new socket : A new socket is created which is to be used by the child process.

(c) Repeating : The child repeats the following steps as long as it has requests from the client :

1. Read
2. Process
3. Write
4. Destroy socket.

Client functions :

- The client performs the following functions :
1. Create a socket
 2. Connect
 3. Repeat the write and read operations
 4. Destroy : Close the connection.

Client and server program :

- Client-server programs are written in the languages such as C, C++, Java.
- It requires advanced knowledge of the particular language.

9.22 Case Study : Socket Programming with TCP :

- Many network applications consist of two programs namely a client program and a server program.
- When these programs are executed a client and a server process are created which communicate with each other by reading from and writing through the sockets.
- When creating a network application, a developer has to write the code for both client and sever programs.
- There are two different types of network applications.
- The first type of network application is an implementation of a protocol standard defined in, for example RFC.



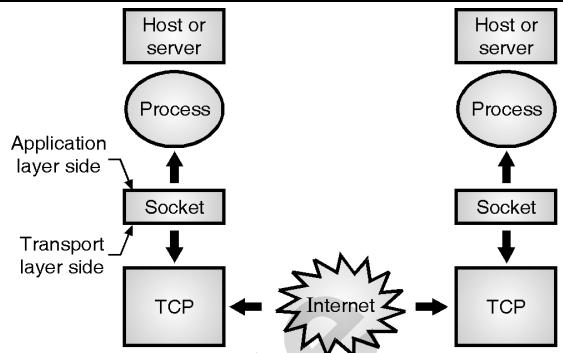
- For such an implementation, the client and server programs must be written as per the rules of RFC.
- It is possible for two independent developers to write the client and server programs that can operate with each other properly.
- The other type of network application is a proprietary application.
- In this case the application layer protocol used by the client and server programs may not conform to any existing RFC.
- A single developer or developing team writes the client and server programs.
- As the code does not implement a public domain protocol, the other independent developers can not develop code that interoperates with the application.
- So when developing a proprietary application, the developer should not use one of the well known port numbers defined in the RFCs.

Key issues in developing proprietary application :

- When developing a proprietary type application, the developer needs to first decide whether the application is to run over TCP or UDP.
- TCP is connection oriented and provides a reliable byte-stream channel for the data to flow between the end systems.
- The UDP is connectionless and sends data in packets between the end systems.
- But it is an unreliable protocol.
- These TCP and UDP applications are written in Java.
- It is possible to write the code in C or C++ but Java has many advantages.

9.22.1 Socket Programming with TCP :

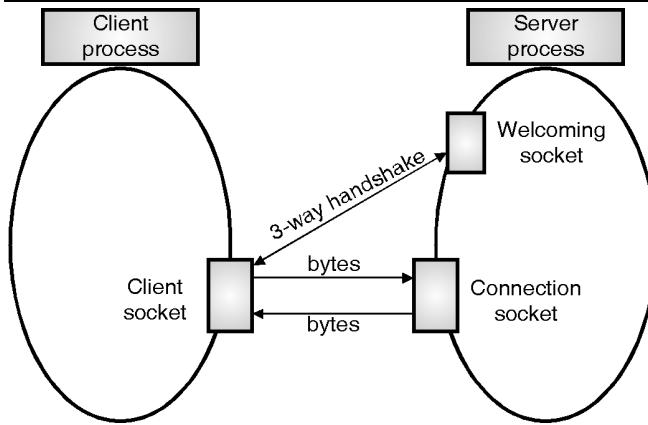
- The processes running on different machines communicate with each other by sending messages into sockets.
- This is demonstrated in Fig. 9.22.1.



- Processes are controlled by application developers
- UDP can be used in place to TCP
- TCP is controlled by the operating system

(G-630) Fig. 9.22.1 : Communicate between processes through TCP sockets

- Socket acts as a door between the application process and TCP as shown in Fig. 9.22.1.
- The application developer controls everything on the application layer side of the socket but does not have any control over the transport layer side of the socket.
- The interaction of the client and server takes place as follows.
 - The client has to initiate contact with the server and when such a contact is being initiated, the server should be ready.
 - That means the server must be a running process (not dormant) when a client initiates contact and the server process must have a socket to welcome the initial contact from the client.
 - With the server process running, the client process can initiate a TCP connection to the server.
 - This is done in the client program by creating a socket.
 - When the client socket is created, the client specifies the address of the server process i.e. the IP address of the server process i.e. the IP address of the server host and the port number of the server process.
 - Then the TCP on the client side initiates a three way handshake and establishes a connection with the server.
 - The three way handshake and the TCP connection establishment is shown in Fig. 9.22.2.



(G-1247) Fig. 9.22.2 : Different types of sockets

- During the three way handshake the client process knocks on the welcoming socket of the server process.
- The server process responds to this knocking by creating a new socket called **connection socket** which is dedicated to that particular client.
- In the last phase of the three way handshake a TCP connection is established between the client socket and the connection socket as shown in Fig. 9.22.2.
- The TCP connection is equivalent to a direct virtual pipe between the clients socket and server's connection socket to allow a reliable byte-stream service between the client process and server process.

9.22.2 Socket Programming with UDP :

- As discussed in the previous section, when two processes communicate over a TCP connection, it is equivalent to communicating over a virtual pipe between the two processes.
- This pipe will remain in place until one of the processes terminates the TCP connection.
- The sending process does not have to insert the destination address to the bytes to be sent because the virtual connection is existing.
- Also the pipe provides a reliable byte transfer without altering the sequence in which the bytes are received.
- Like TCP, the UDP also allows two or more processes running on different hosts to communicate. But there is a major difference.
- The first difference is that UDP provides a connectionless service so there is no handshaking process in order to establish the virtual pipe like TCP.

- As there is no virtual pipe existing, when a process wants to send a batch of bytes to the other process, the sending process has to attach the address of the destination process.
- The destination address is a tuple consisting of the IP address of the destination host and the port number of the destination process.
- The IP address and port number together are called as "**packet**".
- UDP provides an unreliable message oriented service in which there is no guarantee that the bytes sent by the sending process will reach the destination process.
- After creating a "packet", the sending process will push the packet into the network through a socket.
- This packet is then driven in the direction of destination process.
- The code for UDP socket programming is different than that for TCP in the following ways :
 1. No need for a welcoming socket as no handshaking is needed.
 2. No streams are attached to the socket.
 3. The sending host has to create packets.
 4. The receiving process has to obtain information from each received packet.

Review Questions

- Q. 1 Give an example of transport layer in public network and what strategy used in the transport layer for getting recovery from IMP and host crashes.
- Q. 2 What is socket ? Explain the steps followed in socket programming with associated procedures.
- Q. 3 Explain connection management issues at transport layer.
- Q. 4 In a generalized n-army problem the agreement of any two of the armies is sufficient for victory, explain how protocol that allows blue to win exist.
- Q. 5 Describe the system calls that allow an application to obtain socket options available and set new socket options respectively.



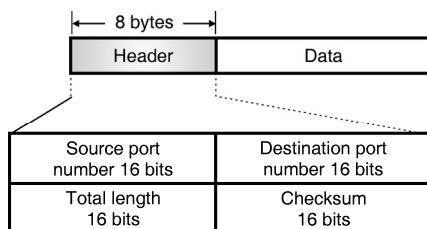
- Q. 6 Write short notes on : Crash recovery.
- Q. 7 What are sockets ? Explain the steps followed in socket programming.
- Q. 8 Describe the procedure of a server accepting connections through a socket. What are the various ways a server handles a connection request ? Why the use of same local protocol port number by multiple processes causes confusion in the concurrent approach ?
- Q. 9 Imagine that a two-way handshake rather than a three-way handshake were used to set up connections. In other words, the third message was not required. Are deadlocks now possible ? Give an example or show that none exist.
- Q. 10 Imagine a generalized n-army problem, in which the agreement of any two of the blue armies is sufficient for victory. Does a protocol exist that allows blue to win ?
- Q. 11 What is TCP and UDP ? Explain how you will choose between TCP and UDP ? Compare them.
- Q. 12 Suppose that the TCP congestion window is set to 18 k bytes and a time act occurs. How big will the window be if the next four transmission bursts are all successful ? Assume that the maximum segment size is 1 kB.
- Q. 13 Explain how TCP connections are established using the three-way handshake ? What happens when two hosts simultaneously try to establish a connection ?
- Q. 14 What is TCP state machine ? Explain its structure and use with suitable diagram.
- Q. 15 Define threshold condition in congestion. How does TCP tackle congestion problem using the internet congestion control algorithm.
- Q. 16 Explain the significance of listen call. Does it apply to all sockets ? What parameters are specified by its various arguments ?
- Q. 17 Explain TCP connection management with the help of TCP connection management finite state machine.
- Q. 18 What is silly window syndrome ? Explain its effect and possible solution.
- Q. 19 Explain in detail how TCP provides flow control ?
- Q. 20 Explain how TCP connections are established using the three way handshake. What happens when two hosts simultaneously try to establish a connection ?
- Q. 21 Describe why an application developer may choose to run an application over UDP than TCP ?
- Q. 22 When TCP sends a {SYN, sequence Num = x} or {FIN, sequence Num = x}, the consequent has Acknowledgement = $x + 1$, that is, SYNs and FINs each take up one unit in sequence number space. Is this necessary ? If so, give an example of an ambiguity that would arise if the corresponding acknowledgement were x instead of $x + 1$; if not, explain why ?
- Q. 23 Datagram fragmentation and reassembly are handled by IP and are invisible to TCP. Does this mean that TCP does not have to worry about data arriving in the wrong order ?
- Q. 24 Define threshold condition in congestion. How does TCP tackle congestion problem using the internet congestion control algorithm.
- Q. 25 Explain the significance of listen call. Does it apply to all sockets ? What parameters are specified by its various arguments ?

9.23 University Questions and Answers :

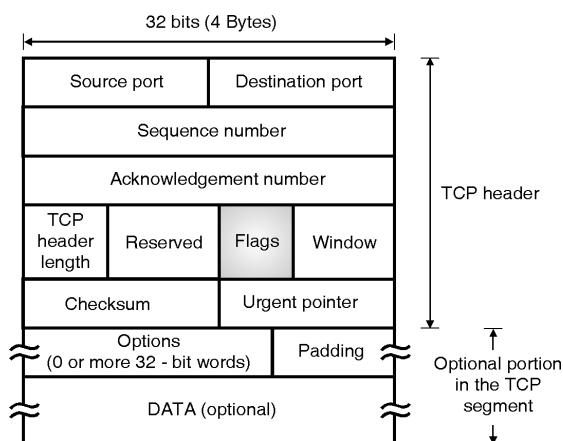
- Q. 1** Compare TCP and UDP header with suitable diagram. **(March 2019, 6 Marks)**

Ans. :

- Fig. 1(a) and (b) shows the header formats of UDP and TCP packets respectively.



(G-624) Fig. 1(a) : UDP(Contd...)



(G-611) (b) TCP

Fig. 1 : Header formats

- The comparison between them is as follows :

Sr. No.	Parameter of comparison	UDP	TCP
1.	Length of the header.	8-bytes.	20-bytes.
2.	Number of fields.	4	12
3.	Common fields.	Source port, destination port, checksum.	Source port, destination port, checksum.
4.	Sequence and acknowledgement number.	NA. Packets are not numbered or acknowledged.	Present. Each packet is numbered and its receipt is acknowledged.